Ispitivanje razlike u znanju i stvarnome ponašanju po pitanju sigurnosti na internetu među studentima na Medicinskom fakultetu u Osijeku

Hardi, Ivana

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
MEDICINSKI FAKULTET OSIJEK

PREDDIPLOMSKI SVEUČILIŠNI STUDIJ MEDICINSKO LABORATORIJSKA DIJAGNOSTIKA

Ivana Hardi

ISPITIVANJE RAZLIKE U ZNANJU I STVARNOM PONAŠANJU PO PITANJU SIGURNOSTI NA INTERNETU MEĐU STUDENTIMA NA MEDICINSKOM FAKULTETU U OSIJEKU

Završni rad

Osijek, 2022.

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
MEDICINSKI FAKULTET OSIJEK

PREDDIPLOMSKI SVEUČILIŠNI STUDIJ MEDICINSKO LABORATORIJSKA DIJAGNOSTIKA

Ivana Hardi

ISPITIVANJE RAZLIKE U ZNANJU I STVARNOM PONAŠANJU PO PITANJU SIGURNOSTI NA INTERNETU MEĐU STUDENTIMA NA MEDICINSKOM FAKULTETU U OSIJEKU

Završni rad

Osijek, 2022.

Rad je ostvaren na Medicinskom fakultetu u Osijeku.

Mentor rada: doc.dr.sc. Krešimir Šolić dipl.ing.

Rad sadrži 20 listova**,** 1 tablicu i 5 slika.

SADRŽAJ

1. UVOD

U današnje vrijeme svakodnevni poslovi u različitim ustanovama prožeti su korištenjem interneta i elektroničkih sustava te su oni tako i nezaobilazni dio svih zdravstvenih ustanova čemu nam svjedoče Bolnički informacijski sustav (BIS) i Laboratorijski informacijski sustav (LIS). U medicini je prisutna sve veća informatizacija, a digitalizacija i povezivanje medicinske dokumentacije uvelike je doprinijela kvaliteti i kvantiteti rada zdravstvenih djelatnika kao i većem povjerenju korisnika. No, istovremeno je uzrokovala probleme prilikom zaštite privatnosti pacijenata koji za medicinske svrhe povjeravaju mnogo svojih osobnih podataka. Iz tih razloga proizlazi kako je od izuzetne važnosti da i studenti biomedicine, kao i svi budući i sadašnji zdravstveni djelatnici, budu kvalitetno educirani na području sigurnosnog korištenja interneta, ne samo zbog sigurnosti njihovih pacijenata, nego i radi sigurnosti vlastitih podataka. Potrebno je na adekvatan način zaštiti osobne podatke kako ne bi došlo do njihove krađe ili zlouporabe. To podrazumijeva korištenje kvalitetno odabrane zaporke te valjane načine memoriranja iste, korištenje antivirusne zaštite na računalima, izrade sigurnosnih kopija, izbjegavanje posjećivanja raznih ponuđenih reklamnih stranica, oprez pri otvaranju sumnjivih mailova i tomu slično.

Činjenica je da mlađa populacija odrasta uz suvremenu tehnologiju nije nužno preduvjet da znaju i s velikom sigurnošću koristiti internet. Veći stupanj školske naobrazbe može omogućiti veće znanje i sposobnost za daljnju sigurnost i privatnost korištenja, pohranu osobnih podataka i općenito obitavanja u online okruženju. Međutim, bez obzira na uvelike rasprostranjenu edukaciju u našem društvu, ne može se utjecati na svakog pojedinca kako bi samostalno kvalitetno i valjano koristio dostupna sredstva ne samo edukacije, već i dostupnih sredstava zaštite i pohrane osobnih podataka. Unatoč tome, moguće je putem raznih medija doprinijeti osvještavanju velikog broja ljudi, što već je znatan pomak u sigurnosti korištenja internetom.

1.1. Informacijski sustavi u bolnicama

U bolnicama je od iznimne važnosti kvalitetna logistička potpora, informacijska te komunikacijska povezanost radi što lakšeg i kvalitetnijeg liječenja pacijenata, stoga postoje informacijski sustavi koji upravo to i omogućavaju.

1.1.1. Bolnički informacijski sustav

Nekakav oblik bolničkog informacijskog sustava postoji otkad postoji bolnički način liječenja pacijenata, ali suvremeni bolnički informacijski sustav (BIS) obavezno uključuje korištenje elektroničkih računala te računalnih mreža (1). Glavni zadatci BIS-a su podrška djelotvornoj opskrbi pacijenata, racionalno korištenje potrošnog materijala i lijekova, automatizirano administriranje, smanjenje vremena potrebnog za pohranu informacija te osiguravanje informacija u upravne, stručne i znanstvene svrhe (2). Postojanje takvog jedinstvenog informacijskog sustava u sklopu bolničke ustanove čini komunikaciju među liječnicima i ostalim osobljem znatno lakšom.

1.1.2. Laboratorijski informacijski sustav

Laboratorijski informacijski sustav (LIS) je program koji omogućava unos te obradu i pohranu podataka koji su nastali kao rezultat laboratorijskih pretraga, no obuhvaća i računalnu opremu koja je potreba kako bi se svi ti procesi odvijali (1). On pruža cjelovitu potporu radu bolničkih laboratorija, pretežito laboratorija koji na dnevnoj bazi obrađuju veći broj uzoraka (npr. biokemijski i hematološki laboratorij) (3). On može djelovati unutar laboratorija, izoliran od ostatka bolnice ili pak može biti uklopljen u bolnički informacijski sustav te uvelike olakšati i ubrzati proces naručivanja pretraga, obavljanja pretraga te prikaza rezultata tih istih pretraga i samim time ubrzava proces otkrivanja dijagnoze i pravovremenog liječenja.

