INFORMATICA MEDICA SLOVENICA

Časopis Slovenskega društva za medicinsko informatiko
Journal of the Slovenian Medical Informatics Association

LETNIK / VOLUME **23 (2018)**, ŠTEVILKA / NO. **1-2**

ISSN 1318-2129 (tiskana izdaja / printed edition)
ISSN 1318-2145 (spletna izdaja / online edition)

http://ims.mf.uni-lj.si/

About the Journal

Informatica Medica Slovenica (IMS) is an interdisciplinary professional journal that publishes contributions from the field of medical informatics, health informatics, nursing informatics and bioinformatics. Journal publishes scientific and technical papers and various reports and news. Especially welcome are the papers introducing new applications or achievements.

IMS is the official journal of the Slovenian Medical Informatics Association (SIMIA). It is published two times a year in print (ISSN 1318-2129) and electronic editions (ISSN 1318-2145, available at http://ims.mf.uni-lj.si). Prospective authors should send their contributions in Slovenian, English or other acceptable language electronically to the Editor in Chief Assoc.Prof. Gaj Vidmar, PhD. Detailed instructions for authors are available online.

The journal subscription is a part of the membership in the SIMIA. Information about the membership or subscription to the journal is available from the secretary of the SIMIA (Mrs. Mojca Paulin, mojca.paulin@gmail.com).

O reviji

Informatica Medica Slovenica (IMS) je interdisciplinarna strokovna revija, ki objavlja prispevke s področja medicinske informatike, informatike v zdravstvu in zdravstveni negi, ter bioinformatike. Revija objavlja strokovne prispevke, znanstvene razprave, poročila o aplikacijah ter uvajanju informatike na področjih medicine in zdravstva, pregledne članke in poročila. Še posebej so dobrodošli prispevki, ki obravnavajo nove in aktualne teme iz naštetih področij.

IMS je revija Slovenskega društva za medicinsko informatiko (SDMI). Izhaja dvakrat letno v tiskani (ISSN 1318-2129) in elektronski obliki (ISSN 1318-2145, dostopna na naslovu http://ims.mf.uni-lj.si). Avtorji člankov naj svoje prispevke pošljejo v elektronski obliki glavnemu uredniku izr.prof.dr. Gaju Vidmarju. Podrobnejša navodila so dosegljiva na spletni strani revije.

Revijo prejemajo vsi člani SDMI. Informacije o članstvu v društvu oziroma o naročanju na revijo so dostopne na tajništvu SDMI (Mojca Paulin, mojca.paulin@gmail.com).

Contents

Research Papers

1 **Julija Ocepek, Nika Goljar, Gaj Vidmar, Mojca Debeljak**
Association between Functional Ability and Prescribed Wheelchair Category among People after Stroke

6 **Larisa Stojanovič**
Euromelanoma Day – the First Ten Years in Slovenia

12 **Branimir Leskošek**
Statistical Learning for Predicting Potential Drug Interactions

Research Review Papers

18 **Uroš Hudomalj, Franc Smole**
Quantum Cryptography

26 **Samanta Mikuletič, Brigita Skela Savič**
Information Security Culture in Health Care – a Systematic Review

Technical Paper

34 **Barbara Smrke, Darja Podsedenšek**
Experience with an Advanced Information System at the Intensive Internal Medicine Department of the Celje General Hospital

SIMLA Bulletin

39 **Ema Dornik**
30 Years of Experience in Support of Digitalisation of Health – Report from the Meeting of the Nursing Informatics Section 2018

Vsebina

Izvirni znanstveni članki

1 **Julija Ocepek, Nika Goljar, Gaj Vidmar, Mojca Debeljak**
Povezava med funkcijsko zmožnostjo in kategorijo predpisanega invalidskega vozička pri osebah po možganski kapi

6 **Larisa Stojanovič**
Evropski dan boja proti melanomu – prvih deset let v Sloveniji

12 **Branimir Leskošek**
Statistično učenje za napovedovanje možnih součinkovanj med zdravili

Pregledna znanstvena članka

18 **Uroš Hudomalj, Franc Smole**
Kvantna kriptografija

26 **Samanta Mikuletič, Brigita Skela Savič**
Informacijska varnostna kultura v zdravstvu – sistematični pregled literature

Strokovni članek

34 **Barbara Smrke, Darja Podsedenšek**
Izkušnje z naprednim informacijskim sistemom na Oddelku za intenzivno interno medicino Splošne bolnišnice Celje

Bilten SDMI

39 **Ema Dornik**
30 let izkušenj v podporo digitalizaciji zdravstva: poročilo s srečanja Sekcije za informatiko v zdravstveni negi 2018

■ *Izvirni znanstveni članek*

Julija Ocepek, Nika Goljar, Gaj Vidmar, Mojca Debeljak

Povezava med funkcijsko zmožnostjo in kategorijo predpisanega invalidskega vozička pri osebah po možganski kapi

Povzetek. Možganska kap je ena izmed najpogostejših zdravstvenih težav, pri kateri so posledice zmanjšane funkcijske zmožnosti, predvsem zmožnosti gibanja. Zato mnogo bolnikov po preboleli možganski kapi za gibanje potrebuje ustrezen invalidski voziček. Izvedli smo retrospektivno analizo podatkov iz medicinske dokumentacije bolnikov po možganski kapi na Univerzitetnem rehabilitacijskemu inštitutu Republike Slovenije – Soča za leto 2017. Zanimala nas je morebitna povezava med oceno funkcijske zmožnosti bolnika po kapi z Lestvico funkcijske neodvisnosti (FIM) in predpisano kategorijo invalidskega vozička. Ugotovili smo, da povezava obstaja, vendar je pri predpisu vozička potrebno upoštevati tudi druge dejavnike.

Association between Functional Ability and Prescribed Wheelchair Category among People after Stroke

Abstract. Stroke is one of the most common health issues, which results in limited functional abilities, mainly in terms of mobility. An adequate wheelchair is therefore required for many patients after stroke to make them mobile. We performed a retrospective analysis of medical records of patients after stroke at the University Rehabilitation Institute in Ljubljana for the year 2017. The purpose of our study was to investigate the association of functional ability of patients after stroke, as measured with the Functional Independence Measure (FIM), with the prescribed wheelchairs category. We found out that an association exists, but other factors have to be taken into account as well in wheelchair prescription practice.

■ **Infor Med Slov** 2018; 23(1-2): 1-5

Institucije avtorjev / Authors' institutions: Univerzitetni rehabilitacijski inštitut Republike Slovenije – Soča, Ljubljana (JO, NG, GV, MD); Medicinska fakulteta, Univerza v Ljubljani (GV); Fakulteta za matematiko, naravoslovje in informacijske tehnologije, Univerza na Primorskem, Koper (GV).

Kontaktna oseba / Contact person: asist. dr. Mojca Debeljak, URI – Soča, Linhartova 51, 1000 Ljubljana, Slovenija. E-pošta / E-mail: mojca.debeljak@ir-rs.si.

Prispelo / Received: 6. 6. 2018. Sprejeto / Accepted: 7. 6. 2018.

Uvod

Možganska kap je najpogostejši vzrok za zmanjšano dejavnost in sodelovanje v družbi,[1] saj kar 25 do 74 odstotkov bolnikov, ki preživijo možgansko kap, v nadaljnjem življenju potrebuje delno ali popolno pomoč pri dnevnih aktivnostih.[2] Pogosta posledica možganske kapi so zmanjšane funkcijske zmožnosti gibanja, kar vpliva na izvajanje vsakodnevnih aktivnosti. Vse to vodi do dolgotrajnih telesnih, čustvenih, socialnih in finančnih posledic tako za bolnika kot za njegove domače.[3] Okrevanje po možganski kapi je dolgotrajno in odvisno predvsem od obsežnosti in mesta možganske okvare ter stopnje okrevanja centralnega živčevja.[4] Funkcijsko okrevanje po možganski kapi je odvisno od časa – telesna kondicija bolnikov doseže vrh okoli pol leta po možganski kapi.[5]

Mnogo bolnikov po preboleli možganski kapi za gibanje potrebuje ustrezen invalidski voziček. Nekateri ga potrebujejo le v zgodnjem obdobju okrevanja, ko še niso sposobni samostojne in varne hoje, drugi ga potrebujejo dolgotrajno.

Testiranje in predpisovanje zahtevnejših invalidskih vozičkov v Sloveniji poteka na Univerzitetnem rehabilitacijskem inštitutu Republike Slovenije – Soča (URI – Soča). Pri tem je potrebna timska obravnava, kjer sodelujejo diplomirani delovni terapevt, tehnik s posebnimi znanji o vozičkih, diplomirani inženir ortotike in protetike, zdravnik specialist fizikalne in rehabilitacijske medicine, bolnik in tudi bolnikovi svojci.[6] Med testiranjem se oceni bolnikovo funkcionalno stanje oziroma stopnjo gibalne oviranosti, koliko potrebuje voziček (občasno, le na daljše razdalje, vedno) in ožje ter širše bivalno okolje. Bolniki po možganski kapi voziček na ročni pogon upravljajo oziroma poganjajo z značilnim vzorcem, in sicer z neprizadetim zgornjim in spodnjim udom.

V raziskavi smo želeli ugotoviti, ali obstaja povezava med funkcijsko zmožnostjo bolnika, ocenjeno z Lestvico funkcijske neodvisnosti (FIM), in kategorijo predpisanega invalidskega vozička.

Metode

Opravili smo retrospektivno analizo podatkov iz medicinske dokumentacije (spol, starost, diagnoza, ocena FIM, kategorija invalidskega vozička) bolnikov po možganski kapi, ki so bili v letu 2017 obravnavani na Oddelku za rehabilitacijo po možganski kapi URI – Soča in jim je bil predpisan invalidski voziček. Raziskavo je odobrila Komisija za medicinsko etiko URI – Soča.

Lestvica funkcijske neodvisnosti

FIM (angl. *Functional Independence Measure*) je standardiziran in najpogosteje uporabljen inštrument za ocenjevanje funkcijskega stanja bolnikov v rehabilitacijski medicini.[7] Lestvica ocenjuje 18 aktivnosti v 6 kategorijah (skrb zase, nadzor sfinktrov, transferji, mobilnost, sporazumevanje in socialni stiki), ki so združene v dve področji – motorično in kognitivno. Vsako aktivnost ocenimo glede na stopnjo pomoči, ki jo posameznik potrebuje za izvedbo. Lestvica je 7-stopenjska (1 – popolna pomoč, 7 – samostojnost). Končni seštevek je med 18 in 126 točkami.[8,9] Če bolnik za izvedbo aktivnosti potrebuje pripomočke, npr. voziček ali berglo, lahko dobi 6 točk in ne 7, čeprav je pri izvedbi samostojen. Za izvedbo ocenjevanja je potrebno približno pol ure, izvajajo ga lahko samo usposobljeni ocenjevalci. Psihometrične lastnosti FIM, kot sta zanesljivost in veljavnost, so bile preverjene v številnih študijah.[10,11] V analizi smo uporabili klasifikacijo po Garrawayu[12] iz leta 1981, kjer so opisane stopnje invalidnosti po kategorijah vrednosti FIM, in sicer blaga (FIM > 80), zmerna (FIM 40-80) in težka (FIM < 40).

Analiza podatkov

Za demografske podatke smo izračunali opisne statistike. Za oceno povezave med oceno FIM in kategorijo invalidskega vozička smo uporabili Somersov koeficient *D*.[13]

Kategorije invalidskih vozičkov

Kategorije invalidskih vozičkov so opredeljene v šifrantu medicinskih pripomočkov, ki ga pripravlja Zavod za zdravstveno zavarovanje Slovenije (ZZZS).[14] Vseh kategorij za odrasle je enajst, za našo raziskavo pa jih je v poštev prišlo devet:[6]

1. *Voziček na ročni pogon – standardni* predpišemo ga bolnikom, ki le občasno potrebujejo voziček. Bolnika izmerimo in določimo širino sedeža ter višino od tal.
2. *Voziček na ročni pogon – aktivni* predpišemo bolnikom, ki za gibanje potrebujejo voziček. Zaradi značilnega vzorca poganjanja je pomembna višina sedeža od tal. Poleg tega je potrebno izmeriti in določiti širino in globino sedeža, višino hrbtnega naslona in višino ter dolžino naslonov za roki. Če je potrebno, se predpiše tudi dodatke (mizica, varovalna kolesa, petni trak, telesni trak in sedežna blazina).
3. *Električni skuter* predpišemo bolnikom, ki ob pomoči druge osebe ali z uporabo pripomočka prehodijo manj kot 100 metrov in ne morejo uporabljati vozička na ročni pogon. Bolniki

morajo imeti zadovoljive psihofizične, predvsem kognitivne sposobnosti.

4. *Voziček na ročni pogon za srednjo gibalno oviranost* predpišemo bolnikom, ki za gibanje stalno potrebujejo voziček in imajo dodatne zdravstvene težave (začetne kontrakture v sklepih spodnjih udov, manjša izguba moči mišic trupa ipd.).
5. *Voziček na ročni pogon za težko gibalno oviranost* predpišemo bolnikom, ki za gibanje stalno potrebujejo voziček. Bolniki imajo pridružene bolezni oziroma zdravstvena stanja (npr. motnje ravnotežja, huda izguba moči mišic trupa, deformacije trupa, slabši nadzor položaja glave).
6. *Voziček na elektromotorni pogon* predpišemo bolnikom, ki za gibanje stalno potrebujejo voziček in zaradi paralize ali izredno oslabele moči obeh zgornjih udov ne zmorejo poganjati vozička na ročni pogon.
7. *Voziček na elektromotorni pogon za težko gibalno oviranost* predpišemo bolnikom, ki za gibanje stalno potrebujejo voziček in pri katerih gre za ohromelost spodnjih udov, za deformacije trupa, za omejeno gibanje zgornjih udov ali pa hoteni ciljani gibi zgornjih udov povzročajo povezane reakcije v drugih delih telesa in patološke vzorce drže.
8. *Voziček na elektromotorni pogon za zelo težko gibalno oviranost* predpišemo bolnikom s prej opisanimi zdravstvenimi stanji, dodatno pa gre za pasivno sedenje in slabši nadzor položaja glave.

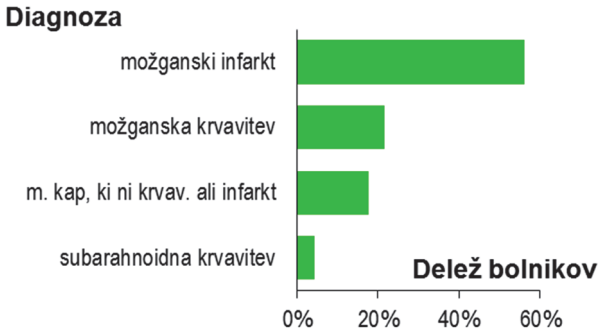
Za vse vozičke na elektromotorni pogon velja tako kot za električni skuter, da morajo bolniki imeti zadovoljive kognitivne sposobnosti (pozornost, načrtovanje, vidno-prostorske sposobnosti).

9. *Serijsko izdelan počivalnik* je namenjen bolnikom z močno zmanjšano zmožnostjo gibanja, ki so trajno vezani na voziček; ne zmorejo samostojnega pomikanja in spreminjanja položaja ter imajo že razvite deformacije in težje nadzorujejo položaj trupa in glave. Taki bolniki ne morejo uporabljati vozička na ročni pogon niti na elektromotorni pogon.

Rezultati

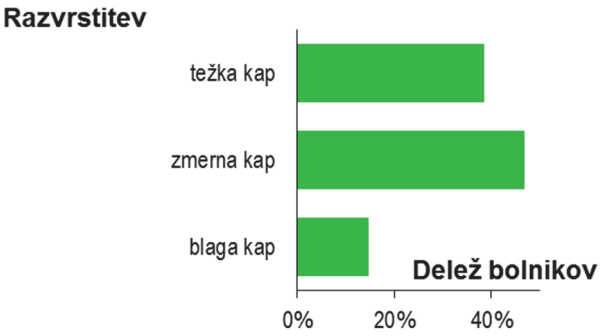
Pregledali smo podatke 1341 bolnikov po možganski kapi. Med njimi je bil 231 bolnikom predpisan invalidski voziček, kar predstavlja vzorec raziskave; 127 je bilo moških in 104 ženske, povprečna starost je bila 68 let (razpon od 22 do 97 let).

Za razvrstitev diagnoz smo uporabili Mednarodno klasifikacijo bolezni.[15] Bolniki so imeli različne diagnoze (slika 1) – več kot polovica bolnikov je utrpela možganski infarkt, dobra petina možgansko krvavitev, redki subarahnoidno krvavitev, šestina bolnikov pa je utrpela možgansko kap, ki ni opredeljena kot krvavitev ali infarkt.



Slika 1 Diagnoze bolnikov (*N*=231).

Analiza ocen skupnega FIM je pokazala, da je bilo na podlagi klasifikacije po Garrawayu v skupino s težko kapjo razvrščenih 89 bolnikov, v skupino z zmerno kapjo 108 bolnikov in 34 v skupino z blago kapjo (slika 2).



Slika 2 Razvrstitev bolnikov na podlagi skupne ocene FIM – klasifikacija po Garrawayu (*N*=231).

Slika 3 Kategorije predpisanih vozičkov (*N*=231).

Največ predpisanih vozičkov je bilo na ročni pogon – aktivnih; sledijo serijsko izdelan počivalnik, vozički na ročni pogon – standardni in vozički na ročni pogon za srednjo gibalno oviranost; zelo malo pa je bilo vozičkov na elektromotorni pogon (običajnih ali za zelo težko gibalno oviranost), električnih skuterjev, vozičkov na elektromotorni pogon za težko gibalno oviranost in ročnih vozičkov za težko gibalno oviranost.

Ugotovili smo precej močno in visoko statistično značilno povezavo med bolnikovo kategorijo FIM in kategorijo predpisanega vozička (simetrična povezava: D=0.57, p<0,001; kategorija vozička, predvidena na podlagi kategorije FIM: D=0.61, p<0,001). Po drugi strani je povezava daleč od popolne, saj razlike v kategorijah predpisanih vozičkov med zmerno in blago kapjo niso velike (tabela 1).

Tabela 1 Povezanost bolnikove kategorije FIM in kategorije predpisanega invalidskega vozička.

	Kategorija predpisanega invalidskega vozička									
Bolnikova kategorija FIM	V. na ročni pogon – standard.	V. na ročni pogon – aktivni	Električni skuter	V. na ročni pogon za sr.gib.ovi.	V. na ročni pogon za tež.gib.ovi.	V. na elektromot. pogon	V. na EM pogon za tež.gib.ovi.	V. na EM pog.za z.t. gib.ovi.	Počivalnik	Skupaj (% vseh)
Težka (FIM<40)	6 (6,7 %)	23 (25,8 %)		2 (2,2 %)				3 (3,4 %)	55 (61,8 %)	89 (38,5 %)
Zmerna (FIM 40-80)	21 (19,4 %)	62 (57,4 %)	1 (0,9 %)	15 (13,9 %)	1 (0,9 %)	3 (2,8 %)	1 (0,9 %)		4 (3,7 %)	108 (46,8 %)
Blaga (FIM>80)	22 (64,7 %)	10 (29,4 %)	1 (2,9 %)	1 (2,9 %)						34 (14,7 %)
Skupaj (% vseh)	49 (21,2 %)	95 (41,1 %)	2 (0,9 %)	18 (7,8 %)	1 (0,4 %)	3 (1,3 %)	1 (0,4 %)	3 (1,3 %)	59 (25,5 %)	N=321 (100 %)

Opomba: odstotek znotraj vrstice je sorazmerno osenčen s sivo.

Razprava

V našem vzorcu je bilo več moških kot žensk, kar delno sovpada s statističnimi podatki iz razvitih držav, ki kažejo, da do starosti 65 let doživi možgansko kap večji delež moških, po 65. letu pa je med žrtvami kapi več žensk.[16]

Več kot polovica bolnikov je utrpela možganski infarkt, kar se sklada z incidenco v svetovnem merilu. Literatura navaja, da je od 68 % do 85 % vseh možganskih kapi posledica možganskega infarkta, kar govori v prid reprezentativnosti našega vzorca.[1,17]

Ocene FIM po Garraawayevi klasifikaciji so pokazale, da je bila najbolj pogosta zmerna kap. Med predpisanimi invalidskimi vozički je bilo največ vozičkov na ročni pogon – aktivnih, saj z njim pokrijemo več stopenj funkcijskih sposobnosti za zmerno kap. Posledično največ vozičkov na ročni pogon – aktivnih dobijo ravno bolniki z zmerno kapjo.

Povezava med kategorijo vozičkov in blago ali zmerno kapjo po oceni FIM kljub velikemu vzorcu ni bila izrazita, kar je razumljivo, ker smo celotni obseg FIM (od 17 do 126 točk) razdelili le na tri kategorije. V prihodnosti bi bilo smiselno upoštevati dosežek na posameznih postavkah FIM, saj menimo, da predpis invalidskih vozičkov velikokrat pogojujejo kognitivne sposobnosti, ki jih ocenjuje pet postavk kognitivnega dela FIM.

Pokazalo se je, da bi bilo smiselno stalno spremljati podatke o predpisanih vozičkih. Tako zbrane podatke bi lahko uporabili tudi za dogovore z Zavodom za zdravstveno zavarovanje Slovenije glede financiranja medicinskih pripomočkov.

Glede na skladnost podatkov iz naše raziskave s podatki iz tuje literature[18,19] smo imeli reprezentativen vzorec, še vedno pa je bilo v redkejših kategorijah vozičkov tako malo predpisov, da posplošitev na celotno populacijo ni zanesljiva.

Zaključek

Funkcijske zmožnosti in posledično težave v gibanju so pri vsakem bolniku po preboleli možganski kapi unikatne, zato testiranje in predpis ustreznega invalidskega vozička zahtevata individualno obravnavo in multidisciplinaren pristop. Pri tem moramo poleg funkcijskih sposobnosti upoštevati tudi bolnikove želje, cilje in vloge, domače in širše bivalno oziroma delovno okolje ter finančni vidik.[20]

Reference

1. Donnan GA, Fisher M, Macleod M, Davis SM: Stroke. *Lancet* 2008, 371(9624): 1612-1623. https://doi.org/10.1016/S0140-6736(08)60694-7

2. Kalra L, Langhorne P: Facilitating recovery: evidence for organized stroke care. *J Rehabil Med* 2007; 39(2): 97-102. https://doi.org/10.2340/16501977-0043
3. Clarke DJ, Forster A: Improving post-stroke recovery: the role of the multidisciplinary health care team. *J Multidiscip Healthc* 2015; 8: 433-442. https://doi.org/10.2147/JMDH.S68764
4. Goljar N, Javh M, Rudolf M, Bizovičar N, Rudel D, Oberžan D, Burger H: Storitev telerehabilitacije na domu za osebe po preboleli možganski kapi. *Rehabilitacija* 2016; 15(3): 63-69. http://www.dlib.si/details/URN:NBN:SI:doc-6VE255PI
5. Chumbler NR, Li X, Quigley P, Morey MC, Rose D, Griffiths P, *et al.*: A randomized controlled trial on stroke telerehabilitation: the effects on falls, self-efficacy and satisfaction with care. *J Telemed Telecare* 2015; 21(3): 139-143. https://doi.org/10.1177/1357633X15571995
6. Zupan A: Najzahtevnejši invalidski vozički. V: Zupan A (ur.), *Rehabilitacijski inženiring in tehnologija: zbornik predavanj*. Ljubljana 2007: Inštitut Republike Slovenije za rehabilitacijo; 15-18.
7. Cohen ME, Marino RJ: The tools of disability outcomes research functional status measures. *Arch Phys Med Rehabil* 2000; 81(Suppl 2): 21-29.
8. Granger CV, Gresham GE: *Functional assessment in rehabilitation medicine*. Baltimore 1984: Williams & Wilkins.
9. Vidmar G, Burger H, Marinček Č, Cugelj R: Analiza podatkov o ocenjevanju z Lestvico funkcijske neodvisnosti na Inštitutu Republike Slovenije za rehabilitacijo. *Infor Med Slov* 2008; 13(1): 21-32. http://ims.mf.uni-lj.si/archive/13(1)/12.pdf
10. Young Y, Fan MY, Hebel JR, Boult C: Concurrent validity of administering the functional indešendence measure (FIM) instrument by interview. *Am J Phys Med Rehabil* 2009; 88(9): 766-770.
11. Stineman MG, Ross RN, Fiedler R, Granger CV, Maislin G: Functional independence staging: conceptual foundation, face validity and empirical derivation. *Arch Phys Med Rehabil* 2003; 84(1): 29-37. https://doi.org/10.1053/apmr.2003.50061
12. Garraway WM, Akhtar AJ, Smith DL, Smith ME: The triage of stroke rehabilitation. J Epidemiol Community Health 1981; 35(1): 39-44.
13. Somers RH: A new asymmetric measure of association for ordinal variables. *Am Sociol Rev* 1962; 27(6): 799-811.
14. Zavod za zdravstveno zavarovanje Slovenije: *Seznami in zbirke podatkov za medicinske pripomočke.* https://partner.zzzs.si/wps/portal/portali/aizv/medicinski_pripomocki/predpisovanje/seznami_in_zbirke_za_mp (8.6.2018)
15. Svetovna zdravstvena organizacija (WHO): *Mednarodna klasifikacija bolezni in sorodnih zdravstvenih problemov za statistične namene, Avstralska modifikacija (MKB-10-AM). Pregledni seznam bolezni, 6. izdaja.* Ljubljana 2016: Nacionalni inštitut za javno zdravje. http://www.nijz.si/sites/www.nijz.si/files/uploaded/podatki/klasifikacije_sifranti/mkb/mkb10-am-v6_v03_splet.pdf (8.6.2018)
16. Appelros P, Stegmayr B, Terent A: Sex differences in stroke epidemiology: a systematic review. *Stroke* 2009; 40(4): 1082-1090. https://doi.org/10.1161/STROKEAHA.108.540781
17. Feigin VL, Forouzanfar MH, Krishnamurthi R, Mensah GA, Connor M, Bennett DA *et al.*: Global and regional burden of stroke during 1990-2010: findings from the Global Burden of Disease Study 2010. *Lancet* 2014; 383(9913): 245-254.
18. Thrift AG, Cadilhac DA, Thayabaranathan T, Howard G, Howard VJ, Rothwell PM, Donnan GA: Global stroke statistics. *Int J Stroke* 2014; 9(1): 6-18. https://doi.org/10.1111/ijs.12245
19. Thrift AG, Howard G, Cadilhac DA, Howard VJ, Rothwell PM, Thayabaranathan T *et al.*: Global stroke statistics: an update of mortality data from countries using a broad code of "cerebrovascular diseases". *Int J Stroke* 2017; 12(8): 796-801. https://doi.org/10.1177/1747493017730782
20. Gillen G, Burkhardt A: *Stroke rehabilitation: a function-based approach* (4th ed.). St. Louis 2015: Elsevier.

