Razvoj i validacija Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava (UZPK)

Velki, Tena; Šolić, Krešimir; Nenadić, Krešimir

Source / Izvornik: **Psihologijske teme, 2015, 24, 401 - 424**

Journal article, Published version
Rad u časopisu, Objavljena verzija rada (izdavačev PDF)

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:141:984004

Psihologijske teme, 24, 2015 (3), 401-424

Izvorni znanstveni rad – UDK – 004.7.056
004.451.056

Razvoj i validacija Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava (UZPK)

Tena Velki

Fakultet za odgojne i obrazovne znanosti u Osijeku

Krešimir Šolić

Medicinski fakultet u Osijeku

Krešimir Nenandić

Elektrotehnički fakultet u Osijeku

Sažetak

Dosadašnja su istraživanja pokazala kako je čovjek najslabija karika u sigurnosnom sustavu te kako ne postoji pouzdan način mjerenja rizičnosti čovjekova ponašanja u vidu narušavanja sigurnosti informacijskog sustava. Cilj je istraživanja bio razviti valjan i pouzdan instrument koji će mjeriti utjecaj korisnika na sigurnost informacijskog sustava. U tu je svrhu kreiran Upitnik znanja i rizičnog ponašanja korisnika informacijskog sustava (UZPK; Velki i Šolić, 2014; prema Velki, Šolić i Očević, 2014). Istraživanje je provedeno u tri vala prikupljanja podataka. Prvi se uzorak sastojao od 135 studenata druge godine preddiplomskog studija na kojem je provjerena konstruktna valjanost, pouzdanost i osjetljivost pojedinih subskala te odabrane odgovarajuće čestice. Drugi se uzorak sastojao od 211 studenata i zaposlenika, a na njemu su provjerene metrijske karakteristike poboljšanog instrumenta te je dobivena konačna verzija UZPK (*k*=33), koja se dijeli na dvije skale: Skala rizičnog ponašanja računalnih korisnika (*k*=17) [sastoji se od tri supskale: Supskala uobičajenih rizičnih ponašanja korisnika računala (*k*=6), Supskala održavanja osobnih računalnih sustava (*k*=6) i Supskala posuđivanja pristupnih podataka (*k*=5)] te Skala znanja o informacijskoj sigurnosti (*k*=16) (također se sastoji od tri supskale: Supskala stupnja sigurnosti računalne komunikacije (*k*=5), Supskala uvjerenja o sigurnosti računalnih podataka (*k*=5) i Supskala važnosti pravilne pohrane računalnih podataka (*k*=6). Treći se uzorak sastajao od 152 zaposlenika i na njemu je validiran UZPK. Dobivena je dobra konstruktna valjanost, sve skale i supskale imaju zadovoljavajuće metrijske karakteristike (pouzdanost i osjetljivost) te je dobivena i dobra kriterijska valjanost. Može se zaključiti kako Upitnik predstavlja valjan i pouzdan mjerni instrument, zadovoljavajućih psihometrijskih karakteristika.

Ključne riječi: validacija, rizično ponašanje računalnih korisnika, sigurnost informacijskog sustava, UZPK

✉ Tena Velki, Fakultet za odgojne i obrazovne znanosti u Osijeku, Sveučilište J.J. Strossmayera u Osijeku, 31000 Osijek, Cara Hadrijana 10. E-pošta: *tena.velki@gmail.com*

Uvod

Sveprisutnost interneta u poslovnom i privatnom životu daleko je nadmašila početni cilj međunarodne razmjene znanstvenih informacija. Javna informacijsko-komunikacijska mreža danas je širokopojasna rasprostranjena mreža koja obuhvaća velik broj manjih mreža te povezuje raznovrsne poslužitelje i širok spektar krajnjih korisnika. U današnje je vrijeme javna mreža postala važan resurs u svim granama ljudskog života te se zbog toga pojavila velika potreba za sigurnosnim i zaštitnim mehanizmima.

Nove napredne digitalne tehnologije omogućuju razvoj novih usluga u javnoj informacijsko-komunikacijskoj mreži što pogoduje naglom razvoju informacijskog društva. Trend je ovog razvoja personalizacija, koja omogućuje proizvođačima novih aplikacija bolju uslugu prilagođenu svakom pojedinom krajnjem korisniku. Iako personalizacija omogućuje bolju uslugu, ona od korisnika istovremeno zahtjeva otkrivanje znatne količine osobnih podataka što može dovesti do povrede privatnosti. Iz toga proizlazi potreba zaštite osobnih podataka s ciljem smanjenja rizika od otuđenja informacija o korisnicima.