1.2. Digitalizacija i zaštita privatnosti pacijenata

Važnost zaštite osobnih podataka pacijenata prepoznata je još iz vremena prije Krista te je i sadržana u Hipokratovoj zakletvi: „Što po svojem poslu budem saznao ili vidio, pa i inače, u saobraćaju s ljudima, koliko se ne bude javno smjelo znati, prešutjet ću i zadržati tajnu“ (4). Pacijentu je zajamčena zaštita privatnosti medicinske dokumentacije pomoću bolničkog informacijskog sustava (BIS) i Laboratorijskog informacijskog sustava (LIS). Zahvaljujući njima liječnici gotovo odmah imaju uvid u pacijentove nalaze, čime se izbjegava mogućnost ikakvog gubljenja prijašnjih papirnatih dokumenata, ali i mogućnost da neka druga, za to neovlaštena osoba

vidi povjerljive podatke. Za pristup informacijskim sustavima medicinsko osoblje se mora prijaviti jedinstvenim korisničkim imenom i lozinkom koja se po pravilu mijenja svakih 90 dana, odnosno svaka 3 mjeseca. Liječnici sa drugih odjela ne mogu imati uvid u pacijentovu medicinsku dokumentaciju, osim ako jedan liječnik ne uputi svog pacijenta drugom zbog nastavka liječenja (2). Moderni LIS sustavi se u pravilu koriste mrežnim preglednicima kao klijentima te je na taj način omogućen upis i dohvat podataka iz LIS-a na bilo kojem računalu koje ima instaliran mrežni preglednik. Pristup LIS-u je strogo ograničen upravo iz sigurnosnih razloga, kako bi se omogućila privatnost i tajnost podataka pacijenata (1).

1.3. Zaštita osobnih podataka na internetu

Informatizacija i tehnološki napredak su uvelike doprinijeli olakšanoj i bržoj obradi, pohrani i pristupu podataka i informacijama, no istovremeno i mnoge opasnosti te je zbog toga vrlo bitna zaštita osobnih podataka. Zaštita podataka provodi se s ciljem sprječavanja krađe podataka ili zlonamjerne manipulacije podatcima (5). Pitanja privatnosti i zaštite osobnih podataka regulirana su međunarodnim konvencijama i obaveza je za sve članice Europske unije. 1981.godine Vijeće Europe donijelo je Konvenciju za zaštitu osoba vezano za automatiziranu obradu osobnih podataka, poznatu kao i Konvencija 108 (po rednom broju donošenja). Konvencija je i danas podloga zaštite osobnih podataka, a njezina svrha je osiguravanje prava i poštovanje temeljnih sloboda svake osobe (6).

1.3.1.Pravo na privatnost kao temeljno ljudsko pravo

U smislu zaštite osobnih podataka pojedinca i podizanjem prava na privatnost na razinu temeljnih ljudskih prava putem Povelje Europske Unije o temeljnim pravima koja je stupila na snagu 1. prosinca 2009. godine, te je ona na razini Europske unije danas svojevrsna sigurnost zaštite osobnih podataka. Iz te Povelje je proizašla Opća uredba o zaštiti podataka (6).

1.3.2. Opća uredba o zaštiti podataka

Opća uredba o zaštiti podataka (NN, SL EU L119), poznata i kao GDPR – *General Data Protection Regulation,* stupila je na snagu 25. svibnja 2018. godine te se od tada primjenjuje na sve članice Europske Unije, pa tako i Republike Hrvatske. Svrha zaštite osobnih podataka je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka te je osigurana svakoj fizičkoj osobi bez obzira na njeno državljanstvo i prebivalište te neovisno o rasi, boji kože, jeziku, vjeri, spolu, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu, rođenju, naobrazbi, imovini, društvenom položaju ili drugim osobinama (7). U Republici Hrvatskoj Zakonom o provedbi Opće uredbe o zaštiti podataka reguliran je nadzor nad prikupljanjem, obradom osobnih podataka i o slobodnom kretanju takvih podataka. Pod osobnim podatcima se smatraju oni iz kojih se s velikom vjerojatnošću može utvrditi identitet pojedinca. Podatci koji se GDPR-om štite su osnovni podatci (ime i prezime, broj osobne iskaznice te lokacijski podatci), zdravstveni karton, biometrijski podatci (npr. sken rožnice ili otisak prsta), podatci s kreditnih kartica, genetski podaci (npr. DNA), vjerska i filozofska uvjerenja, ekonomsko stanje, etička pripadnost, seksualna orijentacija, spolni život, članstvo u sindikatu, IP adrese, kolačići u pregledniju, osobne poruke e-pošte te pseudonimizirane podatke. Ukoliko postoji potreba za obradom podataka, određuju se svrha i sredstva za obradu podataka te voditelj obrade. Oboje mora biti utvrđeno pravom Unije ili pravom državne članice. Pod voditeljem obrade smatra se svaka fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo pravno tijelo (8). U Republici Hrvatskoj Zakonom o zaštiti osobnih podataka osnovana je Agencija za zaštitu osobnih podataka kao samostalno i neovisno tijelo s temeljnom zadaćom provedbe nadzora nad obradom osobnih podataka (9).

2. CILJ

Cilj ovog istraživanja je ispitati stvarno rizično ponašanje studenata 2. i 3. godine na Medicinskom fakultetu te ga usporediti sa njihovom samoprocjenom rizičnog ponašanja na internetu te dodatno ispitati razinu njihovog znanja i razinu svjesnosti o online rizicima.

3. ISPITANICI I METODE

3.1. Ustroj studije

Istraživanje je provedeno kao presječna studija.

3.2. Ispitanici

Ispitanici su studenti 3. godine Preddiplomskog studija medicinsko-laboratorijske dijagnostike te studenti 2. godine Integriranog preddiplomskog i diplomskog studija medicine na Medicinskom fakultetu u Osijeku.