■ *Izvirni znanstveni članek*

Larisa Stojanovič

Evropski dan boja proti melanomu – prvih deset let v Sloveniji

Povzetek. Evropski dan boja prot mealnomu (Euromelanoma Day) je javnozdravstveni projekt, ki poteka od leta 2000. V Sloveniji ga organiziramo od leta 2008. V sklopu tega projekta dermatologi klinično in dermatoskopsko preventivno pregledujejo kožo obiskovalcev v dermatoloških ambulantah v bolnišnicah in zdravstvenih domovih ter zasebnih dermatoloških ambulantah v več mestih po Sloveniji. Obiskovalci dobijo pred pregledom v izpolnjevanje anketni standardiziran vprašalnik, ki ga je pripravila Evropska akademija za dermatologijo in venerologijo (EADV) za vse sodelujoče države. V primeru odkritega melanoma, karcinoma ali drugih potencialno nevarnih sprememb obiskovalce napotijo v nadaljnjo obravnavo. Pričujoči članek predstavlja in primerja podatke, zbrane v letih 2016 in 2017, ter jih primerja s podatki, ki so bili zbrani in objavljeni leta 2008. Pokazalo se je, da število pregledov z leti postopoma upada, narašča pa delež obiskovalcev, ki so že bili preventivno pregledani v preteklosti. Nekateri dejavniki tveganja so bili leta 2008 med obiskovalci precej pogostejši, zlasti opekline v mladosti in uporaba solarija. Multivariatni statistični model z združenimi podatki iz let 2016 in 2017 je kot potencialne neodvisne napovedne dejavnike malignih sprememb na koži izpostavil nedavno opažene spremembe na koži, predhodno diagnozo kožnega raka, hude sončne opekline v preteklosti in neuporabo ali občasno uporabo zaščitnih sredstev pri sončenju. Čeprav osveščenost prebivalstva o nevarnostih pretiranega izpostavljanja kože ultravijoličnim žarkom narašča, bomo s projektom nadaljevali tudi v prihodnjih letih.

Euromelanoma Day – the First Ten Years in Slovenia

Abstract. Euromelanoma Day is a public health project that started in the year 2000. It has been held in Slovenia since 2008. Within that project, dermatologists clinically and dermatoscopically preventively examine visitors in dermatological outpatient clinics in hospitals and community health care centres, as well as in private dermatological practices in several cities across Slovenia. Before the examination, the visitors are asked to fill in a standardised questionnaire that has been prepared by the European Academy of Dermatology and Venereology (EADV) for all the participating countries. If a melanoma, skin carcinoma or other potentially dangerous skin change is discovered, the visitors are referred to further diagnostics and treatment. This paper presents and compares the data gathered in 2016 and 2017 and compares them to the data gathered and published in 2008. It has turned out that the number of visitors is gradually decreasing and the proportion of visitors who had previously been examined is increasing. Some risk factors were much more common among the visitors in 2008, especially severe sunburns during youth and use of solarium. A multivariate statistical model using combined data from the years 2016 and 2017 highlighted recently noticed skin changes and severe sunburns as potential independent prognostic factor for malignant skin changes. Though the public awareness of the dangers of excessive exposure of the skin to ultraviolet radiation is increasing, we will continue the project in the forthcoming years.

■ **Infor Med Slov** 2018; 23(1-2): 6-11

Institucije avtorice / Authors' institutions: Medicinska fakulteta, Univerza v Ljubljani.

Kontaktna oseba / Contact person: doc. dr. Larisa Stojanovič, Anatomski inštitut, Medicinska fakulteta, Univerza v Ljubljani, Vrazov trg 2, 1000 Ljubljana, Slovenija. E-pošta / E-mail: larisa.stojanovic@mf.uni-lj.si.

Prispelo / Received: 20. 6. 2018. Sprejeto / Accepted: 10. 7. 2018.

Uvod

Obolevanje za malignimi obolenji kože je v zadnjih dveh desetletjih 20. stoletja močno naraslo zaradi sprememb v življenjskem slogu in tanjšanja ozonske plasti. V 21. stoletju se je nato razširilo znanstveno razumevanje in javno zavedanje škodljivega vpliva sončevih ultravijoličnih (UV) žarkov.[1] Pomen širjenja in dostopnosti informacij v javnosti ilustrira dejstvo, da so celo med študenti zdravstvenih smeri najpogostejši vir informacij o škodljivih vplivih sončenja mediji.[2]

V okvir javnozdravstvenih prizadevanj za preprečevanje malignih obolenj kože sodi Evropski dan boja proti melanomu (Euromelanoma Day), ki poteka od leta 2000 na pobudo Evropske akademije za dermatologijo in venerologijo (*European Academy of Dermatology and Venereology*, EADV), v Sloveniji pa ga organiziramo od leta 2008.[3] V sklopu tega projekta dermatologi klinično in z dermatoskopom preventivno pregledujejo kožo obiskovalcev v dermatoloških ambulantah v bolnišnicah in zdravstvenih domovih ter zasebnih dermatoloških ambulantah v več mestih po Sloveniji. Obiskovalci dobijo pred pregledom v izpolnjevanje standardiziran anketni vprašalnik, ki ga je pripravila EADV za vse sodelujoče države. V primeru odkritega melanoma, karcinoma ali drugih potencialno nevarnih sprememb obiskovalce napotijo v nadaljnjo obravnavo.

Maligni melanom je rak, ki nastane iz melanocitov – celic, ki proizvajajo pigment melanin. Lahko se pojavi povsod, kjer se melanociti nahajajo (šarenica, možganske ovojnice, prebavila, sluznica ustne votline in spolovil), najpogosteje pa v koži. Melanom v svetu predstavlja le 5 % kožnih rakov, vendar je vzrok večine smrti zaradi kožnih rakov.[4] Nastanek malignega melanoma je povezan z dejavniki tveganja, ki so lahko dedni (mutacije genov CDKN2A, CDK4, BAP1, TERT, MC1R, številna znamenja na koži, svetla koža) ali okoljski oziroma vedenjski (izpostavljanje UV žarkom, nastanek opeklin). Raziskave ugotavljajo, da je nastanek melanoma na koži, ki je zaščitena pred soncem, povezan s povečanim številom znamenj na koži (več kot 100) in občasnim izdatnim izpostavljanjem UV žarkom, melanom, ki nastane na soncu izpostavljeni koži, pa je povezan z manjšim številom znamenj in kroničnim izpostavljanjem UV žarkom.[5,6] Primarni melanom na koži lahko nastane iz predhodnega melanocitnega nevusa ali znamenja, v večini primerov pa nastane v zdravi koži.

Članek predstavlja in primerja podatke, zbrane v letih 2016 in 2017 (ko je projekt potekal pod geslom »Imaš samo eno kožo«), ter jih primerja s podatki, ki so bili zbrani in objavljeni leta 2008 (ko je bilo geslo projekta »Pregledujte svojo kožo redno; odkrijte melanom pravočasno«).[3]

Metode

Analizirali smo podatke, zbrane z anketnim vprašalnikom in dermatološkimi pregledi v letih 2016 in 2017, ter jih primerjali s podatki iz leta 2008. Vprašanja v anketnem vprašalniku so razvidna iz rezultatov.

Uporabili smo opisno statistiko, test χ^2 za primerjavo deležev (v izvedbi Monte-Carlo z 10000-kratnim prevzorčenjem) in logistično regresijo s Firthovim popravkom.[7,8] Statistične analize smo izvedli s programskim paketom IBM SPSS Statistics 23 (IBM Corp., Armonk, NY, 2014).

Rezultati

Primerjava med letoma 2016 in 2017

V letu 2016 je prišlo na preventivni pregled 170 oseb, v letu 2017 pa 132 oseb. Skupaj smo torej pregledali 302 osebi. Število in deleže odgovorov na anketna vprašanja skupaj z rezultati statističnega testiranja razlik med letoma prikazujeta tabeli 1 (za demografske značilnosti in razlog obiska) in 2 (za dejavnike tveganja za kožnega raka).

Povzamemo lahko, da sta se vzorca oseb med letoma 2016 in 2017 razlikovala predvsem glede

- starosti (leta 2016 je bilo povprečje 46 let in razpon od 22 do 72 let, leta 2017 pa povprečje 52 let in razpon od 13 do 83 let),
- izobrazbene strukture (več visoko izobraženih je bilo v letu 2017),
- deleža predhodno pregledanih (višji je bil v letu 2017),
- odziva kože na poletno sonce (v letu 2016 je bilo več oseb z močnejšimi odzivi),
- deleža oseb s hudimi sončnimi opeklinami v preteklosti (višji je bil v letu 2016),
- uporabe sredstev za zaščito kože pri sončenju (pogostejša v letu 2017) in
- pogostosti uporabe solarija (nekoliko večja v letu 2016).

Tabela 1 Demografske značilnosti udeležencev in razlog obiska.

Anketno vprašanje, odgovor	2016 [*N* = 170]	2017 [*N* = 132]	Skupaj [*N* = 302]	*p*
Spol				0,069
moški	68 (40,0 %)	39 (29,5 %)	107 (35,4 %)	
ženski	102 (60,0 %)	93 (70,5 %)	195 (64,6 %)	
Izobrazba		[*N* = 130]	[*N* = 300]	
osnovna šola	12 (7,1 %)	4 (3,1 %)	16 (5,3 %)	0,001
poklicna šola	35 (20,6 %)	15 (11,5 %)	50 (16,7 %)	
srednja šola	85 (50,0 %)	53 (40,8 %)	138 (46,0 %)	
visoka šola	38 (22,4 %)	58 (44,6 %)	96 (32,0 %)	
Razlog za udeležbo*				
imam veliko znamenj	78 (45,9 %)	72 (54,5 %)	150 (49,7 %)	0,164
nedavna sprememba na koži	34 (20,0 %)	24 (18,2 %)	58 (19,2 %)	0,769
predhodno diagnosticiran kožni rak	5 (2,9 %)	7 (5,3 %)	12 (4,0 %)	0,377
družinski član ali prijatelj ima kožnega raka	18 (10,6 %)	11 (8,3 %)	29 (9,6 %)	0,560
Že kdaj prej opravil(a) pregled#	28 (16,5 %)	36 (27,3 %)	64 (21,2 %)	0,253

Opombe: vsi obiskovalci so odgovorili na vsa vprašanja (*N* = 302) razen glede izobrazbe v letu 2017 [kot je navedeno pri vprašanju]; * možno je bilo izbrati več odgovorov, zato so število in delež udeležencev, ki so ga izbrali, ter statistični test razlike med letoma podani za vsak odgovor posebej; # pri vprašanjih z odgovorom "da" ali "ne" sta navedena le število in delež odgovorov "da".

Tabela 2 Odgovori na anketna vprašanja o dejavnikih tveganja za kožnega raka.

Anketno vprašanje, odgovor	2016 [*N* = 170]	2017 [*N* = 132]	Skupaj [*N* = 302]	*p*
Opravljanje poklica na prostem#	37 (21,8 %)	20 (15,2 %)	57 (18,9 %)	0,182
Kako koža reagira na poletno sonce				<0,001
vedno jo opeče	33 (19,4 %)	9 (6,8 %)	42 (13,9 %)	
vedno jo opeče, minimalno porjavi	46 (27,1 %)	12 (9,1 %)	58 (19,2 %)	
najprej jo opeče, potem porjavi	72 (42,4 %)	63 (47,7 %)	135 (44,7 %)	
opeče jo le minimalno, hitro porjavi	19 (11,2 %)	48 (36,4 %)	67 (22,2 %)	
Že imel(a) hude sončne opekline#	79 (46,5 %)	44 (33,3 %)	123 (40,7 %)	0,025
Uporaba zaščitnih izdelkov na prostem		[*N* = 118]	[*N* = 288]	0,081
nikoli	35 (20,6 %)	32 (27,1 %)	67 (23,3 %)	
včasih	110 (64,7 %)	61 (51,7 %)	171 (59,4 %)	
vedno	25 (14,7 %)	25 (21,2 %)	50 (17,4 %)	
Uporaba zaščitnih izdelkov pri sončenju		[*N* = 123]	[*N* = 293]	<0,001
nikoli	9 (5,3 %)	0 (0,0 %)	9 (3,1 %)	
včasih	74 (43,5 %)	28 (22,8 %)	102 (34,8 %)	
vedno	55 (32,4 %)	74 (60,2 %)	129 (44,0 %)	
se ne sončim	32 (18,8 %)	21 (17,1 %)	53 (18,1 %)	
Živel(a) več kot eno leto v državi, bolj izpostavljeni soncu				0,372
ne	163 (95,9 %)	129 (97,7 %)	292 (96,7 %)	
da, pred 18. letom	5 (2,9 %)	1 (0,8 %)	6 (2,0 %)	
da, po 18. letu	2 (1,2 %)	2 (1,5 %)	4 (1,3 %)	
Izpostavljanje soncu v odrasli dobi na poletnih počitnicah				0,025
nič	15 (8,8 %)	15 (11,4 %)	30 (9,9 %)	
do 2 tedna	115 (67,6 %)	69 (52,3 %)	184 (60,9 %)	
več kot 2 tedna	40 (23,5 %)	48 (36,4 %)	88 (29,1 %)	
Uporaba solarija				0,012
ne	163 (95,9 %)	131 (99,2 %)	294 (97,4 %)	
do 20 obiskov letno	7 (4,1 %)	0 (0,0 %)	7 (2,3 %	
več kot 20 obiskov letno	0 (0,0 %)	1 (0,8 %)	1 (0,3 %)	

Opombe: vsi obiskovalci so odgovorili na vsa vprašanja razen glede uporabe zaščitnih izdelkov v letu 2017 [kot je navedeno pri vprašanju]; # pri vprašanjih z odgovorom "da" ali "ne" sta navedena le število in delež odgovorov "da".

Med letoma ni bilo statistično značilne razlike v deležu oseb z odkritimi malignimi spremembami kože (8 % leta 2016, 6 % leta 2017; $p = 0{,}512$). V letu 2016 smo odkrili pri

- 1 osebi melanom,
- 5 osebah ploščatocelični karcinom,
- 8 osebah bazalnocelični karcinom in
- 11 osebah druge spremembe kože, zaradi katerih smo jih napotili v nadaljnjo obravnavo.

V letu 2017 pa smo odkrili pri

- 5 osebah melanom,
- 4 osebah bazalnocelični karcinom (enega poleg melanoma in pri eni osebi dva) in
- 11 osebah druge spremembe kože, zaradi katerih smo jih napotili v nadaljnjo obravnavo.

Napovedni model

Za boljše razumevanje dejavnikov tveganja smo skušali analizirati njihovo povezanost z odkritimi malignimi spremembami kože. V ta namen smo združili podatke iz let 2016 in 2017. Potencialne napovedne dejavnike smo v napovedni model izbrali na podlagi vsebinske pomembnosti in univariatne povezanosti z napovedovanim izidom oziroma izločili zaradi visoke medsebojne povezanosti. Tako smo v model za napoved malignih sprememb kože (v združenem vzorcu odkrite pri 22 osebah od 293; 9 oseb izločenih iz analize zaradi manjkajočih podatkov) vključili 7 dvojiških spremenljivk (tabela 3).

Tabela 3 Povzetek logistične regresije s Firthovim popravkom za napoved malignih sprememb na koži.

Napovedni dejavnik	*b* (SE)	RO (95 % int. zaupanja)	*p*
Spol (ženski vs. moški)	1,010 (0,600)	2,75 (0,89 – 10,29)	0,081
Razlog za udeležbo: imam veliko znamenj (da vs. ne)	0,045 (0,577)	1,05 (0,32 – 3,34)	0,939
Razlog za udeležbo: nedavna sprememba na koži (da vs. ne)	1,781 (0,577)	5,94 (1,92 – 19,83)	0,002
Razlog za udeležbo: predhodno diagnosticiran kožni rak (da vs. ne)	2,056 (0,911)	7,81 (1,21 – 44,66)	0,032
Imel(a) hude sončne opekline (da vs. ne)	1,302 (0,519)	3,68 (1,36 – 11,38)	0,010
Uporaba zaščitnih izdelkov pri sončenju (nikoli ali včasih vs. vedno ali se ne sončim)	1,102 (0,521)	3,01 (1,09 – 8,94)	0,033
Uporaba solarija (da vs. ne)	1,094 (0,979)	2,99 (0,44 – 18,97)	0,253

Oznake: *b* – regresijski koeficient; SE – standardna napaka ocene *b*; RO – razmerje obetov.

Zaradi majhne pogostosti napovedovanega izida in nekaterih napovednih dejavnikov ter njihovih kombinacij smo uporabili logistično regresijo s Firthovim popravkom, ki odpravlja pristranost običajne logistične regresije pri tovrstnih podatkih in hkrati omogoča smiselne ocene parametrov tudi v primeru popolne ločitve (angl. *complete separation*) izida glede na napovedni dejavnik.[7,8] Model kot celota je bil statistično značilno ustreznejši od ničelnega (test razmerja verjetij: $p < 0{,}001$). Kot neodvisne napovedne dejavnike za maligne spremembe kože je izpostavil nedavno opažene spremembe na koži, predhodno diagnozo kožnega raka, hude sončne opekline v preteklosti in neuporabo ali občasno uporabo zaščitnih sredstev pri sončenju (tabela 4).

Primerjava z letom 2008

Ker se je anketni vprašalnik skozi čas nekoliko spremenil, se da z letom 2008 primerjati le del podatkov iz obdobja 2016-2017. Demografska struktura se je nekoliko spremenila, saj so bili obiskovalci v letu 2008 nekoliko mlajši (povprečno starost lahko na podlagi podatkov o starostnih razredih ocenimo na okrog 44 let, v novejšem obdobju pa je bila 48 let) in delež žensk je bil še nekoliko višji (71 %; $p = 0{,}098$). Anketnega vprašanja o izobrazbi leta 2008 ni bilo.[3]

Delež obiskovalcev z odkritim kožnim rakom oziroma sumom nanj je bil leta 2008 podoben (5 % v primerjavi s 7 %; $p = 0{,}335$). Glede dejavnikov tveganja podatki omogočajo naslednje kvantitativne primerjave:[3]

- leta 2008 so bile nedavno opažene spremembe na koži pogosteje motiv za udeležbo (33 % v primerjavi z 19 %; $p < 0{,}001$);
- delež obiskovalcev s predhodno diagnozo kožnega raka je bil enak (4 %; $p = 0{,}923$);
- službo na prostem je leta 2008 opravljalo manj obiskovalcev (5 % v primerjavi z 19 %; $p < 0{,}001$);

- hude sončne opekline v mladosti je leta 2008 imelo kar 62 % obiskovalcev (v primerjavi s 43 %; $p < 0{,}001$);
- leta 2008 je bila uporaba solarija mnogo pogostejša (31 % v primerjavi s 3 %; $p < 0{,}001$).

Poleg tega lahko ocenimo, da so bili odzivi kože obiskovalcev na poletno sonce zelo podobne, saj je leta 2008 60 % obiskovalcev sodilo v fototip III (sonce jih redko opeče in vedno porjavijo),[3] v novejšem obdobju pa je 67 % obiskovalcev navedlo, da jih sonce najprej (ali samo minimalno) opeče, nato pa porjavijo. Izpostavljanja soncu med počitnicami je bilo med obiskovalci leta 2008 najbrž več, saj je v povprečju trajalo tri tedne, v novejšem obdobju pa je le 29 % obiskovalcev navedlo, da se med počitnicami izpostavljajo soncu več kot dva tedna.

Razprava

Poleg izvedbe Evropskega dne boja proti melanomu za splošno javnost je pomembno tudi objavljanje zbranih podatkov in pridobljenih izkušenj za strokovno javnost.[3,9-12] Z javnozdravstvenega vidika je pomembno tudi odkrivanje malignih sprememb v čim bolj zgodni fazi.

Zbrani podatki kažejo, da število pregledov z leti postopoma upada, hkrati pa narašča delež obiskovalcev, ki so že bili preventivno pregledani v preteklosti. Primerjava združenih podatkov za leti 2016 in 2017 z letom 2008 je pokazala, da so bili ob prvi izvedbi projekta dejavniki tveganja med obiskovalci v splošnem pogostejši. Več je bilo nedavno opaženih sprememb na koži, hudih sončnih opeklin v mladosti, uporabe solarija in izpostavljanja soncu med počitnicami. Kljub temu je bil delež obiskovalcev, ki so jim leta 2008 na pregledu odkrili maligne spremembe na koži, praktično enak oziroma celo nekoliko nižji kot v letih 2016 in 2017.

Pri interpretaciji statističnega napovednega modela za maligne spremembe na koži je potrebno upoštevati, da vzorec ne predstavlja splošne populacije, pač pa večinoma osebe, ki imajo višje tveganje za nastanek kožnega raka in se tega zavedajo, zato so prišle na preventivni pregled. Dejavniki tveganja, ki jih je izpostavil model, so znani in pričakovani, pomembno pa je, da so ocenjena razmerja obetov za maligne spremembe na koži pri vseh teh dejavnikih zelo visoka (vse točkovne ocene so nad 3).

Zaključek

Evropski dan boja proti melanomu je pomemben in uspešen javnozdravstveni projekt. Podatki, ki jih zbiramo z anketnimi vprašalniki in dermatološkimi pregledi, pomagajo informirati prebivalstvo o nevarnostih prekomernega in nezaščitenega sončenja. Naraščanje deleža obiskovalcev, ki so že bili preventivno pregledani, kaže na osveščenost populacije o tej problematiki. Rezultati statističnih analiz potrjujejo, da moramo biti za pravočasno diagnozo kožnega raka vseskozi pozorni na spremembe na koži, posebej previdne pa morajo biti osebe, ki so za to boleznijo že zbolele v preteklosti. Poleg tega so naše analize potrdile preventivni pomen zaščite pri sončenju in veliko nevarnost za nastanek kožnega raka po sončnih opeklinah. S projektom bomo nadaljevali tudi v prihodnje.

Zahvala

Zahvaljujem se prof. dr. Gaju Vidmarju za pomoč pri statistični analizi podatkov.