Javno dostupne informacijsko-komunikacijske usluge na internetu stvaraju mnoge nove mogućnosti za korisnike informacijskih sustava. Međutim, istovremeno uzrokuju i nov rizik za osobnu sigurnost i privatnost korisnika. Jedan je od načina smanjivanja rizika povećanje svijesti o sigurnosnim pitanjima kod korisnika informacijskih sustava. Današnja je sveprisutnost interneta u svakodnevnom životu uzrokovala da takozvani virtualni svijet postane stvaran dio realnog svijeta. Moglo bi se reći da internet sve više obuhvaća i sve veći dio postojećega realnog svijeta ulazeći u sva područja čovjekova života. Međutim, način čovjekova ponašanja, a posebno u vezi s vlastitom sigurnošću, nije u skladu s ponašanjem u realnom svijetu, iako je na internetu čak lakše osmisliti i izvesti prijevaru. Zadnjih je godina u porastu tzv. pecanje (engl. *phishing*), odnosno način zlouporabe interneta zavaravanjem i nagovaranjem korisnika da otkrije neke svoje osobne podatke ili da učini nešto neželjeno, najčešće nesvjesno i u neznanju (Symantec, 2010). Socijalni inženjering, koji u internetskim prijevarama cilja upravo na lakovjernoga korisnika, polako postaje glavni način iniciranja same prijevare (Haley, 2011; Mitnick, Simon i Wozniak, 2002). Inicijalno odavanje manjeg dijela osobnih podataka ili instaliranje dodatne aplikacije, na primjer za kućno kino, može u konačnici završiti financijskim ili nekim drugim, manje materijalnim gubitkom, odnosno nekom vrstom gubitka privatnosti.

Mnogi su primjeri raznih vrsta prijevara i gubljenja privatnosti na internetu, što postaje sve veći problem za razvoj suvremenoga informacijskog društva. Razvoj novih aplikacija za društvene mreže, kupovina putem interneta, digitalna javna uprava, elektronički zdravstveni sustav i slične usluge dodatno su povećale problem privatnosti i informacijske sigurnosti korisnika. Nove usluge zahtijevaju od korisnika da otkriju dio svojih osobnih podataka pružateljima ovih usluga. Zbog

sve većeg broja svakodnevno potrebnih internetskih usluga te sve većeg broja redovnih korisnika navedenih usluga pitanje privatnosti i zaštite korisnika ovih usluga postaje sve važniji izazov, koji se vjerojatno neće nikada moći u potpunosti i riješiti.

Zbog porasta novih usluga rastu i potencijalni sigurnosni rizici, no korisnici informacijsko-komunikacijskih sustava i usluga su neoprezni i nesmotreni, nesvjesni postojećih rizika (Haley, 2011; Mitnick i sur., 2002). Nažalost, njihovo neznanje ne uzrokuje oprez, kao što bi bilo očekivano, već bez razumijevanja o potencijalnim rizicima objeručke prihvaćaju i počinju upotrebljavati nove usluge čim se pojave na digitalnome tržištu.

Prema definiciji, odnosno kako bi se osigurala informacijska sigurnost, potrebno je postići stanje povjerljivosti, cjelovitosti te raspoloživosti podatka, a ono se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom (Narodne novine, 79/07).

Iz definicije slijedi kako je za postizanje informacijske sigurnosti prvenstveno potrebno zaštititi podatke. Podaci se štite kroz zaštitu komunikacijskih kanala kojima se razmjenjuju podaci, zaštitu skladišta tih podataka te kontrolu odnosno utjecaj na osobe koje podatke posjeduju i upotrebljavaju. Tehnička rješenja fizičke i programske zaštite, uz razvijene sigurnosne procedure i automatizaciju sigurnosnih kopija, jesu danas na visokoj razini, međutim utjecaj korisnika na sigurnost, iako je znatna, tek je zadnjih godina prepoznata, a rješenja problema kontrole i edukacije korisnika tek su u zasnivanju.

Pokazalo se da korisnik ima značajan utjecaj na sigurnost informacijskog sustava (Lukasik, 2011; Šolić, Šebo, Jović i Ilakovac, 2011) te da bi ga trebalo uzeti u obzir prilikom razvoja novih sigurnosnih rješenja (Johnson i Pfleger, 2011).