3.3. Metode

Za ovo istraživanje korišten je online anonimni validirani upitnik čiji su autori Tena Velki i Krešimir Šolić. Upitnik se sastoji od četiri subskale. Prva subskala za simulaciju stvarnog rizičnog ponašanja stavlja ispitanike u potencijalne rizične situacije s kojima bi se oni mogli susrest pri korištenju računala i interneta (npr. Ukoliko želite primati obavijesti i naše besplatne promotivne materijale molim Vas upišite Vašu e-poštu) na koje ispitanici mogu, ali i ne moraju dati odgovore te pitanja na koja odgovaraju sa da/ne. Preostale tri subskale ispitanici odgovaraju na pitanja koja se boduju po Likterovoj skali sa 5 stupnjeva. Subskala samoprocjene rizičnog ponašanja se sastoji od 4 pitanja (primjer Koliko često posuđujete pristupne podatke za Vašu e-poštu (korisničko ime i lozinka) prijateljima ili rođacima?) sa ponuđenih 5 stupnjeva odgovora od „nikad“ do „uvijek“. Iduća subskala se odnosi na važnost pravilnog i sigurnog korištenja računalnih sredstava s 4 pitanja (poput Kako biste procijenili koliko je važno provjeravanje prijenosnih medija (npr. CD/DVD, USB memorija i sl.) od virusa prije upotrebe?) gdje su stupnjevi odgovora od „nije važno“ do „jako važno“. Posljednja subskala se odnosi na rizično ponašanje ispitanika pri korištenju interneta koja uključuje 5 pitanja (primjer Kako biste procijenili koliko je rizično hakiranje Vašeg osobnog

računala, prijenosnog računala ili pametnog telefona?) na skali Likertova tipa sa 5 stupnja od „nema rizika“ do „jako rizično“ (10).

3.4. Statističke metode

Kategorijski podaci su predstavljeni apsolutnim i relativnim frekvencijama. Numerički podatci su opisani aritmetičkom sredinom i standardnom devijacijom. Normalnost distribucije ispitana je Shapiro-Wilksovim testom.

Povezanost kategorijskih varijabli testirano je Hi-kvadrat testom. Za ispitivanje korelacije simulacije i stvarnog ponašanja korišten je neparametrijski Spearmanov test korelacije. Statistička analiza je učinjena programskim sustavom MedCalc (inačica 20.110., MedCalc Software bvba). Sve P vrijednosti dobivene u statističkoj analizi smatraju se značajnim ako su manje od $\alpha=0,05$ te su dvostrane.

3.5. Etička načela

Prije provođenja ovog istraživanja dobivena je suglasnost Etičkog povjerenstva Sveučilišta J. J. Strossmayera u Osijeku Medicinskog fakulteta Osijek (KLASA: 602-04/22-08/02; URBROJ: 2158-61-46-22-73; Osijek, 1. travnja 2022.)

4. REZULTATI

4.1. Osnovna obilježja ispitanika

Ukupno je sudjelovao 91 ispitanik i osnovna obilježja ispitanika su prikazana u Tablici 1. Raspon godina ispitanika kreće se od 18 do 25 te je prosječna dob ispitanika je bila $\bar{x}$ =20,0 (SD=1,1).

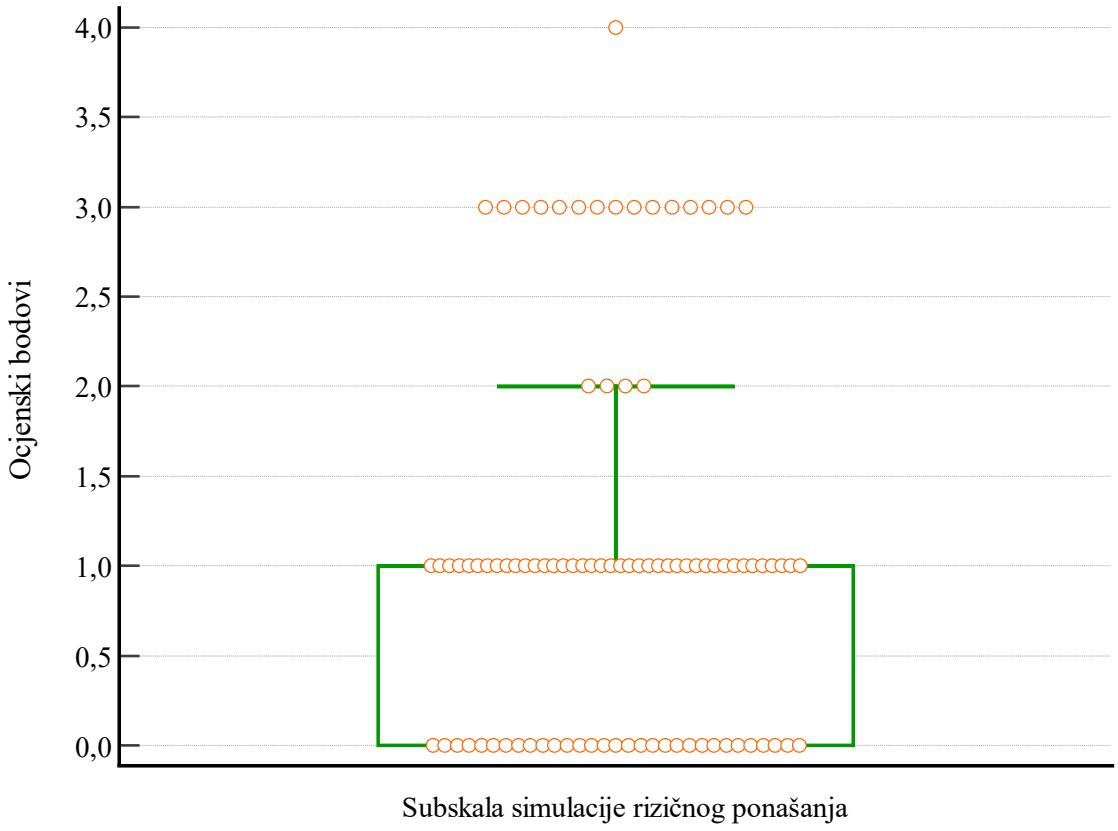
Tablica 1. Osnovna obilježja ispitanika

	Broj (%)	P*
Studij		
MLD	25 (27)	<0,001
Medicina	66 (73)	
Spol		
M	25 (27)	
Ž	66 (73)	<0,001
UKUPNO	91 (100)	