Reference

1. Golob K: *Osveščenost ljudi o preprečevanju kožnega melanoma* (diplomsko delo). Maribor 2010: Univerza v Mariboru, Fakulteta za zdravstvene vede.
2. Kofol M: *Znanje študentov zdravstvene nege o nevarnosti sončenja* (diplomsko delo). Jesenice 2012: Visoka šola za zdravstveno nego Jesenice.
3. Bartenjev I, Benedičič A, Dugonik A, Luft S, Ručigaj T, Stojanovič L, Voda K, Žgavec B: Euromelanoma Day v Sloveniji: analiza aktivnosti in pregled rezultatov. In: Miljković J (ed.), *5. Dermatološki dnevi v Mariboru 2008*. Maribor 2008: Univerzitetni klinični center, Oddelek za kožne in spolne bolezni; 110-117.
4. Ossio R, Roldán-Marín R, Martínez-Said H, Adams DJ, Robles-Espinoza CD: Melanoma: a global perspective. *Nat Rev Cancer* 2017; 17(7): 393-394. https://doi.org/10.1038/nrc.2017.43
5. Whiteman DC, Watt P, Purdie DM, Hughes MC, Hayward NK, Green AC: Melanocytic nevi, solar keratoses, and divergent pathways to cutaneous melanoma. *J Natl Cancer Inst* 2003; 95(11): 806-812.
6. Maldonado JL, Fridlyand J, Patel H, *et al.*: Determinants of BRAF mutations in primary melanomas. *J Natl Cancer Inst* 2003; 95(24): 1878-1890.
7. Firth D: Bias reduction of maximum likelihood estimates. *Biometrika* 1993; 80(1): 27-38. https://doi.org/10.1093/biomet/80.1.27
8. Heinze G, Schemper M: A solution to the problem of separation in logistic regression. *Stat Med* 2002; 21(16): 2409-2419. https://doi.org/10.1002/sim.1047
9. Vandaele MM, Richert B, Van der Endt JD, *et al.*: Melanoma screening: results of the first one-day campaign in Belgtum ("melanoma Monday"). *J Eur Acad Dermatol Venereol* 2000; 14(6): 470-472.
10. Conejo-Mir J, Bravo J, Diaz-Pérez JL, *et al.*: Euromelanoma Day. Results of the 2000, 2001 and 2002 campaigns in Spain. *Actas Dermosifiliogr* 2005; 96(4): 217-221.

11. Stratigos A, Nikolau V, Kedicoglou S, *et al.*: Melanoma/skin cancer screening in a Mediterranean country: results of the Euromelanoma Screening Day Campaign in Greece. *J Eur Acad Dermatol Venereol* 2007; 21(1): 56-62.

12. Bulliard JL, Maspoli M, Panizzon RG, Hohl D, Gueissaz F, Levi F: Evaluation of the Euromelanoma skin cancer screening campaign: the Swiss experience. *J Eur Acad Dermatol Venereol* 2008; 22(3): 365-366. https://doi.org/10.1111/j.1468-3083.2007.02316.x

■ *Izvirni znanstveni članek*

Branimir Leskošek

Statistično učenje za napovedovanje možnih součinkovanj med zdravili

Povzetek. Strojno napovedovanje součinkovanj (interakcij) med zdravili je relativno novo raziskovalno področje na preseku farmakologije in ved o življenju ter računske statistike. V prispevku obravnavamo in ovrednotimo nekatere postopke statističnega učenja za napovedovanje možnih součinkovanj med zdravili. Slednje smo predstavili kot kompleksno omrežje, v katerem se vozlišča nanašajo na zdravila, povezave med vozlišči pa na možna součinkovanja med zdravili. Za napovedovanje potencialnih novih povezav smo uporabili metodologijo napovedovanja povezav v kompleksnih omrežjih. Natančneje, proces napovedovanja povezav smo predstavili kot nalogo uvrščanja na omrežjih možnih součinkovanj. Učinkovitost napovedovanja novih povezav smo ovrednotili s serijo eksperimentov nad naslednjimi omrežji: DrugBank, KEGG, NDF-RT, SemMedDB in Twosides. Za napovedovanje povezav smo uporabili nenadzorovane in nadzorovane postopke statističnega učenja, med drugim klasifikacijsko drevo, *k*-najbližjih sosedov, metodo podpornih vektorjev in slučajne gozdove. Atribute smo konstruirali na osnovi topoloških in semantičnih mer podobnosti med vozlišči. Najboljši napovedni model v smislu ploščine pod ROC krivuljo (AUC) smo dosegli s slučajnimi gozdovi nad omrežjem Twosides (AUC = 0,93). Predstavljena metodologija lahko služi kot primerno orodje za napovedovanje možnih součinkovanj med zdravili, tako na ravni teoretičnega raziskovanja kot tudi v klinični praksi.

Statistical Learning for Predicting Potential Drug Interactions

Abstract. Machine prediction of drug-drug interactions (DDIs) is relatively new research field at the intersection of pharmacology as well as life sciences and computational statistics. In this paper, we deal with selected statistical learning algorithms for predicting possible DDIs. We represent DDIs as a complex network in which nodes refer to drugs and links refer to their potential interactions. We implemented the process of link prediction as a binary classification task on networks of potential DDIs. We used link prediction techniques for predicting unknown interactions between drugs in five large-scale DDIs databases, namely DrugBank, KEGG, NDF-RT, SemMedDB, and Twosides. We estimated the performance of link prediction using a series of experiments on DDIs networks. We performed link prediction using unsupervised and supervised approach including classification tree, *k*-nearest neighbours, support vector machines, random forest, and gradient boosting machine classifiers based on topological and semantic similarity features. Supervised approach clearly outperforms unsupervised approach. The Twosides network gained the best prediction performance regarding the area under the precision-recall curve (AUC = 0.93). The applied methodology can be used as a tool to help researchers to identify potential DDIs. (korespondenčnem avtorju).

■ **Infor Med Slov** 2018; 23(1-2): 12-17

Institucije avtorjev / Authors' institutions: Medicinska Fakulteta, Univerza v Ljubljani; ELIXIR Slovenija.

Kontaktna oseba / Contact person: dr. Branimir Leskošek, Medicinska fakulteta, Univerza v Ljubljani, Vrazov trg 2, 1000 Ljubljana, Slovenija.
E-pošta / E-mail: brane.leskosek@mf.uni-lj.si.

Prispelo / Received: 10. 7. 2018. Sprejeto / Accepted: 26. 11. 2018.

Uvod

Sočasna uporaba več zdravil hkrati (polifarmakoterapija) je v sodobni klinični praksi čedalje bolj pogosta, zlasti pri starejši populaciji bolnikov,[1] kjer je pogosto hkrati prisotnih tudi več bolezni (polimorbidnost).[2] Odstotek populacije v ZDA, ki uživa tri ali več zdravil hkrati, se je zvišal iz 12 % v letih 1988-1994 na 21 % v letih 2007-2010.[3] V takih pogojih lahko pride do součinkovanj (interakcij) med zdravili (DDI). DDI je dogodek, v katerem eno zdravilo s farmakodinamičnega, farmakokinetičnega ali farmacevtskega vidika vpliva na farmakološki učinek drugega zdravila, ko bolniku apliciramo obe zdravili hkrati.

V kliničnih študijah se ne identificirajo vsi neželeni učinki zdravil (NUZ) in vse DDI. Liu[4] poroča, da okoli 10 % vseh možnih parov zdravil lahko izzove NUZ zaradi DDI. Sistematičen pregled zbirk DDI (npr. DrugBank, Drugs.com) je pokazal, da so te nepopolne oz. da vsebujejo veliko število klinično nerelevantnih DDI.[5]

DDI lahko preprosto predstavimo kot omrežje, v katerem se vozlišča nanašajo na zdravila, relacije med vozlišči pa na njihova součinkovanja.[6] Na področju farmakologije so bile doslej že opravljene nekatere raziskave, ki so uporabile metodologijo kompleksnih omrežij, vključno z napovedovanjem DDI.[7, 8] Prav tako so bili za napovedovanje DDI v preteklosti razviti različni statistični postopki. Obstoječe pristope k napovedovanju DDI lahko razvrstimo na: (i) pristope, ki temeljijo na podobnosti med vozlišči, (ii) klasifikacijski pristope in (iii) pristope rudarjenja besedil. Prvi pristop predpostavlja, da bodo podobna zdravila součinkovala s podobnimi zdravili; npr. dve zdravili bosta součinkovali, če bosta imeli podobno molekulsko strukturo. Klasifikacijski pristopi predstavijo napovedovanje DDI kot dvojiško nalogo klasifikacije. Pari zdravil so predstavljeni kot vektorji primerov; razred primera označuje prisotnost oz. odsotnost součinkovanja. Pristopi rudarjenja besedil temeljijo na uporabi metodologije procesiranja naravnega jezika (npr. iz MEDLINE zapisov).

V prispevku se ukvarjamo z napovedovanjem povezav v smislu napovedovanja potencialnih DDI. Glavna cilja prispevka sta: (i) predstaviti proces odkrivanja potencialnih DDI kot dvojiški klasifikacijski izziv in (ii) ovrednotiti učinkovitost metod strojnega učenja za napovedovanje potencialnih DDI. Naš prispevek je inovativen v štirih vidikih: (i) uporabimo veliko množico podatkovnih zbirk vključno z zbirkami DrugBank, KEGG, NDF-RT, SemMedDB in Twosides, (ii) poleg značilk izpeljanih iz topologije omrežij uporabimo tudi semantične značilke, kot so npr. MeSH termini in ATC shema, (iii) poleg nenadzorovanega učenja uporabimo tudi nadzorovano učenje in nenazadnje (iv) rezultate statistično ovrednotimo.

Metode

Omrežja součinkovanj zdravil

Omrežja DDI smo konstruirali na osnovi petih podatkovnih zbirk: DrugBank, KEGG, NDF-RT, SemMedDB in Twosides. Podatkovne zbirke so na kratko predstavljene v nadaljevanju razdelka.

DrugBank je spletno skladišče, ki združuje relevantne biokemijske in farmakološke podatke o zdravilih. Večina informacije je kurirana iz znanstvene literature. DrugBank trenutno vsebuje 10.376 vnosov zdravil in 577.712 usmerjenih DDI. V raziskavi smo uporabili DrugBank različico 5.0, ki smo jo pridobili s spletne strani https://www.drugbank.ca 1. 8. 2017.

KEGG (angl. *Kyoto Encyclopedia of Genes and Genomes*) je eden od najbolj popularnih virov presnovnih/signalnih poti za različne organizme. Del KEGG je tudi zbirka KEGG DRUG, ki vsebuje seznam, informacije o kemijski strukturi, tarčnih molekulah in terapevtskih kategorijah za zdravila, registrirana v Evropi, ZDA in na Japonskem. Zbirko smo prenesli s KEGG FTP strežnika (ftp://ftp.genome.jp/pub/kegg/medicus/drug/) 1. 8. 2017. KEGG DRUG vsebuje 10.340 entitet in 500.254 usmerjenih DDI. S preslikavo na DrugBank smo pridobili 1.194 zdravil in 52.609 relacij.

NDF-RT (angl. *National Drug File Reference Terminology*) je zbirka DDI, za katero jo do nedavnega skrbela Ameriška veteranska administracija. Najprej smo pripravili seznam součinkovanj s pomočjo storitve NCBI SPARQL (http://sparql.bioontology.org/sparql). Na ta način smo pridobili 10.530 usmerjenih DDI. V naslednjem koraku smo jih preslikali na DrugBank identifikatorje z uporabo UMLS Metatezavra. Tako preslikana zbirka je vsebovala 701 DrugBank identifikatorjev in 8.044 DDI.

SemMedDB je zbirka semantičnih predikatov (tj. relacij subjekt-relacija-objekt), izluščenih iz zbirke MEDLINE s pomočjo orodja SemRep. V raziskavi smo uporabili različico SemMedDB v.30. Kot vir potencialnih DDI smo uporabili vse relacije tipa »INTERACTS_WITH«. Tako pripravljena zbirka je vsebovala 1.447.792 usmerjenih DDI med UMLS koncepti, ki se nanašajo na različna zdravila. Nato smo s pomočjo UMLS Metatezavra preslikali UMLS

koncepte v DrugBank identifikatorje; končna zbirka je vsebovala 1.688 zdravil in 37.287 DDI.

Twosides zbirka je na voljo v obliki tekstovne datoteke na http://tatonettilab.org/. Za preslikavo identifikatorjev Twosides na DrugBank identifikatorje smo uporabili storitev PubChem (https://pubchem.ncbi.nlm.nih.gov/). Končna zbirka je vsebovala 340 zdravil in 19.020 DDI.

Predstavitev podatkov

Denimo, da obravnavamo neusmerjeno in neuteženo omrežje, ki ga predstavimo s preprostim grafom $G(V, E)$. Graf sestavljata množica vozlišč V, ki se nanaša na zdravila, in množica povezav E, ki se nanaša na DDI. Z U označimo množico, ki vsebuje vse možne relacije. $U - E$ je potem množica neobstoječih povezav oz. povezav, ki se pojavijo kasneje v času. Izziv napovedovanja povezav je napovedati te manjkajoče relacije. Množico dejanskih povezav E smo razbili na: učno razbitje E^T in testno razbitje E^P, tako da je $E^T \cup E^P = E$ in $E^T \cap E^P = \emptyset$. Za delitev smo uporabili razmerje 66/33 v prid učni množici. Za vse pare vozlišč v učni množici smo izračunali mere podobnosti, ki odražajo verjetnost, da bo par vozlišč povezan v testni množici podatkov. V jeziku strojnega učenja vsak par vozlišč služi kot pozitivni oz. negativni primer, odvisno od tega, ali par sestavlja povezavo v testnem omrežju. Celotno omrežje smo nato predstavili kot seznam relacij. Vsak element seznama sestavljata podatkovni vektor in oznaka relacije (slednja ima vrednost 1, ko je par vozlišč povezan, in 0 sicer). Podatkovni vektor sestavljata dve podmnožici, kot je opisano v nadaljevanju prispevka.

Naša glavna predpostavka je, da bodo topološko bolj podobna vozlišča z večjo verjetnostjo generirala DDI. Za vsak neobstoječ par (x, y) v testni množici podatkov naš algoritem izračuna podobnost $s(x, y) \in U - E^T$, ki je ocena verjetnosti povezanosti vozlišč x in y.

Podatkovni vektorji

Priprava ustrezne množice podatkovnih vektorjev je eden od ključnih elementov statističnega učenja. Večina obstoječih pristopov k napovedovanju povezav v DDI omrežjih uporablja zgolj topološke mere podobnosti. V naši raziskavi smo ta nabor razširili s štirimi semantičnimi merami. Bralca opozarjamo, da zaradi pomanjkanja prostora podrobnosti mer ne navajamo; podroben pregled in opis bo našel v razširjenem članku.[9]

Med topološkimi merami smo uporabili naslednje mere podobnosti: skupne sosede, Jaccardov koeficient, Adamic/Adarjev koeficient, prednostno povezovanje, alokacijo virov ter mero WIC, ki meri podobnost med vozliščema na osnovi gruč v omrežju.

Poleg naštetih smo uporabili še štiri semantične mere podobnosti, in sicer: podobnost na osnovi ATC razvrščanja zdravil, podobnost kemijske strukture, podobnost MeSH deskriptorjev in podobnost na osnovi NUZ.

Statistično učenje

Za učenje smo uporabili nenadzorovan in nadzorovan pristop. Za slednjega smo uporabili pet klasifikatorjev, in sicer klasifikacijska drevesa, *k*-najbližjih sosedov, metodo podpornih vektorjev, slučajne gozdove in stohastični gradientni *boosting*. Za nenadzorovano učenje smo uporabili kombinirano mero podobnosti, ki smo jo dobili s standardizacijo mer podobnosti in njihovim povprečkom. Par vozlišč je povezan, če je vrednost mere nad izbrano pražno vrednostjo t. Nizka pražna vrednost vrne večje število potencialnih DDI in obratno. V naših nastavitvah smo kot pražno vrednost uporabili 90. percentil.

Ovrednotenje učenja

Natančnost algoritmov statističnega učenja smo ovrednotili z uporabo standardne sheme učna/testna množica. Statistične modele smo zgradili z uporabo paketa caret v R. Za vzporedno procesiranje smo uporabili paket doMC. Izbor ustreznega modela smo opravili na osnovi 10-kratnega prečnega preverjanja na učni množici podatkov; model z največjo klasifikacijsko točnostjo smo uporabili za napovedovanje DDI v testni množici podatkov.

Učinkovitost učenja smo predstavili s standardnimi merami, ki se uporabljajo na področju statističnega učenja; uporabili smo natančnost, priklic, F1 mero, ploščino pod ROC krivuljo (AUROC) in ploščino pod krivuljo natančnost-priklic (AUPR). Slednjo mero smo uporabili predvsem zaradi tega, ker klasična ROC krivulja kaže vrsto pomanjkljivosti pri uporabi nad neuravnoteženimi podatkovji.[10]

Programska orodja

Za pripravo podatkov smo uporabili skriptna jezika AWK in Python. Mere podobnosti so bile implementirane z uporabo knjižnice NetworkX v Pythonu. Ostale računske operacije smo opravili s programskim jezikom R. Celotna programska koda je prosto dostopna na naslovu https://github.com/akastrin/ddi-prediction.

Rezultati

Lastnosti omrežij

Povzetek topoloških mer omrežij je prikazan v tabeli 1. Za vsa omrežja je značilna kratka povprečna dolžina poti; z drugimi besedami, med dvema vozliščema sta v povprečju le dobri dve povezavi. Povprečni koeficient zgoščanja znaša $C = 0{,}46$. Povprečni premer omrežja znaša šest povezav.

V naslednjem koraku smo pripravili povzetek skupnih povezav med pari vozlišč v omrežjih (tabela 2). Delež preseka je določen kot razmerje med prekrivajočimi povezavami in manjšim številom povezav v paru omrežij. Rezultati kažejo, da ima večina parov nizek delež prekrivanja. To kaže na komplementarnost uporabljenih omrežij.

Učinkovitost učenja

V tem razdelku najprej predstavimo rezultate nenadzorovanega učenja, nato pa še rezultate nadzorovane klasifikacije.

Rezultati nenadzorovanega učenja so povzeti v tabeli 3. Med vsemi podatkovnimi viri najbolj izstopa omrežje Twosides, ki se ponaša z največjo natančnostjo in hkrati z najmanjšim priklicem. Z izjemo omrežij DrugBank in Twosides kaže nenadzorovana klasifikacija vzorec "majhna natančnost – visok priklic". To pomeni, da obstaja večja verjetnost napačno pozitivnih zadetkov in manjša verjetnost pogreškov.

Rezultati nadzorovanega učenja so predstavljeni v tabeli 4. Najboljše rezultate na testnih podatkih dosežemo z omrežjem Twosides, ki mu sledijo omrežja DrugBank, KEGG, SemMedDB in NDF-RT. Omrežji DrugBank in Twosides dosegata najboljše rezultate tako pri natančnosti kot pri priklicu, medtem ko je pri ostalih omrežjih vzorec izraženosti obraten.

S primerjavo skupin označenih vozlišč smo ugotovili, da je povprečna podobnost pozitivno označenih DDI parov vozlišč statistično značilno višja ($p < 0{,}001$) kot povprečna podobnost negativno označenih DDI parov v vseh petih omrežjih. Ta ugotovitev potrjuje našo domnevo, da imajo podobne učinkovine (kjer podobnost merimo s topološkimi in semantičnimi merami nad omrežjem DDI) večjo verjetnost za DDI.

Razprava

V prispevku smo predstavili računski pristop k identifikaciji potencialnih DDI z uporabo metodologije napovedovanja povezav v kompleksnih omrežjih. Napovedovanje povezav smo opravili na petih izbranih kompleksnih omrežjih DDI. Naši rezultati potrjujejo domnevo o primernosti nadzorovanega napovedovanja povezav za napovedovanje DDI. Napovedna moč je visoka, ne glede na izbrano omrežje.

V sodobni farmakologiji obstaja velik interes za učinkovito in zanesljivo identifikacijo DDI. Zaradi visoke cene eksperimentalnih podatkov in posledično pomanjkanja empirične evidence je uporaba računskih pristopov za določevanje DDI zelo dobrodošla. Pri tem je seveda potrebno poudariti, da računska analiza potencialnih DDI lahko pripelje do pomembnih odkritij, ne more pa še v popolnosti nadomestiti farmakološke introspekcije.

V prihodnje bi bilo v analizo smiselno vključiti tudi genomske kovariate in prosto besedilo. Naša analiza je sicer zasnovana na vseh pomembnejših zbirkah, kljub temu pa smo izpustili nekatere, zlasti klinično relevantne zbirke (npr. Drugs.com, Medscape Multi-Drug Interaction Checker, RxList). Slednjih ni bilo moč vključiti, ker ne ponujajo prostodostopnega API vmesnika.

Zaključek

Napovedovanje povezav v omrežjih je učinkovita metodologija za študij kompleksnih omrežij v različnih znanstvenih disciplinah, vključno s farmakologijo. V prispevku smo prikazali pristop k napovedovanju potencialnih DDI na osnovi metodologije napovedovanja povezav. Študirali smo napovedno točnost nenadzorovanega in nadzorovanega učenja na petih izbranih velikih omrežjih DDI. Kljub temu, da obstaja mnogo različnih pristopov k napovedovanju povezav, pa zanesljivo napovedovanje še zmeraj predstavlja velik izziv. Računski pristop, ki ga predstavljamo v prispevku, omogoča raziskovalcem učinkovito napovedovanje potencialnih DDI.

Tabela 1 Osnovne lastnosti DDI omrežij.

Omrežje	$\|V\|$	$\|E\|$	ϵ	D	L	C	GC
DrugBank	2.551	577.712	452,93	6	2,27	0,52	1,00
KEGG	1.194	52.609	88,12	7	2,51	0,37	1,00
NDF-RT	701	8.044	22,95	8	3,30	0,16	0,99
SemMedDB	1.688	37287	44,18	6	2,58	0,44	1,00
Twosides	340	19.020	111,88	3	1,68	0,83	1,00

Oznake: $|V|$ – št. vozlišč; $|E|$ – št. povezav; ϵ – povprečna stopnja; D – premer; L – povprečna dolžina poti; C – koeficient zgoščanja; GC – velikost glavne komponente.

Tabela 2 Prekrivanje povezav med omrežji.

Omrežje	DrugBank	KEGG	NDF-RT	SemMedDB	Twosides
DrugBank	296.656	0,36	0,45	0,30	0,53
KEGG	11.961	33.474	0,14	0,04	0,04
NDF-RT	1.790	576	4.010	0,10	0,05
SemMedDB	8.603	1.077	390	28.924	0,08
Twosides	7.411	691	199	1396	17.219

Oznake: Vrednosti na glavni diagonali predstavljajo št. neusmerjenih povezav v vsakem od omrežij. Vrednosti v spodnjem trikotniku predstavljajo število prekrivanj med dvema omrežjema. Vrednosti v zgornjem trikotniku predstavljajo delež prekrivanja med paroma omrežij.

Tabela 3 Učinkovitost nenadzorovanega napovedovanja v testni množici.

Omrežje	Prec	Rec	F_1	AUROC	AUPR
DrugBank	0,63	0,68	0,65	0,93	0,70
KEGG	0,28	0,64	0,39	0,91	0,35
NDF-RT	0,08	0,56	0,14	0,84	0,11
SemMedDB	0,17	0,83	0,28	0.95	0,45
Twosides	0,96	0,30	0,45	0,89	0,82

Oznake: Prec – natančnost; Rec – priklic; F_1 – mera F_1; AUROC – ploščina pod ROC krivuljo; AUPR – ploščina pod krivuljo natančnost-priklic.

Tabela 4 Učinkovitost nadzorovanega napovedovanja v testni množici.