Postojeća sigurnosna rješenja koja uzimaju u obzir utjecaj ponašanja korisnika mogu se podjeliti na nekoliko područja: razvoj koncepta povjerenja na internetu (Groš, Golub i Glavinić, 2008; Lukasik, 2011), izrada modela za analizu (Chan, Shoniregun, Akmayeva i Al-Dahoud, 2009), snimanje (Saleh i Habil, 2008; Tang, Zhou i Wang, 2009) i predviđanje ponašanja korisnika (Liqin, Chuang i Sunjinxia, 2006), edukacija korisnika (Furman, Theofanos, Choong i Stanton, 2011; Horcher i Tejay, 2009), odnosno podizanje razine svijesti o pitanjima privatnost (Vuković i sur., 2014) te mnoge upute raznih centara za razvoj sigurnosti (CERT, 2014; ENISA, 2010). Temelj ovih i budućih rješenja treba biti razvoj određenog stupnja nepovjerenja korisnika raznih informacijskih sustava i interneta prema nepoznatom. To bi značilo naučena pravila ponašanja iz realnog svijeta, kao što je na primjer zaključavanje kućnih vrata te nepovjerenje prema strancima, primjeniti na virtualni digitalni svijet.

Dosadašnja su istraživanja (Johnson i Pfleger, 2011; Sasse, Brostoffand i Weirich, 2001) pokazala kako je čovjek, kao korisnik informacijskog sustava, možda i najkritičniji sigurnosni element u informacijskom sustavu. Istovremeno ne postoji pouzdan način koji mjeri rizičnost čovjekova ponašanja u vidu narušavanja

sigurnosti informacijskog sustava te njegovo znanje i svjesnost o potencijalnim sigurnosnim problemima.

Stoga je cilj ovog istraživanja bio razviti instrument za mjerenje razine znanja te razine potencijalno rizičnog ponašanja računalnih korisnika po pitanjima informacijske sigurnosti, a koji će biti primjenjiv na opću populaciju zaposlenika, te napraviti validaciju istog. Kako su prijašnja istraživanja iz područja sigurnosti informacijskog sustava pokazala da je čovjek najslabija karika u sigurnosnom sustavu (Sasse i sur., 2001; Šolić i Ilakovac, 2009; Thompson, 2013), bilo je nužno razviti valjan i pouzdan instrument koji će mjeriti utjecaj korisnika na sigurnost informacijskog sustava (Choo, 2011; Crossler i sur., 2013).

Postojeća slična istraživanja nisu dovoljno univerzalna, odnosno pokrivaju samo neke od segmenata znanja i ponašanja korisnika koja mogu utjecati na cjelokupnu sigurnost informacijskog sustava. Većinom su dosadašnja istraživanja po pitanju ponašanja korisnika informacijskog sustava empirijska istraživanja usmjerena na ispitivanje kvalitete i načina korištenja lozinke, dok ostale elemente ponašanja zanemaruju (Dell'Amico, Michiardi i Roudier, 2010; Kelley i sur., 2012; Šolić, Jović i Blažević, 2013; Voyiatzis, Fisad, Serpanos i Avouris, 2011; Wanli, Campbell, Tran i Kleeman, 2010).

Stoga će razvoj ovog instrumenta omogućiti utvrđivanje novih općih spoznaja o razini znanja i rizičnosti ponašanja općenitog korisnika informacijskih sustava. Nova bi saznanja o korisnicima trebala potaknuti poboljšanja u postojećim rješenjima te razvoj novih sigurnosnih rješenja temeljenih na edukaciji korisnika.

Metoda

Sudionici

U prvoj fazi prikupljanja podataka sudjelovali su studenti druge godine preddiplomskog studija Učiteljskog fakulteta u Osijeku (*N*=41), Medicinskog fakulteta u Osijeku (*N*=51) i Elektrotehničkog fakulteta u Osijeku (*N*=43). U drugom je valu prikupljanja podataka sudjelovalo 119 studenata Elektrotehničkog fakulteta u Osijeku (87 studenata prve godine i 32 studenta pete godine) te 92 zaposlene osobe (zaposlenici Hypo grupacije iz Osijeka, Zagreba i Vinkovaca (*N*=52), Športskih objekata Osijek (*N*=20) i Shimadzu Zagreb (*N*=20)). U trećem je valu istraživanja sudjelovalo 152 zaposlenika (88 zaposlenika Kliničkoga bolničkog centra Osijek i 64 zaposlenika Saponije). Ostali su podaci prikazani u Tablici 1.