*Hi-kvadrat test

4.2. Ocjene subskala

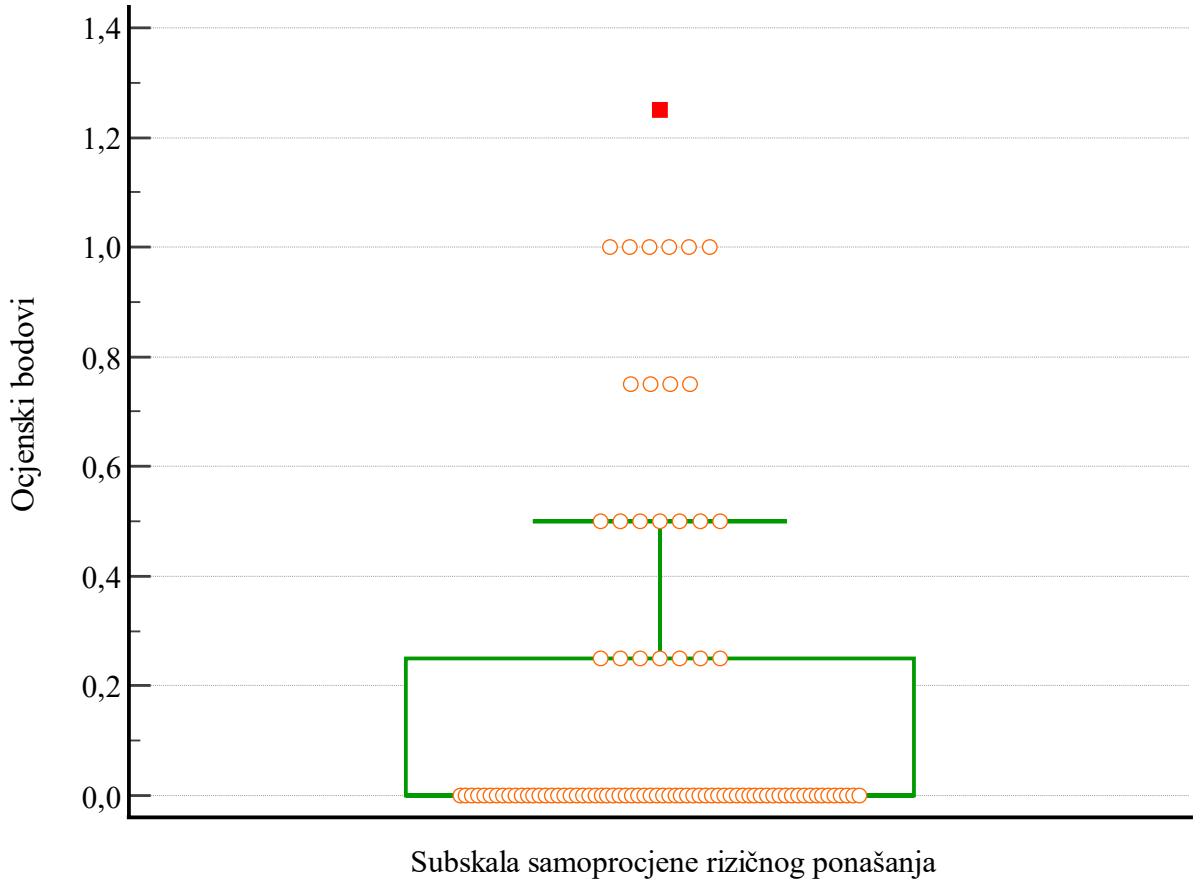
Prosječna ocjena subskale simulacije rizičnog ponašanja svih ispitanika iznosi $\bar{x} = 1{,}07$ uz SD = 1,07 (Slika 1.).



Slika 1. Prikaz ocjena subskale simulacije rizičnog ponašanja

U prvoj subskali upitnika za simulaciju stvarnog rizičnog ponašanja koja stavlja ispitanike u potencijalne rizične situacije s kojima bi se oni mogli susresti pri korištenju računala i interneta, samo 3 ispitanika (3 %) je stavilo da želi primati obavijesti na e-mailu, 21 ispitanik (23 %) je odabrao da želi putem e-pošte primiti besplatni antivirusni softver, te 18 ispitanika (19 %) upisalo svoju e-mail adresu ukoliko žele primati obavijesti i besplatne promotivne materijale.