Omrežje	Klasifikator	Prec	Rec	F1	AUROC	AUPR
DrugBank	DT	0,83	0,55	0,66	0,84	0,63
	kNN	0,83	0,66	0,74	0,94	0,81
	SVM	0,83	0,58	0,69	0,93	0,78
	RF	0,83	0,55	0,66	0,98	0,92
	GBM	0,83	0,65	0,73	0,96	0,82
KEGG	DT	0,66	0,32	0,43	0,79	0,42
	kNN	0,68	0,35	0,46	0,88	0,51
	SVM	0,72	0,21	0,33	0,80	0,47
	RF	0,66	0,32	0,43	0,96	0,69
	GBM	0,67	0,37	0,48	0,95	0,55
NDF-RT	DT	0,60	0,12	0,20	0,70	0,20
	kNN	0,25	0,03	0,06	0,79	0,17
	SVM	0,56	0,07	0,13	0,87	0,21
	RF	0,60	0,12	0,20	0,91	0,36
	GBM	0,63	0,15	0,24	0,90	0,27
SemMedDB	DT	0,73	0,25	0,38	0,75	0,36
	kNN	0,68	0,30	0,42	0,86	0,45
	SVM	0,69	0,29	0,41	0,89	0,50
	RF	0,73	0,25	0,38	0,96	0,55
	GBM	0,68	0,31	0,43	0,96	0,53
Twosides	DT	0,83	0,82	0,82	0,90	0,80
	kNN	0,85	0,77	0,81	0,93	0,90
	SVM	0,86	0,80	0,83	0,95	0,92
	RF	0,83	0,82	0,82	0,96	0,93
	GBM	0,86	0,83	0,85	0,95	0,93

Oznake: Prec – natančnost; Rec – priklic; F_1 – mera F_1; AUROC – ploščina pod ROC krivuljo; AUPR – ploščina pod krivuljo natančnost-priklic.

Reference

1. Lu Y, Shen D, Pietsch M, *et al.*: A novel algorithm for analyzing drug-drug interaction from MEDLINE literature. *Sci Rep* 2015; 5: 17357. https://doi.org/10.1038/srep17357
2. Juurlink DN, Mamdani M, Kopp A, Laupacis A, Redelmeier DA: Drug-drug interactions among elderly patients hospitalized for drug toxicity. *JAMA* 2003, 289(13): 1652-1658. https://doi.org/10.1001/jama.289.13.1652
3. Percha B, Altman RB: Informatics confronts drug-drug interactions. *Trends Pharmacol Sci* 2013, 34(3): 178-184. https://doi.org/10.1016/j.tips.2013.01.006
4. Liu R, AbdulHameed MDM, Kumar K, Yu X, Wallqvist A, Reifman J: Data-driven prediction of adverse drug reactions induced by drug-drug interactions. *BMC Pharmacol Toxicol* 2017, 18: 44. https://doi.org/10.1186/s40360-017-0153-6
5. Ayvaz S, Hom J, Hassanzadeh O, *et al.*: Toward a complete dataset of drug-drug interaction information from publicly available sources. *J Biomed Inform* 2015, 55, 206-217. https://doi.org/10.1016/j.jbi.2015.04.006
6. Hopkins AL: Network pharmacology: the next paradigm in drug discovery. *Nat Chem Biol* 2008, 4(11): 682-690. https://doi.org/10.1038/nchembio.118
7. Lu Y, Figler B, Huang H, Tu YC, Wang J, Cheng F: Characterization of the mechanism of drug-drug interactions from PubMed using MeSH terms. *PLoS One* 2017; 12(4): e0173548. https://doi.org/10.1371/journal.pone.0173548
8. Zhang W, Chen Y, Liu F, Luo F, Tian G, Li X: Predicting potential drug-drug interactions by integrating chemical, biological, phenotypic and network data. *BMC Bioinformatics* 2017; 18: 18. https://doi.org/10.1186/s12859-016-1415-9
9. Kastrin A, Ferk P, Leskošek B: Predicting potential drug-drug interactions on topological and semantic similarity features using statistical learning. *PLoS One* 2018; 15(5): e0196865. https://doi.org/10.1371/journal.pone.0196865
10. Lobo JM, Jimenez-Valverde A, Real R: AUC: a misleading measure of the performance of predictive distribution models. *Global Ecol Biogeogr* 2008; 17(2): 145-151. https://doi.org/10.1111/j.1466-8238.2007.00358.x.

■ *Pregledni znanstveni članek*

Uroš Hudomalj, Franc Smole

Kvantna kriptografija

Povzetek. Zaradi množičnega nadzora in trgovanja z informacijami ima zasebnost vedno večji pomen. Za zagotavljanje zasebnosti pri izmenjavi informacij se uporablja šifriranje sporočil. V dobi informacijske tehnologije uporaba šifriranja vse bolj narašča. Ustrezni postopki šifriranja omogočajo elektronske storitve od spletnega bančništva do elektronskega glasovanja, med najbolj občutljiva področja, ki zahtevajo uporabo šifriranja, pa sodi tudi medicina. Članek podaja pregled klasičnih načinov šifriranja, s poudarkom na njihovih slabostih. Te pomanjkljivosti odpravljajo novi kriptografski postopki v sklopu post-kvantne in kvantne kriptografije, ki predstavlja teoretično nezlomljivo šifriranje. Predstavljena so načela delovanja kvantne kriptografije, in sicer na podlagi praktično najbolj razširjenega algoritma kvantne izmenjave ključa BB84. Opisane so pomanjkljivosti algoritma in predstavljeni možni vdori, nakazane pa so tudi izboljšave, ki preprečijo vsakršne zlorabe.

Quantum Cryptography

Abstract. In the era of mass surveillance and information trading, privacy is increasingly gaining importance. Encryption of messages is used to provide privacy while exchanging information. Data encryption is becoming widespread with the rise of information technology. Encryption enables various applications from online banking to electronic voting. Another sensitive area that requires the use of encryption is medicine. The paper presents an overview of the classic encryption methods, with an emphasis on their weaknesses. These are overcome using new cryptographic methods, namely post-quantum and quantum cryptography. The latter represents theoretically unbreakable encryption. The principles of quantum cryptography are presented based on the most widely used algorithm for quantum key distribution, the BB84. Its weaknesses are described, together with potential threats and improvements that prevent them.

■ **Infor Med Slov** 2018; 23(1-2): 18-25

Institucije avtorjev / Authors' institutions: Fakulteta za elektrotehniko, Univerza v Ljubljani (UH, FS).

Kontaktna oseba / Contact person: Uroš Hudomalj, Preglov trg 13, 1000 Ljubljana, Slovenija. E-pošta / E-mail: uh3370@student.uni-lj.si.

Prispelo / Received: 27. 6. 2018. Sprejeto / Accepted: 29. 6. 2018.

Uvod

Zaradi množičnega nadzora in trgovanja z informacijami ima zasebnost vedno večji pomen.[1] Za zagotavljanje zasebnosti pri izmenjavi informacij se uporablja šifriranje sporočil.[2] Namen tega je preprečiti nenaslovljeni osebi, da bi razbrala pomen sporočila, četudi ga prestreže, in preprečiti, da bi sporočilo ponaredila.

V dobi informacijske tehnologije uporaba šifriranja vse bolj narašča. Ustrezni postopki šifriranja omogočajo elektronske storitve od spletnega bančništva do elektronskega glasovanja.[1] Med občutljiva področja, ki zahtevajo uporabo šifriranja, sodi tudi medicina. Primer rabe šifriranja tam najdemo v informacijskih sistemih za medicinsko oskrbo na daljavo, ki omogočajo spremljanje pacientovega zdravstvenega stanja od doma. S tem zagotavljajo hitrejšo, sprotno in cenejšo obravnavo. Posebej pomemben je hiter razvoj medomrežja stvari (angl. *Internet of Things, IoT*) v medicinske namene,[3] kamor sodijo npr. priročni in nizkocenovni sistemi za beleženje srčnega utripa ali merjenje sladkorja v krvi. Vse te podatke je potrebno varno prenesti od pacienta do medicinskega centra. Pri tem moramo zagotoviti, da lahko do teh podatkov dostopajo le pooblaščene osebe, in onemogočiti njihovo ponarejanje. To zagotavlja ustrezna uporaba kriptografije.[4,5] V sklopu zagotavljanja učinkovitega e-zdravja uvajajo tudi elektronske kartoteke pacientov, ki omogočajo celovitejšo obravnavo posameznika. Tudi tu mora biti omogočen dostop do teh kartotek le določenim osebam.[6] V bolnišnicah pa se že uporabljajo sistemi za avtomatizirano dajanje zdravil in njihovih ustreznih doz pacientom, kar zmanjša človeške napake. Da pri tem ne pride do zlorab, je prav tako potrebno ustrezno šifriranje.[7] V nadaljevanju podajamo pregled klasičnih načinov šifriranja, s poudarkom na njihovih slabostih. Te pomanjkljivosti odpravljajo novi kriptografski postopki v sklopu post-kvantne in kvantne kriptografije, ki predstavlja teoretično nezlomljivo šifriranje. Zato so kasneje predstavljena načela delovanja kvantne kriptografije, njene pomanjkljivosti in izboljšave.

Kriptografija

Sporočilo lahko varno prenesemo na dva načina. Prvi je, da izvirno sporočilo prenesemo preko zaupanja vrednega medija. Tu tvegamo, da mediju prisluškujejo oziroma nanj vplivajo nepovabljeni gostje. Primer takega pošiljanja sporočila je uporaba zaupanja vrednega kurirja, ki mu fizično izročimo sporočilo, ki ga dostavi naslovniku. Naslovnik mora vedeti, da bo naše sporočilo prišlo le preko tega kurirja, da s tem zagotovimo avtentičnost sporočila. A že tu se vidi pomanjkljivost tega načina komuniciranja. Kurir je lahko nepošten ali pa ga na poti oropajo. Sodobnejša izvedba takšnega načina prenosa sporočil je izgradnja namenske komunikacijske linije, npr. iz optičnih vlaknen, neposredno od pošiljatelja do naslovnika. A tudi te niso povsem varne, saj je praktično nemogoče zagotoviti, da nihče ne prisluškuje prenosnemu mediju.[1]

Pogosteje se uporablja varnejši način prenosa sporočil, ki je uporaben tudi pri t. i. nezavarovanem kanalu, ki mu lahko prisluškujejo. Vsebino sporočila zakrijemo pred prisluškovalci z uporabo raznih šifrirnih postopkov. Z razvojem teh postopkov se ukvarja kriptografija. Šifrirni postopki lahko tudi zagotovijo dokaz o avtentičnosti sporočila. S tem prejemnik lahko preveri, ali je bilo sporočilo ponarejeno in ne izhaja od pravega pošiljatelja.

Seveda zagotavlja največjo varnost kombinacija obeh opisanih postopkov. Toda prvi se zaradi velikega finančnega vložka le redko uporablja v vsakdanji praksi.

Osnovno načelo šifriranja je, da originalno sporočilo pošiljatelj spremeni v obliko, ki jo zna razbrati le naslovnik. Da lahko naslovnik edini razbere sporočilo, mora imeti dodatno informacijo, ki je ostali nimajo. Ta se v kriptografiji imenuje *ključ*. Ključ se uporabi tudi pri formiranju šifriranega sporočila. Šifrirano sporočilo naj bi bilo možno razbrati (v omejenem času) le s pomočjo pravega ključa in z vnaprej dogovorjenim šifrirnim algoritmom. Ločimo dva načina šifriranja, in sicer *simetrično* in *asimetrično*. Vsak način ima svoje prednosti in slabosti.

Simetrična kriptografija

Simetrični šifrirni postopki uporabljajo isti ključ tako za šifriranje kot za dešifriranje sporočila. Šifriranje in dešifriranje s simetričnimi postopki je veliko hitrejše kot pri uporabi asimetričnih, a imajo veliko pomanjkljivost: pošiljatelj in naslovnik morata poznati ključ. Prenos tega mora biti povsem varen, sicer je vsa nadaljnja komunikacija ogrožena. Za zagotavljanje dolgotrajne varne komunikacije je potrebno ključe pri simetričnemu šifriranju dovolj pogosto menjati.[1,8] Problem prenosa ključa pa odpravljajo asimetrični postopki.

One-time pad

Oznaka *one-time pad* pomeni poseben simetrični šifrirni postopek, ki zagotavlja popolno varnost pošiljanja sporočil. Takšno varnost lahko zagotovimo le, če

uporabimo povsem naključen ključ, dolžine večje ali enake kot je poslano sporočilo. Ključ pa smemo uporabiti le enkrat. Če so ti pogoji izpolnjeni, je takšno sporočilo nemogoče razbrati brez poznavanja ključa.[9] Največja slabost tega postopka je ravno generacija povsem naključnega ključa in njegov prenos do naslovnika. To težavo odpravlja kvanta kriptografija.

Asimetrična kriptografija

Asimetrično kriptografijo imenujemo tudi kriptografija z javnim ključem. Pri tem načinu se za varno komunikacijo uporabljata dva različna ključa – en zasebni in en javni. Javni ključ da uporabnik na voljo vsem, zasebnega pa skrije. S pomočjo javnega ključa prejemnika lahko vsak šifrira svoje sporočilo, ki ga želi poslati prejemniku. S svojim zasebnim ključem pa lahko le prejemnik dešifrira sporočilo, ki mu ga je pošiljatelj poslal z uporabo prejemnikovega javnega ključa.

Asimetrična kriptografija omogoča tudi avtentikacijo sporočila. Pošiljatelj se poleg poslanega sporočila podpiše, za kar uporabi svoj zasebni ključ. Podpis lahko prejemnik enostavno dešifrira z javnim ključem pošiljatelja. Pri tem ugotovi, ali je sporočilo pristno (tj. poslano od pravega pošiljatelja).

Pri asimetričnih šifrirnih postopkih ni težav s pošiljanjem ključev. Toda tudi asimetrični postopki imajo svojo slabost, in sicer računsko zahtevnost. Ker so veliko počasnejši kot simetrični algoritmi, niso uporabni za dolga sporočila. Zato se v praksi uporablja kombinacija obeh šifrirnih postopkov. S pomočjo asimetričnega postopka šifriramo ključ za simetrično šifriranje, s katerim šifriramo sporočilo. S tem lahko hkrati varno in hitro pošljemo naslovniku tako ključ kot tudi sporočilo. Z asimetričnim šifriranjem dodamo sporočilu še podpis, s čimer zagotovimo avtentikacijo.[1,10]

Asimetrični šifrirni postopki se samostojno ali v kombinaciji s simetričnimi uporabljajo v ogromno različnih aplikacijah, ki segajo od šifriranja elektronske pošte do povezav VPN (angl. *virtual private network)*.[11] Zaradi narave komunikacije v e-zdravstvu se tudi tu množično uporablja asimetrično šifriranje.[4,5]

Asimetrični šifrirni postopki temeljijo na matematičnih problemih, za katere ne obstajajo hitri računalniški algoritmi. Eden takih problemov je iskanje praštevil, na čimer temelji tudi eden izmed najbolj razširjenih asimetričnih šifrirnih postopkov, imenovan RSA. Pri postopku RSA se (poenostavljeno rečeno) zasebni ključ sestavi iz dveh naključno izbranih praštevil, javni pa iz njunega produkta. Če bi javni ključ razbili nazaj na njegove prafaktorje, bi s tem razkrili zasebni ključ. A slednje je v praksi malo verjetno. Tudi najhitrejši algoritmi iskanja prafaktorjev imajo namreč eksponentno časovno odvisnost (e^x). To pomeni, da če vzamemo za javni ključ dovolj veliko število, praktično ni verjetno, da bi našli njegove prafaktorje. Za velikosti števil iz 1024 ali 2048 bitov bi za izračun prafaktorjev potrebovali več časa, kot je staro vesolje, četudi bi hkrati uporabili vse računalnike na svetu.[1,12]

Kvantni računalniki – nevarnost dosedanji kriptografiji

Kvantni računalniki predstavljajo grožnjo komunikaciji, ki uporablja široko razširjene asimetrične postopke, kot je RSA (poimenovan po avtorjih Rivestu, Shamirju in Adlemanu). Sicer so šele v začetnem razvoju, a napredujejo hitro in vztrajno. Gonilo tega napredka so tudi nova dognanja na področju kvantne mehanike, kjer sodelujejo tudi slovenski znanstveniki. Nedavno so ravno strokovnjaki z Instituta Jožef Stefan potrdili obstoj posebnih kvazidelcev – anyonov, za katere je pričakovati, da bodo zaradi svoje stabilnosti pomembni za razvoj kvantnega računalništva.[13,14]

Kvanti računalniki uporabljajo drugačne algoritme kot klasični in za nekatere probleme so kvantni algoritmi znatno hitrejši. Eden izmed takšnih je Shorov kvantni algoritem za iskanje prafaktorjev, ki ima polinomsko časovno zahtevnost (x^3) za razliko od eksponentne časovne zahtevnosti klasičnih algoritmov.[15-17]

Sicer kvantni računalniki še niso dovolj obsežni, da bi lahko tudi kljub znatno hitrejšim algoritmom strli RSA in podobne asimetrične šifrirne algoritme, a v prihodnjih 10 do 15 letih se bo to zelo verjetno zgodilo.[11,17] Tedaj bo ogrožena tudi vsa varnost in zasebnost pri obstoječih komunikacijah v medicinske namene. Zato že danes iščejo nove šifrirne postopke, ki bi bili odporni na napade s kvantnimi računalniki. Ponujata se dve rešitvi. Prva rešitev je uporaba t. i. post-kvantne kriptografije, drugo rešitev pa omogoča ravno kvantna mehanika, ki je pripeljala do kvantnih računalnikov in ogrozila varnost dosedanje kriptografije.

Trenutno stanje še ni kritično. Google je nedavno objavil, da so razvili računalnik s 72 qubiti.[18] A predvideva se, da bi bilo za zlom šifriranja RSA z dolžino ključa 2048 bitov v doglednem času potreben kvantni računalnik s 4000 qubiti in 100 milijoni vrat[17] oziroma po drugih predvidevanjih 10000 qubitni računalnik,[19] za kar pa bo potrebnih še kar nekaj let.

Post-kvantna kriptografija

Post-kvantna kriptografija se osredotoča na razvoj kriptografskih metod v času, ko bodo imeli kvantni računalniki dovolj računske moči, da zlomijo obstoječe asimetrične načine šifriranja podatkov. Predvideva, da kvantni računalniki ne bodo sposobni razbiti vseh obstoječih metod šifriranja. Simetrične šifrirne algoritme naj bi bilo enostavno narediti odporne proti napadom s kvantnimi računalniki z enostavnim povečanjem (podvojitvijo) dolžine ključa.[17] A kot smo že omenili, imajo ti slabost zaradi potrebne razdelitve ključev preko varnega kanala. Tudi nekateri načini šifriranja z uporabo javnih ključev naj bi bili sicer odporni na napade s kvantnimi računalniki. Primer takšnih postopkov je šifriranje, ki temelji na enosmernih zgoščevalnih funkcijah, a te imajo omejitev v številu uporabe enega kompleta ključev za šifriranje.[20] Obstajajo še drugi načini šifriranja, odporni na kvantne napade,[11] vendar imajo za enkrat še vsak svojo pomanjkljivost (zelo dolgi ključi, časovno zahtevni šifrirni postopki, ne omogočanje avtentikacije itd.[21]), zato še niso splošno razširjeni. Ključna prednost post-kvantne kriptografije pred ostalimi tehnikami, odpornimi na napade s kvantnimi računalniki, kot je uporaba kvantne kriptografije, je njena preprostost in poceni implementacija na obstoječih sistemih.[21]

Glede razvoja kvantnih računalnikov je sicer še veliko vprašanj, predvsem glede kvantnih algoritmov. Dejstvo je, da je to področje zelo novo v primerjavi z razvojem klasičnih algoritmov. Tako obstaja možnost, da bodo razvili tudi kvantne algoritme, ki bi lahko razbili predlagane post-kvantne algoritme šifriranja. Na srečo se ponujajo še drugi načini šifriranja, odporni na napade s kvantnimi računalniki, z uporabo kvantne kriptografije.

Kvantna kriptografija

Kvantna kriptografija predstavlja drugi način šifriranja podatkov, ki bi bil odporen tudi na napade s kvantnimi računalniki. Še več, kvantna kriptografija vsaj teoretično omogoča nezlomljivo šifriranje.

Kot smo že omenili, je za vsako varno komunikacijo potrebno podatke šifrirati s ključem. Ta ključ mora biti znan le naslovniku in pošiljatelju. Najbolje je, da je ključ povsem naključno generiran, ker ga je tako najtežje uganiti, a popolno naključnost je težko zagotoviti. Primeri povsem naključnih pojavov so kvantne narave. Te uporablja kvantna kriptografija in z njimi odpravlja težave na področju generiranja naključnega ključa.[1]

Ko je ključ generiran, se ga lahko uporabi za komunikacijo preko nezavarovanega kanala z znanimi šifrirnimi postopki. Če se pri teh uporabi šifriranje po načelu one-time pad, lahko zagotovimo povsem nezlomljivo komunikacijo.[17,22-24]

Obstaja več protokolov za t. i. kvantno izmenjavo ključa (angl. *quantum key distribution, QKD*). Najbolj razširjena je uporaba protokola BB84 oziroma njegovih izvedenk. Te protokole so že uporabili za šifriranje podatkov pri telemedicinski oskrbi na daljavo.[25] Protokol BB84 deluje na podlagi oddajanja in sprejemanja posamičnega fotona. Ta protokol, njegovo fizično izvedbo in trenutne pomanjkljivosti predstavljamo v nadaljevanju. Na voljo so še drugi protokoli, ki delujejo npr. na podlagi kvantne prepletenosti, a so zaradi težavne praktične izvedbe le eksperimentalno uporabni.[22,26-28]

Delovanje

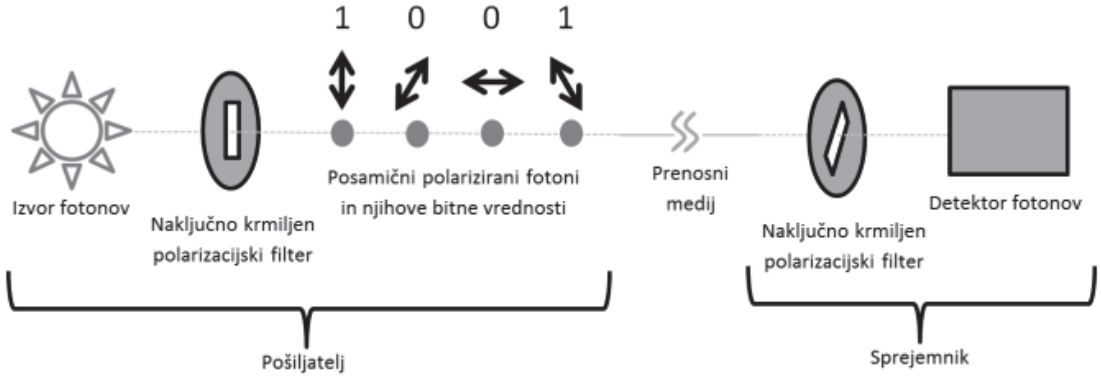
Kvantna kriptografija deluje po načelu oddajanja in sprejemanja posamičnih fotonov z različnimi polarizacijami (slika 1).

Uporabimo dve polarizacijski bazi, in sicer premočrtno in diagonalno. Pri premočrtni bazi so fotoni lahko polarizirani v vodoravni smeri (kot polarizacije 0°) ali v navpični smeri (kot polarizacije 90°), pri diagonalni bazi pa je kot polarizacije 45° ali 135°. Pri tem po ena polarizacija fotona v vsaki bazi predstavlja bit z vrednostjo 0 (na primer horizontalna polarizacija s kotom 0° v premočrtni bazi in polarizacija s kotom 45° v diagonalni), druga polarizacija pa bit z vrednostjo 1 (navpična polarizacija in polarizacija s kotom 135°).

Bazi sta tako izbrani s posebnim namenom. Če namreč pri detekciji polarizacije fotona uporabimo napačno bazo, je verjetnost 50 %, da zaznamo foton, kot da bi bil polariziran s polarizacijo, ki predstavlja bit z vrednostjo 0, verjetnost 50 % pa tudi, da ga zaznamo kot foton, ki nosi bit z vrednostjo 1. Zato z uporabo napačne baze pri detekciji ne moremo pravilno razbrati bitne vrednosti fotona.

Postopek generacije ključa poteka tako, da pošiljatelj zaporedoma oddaja posamične fotone. Pri vsakem fotonu se naključno odloči za polarizacijsko bazo in prav tako za njegovo vrednost. S tem naključno izbere polarizacijo fotona in njegovo bitno vrednost. Prejemnik sprejema oddane fotone. Pri tem želi razbrati vrednost bita. Ker ne ve, s katero polarizacijsko bazo je bil foton oddan, se naključno odloči za eno od možnih. Tako razbere bitno vrednost nekaterih fotonov pravilno, drugih napačno. Ko pošiljatelj neha oddajati, mu sprejemnik pošlje

njegovo zaporedje uporabljenih baz. Ta preveri, pri katerih fotonih sta uporabila enako bazo (za oddajo in sprejem), kar sporoči prejemniku. Nato ohranita le tiste bite, pri katerih sta uporabila enako bazo, saj imata pri teh oba pravilno razbrano vrednost. Ti sprejeti biti predstavljajo ključ. Ta je naključen, ker se je pošiljatelj naključno odločal za posamično vrednost bita. Za nadaljnjo komunikacijo preko nezavarovanega kanala uporabita dobljeni ključ, kjer lahko uporabita klasične simetrične postopke šifriranja.



Slika 1 Poenostavljen shematski prikaz kvantne izmenjave ključa.

Velika prednost takega načina pridobitve ključa je, da tretja oseba, ki morda prisluškuje kanalu, ne more ugotoviti ključa, ne da jo pri tem odkrili. To izhaja iz Heisenbergovega načela nedoločenosti. Posledica načela nedoločenosti je, da je nemogoče narediti kopijo neznanega kvanta, ne da bi z njegovo meritvijo spremenili njegove lastnosti.[23,29]

Tudi če v predstavljenem primeru prisluškovalec prisluškuje komunikaciji in prestreže vsak foton, ne ve, v kateri bazi je bil foton oddan. Tako se mora tudi on naključno odločiti. Če slučajno izbere pravo bazo, bo pravilno razbral tudi poslani bit. Ko pa se odloči za napačno, lahko pravilno razbere bit ali ne. Toda pri tem bo spremenil polarizacijo fotona v napačno bazo. Če pri sprejemu tega fotona sprejemnik uporabi enako polarizacijsko bazo za sprejem fotona, kot jo je pošiljatelj pri oddajanju, je 50 % verjetnosti, da bo kljub pravi bazi zaznal napačno vrednost bita. Zato po koncu postopka določanja ključa pošiljatelj in sprejemnik naključno primerjata nekaj bitov, pri katerih sta uporabila enako bazo. Zaradi enake baze bi morala dobiti enako vrednost. Če vrednosti primerjanih bitov niso povsem enake, vesta, da je nekdo prisluškoval kanalu in pri tem spremenil vrednost bita. Zato šifra ni varna. Če pa se vsi primerjani biti ujemajo, je velika verjetnost, da je bil ključ varno generiran. Iz končnega ključa se izvzamejo primerjani biti. Da se lahko določi prisotnost prisluškovalca na kanalu z verjetnostjo 0,999999999, je potrebno primerjati 72 bitov.

Zaradi povsem naključne izbire polarizacijske baze na pošiljateljevi in sprejemni strani ter naključne izbire poslanih bitov lahko poteka končno preverjanje bitov in vmesno deljenje informacij o izbiri baz po nezavarovanem kanalu. Tudi če prisluškovalec te informacije prestreže, mu nič ne koristijo. Primerjane vrednosti dobljenih bitov se namreč, kot rečeno, na koncu izvzamejo. Podatki o izbiri baz pa so prisluškovalcu prav tako nekoristni, če je sam uporabil napačne baze pri prestrezanju posamičnega fotona, saj potem ne ve, ali je pri njih razbral pravo vrednost.[30]

Izvedba kvantne kriptografije

Za kvantno izmenjavo ključa potrebujemo ustrezno opremo. Sestavljajo jo štirje deli: generator naključnih števil oziroma bitov, izvor fotonov, prenosni kanal in detektor fotonov, ki so v nadaljevanju podrobneje predstavljeni.

Generator naključnih števil oziroma bitov

Izhod generatorja naključnih števil za kvantno izmenjavo ključa mora biti povsem naključen, sicer je ogrožena varna generacija ključa v primeru prisluškovanju prenosnemu kanalu. Prisluškovalec bi lahko tako ugotovil, kakšne vrednosti bitov oddaja pošiljatelj ali kakšne polarizacijske baze uporabljata pošiljatelj in sprejemnik. Tako bi ključ lahko ugotovil zelo hitro.

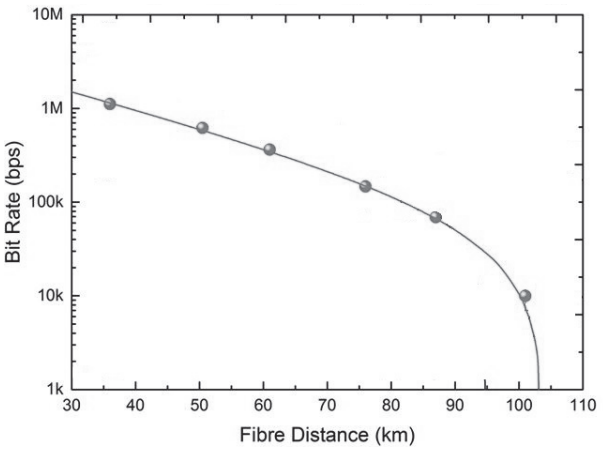
Programski generatorji psevdonaključnih števil ne delujejo povsem naključno in se zato kljub nizki ceni ne uporabljajo. Potrebno je uporabiti mnogo dražje strojne generatorje naključnih števil. Ti temeljijo na nedeterminističnih fizikalnih pojavih, kot so termični in Zenerjev šum, radioaktivni razpad in prehod fotona skozi polprepustno zrcalo.[24,31]

Izvor fotonov

Za idealno kvantno izmenjavo ključa, ki je povsem varna, bi potrebovali izvor posamičnih fotonov. V praski se pogosto uporabljajo atenuirani laserji, ki sicer ne omogočajo izvora posamičnega fotona. Nevarnost te neidealnosti lahko do neke mere odpravimo z dopolnjenimi protokoli. Kljub temu te nadgradnje niso povsem varne, zato se veliko raziskuje na področju eno-fotonskih izvorov. Cilj je, da delujejo pri valovnih dolžinah v infrardečem spektru, ki se najmanj absorbirajo v optičnih vlaknih, ki so najbolj pogost medij prenosa pri kvantni izmenjavi ključa.[22,24,32,33]

Prenosni kanal

Najbolj pogosto je izveden kot optično vlakno. Po njih se dosegajo največje hitrosti izmenjave kvantnega ključa. Nedavno so dosegli 13,7 Mbit/s na razdalji 10 km,[33] na daljših razdaljah pa 1 Mbit/s na 50 km[34] oziroma 12,7 kbit/s na 307 km (slika 2).[22] Vedno bolj se razvijajo tudi načini izmenjave kvantnega ključa preko satelitov.[24,27]



Slika 2 Primer izmerjene odvisnosti hitrosti prenosa kvantnega ključa od dolžine optičnega vlakna.[36]

Detektor fotonov

Za detekcijo fotonov se pogosto uporabljajo diode s plazovno ionizacijo, kot so InGaAs diode. Te delujejo pri valovnih dolžinah v infrardečem spektru, kakršni so pogosto tudi viri fotonov pri kvantni izmenjavi ključa.[35,37] Veliko pa se raziskuje tudi na eno-fotonskih detektorjih, narejenih npr. iz superprevodnih nanocevk.[32]

Trenutne pomanjkljivosti kvantne kriptografije

Čeprav naj bi kvantna kriptografija zagotavljala popolnoma varno komunikacijo, je trenutno še ne. Elementi, uporabljeni za izgradnjo sistema za kvantno izmenjavo ključa, niso idealni. Neidealnosti v izvirih in detektorjih fotonov lahko izrabijo napadalci.[22-24,28] Da se izognemo takšnim napadom, je potrebno nadgraditi protokole kvantne izmenjave ključa. Kot smo že omenili, potekajo raziskave eno-fotonskih izvorov in detektorjev, ki bi odpravili te pomanjkljivosti.[32]

Nezmožnost oddaje posamičnega fotona

Praktično uporabljeni fotonski izvori ne proizvedejo le enega fotona, ampak lahko več, ki vsebujejo enako informacijo. To neidealnost lahko izkoriščajo prisluškovalci tako, da detektirajo le en poslani foton. Ker je bilo teh več, lahko sprejemnik še vedno pravilno zazna foton in informacijo. Zato je potrebno predstavljen protokol BB84 nadgraditi. Najbolj razširjena je nadgradnja z vabami (angl. *decoy-state QKD*). Pri tem pošiljatelj naključno pošlje vabo – namensko drugačno število fotonov, ki ne vsebujejo sporočila. Prisluškovalec ne ve, kdaj je poslana vaba in kdaj ne. Če prestreže vabo, potem do sprejemnika prispe napačno število fotonov. Na koncu komunikacije pošiljatelj sporoči sprejemniku, kdaj je poslal vabo. Če je takrat ta zaznal nepravilna števila zaznanih fotonov, sta odkrila prisotnost prisluškovalca.[28,30,37-39]

Trojanski konj

Napad s trojanskim konjem v kvantni kriptografiji poteka tako, da napadalec z močnim svetlobnim snopom obsveti sprejemnik. Iz odbite svetlobe lahko napadalec pravilno sklepa o uporabljeni polarizacijski bazi sprejemnika, s čimer enostavno zlomi šifriranje. Kot ustrezna zaščita proti takšnim napadom se uporabljajo optični izolatorji in filtri.[22]

Napad na kalibracijski postopek

Napadalci lahko izrabijo tudi neidealnosti v detektorjih fotonov. V procesu kalibracije pred začetkom dejanske komunikacije lahko prestrežejo kalibracijski proces in vsilijo svojega. Z njim lahko vsilijo oziroma spremenijo polarizacijsko bazo detektorja. S tem lahko napadalec kasneje med izmenjavo ključa prestreže več fotonov, ne da bi ga odkrili. To pomanjkljivost naj bi v prihodnosti odpravili s samo-preizkuševalnimi metodami za detektorje fotonov v sistemu, kar pa naj bi dodatno dvignilo njihovo ceno.[23,28]

Drugi možni vdori in zlorabe

Kot pri drugih varnostnih sistemih, je tudi tu potrebno preprečiti fizični dostop napadalcev do komunikacijskega sistema. Zagotoviti je potrebno

tudi povsem naključne generatorje števil. Če ta pogoja nista izpolnjena, je verjetnost uspešnega vloma v sistem bistveno večja.

Trenutna pomanjkljivost kvantne kriptografije je tudi avtentikacija pošiljatelja in sprejemnika. Z njo ugotovimo oziroma potrdimo identiteto sogovorca. Doslej še niso razvili kvantnih metod avtentikacije, zato se uporabljajo klasične. Če se napadalcu uspe izdajati za zaupanja vrednega sogovornika, je varna komunikacija zlomljena.

Poleg tega je pri kvantni kriptografiji potrebno imeti vzpostavljen neprekinjen kanal med pošiljateljem in sprejemnikom. Napadalec lahko enostavno prekine ta kanal in tako izvede napad zavrnitve storitve (angl. *Denial of Service*, *DoS*). Komunikacijski kanali so trenutno še tudi zelo omejeni glede dolžine, na kateri je mogoče zagotoviti prenos uporabne hitrosti. Da bi jo povečali, raziskujejo v smeri satelitske kvantne izmenjave ključa in razvoja omrežij za kvantno izmenjavo ključa. Slednja bi tudi povečala zahtevnost izvedbe napada DoS, saj bi lahko komunikacija potekala preko različnih kanalov. Toda za zdaj še niso uspeli izdelati kvantnega usmerjevalnika, ki bi bil v takih omrežjih potreben. Moral bi namreč za nekaj časa shraniti foton, ga pri tem ne spremeniti, in poslati naprej, česar pa za zdaj še ne znamo.[17,22,24,27]

Zaključek

Trenutno še ni razloga za preplah zaradi mogočega padca klasične kriptografije in kaosa, ki bi temu sledil – zloma finančnih sistemov, kraje osebnih identitet in zdravstvenih kartotek, manipulacije z osebnimi podatki itd. Kvantni računalniki, ki predstavljajo največjo grožnjo tradicionalni kriptografiji, še niso dovolj razviti. To naj bi se po nekaterih ocenah spremenilo v roku 10 do 15 let. V sklopu post-kvantne kriptografije in kvantne kriptografije se že pojavljajo načini šifriranja, ki so odporni tudi na napade s kvantnimi računalniki.

Obe tehnologiji sta novi in še ne povsem uporabni v praksi. Post-kvantna kriptografija predstavlja cenejšo rešitev, saj naj bi le nadgradili kriptografske postopke, ki so sedaj v uporabi. Zanjo ni potrebna nobena nova strojna oprema. A tudi ta se bo mogoče izkazala za zlomljivo, saj je razvoj kvantnih računalnikov in kvantnih algoritmov šele v povojih. Tako se bo morda kljub višji ceni in potrebni novi strojni opremi izkazala kvantna kriptografija za boljšo rešitev, saj je teoretično nezlomljiva. Za zdaj pa ima še kar nekaj pomanjkljivosti, predvsem zaradi praktičnih omejitev izvorov in detektorjev fotonov.

Reference

1. Singh S: *Knjiga šifer: umetnost šifriranja od starega Egipta do kvantne kriptografije*. Tržič 2008: Učila International.
2. Anon: *History of crypthography*. https://en.wikipedia.org/wiki/History_of_cryptography (4. 5. 2018)
3. Thibaud M, Chi H, Zhou W, Piramuthu S: Internet of Things (IoT) in high-risk environment, health and safety (EHS) industries: a comprehensive review. *Deci Support Syst* 2018; 108: 79-95. https://doi.org/10.1016/j.dss.2018.02.005
4. Tan Z: A user anonymity preserving three-factor authentication scheme for telecare medicine information systems. *J Med Syst* 2014; 38(3): 16-25. https://doi.org/10.1007/s10916-014-0016-2
5. Chaudhry SA, Mahmood K, Naqvi H, Khan MK: An improved and secure biometric authentication scheme for telecare medicine information systems based on elliptic curve cryptography. *J Med Syst* 2015; 39(11): 175-187.
6. Odelu V, Das AK, Goswami A: An Effective and Secure Key-Management Scheme for Hierarchical Access Control in E-Medicine System. *J Med Syst* 2013; 37(2): 9920-9938. https://doi.org/10.1007/s10916-012-9920-5
7. Jin C, Xu C, Zhang X, Li F: A secure ECC-based RFID mutual authentication protocol to enhance patient medication safety. *J Med Syst* 2016; 40 (1): 12-18. https://doi.org/10.1007/s10916-015-0362-8
8. Anon: *Symmetric-key algorithm*. https://en.wikipedia.org/wiki/Symmetric-key_algorithm (6. 5. 2018)
9. Anon: *One-time pad*. https://en.wikipedia.org/wiki/One-time_pad (6. 5. 2018)
10. Anon: *Public-key cryptography*. https://en.wikipedia.org/wiki/Public-key_cryptography (6. 5. 2018)
11. Mulholland J, Mosca M, Braun J: The Day the Cryptography Dies. *IEEE Security & Privacy* 2017; 15(4): 14-21.
12. Anon: *RSA (cryptosystem)*. https://en.wikipedia.org/wiki/RSA_(cryptosystem) (7. 5. 2018)
13. Janša N, Zorko A, Gomilšek M, *et al*: Observation of two types of fractional excitation in the Kitaev honeycomb magnet. *Nat Phys* 2018; 14: 786-790. https://doi.org/10.1038/s41567-018-0129-5 (3. 10. 2018)
14. Masten A: *Raziskovalci IJS-ja potrdili obstoj delcev, o katerih je razmišljal že Nobelov nagrajenec*. https://www.rtvslo.si/znanost-in-tehnologija/raziskovalci-ijs-ja-potrdili-obstoj-delcev-o-katerih-je-razmisljal-ze-nobelov-nagrajenec/454399/ (9. 5. 2018)
15. Smole F: *Nanoelektronika*. Ljubljana 2014: Založna FE in FRI.
16. Anon: *Shor's algorithm*. https://en.wikipedia.org/wiki/Shor%27s_algorithm (7. 5. 2018)

17. Moses T: *Quantum Computing and Cryptography: Their impact on cryptographic practice*. Addison 2009: Entrust Inc.
18. Oberhaus D: *Google Engineers Think This 72-Qubit Processor Can Achieve Quantum Supremacy*. https://motherboard.vice.com/en_us/article/pam958/bristlecone-google-quantum-computer-72-qubits/ (7. 5. 2018)
19. Ziegler L: *Online security, cryptography, and quantum computing*. Forum Lectures, paper 119. https://digitalcommons.csbsju.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1118&context=forum_lectures/ (7. 5. 2018)
20. Anon: *Post-quantum cryptography*. https://en.wikipedia.org/wiki/Post-quantum_cryptography (7. 5. 2018)
21. Sendrier N: Code-Based Cryptography: State of the Art and Perspectives. *IEEE Security & Privacy* 2017; 15(4): 44-50.
22. Anon: *Quantum key distribution*. https://en.wikipedia.org/wiki/Quantum_key_distribution (10. 5. 2018)
23. Xu F, Curty M, Qi B, Lo HK: Measurement-device-independent quantum cryptography. *IEEE J Sel TopQuantum Electron* 2015; 21(3). https://doi.org/10.1109/JSTQE.2014.2381460
24. Lo HK, Curty M, Tamaki K: Secure quantum key distribution. *Nat Photonics* 2014; 8: 595-604. https://doi.org/10.1038/nphoton.2014.149
25. Lai H, Luo M, Qu Z, Xiao F, Orgun MA*:* A hybrid quantum key distribution protocol for tele-care medicine information systems. *Wirel Pers Commun* 2018; 98(1): 929-943. https://doi.org/10.1007/s11277-017-4902-z
26. Stein B: *Cost Effective QKD System Developed By NIST*. https://www.nist.gov/information-technology-laboratory/cost-effective-qkd-system-developed-nist/ (10. 5. 2018)
27. Bedington R, Arrazola JM, Ling A: Progress in satellite quantum key distribution. *NPJ Quantum Infmn* 2017; 3(30). https://doi.org/10.1038/s41534-017-0031-5
28. Fei YY, Meng XD, Gao M, *et al*: Quantum man-in-the-middle attack on the calibration process of quantum key distribution. *Scientific Reports* 2018; 8(4283). https://doi.org/10.1038/s41598-018-22700-3
29. Anon: *No-cloning theorem*. https://en.wikipedia.org/wiki/No-cloning_theorem (8. 5. 2018)
30. Anon: Quantum cryptography. https://en.wikipedia.org/wiki/Quantum_cryptography (8. 5. 2018)
31. Stipčević M: *Quantum random number generators and their use in cryptography*. https://arxiv.org/ftp/arxiv/papers/1103/1103.4381.pdf (9. 5. 2018)
32. Takemoto K, Nambu Y, Miyazawa T, *et al*: Quantum key distribution over 120 km using ultrahigh purity single-photon source and superconducting single-photon detectors. *Sci Rep* 2015; 5(14383). https://doi.org/10.1038/srep14383
33. Slachter A: *Single Photon Emitters*. https://www.rug.nl/research/zernike/education/topmasternanoscience/ns190slachter.pdf (9. 5. 2018)
34. Anon: *Toshiba Pushes Quantum Key Distribution Speed Beyond 10Mbps*. https://www.toshiba.co.jp/about/press/2017_09/pr1501.htm (9. 5. 2018)
35. Anon: *Toshiba QKD system*. https://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information/Quantum-Key-Distribution/Toshiba-QKD-system/ (9. 5. 2018)
36. Dynes JF: Ultra-high bandwidth quantum secured data transmission. *Sci Rep* 2016; 6(35149). https://doi.org/10.1038/srep35149
37. Pljonkin A, Rumyantsev K, Singh PK: Synchronization in Quantum Key Distribution Systems. *Cryptography* 2017; 1(3): 18.
38. Maroy O, Makarov V, Skaar J: Secure detection in quantum key distribution by real-time calibration of receiver. *Quantum Sci Technol* 2017; 2(4).
39. Huang A, Sun SH, Liu Z, Makarov V: *Decoy state quantum key distribution with imperfect source*. https://arxiv.org/abs/1711.00597/ (11. 5. 2018)

■ *Pregledni znanstveni članek*

Samanta Mikuletič, Brigita Skela Savič

Informacijska varnostna kultura v zdravstvu – sistematični pregled literature

Povzetek. Kršitve na področju varovanja podatkov največkrat izhajajo iz kraje ali izgube podatkov, nepooblaščenih dostopov, razkritja in vdiranja. Zaradi strahu pred razkritjem lahko pacient ne poda natančne anamneze, saj bi razkritje podatkov lahko povzročilo socialno stigmo in diskriminacijo. Močna informacijska varnostna kultura pripomore k učinkovitejšemu soočanju z varnostmi tveganji. Gre za niz značilnosti varovanja informacij in eno od vrednot organizacije, ki jo razvijejo zaposleni. Preko informacijske varnostne kulture se razvijejo norme, stališča in vedenja. Izvedli smo sistematičen pregled literature na to temo. Uporabili smo naslednje ključne besede: informacijska varnostna kultura, informacijska varnost, varovanje podatkov, zdravstveni podatki/pacientovi podatki in zdravstvo/zdravstveni delavci. V podatkovnih zbirkah DiKul, COBIB.SI, CINAHL, MEDLINE in ProQuestDissertations & Theses Global smo iskali slovenske in angleške znanstvene raziskave, objavljene od leta 2008 do leta 2018. Iskalni nabor je dal 1457 zadetkov. V končno analizo je bilo vključenih 6 raziskav. Identificirali smo 40 kod in 4 glavne kategorije: varnostna praksa, znanje/usposabljanje/izkušnje, zavedanje/odnos/stališče in dejavniki tveganja/zaupanje. Pregled je pokazal, da obstaja vrzel v odnosu in stališčih in da imajo različne poklicne skupine zdravstvenih delavcev različen pristop do varovanja informacij. Organizacije razmeroma malo ali skoraj nič ne vlagajo v izobraževanje zaposlenih in tako posledično ne razvijajo potrebne informacijske varnostne kulture.

Information Security Culture in Health Care – a Systematic Review

Abstract. Data protection violations mostly result from theft or loss of data, unauthorized data access, disclosure and security breaches. Due to the fear of disclosure, the patient may not give a detailed anamnesis, as the disclosure of the data could lead to social stigma and discrimination. A strong information security culture contributes to more effective management of security risks. It is reflected in information security characteristics and represents one of the organisational values developed by the employees. In order to achieve good information security, norms, positions and knowledge should be developed. A literature review and thematic synthesis were performed on this topic. We used the following keywords: information security culture, information security, data protection/data security, health data/patient data, and healthcare/healthcare professionals. The COBIB.SI, CINAHL, MEDLINE, ProQuest Dissertations & Theses Global, and DiKul databases were searched for scientific publications in Slovene and English from 2008 to 2018. Among the 1457 hits, six studies were included in the final analysis. We identified 40 codes and 4 main categories: security practice; knowledge, training, experience; awareness, behaviour and risk factors, trust. The review showed that there are differences in attitudes of different professional groups and that different health professional have a different approach to protecting information. Health organizations do not invest enough into education of their employees, and do not develop a good information security culture.

■ **Infor Med Slov** 2018; 23(1-2): 26-33

Institucija avtoric / Authors' institution: Fakulteta za zdravstvo Angele Boškin, Jesenice.

Kontaktna oseba / Contact person: Samanta Mikuletič, mag. zdr. nege, Fakulteta za zdravstvo Angele Boškin, Spodnji Plavž 3, 4270 Jesenice. E-pošta / E-mail: samanta.mikuletic@gmail.com.

Prispelo / Received: 4. 10. 2018. Sprejeto / Accepted: 21. 12. 2018.