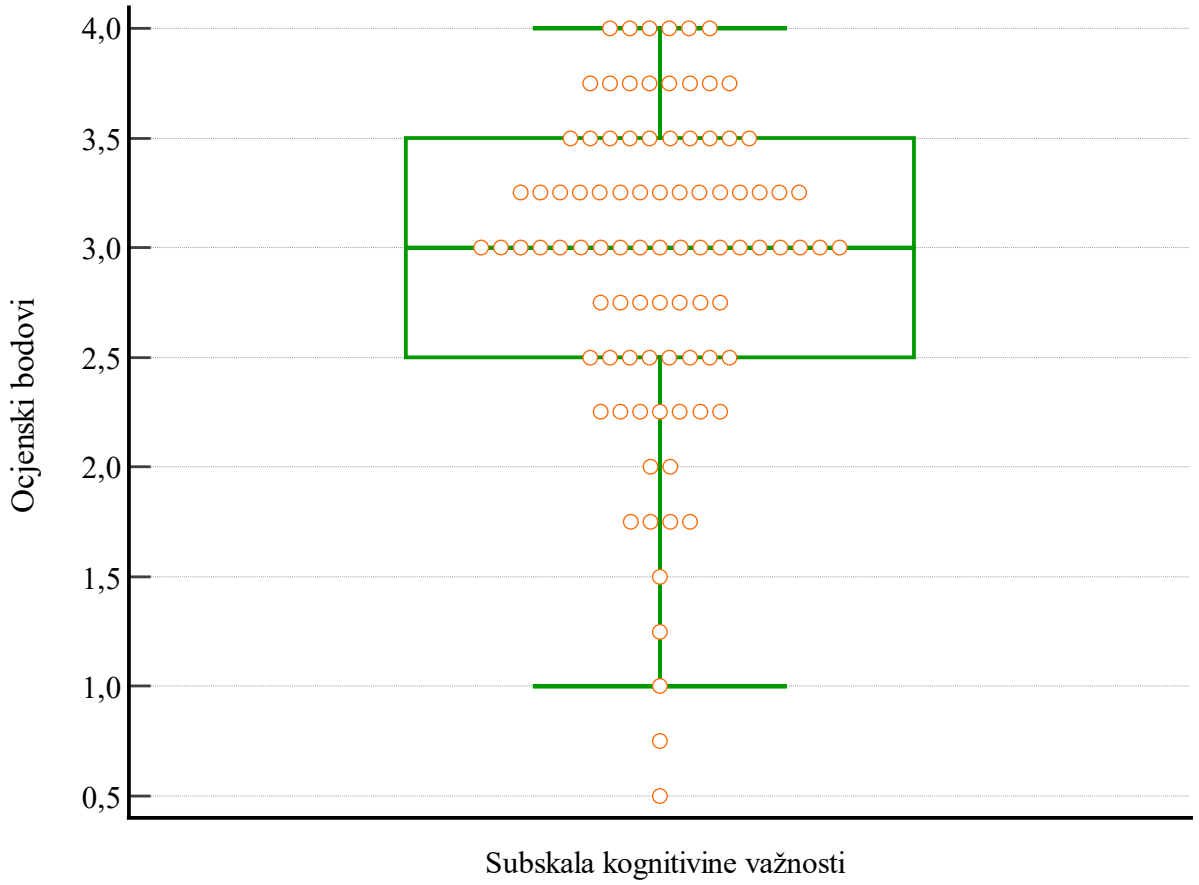
Prosječna ocjena subskale samoprocjene rizičnog ponašanja iznosi $\bar{x} = 0{,}17$, SD = 0,32 (Slika 2.).



Slika 2. Prikaz ocjena subskale samoprocjene rizičnog ponašanja

Samoprocjena ispitanika je na visokoj razini.

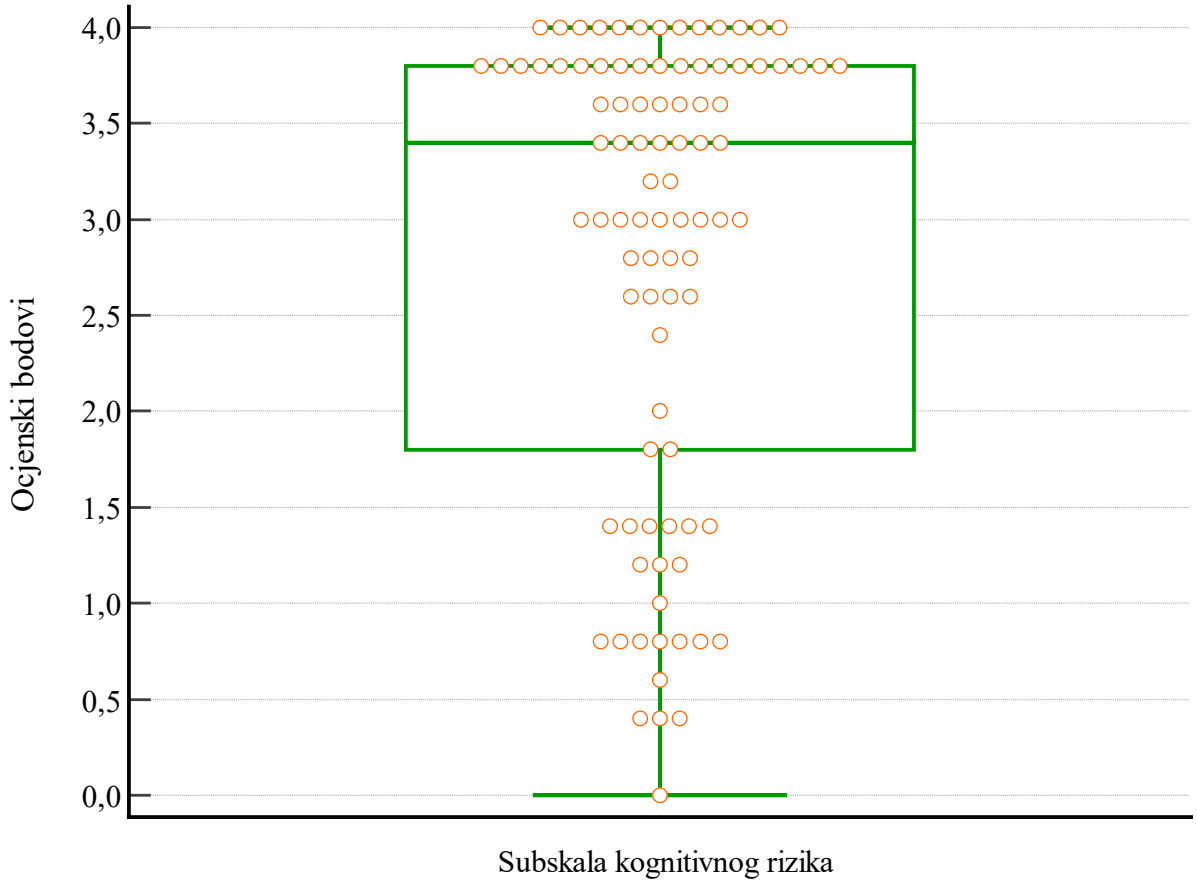
Prosječna ocjena subskale kognitivne važnosti $\bar{x} = 2{,}92$, SD = 0,73 (Slika 3.).



Slika 3. Prikaz ocjene subskale kognitivne važnosti

Ispitanicima je bilo teško odrediti važnost pravilnog i sigurnog korištenja računalnih sredstava te je većina odgovarala sa „nisam siguran“.

Prosječna ocjena subskale simulacije kognitivnog rizika iznosi $\bar{x} = 2{,}82$, SD = 1,19 (Slika 4.).