Uvod

Informacijska varnostna kultura je »duša« organizacije in jo razumemo kot predpostavko o tem, kaj v zvezi z informacijsko varnostjo je spremenljivo in kaj ni. Pojem informacijske varnosti je povezan z preprečevanjem nepooblaščenega ali neželenega uničenja, spreminjanja, naključne ali namerne uporabe informacijskih virov. Informacijska varnostna kultura zajema socialne, kulturne in etične ukrepe za izboljšanje varnostnega ravnanja zaposlenih in velja za subkulturo organizacijske kulture. Vzpostavitev kulture varnosti informacij je nujna za učinkovito informacijsko varnost.[1]

Razvoj informacijske varnosti

Razvoj informacijske varnosti je potekal v več valovih – doslej v štirih in trenutno se nahajamo v petem. Prvi ali *tehnični val* se je začel v osemdesetih letih 20. stoletja in je zajemal predvsem tehnična vprašanja informacijske varnosti. Z razvojem interneta je nastopil drugi ali *menedžerski val*. Organizacije so se začele zavedati pretečih se nevarnosti in dale večji pomen varnosti. Začele so oblikovati varnostne politike in postopke. Tretji, *institucionalni val* se je začel v devetdesetih letih 20. stoletja. Nakazal je potrebe po določenih oblikah standardizacije, merjenja in nadzora informacijske varnosti. Takrat se je začel razvoj informacijske varnostne kulture. Četrti ali *upravljavski val* se je začel leta 2000 s poudarkom na področju upravljanja informacijske varnosti. V petem valu ali *kibernetskem valu* se nahajamo danes. Osredotoča se na zaščito računalnikov in računalniške opreme pred nepooblaščenim dostopom.[2,3,4]

Tehnični in ne-tehnični vidik zagotavljanja varovanja informacij

Pri zagotavljanju varnosti informacijskih virov so tehnološke metode (požarni zidovi in gesla) varovanja informacij učinkovite do določene mere. Ne-tehnična vprašanja so enako pomembna kakor tehnična. Tehnični varnostni nadzor je potrebno natančno določiti, oblikovati, razviti, implementirati, konfigurirati in vzdrževati, za kar je v prvi vrsti pomemben človek.[5]

Merjenje informacijske varnostne kulture

Orehek[6] je z meta-analizo ugotavljala obstoj in kakovost merskih instrumentov za merjenje informacijske varnostne kulture. Kakovostnih vprašalnikov, veljavnih in zanesljivih, ki naj bi merili ta koncept, ni, obstaja pa več merskih instrumentov, ki merijo sorodne koncepte. Pri tem navaja, da se z anketnim merjenjem informacijske varnostne kulture ukvarja le peščica raziskovalcev iz Južne Afrike, Avstralije in Azije, ter da je v evropskem prostoru čutiti primanjkljaj.[6]

Faktorji, ki vplivajo na informacijsko varnostno kulturo za področje zdravstva

Kršitve varnosti zdravstvenih informacij imajo pomemben vpliv na paciente in na zdravstvene organizacije. Noor in Zuraini[7] sta razvila konceptualni model faktorjev, ki vplivajo na informacijsko varnostno kulturo za področje zdravstva. Izpostavila sta jih šest: vedenje zaposlenih, upravljanje sprememb, informacijsko varnostno zavedanje, varnostna priporočila, organizacijski sistem in znanje.[7]

Zlorabe zdravstvenih podatkov

V ZDA je o zlorabah podatkov poročalo 43 % zdravstvenih organizacij. Preučevanje incidentov kaže na pomembnost človeškega dejavnika pri zagotavljanju varovanja informacij. Zdravstveni sektor je izpostavljen kot najranljivejši glede stroškov razkritih zapisov.[8] Od leta 2009 do 2013 je število zabeleženih kršitev v ZDA doseglo 27 milijonov. Oddelek za zdravstvo in državljanske storitve (US Department of Health and Human Services) na spletnem portalu redno objavlja kršitve, povezane z varovanje zdravstvenih informacij. Viri razkritja so računalniški sistemi in omrežja, osebni računalniki, prenosni računalniki, podatki na papirju, elektronska pošta, elektronski zdravstveni zapisi in prenosne naprave (CD-ji, USB-ji, rentgenske slike).[9] V Sloveniji tovrstne analize izvaja skupina SI-CERT, ki deluje v okviru akademske raziskovalne mreže Arnes. Poročilo o omrežni varnosti kaže, da se vsak dan v letu v Sloveniji v povprečju prijavi 11 incidentov. Arnes veliko prizadevanj vlaga v ozaveščanje javnosti preko projektov, kot sta »Varni na internetu« in »Safe.si«.[10]

Posebnost zdravstvenega sektorja je zasebnost obravnav ter načelo odnosa med pacientom in zdravstvenim osebjem. Zaradi strahu pred razkritjem podatkov lahko pacient ne poda natančne anamneze (duševne bolezni, HIV ipd.), saj bi razkritje teh podatkov lahko povzročilo socialno stigmo in diskriminacijo.[11]

Namen in cilj

Namen raziskave je bil s sistematičnim pregledom literature preučiti koncept informacijske varnostne kulture v zdravstvu in možne metodološke pristope, ki so bili uporabljeni pri raziskovanju tega koncepta. Cilj pregleda je bil opredeliti komponente koncepta ter iz obstoječih raziskave povzeti, kaj so razlogi za

neupoštevanje informacijske varnosti in koliko je le-ta poznana med zdravstvenim osebjem.

Metode

Najprej smo razvili *Protokol sistematičnega pristopa k pregledu literature*, povzet po Booth in sod.[12] Analizo podatkov smo izvedli po metodi tematske integrativne analize. Gre za kvalitativno vsebinsko analizo rezultatov dveh ali več primarnih kvalitativnih in kvantitativnih raziskav, pri kateri se lahko uporabi dve ali več iskalnih strategij. Tovrstna analiza je ustvarjalna, a kritična, in je ključna za prepoznavanje in primerjanje pomembnih vzorcev in tem. Uporablja najširšo vrsto raziskovalnih metod, ki omogočajo vključitev eksperimentalnih in neeksperimentalnih raziskav, vse z namenom, da bi bolje razumeli raziskovalni problem.[12]

Metode pregleda literature

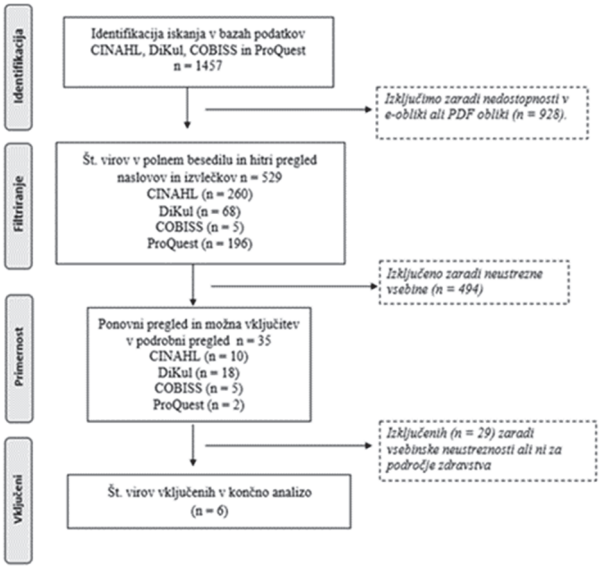
S pomočjo odgovorov na vprašanja PICO smo tvorili ključne besede: informacijska varnostna kultura (angl. *information security culture*), informacijska varnost (angl. *information security*), varovanje podatkov (angl. *data protection / data security*), zdravstveni podatki / pacientovi podatki (angl. *health data / patient data*) in zdravstvo / zdravstveni delavci (angl. *helathcare / helathcare professionals*). Ključne besede smo z uporabo Boolovimih operatorjev AND, OR in NOT združevali v iskalne nize v različnih elektronskih bibliografskih podatkovnih zbirkah. Iskali smo v zbirkah COBIB.SI, DiKul, CINAHL in ProQuest. Zadetke smo zožili z omejitvenimi kriteriji: obdobje objave (od 2010 do 2018), angleški in slovenski jezik, znanstvene revije, doktorske disertacije in magistrska dela dostopna v obliki PDF. V pregled smo vključili randomizirane in nerandomizirane kvantitativne in kvalitativne raziskave.

Potek pregleda

Skupno smo v podatkovnih zbirkah identificirali 1457 zadetkov (slika 1). Izbranih zadetkov za pregled v polnem besedilu in morebitno vključitev v rezultate je bilo 35. V končni pregled literature smo vključili 6 raziskav. Uporabili smo metodo PRISMA – mednarodni standard za prikaz rezultatov pregleda literature.

Ocena kakovosti pregleda

Izbor literature je temeljil na aktualnosti, vsebinski ustreznosti in dostopnosti virov. Oceno kakovosti pregleda smo podali na podlagi hierarhije dokazov v znanstveno raziskovalnem delu.[13] Izbrane raziskave za smo analizirali v skladu s smernicami STROBE in COREQ.



Slika 1 Diagram PRISMA (potek iskanja, pregleda in vključenosti virov).

Obdelava podatkov iz pregleda literature

Uporabili smo deskriptivno metodo in metodo tabeliranja. Podatke smo obdelali s tematsko integrativno analizo. Kvalitativno sintezo smo naredili na podlagi znanstvenih vsebin, ki smo jih kodirali in kasneje združili po kategorijah. Pred analizo vsebine izbranih raziskav smo zbrali podatke o značilnosti vsake posamezne raziskave (avtorji, država, raziskovalni načrt, vzorčenje, raziskovalni instrument, preučevane spremenljivke, ključne ugotovitve).

Rezultati

V končni pregled literature smo vključili šest raziskav, ki se navezujejo na obravnavano tematiko (tabeli 1 in 2).

Tabela 1 Raziskave, vključene v končni pregled.

Avtorji	Leto objave	Država
Gebrasilase in Lessa[14]	2011	Etiopija
Kwon in Johnson[15]	2013	ZDA
Agaku, Ayo-Yusuf in Connoly[16]	2014	ZDA
He in Johnson[17]	2017	Kitajska
Noor idr.[18]	2017	Malezija
Božić[19]	2016	Slovenija

Skupno smo identificirali 40 kod, ki smo jih glede na lastnosti in medsebojno povezanost združili v štiri vsebinske kategorije (tabela 3).

Tabela 3 Povzetek rezultatov.

Raziskava	Namen raziskave	Raziskovalni načrt	Vzorec in metoda vzorčenja	Raziskovalni instrument	Proučevane spremenljivke	Ključne ugotovitve
Gebrasilase & Lessa, 2011, Etiopija[14]	Izboljšati prakso varovanja informacij in identificirati dejavnike, ki vplivajo na informacijsko varnostno kulturo v bolnišnici Hawassa.	Mešani raziskovalni načrt. Izvedba ankete, poglobljenih intervjujev in pregled/analiza dokumentov.	564 enot (zdravniki, medicinske sestre, laboranti, farmacevti, študenti, administratorji in drugi zaposleni, ki prihajajo v stik z zdravstvenimi podatki). Najprej startificiran vzorec, nato tehnika enostavnega naključnega vzorčenja (tehnika loterije).	Uporabili so obstoječ vprašalnik za oceno informacijske kulture, ki je bil preveden v amharsko različico.	Znanje, odnos, prepričanje, ukrepi, ki se jih poslužujejo zaposleni v zvezi z informacijsko varnostno kulturo.	Zaznano pomanjkanje zavesti med zaposlenimi, pomanjkanje zavezanosti in podpore vodstva za delovanje in izvajanje informacijske varnosti. Odsotnost ozaveščenosti je najverjetneje posledica odsotnosti usposabljanja. Ozaveščenosti lahko ovira vodstvo, premalo sredstev za izvajanje informacijske varnosti. Večina zaposlenih nikoli ni bila na usposabljanju.
Kwon & Johnson, 2013, ZDA[15]	Preučiti varnost pacientovih podatkov v zdravstvenih ustanovah v ZDA.	Randomizirana kvantitativna raziskava. Izveden t-test, faktorska analiza, diskriminantna analiza, preverjena zanesljivosti in veljavnosti konstrukta.	Iz vsake od 250 bolnišnic so izbrali po eno osebo, (upravljavci IT oddelkov, direktorji IT, glavni varnostni akterji). Zaradi manjkajoči vrednosti so iz vzorca izpustili 46 bolnišnic, tako, da je realizirani vzorec obsegal 204 bolnišnice.	Podatke so zbirali s telefonsko anketo med zaposlenimi, ki so skrbeli za zasebnost in varnost zdravstvenih podatkov v bolnišnicah.	Vzorci varnostnih praks in odnosi med vzorci in skladnostjo s predpisi. Klasifikacija zdravstvenih ustanov na podlagi varnostnih praks s pomočjo združevanja v skupine (clustering).	204 bolnišnice so razvrstili v tri skupine, ki so imele podobno prakso skladnosti. Vse skupine so sprejemale tehnične prakse. Uravnotežile so varnostno prakso preko varovanja, revizije, upravljanja s človeškimi viri in upravljanja varnosti tretjih oseb.
Agaku, Adisa, Ayo-Yusuf & Connoly, 2014, ZDA[16]	Oceniti dojemanje in vedenje odraslih v ZDA na področju varovanja in zaščite zdravstvenih informacij.	Kvantitativni načrt, presečna raziskava. Gre za prvo od štirih ponovljenih anket (*Health Information National Trends Survey*). Izvedena multipla logistična regresija.	3959 respondentov – odrasli prebivalci ZDA.	Nacionalna reprezentativna anketa. Vprašalnik poslan po pošti. Stopnja odzivnosti 37 %.	Zaznavanje zaščitnih ukrepov; varnost in zasebnost informacij; nadzor nad zbiranjem, uporabo in izmenjavo informacij.	Zaskrbljenost respondentov zaradi kršitve varnosti zdravstvenih podatkov, predvsem pri pošiljanju dokumentov preko faksa ali elektronsko. Približno 12 % anketirancev je zaradi varnostnih pomislekov zdravstvenim delavcem zamolčalo določene informacije.

Raziskava	Namen raziskave	Raziskovalni načrt	Vzorec in metoda vzorčenja	Raziskovalni instrument	Proučevane spremenljivke	Ključne ugotovitve
He & Johnson, 2017, Kitajska[17]	Raziskati ovire, pri uporabi učenja iz incidentov kršenja varnosti zdravstvenih informacij.	Kvalitativni raziskovalni načrt –študija primera ene zdravstvene organizacije na terciarni ravni. Izvedeni so bili polstrukturirani intervjuji in pregledi oz. analiza dokumentov.	V vzorec ene zdravstvene ustanove je bilo izbranih 10 zdravstvenih delavcev (6 zdravnikov in 4 medicinske sestre) in 5 strokovnjakov za IT.	Vprašalnik z demografskimi vprašanji, polstrukturirani intervju.	Vprašanja o zbiranju podatkov oz. evidentiranju varnostnih incidentov; pridobivanje znanja o incidentih in povratne informacije.	Obravnave varnostnih incidentov z nizko stopnjo resnosti so se osredotočile na tehnične vidike, in manj poudarile pridobivanje znanja iz teh izkušenj. Podrobnosti ob ravnanju z incidenti niso bile ali so bile slabo dokumentirane. Organizacija ni imela strukturiranega načina za pridobivanje znanja iz nastalih incidentov.
Noor idr., 2017, Malezija[18]	Pregledati dejavnike, ki lahko vplivajo na informacijsko varnostno kulturo v okolju informatike v zdravstvu.	Izveden kvalitativni pristop, izvedba polstrukturiranega intervjuja.	7 zdravnikov, 5 medicinskih sester, 3 farmacevti in 4 administratorji. Merili za izbor udeležencev v študijo sta bili zaposlitev v zdravstveni organizaciji vsaj eno leto in uporaba IS.	Polstrukturiran vprašalnik. Pridobljeni podatki so bili urejeni z orodjem Atlas.	Identifikacija dvanajstih kategorij glede na pridobljene odgovore anketirancev.	Osveščenost o varnosti, varnostno znanje in varnostno vedenje so trije najpomembnejši dejavniki, ki ustvarjajo kulturo informacijske varnosti. Za te tri dejavnike je potrebna visoka zaveza glavnega vodstva, da se kultura informacijske varnosti oblikuje med zdravstvenimi delavci.
Božić, 2016, Slovenija[19]	Predstaviti učinek in pomen ozaveščanja zaposlenih pri vzpostavljanju in izvajanju varovanja informacijske varnosti.	Mešani raziskovalni načrt. Analiza tveganja, izveden družbeni inženiring in 10 delavnic ozaveščanja.	*Analiza tveganja*: eno svetovalno podjetje. *Družbeni inženiring:* naključna izbira 86 malih in srednje velikih organizacij (javni, zdravstveni in bančni sektor) v osrednjeslovenski regiji. *Vprašalnik in delavnice*: 253 zaposlenih v zdravstveni ustanovi.	*Analiza tveganja* z orodjem SBR. *Izvedba družbenega inženiringa* (nadzor nad poslanim USB ključkom organizacijam –kontrola uporabe ključka). *Vprašalnik* za zaposlene v zdravstveni ustanovi v Ljubljani pred začetkom delavnic.	*Analiza tveganja:* ocenitev tveganja informacijske varnosti. *Družbeni inženiring:* avtomatizirana analitika evidentiranja, iz katere je bilo razvidno, kdaj je določena organizacija odprla datoteke s ključka.	*Analiza tveganja:* človeški dejavnik je odgovoren za več kot polovico incidentov, povezanih z varovanjem informacij v organizaciji. *Izvedba družbenega inženiringa:* 90 % organizacij je ključek uporabilo, le v 11 % je prišel v roke IT-službe; 7 % organizacij je zanikalo, da bi prejeli pošiljko, čeprav so ključek uporabili. Zaposleni slabo poznajo varnostne politike; 22 % jih je že bilo priča varnostnemu incidentu. Večina uporablja premalo različnih gesel; 36 % gesla deli med seboj.

Tabela 2 Prikaz rezultatov po kodah in kategorijah.

Kategorija: varnostna praksa[15,17,18]
Varovanje – revizija – upravljanje s človeškimi viri – upravljanje varnosti tretjih oseb – preverjanje ozadja pred zaposlovanjem – prednost sprejemanju tehničnih rešitev pred postopki upravljanja varnosti – obravnave varnostnih incidentov z nizko stopnjo resnosti se osredotočajo na tehnične vidike – podrobnosti o ravnanju z incidenti so le delno ali sploh niso dokumentirane – občutljivost teme – izvajanje varnostne politike – potrebno je izboljšanje informacijske varnosti – zaposleni bi morali sodelovati pri izboljšanju informacijske varnosti – za dobro informacijsko varnost je potrebno sodelovanje – potrebna visoka zaveza glavnega vodstva, da se kultura informacijske varnosti razvije med zdravstvenimi delavci.
Kategorija: Znanje, usposabljanje, izkušnje[14,18]
Odsotnost usposabljanja vpliva na ozaveščenost – usposabljanje ovira vodstvo – ni zadosti sredstev za izvedbo izobraževanj in usposabljanj – večina zaposlenih nikoli ni prejela usposabljanja – zaposleni ne vedo, kaj je informacijska varnost – nepoznavanje organizacijske politike o informaciji varnosti – raven varnostnega znanja zaposlenih je nizka – potrebno motiviranje zaposlenih, da upoštevajo varnostne politike in postopke – izvajanje izobraževanja zaposlenih na področju varovanja informacij je na nizki stopnji – zaposleni razmeroma slabo poznajo varnostne politike – so priče varnostnemu incidentu – zlorabe gesel za dostop med zaposlenimi in študenti – uhajanje občutljivih podatkov novinarjem.
Kategorija: Zavedanje, odnos, stališče [14,18,19]
Pomanjkanje zavesti med zaposlenimi – odsotnost ozaveščenosti je najverjetneje posledica odsotnosti usposabljanja v bolnišnici – zaposleni želijo več izobraževanj in usposabljanj v zvezi z varnostjo informacij – stopnja zavedanja/ozaveščenosti je med zdravstvenimi delavci še vedno na srednji ravni – različne skupine zaposlenih imajo različen pristop do informacijske varnosti – zanikanje organizacije, da so uporabili nepoznano napravo za shranjevanje podatkov.
Kategorija: Dejavniki tveganja, zaupanje [14,16,19]
Pomanjkanje zavezanosti in podpore vodstva – zaposleni ne vedo, kaj je informacijska varnost – zaposleni ne poznajo vprašanj o varnosti informacij, povezanih z njihovim delovnim mestom – zaskrbljenost pacientov zaradi kršitve varnosti zdravstvenih podatkov – zaradi varnostnih pomislekov pacienti zdravstvenim delavcem zamolčijo določene informacije – človeški dejavnik je odgovoren za več kot polovico incidentov – nepravilna uporaba nepoznanih nosilcev podatkov – premalo različnih gesel – zaposlenih svoja gesla delijo med seboj.

Razprava

Organizacije razmeroma malo ali skoraj nič ne vlagajo v izobraževanja svojih zaposlenih s področja informacijske varnosti in tako posledično tudi ne razvijajo dobre informacijske varnostne kulture, ki je pomembna za vsakodnevno delovaje organizacije. Varnostna praksa organizacij ni na visokem nivoju, saj organizacije dajejo prednost sprejemanju tehničnih rešitev za zaščito in ne postopkom upravljanja varnosti, človeški dejavnik pa je vzrok za večino varnostnih tveganj ali kršitev.

Bolnišnice se raje poslužujejo preverjanja preteklosti pred zaposlovanjem kot pa organiziranju ali izvedbi izobraževanj. Ob varnostnih incidentih organizacije preidejo v reševanje tehničnih težav, pozabljajo pa na pozitivne strani pridobivanja znanja in ozaveščenosti, ki bi jih lahko bili deležni zaposleni.[17] Znanje, usposabljanje in izkušnje so pomembni dejavniki pri razvijanju dobre informacijske varnostne kulture v organizaciji, saj so zaposleni, pogosto zaradi pomanjkanja znanja, največja grožnja varnosti informacij.[20]

S pregledom smo ugotovili, da večina zdravstvenih delavcev nikoli ni bila deležna izobraževanj ali usposabljanj, kar se je pokazalo tudi v tem, da jih večina ni poznala varnostne politike. V veliki meri je bilo za takšno stanje odgovorno vodstvo, ker ni vlagalo zanimanja ali sredstev. Odnos, prepričanje in ravnanje zaposlenih do informacij morajo biti sprejemljivi in morajo biti del vsakdanjega »življenja« organizacije. Ocenjevanje odnosa in znanja zaposlenih do informacijske varnosti lahko pomaga organizaciji razumeti vedenja in prepoznati probleme. Ugotovili smo, da obstaja vrzel v odnosu oziroma stališčih in da imajo različne poklicne skupine različen pristop do varovanja informacij, je pa stopnja zavedanja še vedno na srednji ravni. Iz raziskav, ki so bile opravljene na področju zdravstvene nege v tujini, je jasno, da je problematika informacijske varnosti slabo oziroma premalo obravnavana. Albarrak[21] v svoji raziskavi opozarja, da se medicinske sestre zavedajo problematike informacijske varnosti, a kljub temu njihove navade predstavljajo resno grožnjo za varnost in zaupnost pacientovih podatkov.[21] Niimi in Ota[22] sta ugotovila, da nekatere bolnišnice sledijo različnim varnostnim ukrepom, veliko medicinskih sester pa ni prepoznalo varnostnih vzdrževalnih ukrepov.[22] V Sloveniji je bila v letu 2016 izvedena serija desetih delavnic ozaveščanja za zaposlene v eni od zdravstvenih ustanov. Pred delavnicami je bila izvedena anketa z namenom pridobiti splošen vpogled v trenutno stanje ozaveščenosti. Zaposleni so slabo poznali varnostne politike; četrtina anketirancev jih je že bila priča varnostnemu incidentu (od zlorabe gesel za dostop med zaposlenimi in študenti do uhajanja občutljivih podatkov novinarjem). Večina zaposlenih uporablja premalo različnih gesel (gesla enaka za več sistemov); 36 % pa jih svoja gesla deli

med seboj, kar pomeni, da jih je ravno toliko bilo v prekršku glede varnostne politike uporabe gesel.[19]

Nove tehnologije lahko dodatno povečajo ranljivost zasebnih informacij, vključno z zdravstvenimi. Še večji problem je, da je možno te naprave izgubiti ali ukrasti in hranijo veliko pomembnih informacij. Skrb vzbuja to, da so respondenti v raziskavi (odrasli prebivalci ZDA) zaradi varnostnih pomislekov zdravstvenim delavcem zamolčali določene pomembne informacije.[16] Pojem informacijske varnostne kulture za področje zdravstva opisuje le ena raziskava,[14] ostale opisujejo podobne oziroma sorodne koncepte,[15-19] kot je varnost informacij ali informacijska varnost. Med zadetki je bilo zaslediti veliko dobrih raziskav na omenjeno temo, vendar za področje zdravstva malo. Spremenljivke, ki so bile znanstveno preučevane, so bile predvsem znanje, odnos, prepričanje o informacijski varnosti, vzorci varnostnih praks, skladnost s predpisi ter zaščitni ukrepi za zavarovanje zdravstvenih podatkov.