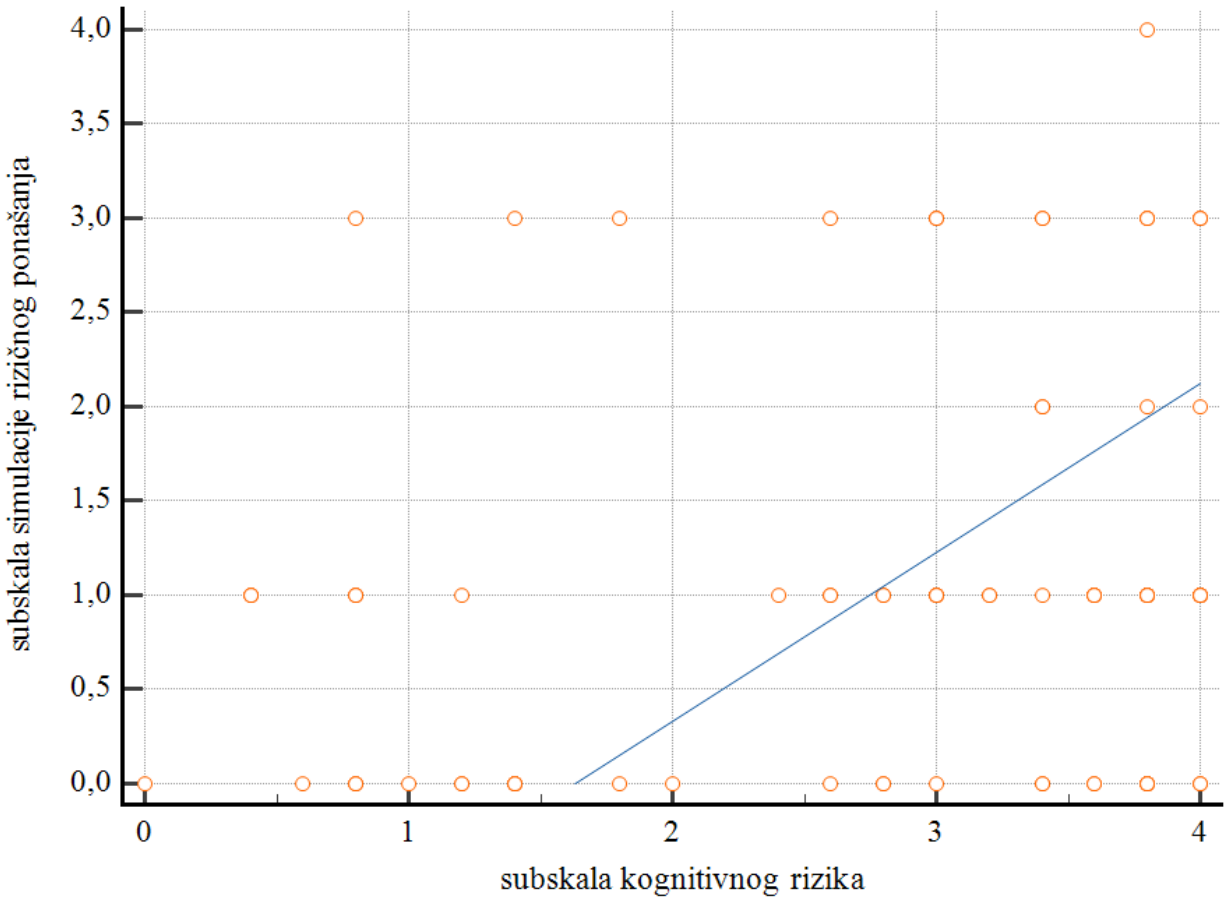


Slika 4. Prikaz ocjena subskale kognitivnog rizika

Na posljednje pitanje u upitniku, koje je trik pitanje da daju svoju lozinku radi provjere kvalitete sigurnosti, 55 ispitanika (60 %) ju je unijelo.

4.3. Korelacija subskale simulacije rizičnog ponašanja i kognitivnog rizika

Spearmanov test pokazuje slabu pozitivnu, ali statistički značajnu korelaciju subskale kognitivnog rizika i subskale simulacije rizičnog ponašanja sa koeficijentom korelacije rho = 0,247 te 95%-tnim intervalom pouzdanosti od 0,044 do 0,431 uz P = 0,02 (slika 5).



Slika 5. Prikaz korelacije subskala simulacije rizičnog ponašanja i kognitivnog rizika

5. RASPRAVA

U istraživanju je sudjelovao ukupno gotovo sto ispitanika, studenti sa 3.godine Preddiplomskog studija medicinsko-laboratorijske dijagnostike te druge godine integriranog preddiplomskog i diplomskog studija medicine Medicinskog fakulteta u Osijeku.

Čini se kako postoji blaga korelacija između subskale simulacije rizičnog ponašanja i subskale kognitivnog rizika. Studenti shvaćaju kako postoji rizik pri korištenju interneta i računala te su zbog te svjesnosti na opreznu pri korištenju istih. Sa većim povećanje svjesnosti za očekivati je kako će se koristit računala i internet sa smanjim rizikom.

Prosječna ocjena subskale stvarnog rizičnog ponašanja je nešto manja u odnosu na prijašnje istraživanje (10). Mlađe generacije se od malih nogu koriste računalnima i Internetom te je ovo vjerojatno uvelike doprinijelo činjenici da su mladi upoznati s rizicima i pravilima opreznog ponašanja na internetu i korištenjem računala, pa se sukladno tome i njihovo ponašanje je manje rizično.

U subskali samoprocjene rizičnog ponašanja ispitanici pokazuju nižu prosječnu ocjenu u odnosu na referentno istraživanje, što znači da imaju samopouzdanja u svoje znanje i vještine i njihova je samoprocjena na visokoj razini. Većina njih smatra kako se uopće ne ponaša rizično za vrijeme korištenja računala i Interneta te je to u skladu sa prijašnjim istraživanjem. Ipak, ispitanici ovog istraživanja smatraju kako se ponašaju nešto manje rizično nego ispitanici prijašnjeg istraživanja, što je vjerojatno povezano i s činjenicom da je četvrtina ispitanika odgovorilo kako koristi Internet otkad zna za sebe, a čak svaki drugi ispitanik kako ga koristi pola svoga života.

Svi ispitanici koji su sudjelovali u istraživanju shvaćaju rizike prilikom korištenja računala i Interneta, no nisu sigurni za veliku važnosti pravilnog i sigurnog korištenja računalnih sredstava poput stalnog ažuriranja i mijenjanja starih lozinki i provjeravanja prijenosnih medija (npr. CD, DVD, USB memorija) od virusa te je to razlog što u trećoj subskali većina njih odgovara sa „nisam siguran“.

To bi mogao biti jedan od razloga zašto bi se kroz školovanje trebalo više uputiti i obratiti pozornosti na niz preventivnih mjera radi zaštite od zaraze računala poput korištenja antivirusnog *softvera*, potrebama redovite nadogradnje i održavanje operacijskog sustava, korisnosti uključenog

firewalla, izbjegavati ignoriranje skenera pri upozorenju na virus te važnost redovite izrade rezervnih kopija vlastitih podataka jer ne postoji bolji način zaštite digitalnih podataka od sigurnosne kopije (11).

U posljednjoj subskali za rizično ponašanje pri korištenju Interneta prosječna ocjena subskale je vrlo slična s referentnim istraživanjem. Zanimljivo je primijetiti korelaciju analize samoprocjene i stvarnog rizika prilikom korištenja računala i Interneta.

Zabrinjavajući su rezultati posljednjeg pitanja upitnika koji je korišten za ovo istraživanje, a koje je trik pitanje tj. da daju svoju lozinku radi navodne provjere kvalitete i sigurnosti, čak nešto više od polovine ispitanika ju je pritom doista i unijelo. Nedostatak rezultata ovog pitanja je što se ne može znati jesu li lozinke koje su ispitanici unijeli prave i koriste li se one aktivno, no svakako je alarmantno što osobe sa visokom ocjenom samoprocjene rizičnog ponašanja tako olako upisuju svoje lozinke kada je očekivan i ispravan odgovor ostaviti navedeno polje prazno.

Još jedna od stvari koja ima veliki utjecaj na zaštitu osobnih podataka je kvalitetna lozinka. Lozinke su često na meti hakiranja radi manipulacije, krađe identiteta i novčane ucjene, stoga je vrlo važno odabrati kvalitetnu lozinku. Ona mora biti dovoljno kratka da ju korisnik može zapamtiti, ali ipak dovoljno sigurna i duga radi bolje zaštite od hakiranja. Po preporuci je koristiti kombinaciju veličine slova, imati zasebne lozinka za svaki račun, ne zapisivati lozinke u datoteku koja je spremljena na računalu niti na papir te mijenjati lozinku redovito, preporučuje se svaka tri mjeseca (12).

Dobiveni rezultati su na nekim poljima bolji nego na referentnom istraživanju. Učestalo se radi na poboljšanju edukacije i obrazovanju populacije, dokaz tome je i činjenica da je nedavno u osnovnim školama uvedena informatika kao obavezni nastavni predmet već od prvog razreda. U skladu s time, za očekivati je kako će u bližoj budućnosti korištenje znanja i vještina doprinijeti boljoj ocjeni pri većem postotku populacije koja sigurno koristi računala te Internet i kako bi rezultati budućih generacija, ukoliko bi se ovakvo istraživanje provelo na generacijama koje je obuhvatio kurikulum informatike kao obaveznog predmeta od prvog razred osnovne, bili zaista i bolji u usporedbi na dosadašnje rezultate.

6. ZAKLJUČAK

Temeljem provedenog istraživanja i dobivenih rezultata mogu se izvesti sljedeći zaključci:

- dobivena je postojeća blaga korelacija stvarnog rizičnog ponašanja ispitanika i njihove samoprocjene rizičnog ponašanja
- na subskali simulacije rizičnog ponašanja prosječna ocjena je niža od očekivanog, što znači da se ispitanici ne ponašaju rizično na računalima i internetu te su dobiveni rezultati bolji u usporedbi s referentnim istraživanjem
- prosječna ocjena je na subskali samoprocjene rizičnog ponašanja je niska te je niža i od prijašnjeg istraživanja, što znači da ispitanici imaju više samopouzdanja u svoje znanje i vještine i njihova je samoprocjena na visokoj razini
- prosječna ocjena na subskali kognitivne važnosti je 2,92, većina ih odgovara sa „nisam siguran“ za važnosti pravilnog i sigurnog korištenja računalnih sredstava
- na subskali kognitivnog rizika dobivena je nešto niža prosječna ocjena od referentnog istraživanja
- na trik pitanje je čak 55 ispitanika odalo svoju lozinku
- čak svaki drugi ispitanik tvrdi da koristi Internet pola svog života, a četvrtina njih otkad znaju za sebe

Ispitanici su pokazali da se znaju na računalima i internetu ponašati gotovo bez rizika te s pravom imaju više samopouzdanja u svoje znanje u odnosu na referentno istraživanje, koje vjerojatno proizlazi iz činjenice da ih koriste veći dio svog života. Samim time što su svjesni mogućeg rizika trebali bi biti oprezniji pri korištenju.

7. SAŽETAK

Ciljevi istraživanja: Ispitati stvarno rizično ponašanje studenata Medicinskog fakulteta te ga usporediti sa njihovom samoprocjenom rizičnog ponašanja na internetu i dodatno ispitati razinu njihovog znanja i razinu svjesnosti o online rizicima.

Nacrt studije: Istraživanje je provedeno kao presječna studija.

Ispitanici i metode: U istraživanju su sudjelovali studenti 3. godine Preddiplomskog studija medicinsko-laboratorijske dijagnostike te studenti 2. godine Integriranog preddiplomskog i diplomskog studija medicine te je ono provedeno na Medicinskom fakultetu u Osijeku. Za istraživanje se koristio validirani upitnik čiji su autori Krešimir Šolić i Tena Velki. Statistička obrada učinjena je u računalnom programu MedCalc.