Omejitve

V raziskavi smo se osredotočili na pregled aktualnih raziskav, starih do 8 let, in sicer znanstvenih prispevkov, objavljenih v angleškem in slovenskem jeziku. Izbor jezika lahko povzroči pristranskost, zato bi bilo smiselno nadaljnje raziskovanje usmeriti v iskanje relevantnih prispevkov v drugih jezikih in iz drugih zbirk podatkov. Iskanje, pregled in izbor raziskav je opravil samo en raziskovalec. V bodoče bi lahko več raziskovalcev skupaj razvilo raziskovalno strategijo, jo uporabilo v različnih podatkovnih zbirkah in bi ločeno izbirali relevantne raziskave, čemur bi v primeru neskladja sledilo iskanje konsenza. Analizirane raziskave so se glede na raven dokazov[13] vse razen ene uvrstile nizko.

Zaključek

Za področje zdravstva je koncept informacijske varnostne kulture slabo raziskan, tako v Sloveniji kot v tujini. Informacije, ne glede na obliko, zahtevajo ustrezno zaščitno, njihovi uporabniki pa so ključni potencialni predstavniki groženj. Kršitve varnosti zdravstvenih informacij imajo pomemben vpliv ne le na paciente, ampak tudi na zdravstvene ustanove. Glede na večanje pogostosti zlorab podatkov, je tema aktualna in pomembna, vzpostavitev informacijske varnostne kulture pa nujna.

Sistematični pregled obstoječih dokazov je dal vpogled v trenutno situacijo. V končno analizo je bilo vključenih šest raziskav (eno magistrsko delo in pet drugih znanstvenih prispevkov). V prihodnje bi bilo potrebno bolj celostno raziskati stanje v slovenskih zdravstvenih ustanovah in za ta namen razviti kakovosten merski instrument, ki bi meril celoten koncept informacijske varnostne kulture. Za zaposlene v zdravstvenih organizacijah je potrebno organizirati kontinuirana izobraževanja in delavnice, prav tako poudariti pomembnost organiziranja izobraževanj pri vodstvu. Kako uspešne so bile izvedene delavnice, bi lahko preverili z izvedbo kvazieksperimenta.

Konflikt interesov

Del rezultatov je bil predstavljen na 11. Mednarodni znanstveni konferenci Fakultete za zdravstvo Angele Boškin (Bled, 7 .6. 2018).

Reference

1. Alnatheer M, Nelson K: Proposed framework for understanding information security culture and practices in the Saudi context. In: *Proceedings of the 7th Australian Information Security Management Conference, Perth, Western Australia, 1.-3. 12. 2009*. Perth 2009: Security Research Centre, School of Computer and Security Science, Edith Cowan University; 6-17.
2. Von Solms B: Information security – the third wave? *Comp Secur* 2000; 19(7), 615-620.
3. Von Solms B: Information security – the fourth wave? *Comp Secur* 2006, 25(165), 165-168.
4. Kuusisto R, Kuusisto T: Strategic communication for cyber security leadership. In: Kuusisto R, Kurkinen E (eds.), *Proceedings of the 12th European conference on information warfare and security, University of Jyvaskyla, Finland, 11.-12. 7. 2013*. UK 2013: Academic Conferences and Publishing International Limited; 167.
5. Williams PA: What does security culture look like for small organizations? In: *7th Australian Information Security Management Conference*. Perth, Western Australia 2009: Security Research Centre, School of Computer and Security Science, Edith Cowan University; 47-54. https://doi.org/10.4225/75/57b4029530dea (15. 12. 2018).
6. Orehek Š: *Merjenje informacijske varnostne kulture: metaanaliza anketnih merskih inštrumentov: magistrsko delo.* Ljubljana 2017: Univerza v Ljubljani, Fakulteta za družbene vede.
7. Noor H, Zuraini I: A conceptual model for investigating factors influencing information security culture in healthcare environment. *Procedia Soc Behav Sci* 2012; 65: 1007-1012. https://doi.org/10.1016/j.sbspro.2012.11.234 (15. 12. 2018)
8. Ponemon Institute: *Cost of data breach study: global analysis*. [S. l.] 2015: Ponemon Institute. https://nhlearningsolutions.com/Portals/0/Documents/2015Cost-of-Data-BreachStudy.pdf (2. 12. 2017)
9. US Department of Health and Human Sercices, Office for Civil Rights: *Breach portal: notice to the secretary of HHS*

breach of unsecured protected health information. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (2. 12. 2017)
10. SI-CERT: *Poročilo o omrežni varnosti za leto 2015*. https://www.cert.si/wp-content/uploads/2016/06/SI-CERT_LP_2015.pdf (2. 12. 2017)
11. Appari A, Johnson E: Information security and privacy in healthcare: current state of research. *IJIEM* 2010; (6)4: 279-314.
12. Booth A, Sutton A, Papaioannou D: *Systematic approaches to a successful literature review*. Los Angeles: 2012 Sage; 59-60.
13. Polit D, Beck CT: *Essentials of nursing research: appraising evidence for nursing practice*. Philadelphia 2008: Lippincott Williams & Wilkins.
14. Gebrasilase T, Lessa LF: Information security culture in public hospitals: the case of Hawassa referral hospital. *Afr J Inf Syst* 2011; 3(3): 72-86.
15. Kwon J, Johnson ME: Security practices and regulatory compliance in the healthcare industry. *J Am Med Infor Assoc* 2013; 20(1): 44-51. https://doi.org/10.1136/amiajnl-2012-000906 (15. 12. 2018)
16. Agaku I, Adisa A, Ayo-Yusuf A, Connolly, N: Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. *J Am Med Infor Assoc* 2014; 21(2): 374-378. https://doi.org/10.1136/amiajnl-2013-002079 (15. 12. 2018)
17. He Y, Johnson C: Challenges of information security incident learning: an industrial case study in a Chinese healthcare organization. *Inform Health Soc Care* 2017; 42(4): 393-408. https://doi.org/10.1080/17538157.2016.1255629 (15. 12. 2018)
18. Noor H, Norazen M, Maarop N, Ismail Z, Wardah A: Information security culture in health informatics environment: a qualitative approach. In: *International Conference on research and innovation in information systems (ICRIIS)*. Langkawi, Malaysia 2017; 1-6. https://doi.org/10.1109/ICRIIS.2017.8002450 (16. 12. 2018)
19. Božić F: *Človeški dejavnik pri zagotavljanju informacijske varnosti: magistrsko delo*. Ljubljana 2016: Univerza v Ljubljani, Fakulteta za računalništvo in informatiko.
20. Niekerk JF, Solms R: Information security culture: a management perspective. *Comp Secur* 2010; 29(4): 476-486. https://doi.org/10.1016/j.cose.2009.10.005 (16. 12. 2018)
21. Albarrak A: Information security behavior among nurses in an academic hospital. *HealthMED* 2012; 6(7): 2349-2354.
22. Niimi Y, Ota K: Privacy recognition by nurses and necessity of their information security education. In: Shaw T (ed.), *International conference on education reform and modern management*. Amsterdam 2014: Atlantis Press; 358-361.

■ *Strokovni članek*

Barbara Smrke, Darja Podsedenšek

Izkušnje z naprednim informacijskim sistemom na Oddelku za intenzivno interno medicino Splošne bolnišnice Celje

Povzetek. Dokumentiranje je pomemben del v procesu zdravljenja in izvajanja zdravstvene nege. Biti mora varno, zanesljivo in čitljivo. Na oddelku za intenzivno interno medicino v Celju smo izvedli kratko anketo z odprtim tipom vprašanj na temo uporabnosti elektronskega temperaturnega lista. Anketni vzorec sicer ni reprezentativen, a vseeno predstavlja posnetek uporabnikove izkušnje z elektronskim temperaturnim listom. Veseli nas dejstvo, da so uporabniki sistema prepoznali delovno orodje kot uporabno. Največ prednosti elektronskega temperaturnega lista predstavlja opomnik za delo (20 %), največja slabost po je mnenju anketiranih nepreglednost izvidov (19 %) ter slaba zmogljivost računalnikov in odzivnost računalniškega programa (12 %). Elektronski temperaturni list predstavlja za delo v intenzivni enoti popolno brezpapirno dokumentiranje s svojimi prednostmi in slabostmi.

Experience with an Advanced Information System at the Intensive Internal Medicine Department of the Celje General Hospital

Abstract. Documentation is an important part of the treatment process in nursing care. It must be safe, reliable and legible. At the Intensive Internal Medicine Department in Celje, a short survey with an open-ended questionnaire on the applicability of the electronic temperature sheet was conducted. Although the survey sample is not representative, it is a snapshot of the users' experience. We were glad to observe that the users recognised the tool as useful. According to the respondents, the electronic temperature sheet is a good reminder for work (20 %). Its main drawbacks are lack of transparency (19 %) and poor performance and responsiveness of the software (12 %). The electronic temperature sheet represents completely paper-free documenting, with its advantages and disadvantages.

■ **Infor Med Slov** 2018; 23(1-2): 34-38

Institucija avtoric / Authors' institution: Splošna bolnišnica Celje, Oddelek za intenzivno interno medicino.

Kontaktna oseba / Contact person: Barbara Smrke, mag. zdr. nege, Splošna bolnišnica Celje, Oblakova ulica 5, 3000 Celje, Slovenija. E-pošta / E-mail: barbarasmrke79@gmail.com.

Prispelo / Received: 6. 12. 2018. Sprejeto / Accepted: 20. 12. 2018.

Uvod

Dokumentacija v zdravstveni negi (ZN) je komunikacijska metoda, ki vse zdravstvene delavce stalno informira o tem, kakšno ZN in oskrbo pacient potrebuje, kakšno ZN in oskrbo je prejel ter jasno opredeli vse pomembne in potrebne informacije o pacientu. Namen dokumentiranja je tudi doseganje zakonskih in profesionalnih standardov. Kakovostno izvedeno dokumentiranje je izjemno pomembno tako za kakovost ZN, kot tudi za razvoj stroke ZN in tudi kot zaupanje znotraj ZN.[1] Namen dokumentacije ZN je zagotoviti splošen pregled nad planirano in izvedeno ZN ter zagotavljanje kakovostne in kontinuirane ZN med zdravstveno obravnavo posameznika.[2] Dokumentacija ZN ni je sestavni del dela medicinskih sester (MS) in jo razumemo kot pomembno orodje, ki ga MS uporabljajo za zagotavljanje visoke kakovosti zdravstvene oskrbe pacienta.[3]

Dobra dokumentacija je lahko v pomoč MS pri morebitnih odškodninskih zahtevkih oziroma tožbah zaradi malomarnosti ter v disciplinskih ukrepih in sporih, ki izhajajo iz etičnih dilem. Verodostojnost je bistvenega pomena v zdravstvenem popisu pacienta, kajti vsi izvajalci zdravstvenega varstva, ki skrbijo za določenega pacienta, se pri odločanju o zdravljenju sklicujejo na zapise. Torej so potrebne pri dokumentiranju dejanske, konkretne, opisne in resnične navedbe.[4] Dokumentacija ZN je kontinuiran zapis o izvedbi vseh faz procesa ZN glede na strokovna dognanja, smernice, protokole in standarde ZN. Z dokumentiranjem v ZN tako zagotavljamo zapis o vseh bistvenih spremembah pacientovega stanja in odstopanja glede na predviden načrt ZN ter učinkovitost izvedenih aktivnosti.[5]

Digitalizacija temperaturnega lista v bolnišnici je eden izmed izzivov medicinske informatike. Uvedba prinaša transparentnost medicinske oskrbe in s tem večjo varnost za paciente, višjo učinkovitost dela v bolnišnici, lažje ter preglednejše vodenje podatkov v procesih zdravljenja in oskrbe ter znižanje skupnih stroškov.[6] Elektronski temperaturni list (ETL) predstavlja korak v razvoju sodobne medicine v povezavi z napredkom informacijske tehnologije. Elektronski negovalni list naj bi postal delovno orodje medicinske sestre v prihodnosti, ki bo omogočal medicinski sestri dostop do raznih informacij, ki bodo pomembne za njeno delo in obravnavo pacienta, hkrati pa bo povezoval dokument zdravstvene nege z drugimi dokumenti, ki se tičejo obravnave pacienta.[1]

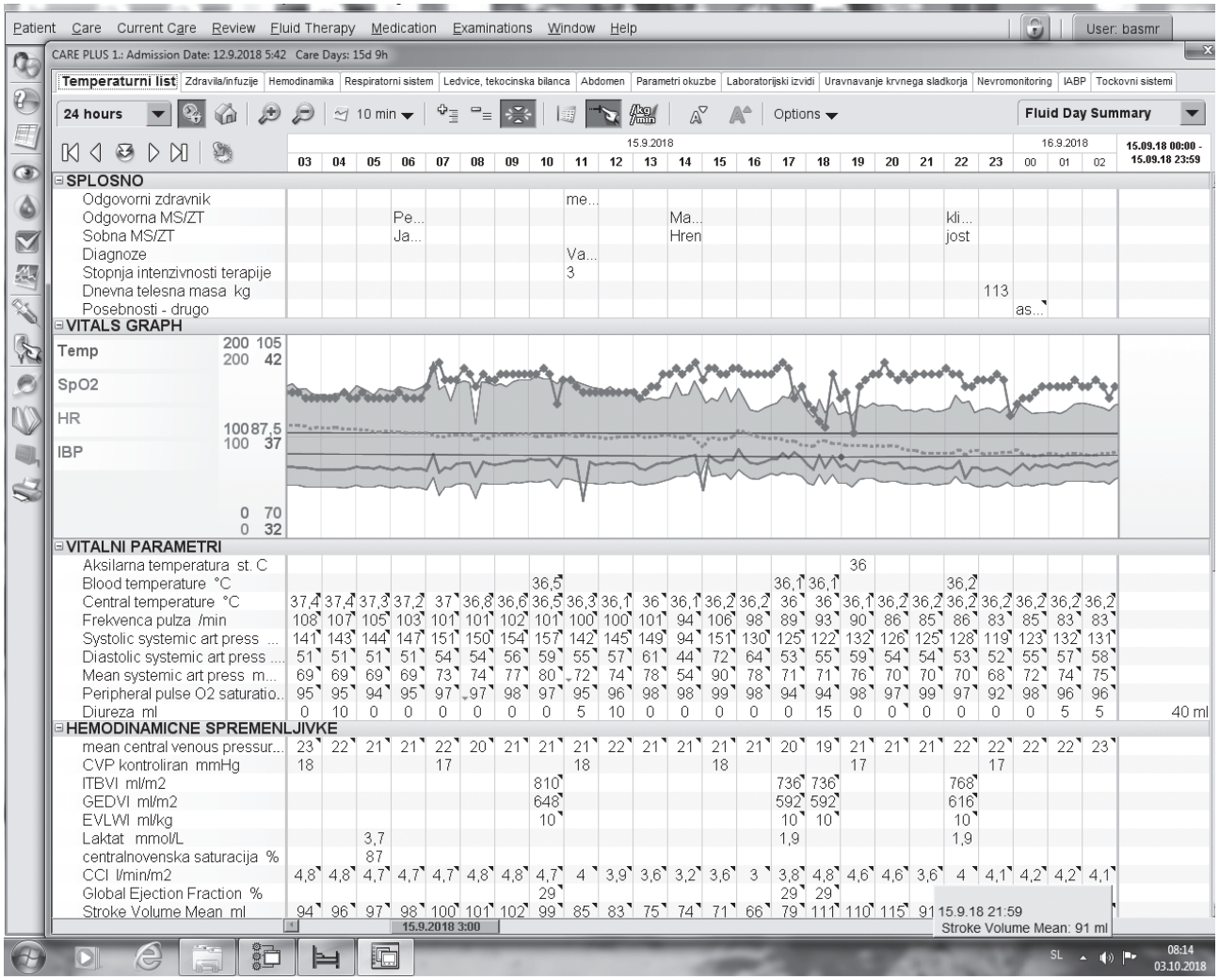
Razvoj informacijsko-komunikacijske tehnologije je pripeljal do informatizacije v zdravstvu, s čimer klasično papirnato dokumentiranje zamenjuje elektronsko zasnovana dokumentacija. Razvoj elektronskega temperaturnega lista v patronažnem varstvu predstavlja hitrejšo komunikacijo s pacienti in z zdravniki ter hitrejše odkrivanje zapletov;[7] hkrati naj bi prišlo do večjega pretoka informacij med posameznimi profili delavcev znotraj zdravstvenega tima, večjega nadzora nad opravljenim delom in visoke razpoložljivosti statističnih poročil.[8] Pri teh novitetah pa prihaja tudi do slabosti, ki se kažejo predvsem kot depersonalizacija zdravstvene nege in neizpolnjevanje etičnih norm. Razlog za to je predvsem neznanje MS pri rokovanju z elektronsko dokumentacijo.[7] Kelc in Dinevski menita, da bo ETL v svet zdravstva prinesel "transparentnost medicinske oskrbe in s tem večjo varnost za pacienta, višjo učinkovitost dela v bolnišnici, lažje ter preglednejše vodenje podatkov v procesih zdravljenja in oskrbe ter ne nazadnje tudi znižanje skupnih stroškov".[6] Kovačič dodaja, da se bodo pozitivne posledice ETL kazale kot "hitrejše zbiranje podatkov, lažje shranjevanje podatkov, hitrejša in natančnejša obdelava podatkov, hitrejša in natančnejša obdelava povratnih informacij, manjša poraba človeške energije, prihranek materiala (npr. papirja), prihranek časa, lažji in hitrejši dostop do določenih informacij, lažje razumevanje obdelanih podatkov in boljša kakovost".[9] Vsaka novost, še posebej če je v fazi razvoja, ima zraven pozitivnih lastnosti tudi nekatere negativne lastnosti ali omejitve, katere je potrebno izboljšati. Z elektronskim dokumentiranjem zdravstvene nege tako obstaja bojazen, da se bo delo preselilo od pacienta k računalniku. Purkart[8] izpostavlja problem pomanjkanja prenosnih naprav, zato je beleženje podatkov ob pacientu omejeno. Kovačič[9] pa izpostavlja pomanjkljivosti računalniške dokumentacije, odsotnost povratne informacije, individualizem, izključenost iz informacijske mreže in računalniško nepismenost ter problem izpada električne energije, ki lahko privede do zrušenja računalniškega sistema.

Uvajanje novosti na vseh delovnih področjih predstavlja izzive pri zaposlenih. Prihaja tudi do odpora, saj novosti vedno spremenijo rutino dela. Študija iz ZDA[10] poroča, da so ovire pri vpeljevanju elektronskega dokumentiranja pomanjkanje financ za nakup ustrezne opreme, stroški vzdrževanja, odpor zdravnikov, nejasen donos naložb ter pomankanje kadra z ustrezno izobrazbo s področja informacijske tehnologije. Komunikacija pomeni osnovo dobrega sodelovanja znotraj zdravstvenega tima in predstavlja pomembno komponento, ki vpliva na izid zdravljenja pacienta. Elektronska dokumentacija je komunikacijski kanal med različnimi profili znotraj

zdravstvenega tima in tako pomembno neposredno varnost pacienta.[11] Informatizacija zdravstva in zdravstvene nege je neizogibna. V sodobnem času, kjer je čas dragocena dobrina, postaja učinkovit način dokumentiranja zelo pomemben. Splošno znano je, da so medicinske sestre znotraj zdravstvene obravnave najpogosteje v stiku s pacientom. Dokumentiranje predstavlja pomembno delo, za kar medicinske sestre porabijo tudi do tretjino svojega delovnega časa.[12] Z učinkovitim sistemom elektronskega dokumentiranja bi se ta čas lahko zmanjšal, medicinske sestre pa bi se lahko še bolj posvetile pacientom, kar bi nedvomno imelo pozitivne učinke na izide zdravljenja.

V letu 2017 smo na Oddelku za intenzivno interno medicino nadgradili in prilagodili desetletje star informacijski sistem, kar nam je omogočilo, da ne uporabljamo nobenih papirnatih dokumentov v procesu zdravljenja in zdravstvene nege. Papirne oblike obrazcev uporabimo le v primeru, ko potrebujemo medicinsko-tehnično podporo izven oddelka. Informacijski sistem nam omogoča samodejno beleženje vitalnih parametrov, kontinuirano spremljanje infuzije zdravil in tekočin, nadzor nad vstavki in katetri pri pacientih, nadzor krvnega sladkorja in posebnih varovalnih ukrepov ter načrtovanje in natančno dokumentiranje ZN, skratka vse, kar potrebujemo za kakovostno in natančno delo v intenzivni enoti. ETL uporabljamo MS, zdravniki in fizioterapevti, ki so zaposleni na našem oddelku (slika 1). Obstoječi program smo nadgradili in prilagodili naši uporabi.

Za nadgradnjo sistema je zaslužen asist. Miha Mežnar, ki je pri projektu upošteval naše želje in ga prilagodil uporabi na našem oddelku. Pri uvajanju smo nekaj časa vodili papirno in elektronsko obliko dokumentacije, zaradi velikega števila podatkov pa se to ni izšlo in smo po dobrem tednu dvojno dokumentiranje opustili. Zelo koristen je bil uvajalni seminar, nato pa smo si iz izmene v izmeno predajali novosti, jih zapisovali in tako postali računalniško pismeni.



Slika 1 Elektronski temperaturni list.

Metode

Za izvedbo raziskave smo uporabili strukturiran instrument v obliki kratkega anketnega vprašalnika, ki smo ga oblikovali na podlagi pregledane literature. Vsa vprašanja so bila odprtega tipa. V anketo smo vključili medicinske sestre, zaposlene na oddelku za intenzivno interno medicino. Udeležba v anketi je bila prostovoljna. Anketo smo izvedli avgusta 2018.

Rezultati

Za preverjanje enoletne uporabniške izkušnje z ETL smo anketirali 14 sodelavcev, članov tima zdravstvene nege. Prosili smo jih, da navedejo, katere prednosti in slabosti lahko izpostavijo pri uporabi ETL. Prav tako smo jih prosili, da navedejo predloge za morebitne spremembe ETL v prihodnje.

V anketi so sodelovale medicinske sestre z delovno dobo

- od 1 do 10 let – 25 % anketiranih,
- od 11 do 20 let – 18 % anketiranih,
- od 21 do 30 let – 50 % anketiranih,
- 30 let in več – 7 % anketiranih.

Od vseh anketiranih je bilo 13 diplomiranih in ena srednja medicinska sestra. V starostni strukturi anketirancev prevladujejo diplomirane medicinske sestre z delovno dobo do 7 let.

Pri navajanju prednosti ETL so anketiranci izpostavili:

- čitljivost (23 %),
- opomniki (20 %),
- preglednost (14 %),
- hitrost (9 %),
- avtomatsko računanje bilance tekočin (9 %),
- varovanje podatkov (9 %),
- sledljivost (7 %) in
- natančnost (7 %).

Navedene slabosti ETL so:

- nepreglednost izvidov (19 %),
- slaba zmogljivost računalniške opreme (12 %),
- nepotrebna vidnost ukinjene terapije (12 %),
- zamuda s prijavo v sistem (10 %),
- postavitev monitorja za pacienta (7 %),
- zastarel uporabniški vmesnik; nepreglednost vitalnih parametrov zaradi velike količine podatkov; nepovezanost z bolnišničnim informacijskim sistemom; ni vpisovanja razjed zaradi pritiska; ni vpisanih vseh zdravil; vizita izven bolniške sobe (vse po enkrat, tj. 7 %).

Od 14 anketiranih jih je le šest opredelilo željo po spremembah oziroma dopolnitvah ETL. Najbolj si želijo spremembe lokacije monitorja (38 %), ki naj bo nameščen ob bolniku. Želijo ekran na dotik, saj olajšuje vnose podatkov. Opozarjanje na nedokončana opravila, hitrejše prijavljanje v sistem in večja avtomatizacijo predstavljajo enak delež (12 %) med predlogi za spremembe in dopolnitve sistema.