Rezultati: Objedinjeno su objašnjeni i prikazani rezultati svih sudionika istraživanja i analizom korelacije između subskale simulacije rizičnog ponašanja i subskale kognitivnog rizika dobivena je slaba, ali pozitivna i statistički značajna korelacija. Ispitanicima je bilo teško odrediti važnost pravilnog i sigurnog korištenja računalnih sredstava te je većina odgovarala sa „nisam siguran“. Čak 60 % ispitanika je odalo svoju lozinku na trik pitanje. Ispitanici većinu svog života koriste Internet, 26 % njih otkad znaju za sebe, a 65 % pola svog života te su vjerojatno zbog toga i dobro upoznati s mogućim rizicima.

Zaključak: Dobiveni rezultati su djelomično zadovoljavajući i istovremeno su poticaj za daljnji napredak edukacije kako bi se što prije u što većoj mjeri osiguralo sigurno korištenje Interneta i računala.

Ključne riječi: internet, rizično ponašanje, sigurnost na internetu, zaštita osobnih podataka

8. SUMMARY

Examining the difference in knowledge and actual behavior regarding internet security among students at the Faculty of Medicine in Osijek

Objectives: Examine the actual risky behavior of medical students and compare it with their self-assessment of risky behavior on the Internet and further examine the level of their knowledge and awareness of online risks.

Study Design: Study was conducted as a cross-sectional study.

Participants and Methods: The research was partaken in by 3rd year students of the Undergraduate Study of Medical Laboratory Diagnostics and 2nd year students of the Integrated Undergraduate and Graduate Study of Medicine, and was conducted at the Faculty of Medicine in Osijek. The validated questionnaire was authored by Krešimir Šolić and Tena Velki. Statistical data was processed in the MedCalc computer program.

Results: The results of all research participants were jointly explained and presented, and the analysis of the correlation between the subscale of simulation of risk behavior and the subscale of cognitive risk showed a weak but positive and statistically significant correlation. Respondents found it difficult to determine the importance of proper and safe use of computer resources, and most responded with "I'm not sure". As many as 60 % of respondents gave their password to a trick question. Respondents had been using the Internet most of their lives, 26 % of them since they knew about themselves, and 65 % half of their lives, which is probably why they were well aware of the possible risks.

Conclusion: The obtained results are partially satisfactory and, at the same time, are an incentive for further progress of education in order to ensure the safe use of the Internet and computers as soon as possible.

Keywords: internet, risky behavior, internet security, personal data protection

9. LITERATURA

1. Kern J, Petrovečki M. Medicinska informatika. Medicinska naklada. Zagreb; 2009.
2. Poje I, Braović M. Bolnički informacijski sustav - prednosti i nedostaci u radu. Bilten Hrvatskog društva za medicinsku informatiku (Online) [Internet]. 2019 [pristupljeno 28.03.2022.];25(1):20-28. Dostupno na: https://hrcak.srce.hr/222611
3. "Laboratory Information System (LIS): Definition & Functions." Study.com, 23 January 2018. Dostupno na adresi: study.com/academy/lesson/laboratory-informationsystem-lis-definition-functions.html [pristupljeno 28.2.2022.]
4. Borovečki, A., Mustajbegović, J. i Jakšić, Ž. (2013). Izborni predmet iz područja medicinske etike: Kako primijeniti Hipokratovu zakletvu? Zagreb: Medicinski fakultet, Škola narodnog zdravlja „Andrija Štampar“
5. Varga M. Zaštita elektroničkih podataka. Tehnički glasnik [Internet]. 2011 [pristupljeno 31.03.2022.];5(1):61-73. Dostupno na: https://hrcak.srce.hr/85799
6. Velki T, Krešimir Š, ur. Izazovi digitalnog svijeta. Osijek: Fakultet za odgojne i obrazovne znanosti Sveučilišta Josipa Jurja Strossmayera u Osijeku; 2019
7. Velki T, Šolić K, Priručnik za informacijsku sigurnost i zaštitu privatnosti. Osijek: Fakultet za odgojne i obrazovne znanosti, Sveučilište Josipa Jurja Storssmayera u Osijeku; 2018.
8. Vodič kroz GDPR za početnike, GDPR informer [Interner, pristupljeno 29.5.2022.], dostupno na: https://gdprinformer.com/hr/vodic-kroz-gdpr
9. Agencija za zaštitu osobnih podataka [Internet, pristupljeno 29.5.2022.], dostupno na: https://azop.hr/
10. Velki T, Šolić K. Razvoj instrumenta za istraživanje socijalnog inženjeringa u populaciji studenata: Bihevioralno-kognitivni upitnik internetske sigurnosti (BKUIS). Policija i sigurnost [Internet]. 2020 [pristupljeno 28.03.2022.];29(4/2020):341-355. Dostupno na: https://hrcak.srce.hr/249659
11. CERT – savjeti za zaštitu [Internet, pristupljeno 4.6.2022.], dostupno na: https://www.cert.hr/savjeti/
12. Sini.hr – Kako napraviti sigurnu lozinku [Internet, pristupljeno 8.6.2022.]. Dostupno na: https://sini.hr/2021/04/kako-napraviti-sigurnu-lozinku/

10. ŽIVOTOPIS

Ime i Prezime: Ivana Hardi

Datum i mjesto rođenja: 23. studenog 2000., Vukovar

Adresa: Stjepana Radića 46, 32 000 Vukovar

Mobitel:091 604 9337

E-mail: hardi.ivana@gmail.com

Obrazovanje:

- 2007. - 2015. Osnovna škola Antuna Bauera, Vukovar
- 2015. – 2019. Jezična gimnazija Vukovar, Vukovar
- 2019.-2022. Preddiplomski sveučilišni studij medicinsko laboratorijske dijagnostike, Medicinski fakultet Osijek