Razprava

Anketni vzorec sicer ni reprezentativen, a vseeno predstavlja posnetek uporabnikove izkušnje z ETL. Veseli nas dejstvo, da so uporabniki sistema prepoznali delovno orodje kot uporabno, hitro, zanesljivo, predvsem pa varno, tako za paciente kot za medicinsko osebje. Kljub temu, da smo z uporabniškim vmesnikom, ki je v angleškem jeziku, od začetka imeli kar nekaj težav, pa anketiranci angleščine niso navajali kot komunikacijski problem. Čitljivost predpisane terapije je ena od bistvenih pridobitev – pri papirnati verziji temperaturnega lista je bila velikokrat problematičen, morda tudi varnostno sporen dejavnik. Personalizirana identifikacija uporabnikov sicer predstavlja bistven napredek v sledljivosti vnosov podatkov v ETL, hkrati pa upočasnjuje dostop do sistema in predstavlja moteč dejavnik za anketirance. Potrebno bi bilo spremeniti način identifikacije uporabnika v sistem. Možnost identifikacije z brezkontaktnim ključkom, ID kartico ali prstnim odtisom bi skrajšala postopek vpisa v sistem, predvsem pa bolj učinkovito preprečila vnose v sistem pod napačnimi uporabniškimi podatki. Lokacija monitorja moti kar 38 % anketiranih uporabnikov. Kljub temu, da se mnogo meritev vitalnih funkcij avtomatsko prenaša v ETL in da nas sistem opozarja o potrebnih nadaljnjih korakih predpisane parenteralne terapije, pa je za medicinsko osebje še vedno neobhodno potreben neposreden stik s pacientom pri izvajanju procesnih korakov v ETL. Monitor na dotik bi zagotovo olajšal vnos posameznih parametrov in s tem pospešil postopke rokovanja z ETL. Naša strojna oprema sistema ETL je že zastarela (iz leta 2007), zato predstavlja varnostno tveganje pri izvajanju diagnostično terapevtskih postopkov, ki so opredeljeni za enoto intenzivne terapije III. Kljub temu, da je zagotovljena redundantnost sistema, zastarela oprema povečuje tveganje za nenačrtovane izpade delovanja. Kar nekaj anketirancev opozarja na posamezne pomanjkljivosti uporabniškega vmesnika, predvsem v smislu njegove funkcionalnosti in prilagodljivosti. Pred načrtovanjem posodobitve sistema ETL bi bilo potrebno preveriti uporabniške izkušnje tudi na drugih medicinskih oddelkih po Sloveniji in v tujini, ki so že

implementirali ali pa so v fazi implementacije sistema ETL. S primerjalno analizo sistemov bi tako lažje in bolj objektivno opredelili pomanjkljivosti in optimizirali postopke ter funkcionalnosti uporabniškega vmesnika ETL.

Zaključek

Pri uvajanju sistema glede sodelovanja osebja ni bilo večjih težav, je pa to obdobje predstavljalo dodatno obremenitev, a smo jo s pozitivno energijo premostili in po dobrem letu še vedno uspešno uporabljamo brezpapirno dokumentacijo.

Reference

1. Ramšak Pajk J: Dokumentacija v zdravstveni negi: pregled literature. *Obzor Zdrav Neg* 2006; 40(3): 137-142. http://www.obzornikzdravstvenenege.si/2006.40.3.137 (28. 1. 2019)
2. Kroell V, Birth Garde A: *Strategy for documentation in nursing at a national and a local level in Denmark*. In: Oud N, Sermeus W, Ehnfors M (eds.), ACENDIO 2005: documenting nursing care. Bern 2005: H. Huber; 73-77.
3. Blair W, Smith B: Nursing documentation: frameworks and barriers. *Contemp Nurse* 2012; 41(2): 160-168. https://doi.org/10.5172/conu.2012.41.2.160 (28. 1. 2019)
4. Blažič M: Z dokumentiranjem se preprečujejo napake v zdravstveni negi. In: Podhostnik, A (ed.), *Napake v zdravstveni negi: zbornik prispevkov. 5. dnevi Marije Tomšič, Dolenjske Toplice, 24. in 25. januar 2013*. Novo mesto 2013, Visoka šola za zdravstvo, 11-14.
5. Paans W, Sermeus W, Nieweg RM, Van der Schans CP: Prevalence of accurate nursing documentation in patient records. *J Adv Nurs* 2010; 66(11): 2481-2489. https://doi.org/10.1111/j.1365-2648.2010.05433.x (28. 1. 2019)
6. Kelc R, Dinevski D: Koncept digitalizacije temperaturnega lista v informatizirani bolnišnici. *IMS* 2010; 15(supl): 31-32. http://ims.mf.uni-lj.si/archive/15(supl)/31.pdf (28. 1. 2019)
7. Pust B, Lokajner, G: *Računalnik ob pacientovi postelji.* https://www.zbornica-zveza.si/sites/default/files/publication__attachments/14._simpozij_zdravstvene_in_babiske_nege.pdf (7. 5. 2018)
8. Purkart M: Zdravstvena nega in informacijski sistem na Pediatrični kliniki Univerzitetnega kliničnega centra Ljubljana – od zasnove preko težav do uporabe. https://www.zbornica-zveza.si/sites/default/files/publication__attachments/14._simpozij_zdravstvene_in_babiske_nege.pdf (7. 5. 2018).
9. Kovačič U: *Dejavniki, ki vplivajo na dokumentiranje.* http://www.dmszt-nm.si/media/pdf/zbornik-dmt-2013.pdf#page=89 (6. 6. 2018)
10. Jha AK, DesRoches CM, Campbell EG, *et al.*: *Use of electronic health records in U.S. hospitals.* http://www.nejm.org/doi/full/10.1056/NEJMsa0900592#t=articleResults (6. 1. 2018).
11. Lavin MA, Harper E, Barr N: Health information technology, patient safety, and professional nursing care documentation in acute care settings. *OJIN* 2015; 20(2). http://www.nursingworld.org/MainMenuCategories/ANAMarketplace/ANAPeriodicals/OJIN/TableofContents/Vol-20-2015/No2-May-2015/Articles-Previous-Topics/Technology-Safety-and-Professional-Care-Documentation.html (28. 1. 2019)
12. Prinčič B, Purkart M, Oštir M, Štih A: *Sodobno dokumentiranje v zdravstveni negi – elektronsko vodenje zdravstvene nege.* http://www.slovenskapediatrija.si/portals/0/clanki/2015_1-2_22_028-035-izv.pdf (17. 12. 2017).

Ema Dornik

30 let izkušenj v podporo digitalizaciji zdravstva: poročilo s srečanja Sekcije za informatiko v zdravstveni negi 2018

Tradicionalno srečanje članov Sekcije za informatiko v zdravstveni negi (SIZN), ki deluje pri Slovenskem društvu za medicinsko informatiko (SDMI), je potekalo v Zrečah 16. novembra 2018. SDMI je z organizacijo kongresa MI'2018 z mednarodno udeležbo obeležilo jubilej – 30 let delovanja. Programski sklop SIZN je bil tudi tokrat namenjen strokovni rasti, izobraževanju in druženju članov.

V nadaljevanju so predstavljeni povzetki predstavitev v zaporedju, kot so si sledili po programu.

Klemen Cvirn, Vesna Prijatelj: Vloga medicinske sestre kot promotorke uporabe mobilnih aplikacij za podporo zdravju

Pri uporabi mobilnih aplikacij je zelo pomembna varnost osebnih podatkov, saj aplikacije za svoje delovanje od uporabnika zahtevajo vnos in dostop do vrste osebnih podatkov. Namen naše raziskave je pridobiti podatke o ozaveščenosti uporabnikov mobilnih aplikacij za podporo zdravju glede varnosti in zasebnosti podatkov ter identificirati pričakovanja uporabnikov mobilnih aplikacij, kar je temelj za nadaljnje aktivnosti zdravstvene nege na področju ozaveščanja pacientov. Pri raziskavi je bil uporabljen kvantitativni raziskovalni pristop. Podatki so bili zbrani preko odprtokodne aplikacije za spletno anketiranje 1KA in tudi obdelani v njej, dodatno pa še s programom Excel. Med 143 vprašanimi jih 98 % navaja, da mobilne aplikacije uporabljajo, in sicer povprečno vsak vprašani uporablja vsaj tri različne aplikacije; 45 % anketiranih že uporablja mobilne aplikacije za podporo zdravju. Rezultati raziskave kažejo, da je splet v 38 % glavni vir informacij o aplikacijah za podporo zdravju, zgolj 6 % jih je za te aplikacije izvedelo od zdravstvenega osebja. Polovica vprašanih se ne more opredeliti o varnosti mobilnih aplikacij z vidika varnosti osebnih podatkov, 35 % pa jih meni, da so varne. Sklenemo lahko, da je uporaba aplikacij za podporo zdravju je v slovenskem prostoru sicer prisotna, vendar nezadostno promovirana. Rezultati kažejo, da o možnosti uporabe teh aplikacij anketirani zgolj malo informacij dobijo s strani zdravstvenega osebja, bi si jih pa želeli veliko več. Vloga medicinske sestre kot promotorke uporabe mobilnih aplikacij za podporo zdravju se bo z nadaljnjim razvojem e-zdravja v slovenskem zdravstvenem sistemu morala še okrepiti, posebno pozornost pa bo potrebno nameniti varnosti osebnih podatkov.

Rok Drnovšek, Marija Milavec Kapun: Izzivi in priložnosti informatike v zdravstveni negi

Informatika v zdravstveni negi postaja relevantno specialno področje zdravstvene nege, ki se osredotoča na vključevanje sodobne informacijsko komunikacijske tehnologije v delovne procese zdravstvenih organizacij. Digitalizacija vpliva na način dela in procesiranja podatkov in s tem spreminja vloge zdravstvenih delavcev ter pacientov. Zaradi naraščajoče pomembnosti lahko pričakujemo, da bo informatika v zdravstveni negi postala komplementarno področje v zdravstvu, četudi njena vloga v kliničnem okolju še ni popolnoma jasna. Predstaviti želimo objavljene izsledke mednarodne raziskave o trendih informatike v zdravstveni negi, ki jo je izvedla raziskovalna skupina Mednarodnega združenja za medicinsko informatiko, sekcije za zdravstveno nego – študenti in profesionalni delavci v razvoju. V anketi so sodelovali strokovnjaki, aktivni na področju informatike v zdravstveni negi iz držav Azije, Evrope, celotne Amerike in Avstralije. V rezultatih so zbrana mnenja informatikov v zdravstveni negi, ki opozarjajo na aktualne in potencialne izzive tega področja. Po mnenju anketirancev je informatika v zdravstveni negi razvijajoče se področje z velikim potencialom in možnostjo vsestranske uporabnosti v stroki. Prioritetno je uporabna kot orodje za raziskovalno dejavnost, implementacijo standardiziranih jezikov, izobraževanje in podporo pri odločanju v kliničnem okolju. Kot glavne izzive so v raziskavi izpostavili nezadovoljstvo nad financiranjem informatike v zdravstveni negi in neustrezno zasnovo programske opreme za dokumentiranje zdravstvene nege. Razvoj informacijskih rešitev mora temeljiti na

neprekinjenem sodelovanju med njihovimi snovalci in medicinskimi sestrami, kar omogoča razvoj in uspešno implementacijo programske opreme, prilagojene potrebam stroke. Izsledki raziskave imajo lahko uporabno vrednost za slovensko strokovno javnost, saj ponujajo referenčni okvir in izhodišča za raziskovalno, razvojno in izobraževalno dejavnost ter za spodbujanje interdisciplinarnega sodelovanja pri razvoju in implementaciji trajnostnih informacijskih rešitev.

Alja Mikec, Samo Kotnik: Model ocene vedenja za srčno-žilno zdravje pri starejših

Srčno-žilne bolezni so vrsta obolenj, ki prizadenejo obtočila ter predstavljajo vodilni vzrok prezgodnje smrti starejše populacije v EU. Z vse večjim deležem populacije nad 65 let, ki naj bi leta 2050 obsegala 35 %, predstavlja največji izziv zagotoviti zdravo in kvalitetno staranje. Pri spremljanju pacientov bi nam koristil model, s katerim bi medicinska sestra v referenčni ambulanti ali patronažna medicinska sestra na domu ocenila vedenje v povezavi s srčno-žilnim zdravjem in tako vplivala na boljše zdravstvene izide. Predmet odločitvenega modela je stopnja tveganega vedenja za srčno-žilne bolezni pri starejši populaciji. Za utemeljitev raziskovalnega problema smo uporabili deskriptivno metodo dela. S pomočjo večparametrskega modela, izdelanega s programom DEXi, želimo oceniti vedenje posameznika, ki je lahko nizko, srednje ali visoko tvegano za srčno-žilne bolezni. S pomočjo teh znanj bi nudili ustrezno zdravstveno vzgojo ter pomoč pri spreminjanju življenjskega sloga v okviru primarnega zdravstvenega varstva. S pomočjo modela bi lahko izboljšali zdravstvene izide, preprečili zaplete srčno-žilnih bolezni in starejšim omogočili kakovostno staranje. Osnovna zamisel je torej, da lahko zdravstveni delavci s pomočjo postavljenih kriterijev za oceno stopnje tveganega vedenja starostnikov v povezavi s srčno-žilnimi obolenji le-ta ocenijo glede na ponujene možnosti odgovorov v modelu. Ugotovili smo, da naš model pripomore k ugotavljanju stopnje tveganega vedenja in ogroženosti ter pomaga pri določanju tistih, ki bi s strani zdravstvenih delavcev najbolj potrebovali pomoč oziroma zdravstveno vzgojo.

Lara Menhart, Nika Rožmanec, Draga Štromajer, Vladislav Rajkovič: Model za pomoč pri izbiri naprave za izvajanje testov koagulacije

Število pacientov, ki potrebujejo antikoagulantno zdravljenje, narašča. Ocenjuje se, da je prizadetih 0,5 % ljudi, starih od 50 do 59 let, in približno 8 % ljudi, starih nad 65 let. To pomeni vse večjo zasedenost antikoagulacijskih ambulant in vse več opravljanj meritev testov koagulacije. Namen prispevka je predstaviti model za izbiro najprimernejše naprave POCT za merjenje časa strjevanja krvi na pacientovem domu. Uporabljena je bila deskriptivna metoda pregleda literature in načrtovanje odločitvenega modela s pomočjo metode DEX in programskega orodja DEXi. Najbolj ustrezna naprava POCT je bila izbrana na podlagi treh osnovnih parametrov (ekonomski vidik, funkcionalnost, kakovost). Največjo težo pri odločanju so imele funkcije naprave, sledila je cena testnih lističev in kakovost. Vse ocenjevane naprave so dosegale vsaj minimalne standarde kakovosti.

Vesna Rugelj: Implementacija informatiziranih zdravstvenih procesov – zakaj nam ne gre?

Še nedolgo tega so bili informacijski sistemi v zdravstvu namenjeni le za potrebe obračuna opravljenih zdravstvenih storitev ter vodstvom bolnišnic za potrebe analiz in spremljanja stroškov poslovanja. V zadnjem desetletju se v bolnišnične informacijske sisteme uvaja vedno več modulov za evidentiranje in spremljanje strokovnih podatkov. Informacijske hiše imajo različne pristope pri informatizaciji procesov in dejavnosti, vodstva zdravstvenih zavodov pa za to namenjajo vedno več denarja. Uvedeni moduli niso zgolj digitalizirani obstoječi papirni obrazci, temveč uporabnika vodijo skozi proces dela, preko vključenih navodil, opozoril in kontrol vnosa podatkov jim nudijo podporo pri odločanju. Pričakovati bi bilo povečano število elektronsko nastalih in arhiviranih dokumentov in posledično zmanjševanje papirne dokumentacije. Kljub temu pa je uporaba strokovnih modulov, vključenih v informacijski sistem zavoda, redka. Z analiziranjem deleža uporabe različnih modulov za spremljanje strokovnih podatkov in aplikacij eZdravja ter pogovori z uporabniki informacijskega sistema Hipokrat smo ugotavljali vzroke za (pre)počasno implementacijo novih modulov v redno delo. Uporabniki najpogosteje uporabljajo aplikacije, ki so jih sami predlagali in/ali so sodelovali pri njihovem nastanku. Velik motivator za uporabo je tudi vzgled starejših sodelavcev in nadrejenih. Samo deklarativno rečena ali napisana obveznost jih ne prepriča, uporaba aplikacij pa se močno poveča, ko v informacijski sistem vključene kontrole preprečujejo nadaljnje aktivnosti (npr. tiskanje izvidov). Kot negativno motivacijo omenjajo do uporabnika neprijazne informacijske sisteme, preobsežno dokumentiranje, preslabo in nezadostno strojno opremo, premalo izobraževanj, nobenih nagrad za tiste, ki module uporabljajo, in nobene kazni za tiste, ki jih ne.

Tina Kamenšek, Špela Plesec, Tina Gogova, Marija Milavec Kapun: E-dokumentiranje in prihranek časa v zdravstveni negi

Dokumentiranje zajema vedno večji obseg delovnega časa medicinskih sester. Zahtevnost dokumentiranja narašča z naraščanjem kompleksnosti delovnih procesov, zato medicinskim sestram primanjkuje časa za delo z in ob pacientu. E-dokumentiranje je pogosto predstavljeno kot učinkovita rešitev omenjenega problema. Namen prispevka je s pregledom literature ugotoviti, ali z informacijsko tehnologijo podprto dokumentiranje v zdravstveni negi prispeva k prihranku časa zaposlenih. Opravili smo pregled literature v podatkovnih bazah CHINAL, MEDLINE in ERIC. Za iskanje smo uporabili ključne besede oziroma besedne zveze: *time efficiency, time documentation, time saving, nurse, nursing, healthcare professional, electronic health records, electronic medical records, EMR* in *EHR*. Vključitveni kriteriji so bili dostopnost članka v celotnem obsegu besedila, angleški jezik, da objava ni bila starejša od 10 let in da je obravnavala dokumentiranje medicinskih sester. Z raziskovanjem se je ugotovilo, da se je čas dokumentiranja medicinskih sester po vpeljavi e-dokumentiranja povečal iz 9 % na 23 % tedenske delovne obremenitve. Razlogi za to so predvsem uvajanje novega pristopa, ki je časovno zamudno, dvojno dokumentiranje v prehodnem obdobju, premalo usmerjenih usposabljanj in izobraževanj uporabnikov, vedno bolj obsežna vsebina ter osebne izkušnje in odnos zaposlenih do novosti v delovnem procesu. Uporabniki po uvedbi e-dokumentiranja navajajo težave z dostopnostjo in zastarelostjo opreme ter napake v tehničnem delovanju, kar moti potek dela. Dokumentiranje v zdravstveni negi, podprto z informacijsko tehnologijo, torej ne prispeva k prihranku časa medicinskih sester. Glede na analizo glavnih razlogov podajamo predloge za izboljšavo. Slednje vidimo predvsem v postopnem uvajanju e-dokumentacije, organiziranem izobraževanju in usposabljanju medicinskih sester, pregledu obsega in prilagoditvi dokumentiranja z izločanjem podvojenih in nepotrebnih vsebin. Dolgoročno se pričakuje prilagoditev na nov način dokumentiranja, časovni prihranek in lažjo obdelavo podatkov.

Janja Lorber, Nino Fijačko, Mateja Lorber, Gregor Štiglic: Zadovoljstvo obravnavanih oseb s spletno aplikacijo za vizualizacijo tveganja pri zgodnjem odkrivanju sladkorne bolezni tipa 2

V referenčnih ambulantah je zgodnje prepoznavanje oseb, ki so izpostavljene tveganju za razvoj sladkorne bolezni tipa 2, ena izmed pomembnih nalog diplomirane medicinske sestre oz. diplomiranega zdravstvenika. V tem povzetku predstavljamo rezultate preliminarne študije uvajanja napovednih modelov za zgodnje odkrivanje nediagnosticiranega prediabetesa in sladkorne bolezni tipa 2, ki temeljita na podatkih iz elektronskih zdravstvenih zapisov iz petih slovenskih zdravstvenih domov. Poleg trenutne ocene tveganja omogoča razvita aplikacija tudi prikaz tveganja v prihodnjih 10 letih, kar omogoča uporabniku bolj učinkovito zdravstveno-vzgojno delo v referenčni ambulanti. V okviru študije smo uporabili prilagojen in preverjen vprašalnik za oceno zadovoljstva obravnavanih oseb (n = 53) v obliki spletne aplikacije. Po prikazu delovanja spletne aplikacije so posamezniki odgovorili na vprašanja, ki so se nanašala na kazalnike kakovosti in uporabnosti spletne aplikacije SLORISK. Podatki so bili zbrani v referenčni ambulanti na področju severovzhodne Slovenije v obdobju od oktobra 2017 do aprila 2018. Uporabniki so na lestvici od 1 do 5 najvišjo oceno pripisali razumljivosti aplikacije (povprečje 4,8), sledila pa je koristnost aplikacije (povprečje 4,7). Splošna ocena zadovoljstva uporabnikov z aplikacijo je na lestvici od 1 do 10 znašala 8,5. Rezultati študije kažejo na dobro sprejetost aplikacije pri obravnavanih osebah, saj omogoča vizualizacijo tveganja za nastanek oz. prisotnost nediagnosticirane sladkorne bolezni tipa 2, lažje svetovanje in podajanje zdravstvenih priporočil glede zmanjševanja dejavnikov tveganja za razvoj sladkorne bolezni 2. Potrebne bodo dodatne študije za oceno zadovoljstva z aplikacijo pri diplomiranih medicinskih sestrah oziroma diplomiranih zdravstvenikih.

Rok Drnovšek, Marija Milavec Kapun, Vladislav Rajkovič, Saša Šajn Lekše, Brigita Jeretina, Uroš Rajkovič: Analiza kakovosti načrtov zdravstvene nege – primerjava uporabnosti dveh aplikacij za dokumentiranje v zdravstveni negi

Elektronsko beleženje, hranjenje in upravljanje podatkov pripomore k večji uspešnosti in učinkovitosti organizacij, zato se tudi v zdravstveni dejavnosti pojavljajo informacijske rešitve z namenom izboljšanja delovnih procesov in kakovosti oskrbe. Zdravstvena nega temelji na neprekinjenem zbiranju in analizi velike količine podatkov, kar zahteva uporabo ustreznih pristopov za elektronsko dokumentiranje zdravstvene nege. V raziskavi smo primerjali uporabnost dveh aplikacij za izdelavo načrta zdravstvene nege: E dokumentacija v patronažni zdravstveni negi in Think!Med Clinical™. Analizirali smo načrte zdravstvene nege, ki so jih izdelali dodiplomski študenti rednega študijskega programa Zdravstvena nega. Vsak sodelujoči študent

je v okviru raziskave uporabljal eno izmed aplikacij. Tričlanska strokovna komisija je vrednotila pravilnost načrtov zdravstvene nege ter naredila analizo prednosti, slabosti, priložnosti in nevarnosti uporabe posamezne aplikacije. Aplikacija Think!Med Clinical™ je hitra in preprosta za uporabo, vendar uporabnika usmerja v načrtovanje generičnih načrtov zdravstvene nege, ki niso individualno prilagojeni pacientovim potrebam. Aplikacija E-dokumentacija v patronažni zdravstveni negi je zamudna in zahtevna za uporabo, vendar uporabnika usmerja k kritičnemu razmišljanju in načrtovanju pacientovim potrebam individualno prilagojenih načrtov zdravstvene nege. Aplikacija Think!Med Clinical™ v primerjavi z aplikacijo E dokumentacija v patronažni zdravstveni negi manj dosledno sledi procesu zdravstvene nege, kar se kaže v pomanjkljivi strukturi izdelanih načrtov zdravstvene nege. Aplikacije za dokumentiranje zdravstvene nege morajo uporabnika spodbujati h kritičnemu razmišljanju, procesni metodi dela in celostni obravnavi pacienta, saj tako pripomorejo k dvigu kakovosti oskrbe. Medicinske sestre morajo aktivno vključevati svoje strokovno znanje pri snovanju, implementaciji in kritičnem testiranju aplikacij za dokumentiranje v zdravstveni negi.

Zaključek

Ob zaključku rednega letnega srečanja je potekal sestanek članov SIZN, kjer je predsednica sekcije doc. dr. Ema Dornik podala poročilo o delu SIZN za leto 2018. Poleg tega je Sekcija opredelila načrte in usmeritve za nadaljnje delo. Člani smo srečanje zaključili z naslednjimi sklepi:

Še naprej moramo skrbeti za večjo prepoznavnost informatike v zdravstveni negi z bolj aktivno vlogo članov SIZN. V SIZN bomo vztrajali pri prizadevanjih za aktivno delo sekcije društva.

Treba je krepiti aktivnosti na področju raziskav in razvoja dokumentiranja v ZN in pridobivanju finančnih sredstev za te naloge.

Sodelovati je potrebno na področju informacijske varnosti z upoštevanjem smernic iz mednarodne raziskave, ki je bila predstavljena na kongresu.

Celotne prispevke in povzetke prispevkov članov SIZN in ostalih sodelujočih na kongresu MI'2018 lahko preberete v jubilejnem zborniku.

Zahvala

Zahvaljujemo se SDMI, ki je omogočilo naše srečanje. Hvala tudi članom SIZN, ki sodelujejo v naših aktivnostih, ter avtorjem za sodelovanje na srečanju.

■ **Infor Med Slov** 2018; 23(1-2): 39-42