Tablica 1. *Prikaz podataka o sudionicima svih triju faza istraživanja*

	Prva faza istraživanja *N*=135	Druga faza istraživanja *N*=211	Treća faza istraživanja *N*=152	Ukupno *N*=498
studenti (*N*)	135	119	-	254
dob	19.85 (*SD*=0.85)	20.44 (*SD*=2.07)	-	20.13 (*SD*=1.35)
m	47.6%	86.6%	-	65.8%
ž	52.4%	13.4%	-	34.2%
zaposlenici (*N*)	-	92	152	244
NKV	-	1.1%	-	0.4%
SSS	-	42.4%	29.8%	34.4%
VŠS	-	13.0%	19.9%	17.2%
VSS	-	43.5%	50.3%	48.0%
dob	-	38.57 (*SD*=10.37)	40.73 (*SD*=9.94)	39.93 (*SD*=10.10)
m	-	48.9%	32.9%	38.9%
ž	-	51.1%	67.1%	61.1%

Napomene: m – muški spol; ž – ženski spol.

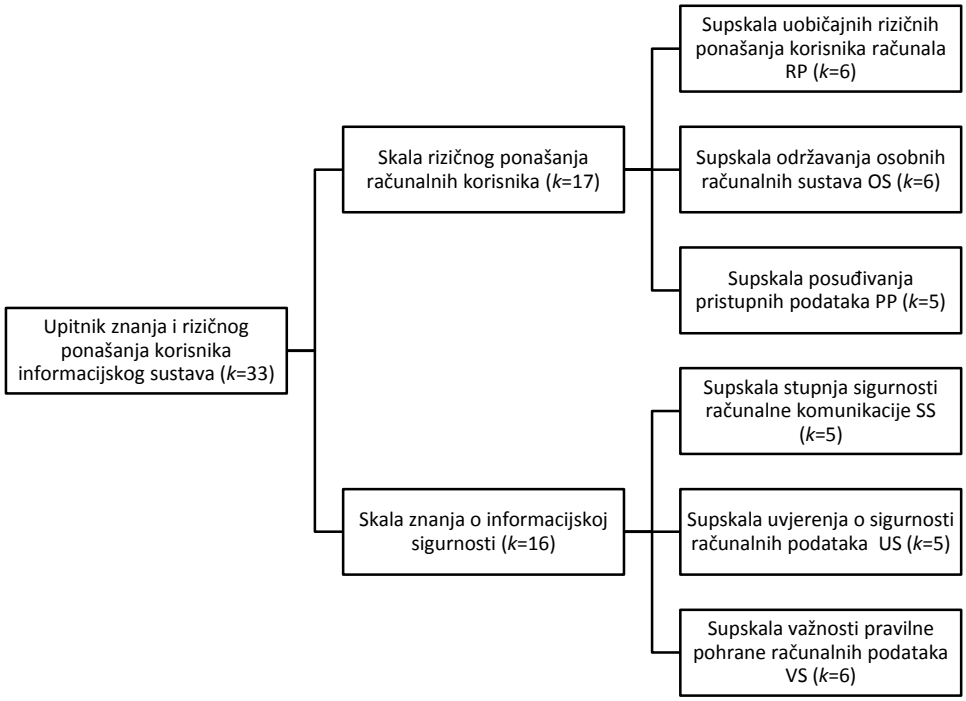
Instrumenti

Početna verzija *Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava* (UZPK; Velki i Šolić, 2014; prema Velki, Šolić i Očević, 2014) koji su autori na temelju pregleda literature sastavili sastojala se od 37 čestica te je podijeljena na dva dijela. Prvi se dio Upitnika sastojao od 20 čestica kojima ispitujemo uobičajena rizična ponašanja korisnika računalnih informacijskih sustava. Drugi se dio upitnika sastojao od 17 čestica podijeljenih u dvije skale koje su ispitivale znanje, odnosno svjesnost o informacijskoj sigurnosti. Konačna verzija Upitnika (Slika 1.) sastoji se od 33 čestice. Sudionici trebaju zaokružiti odgovor na skali Likertova tipa (od 1 do 5) pri čemu (ovisno o skali/supskali) ponuđeni odgovori imaju različita značenja (npr. učestalost, stupanj sigurnosti, stupanj uvjerenja i stupanj važnosti). Rezultat se dobiva za svaku supskalu na temelju aritmetičkih sredina određenih čestica pri čemu se, teoretski, kreću od 1 (*potpuno sigurno ponašanje korisnika računala*) do 5 (*visoko rizično ponašanje pri korištenju računala*). Viši rezultat upućuje na rizičnije ponašanje pri korištenju računala. U završnoj se verziji prvi dio upitnika sastoji od 17 čestica podijeljenih u tri supskale, pri čemu prva supskala (*k*=6) mjeri različita rizična ponašanja [npr. *Bez provjere otvarate priloge nepoznatih pošiljatelja* ili *Prosljeđujete/šaljete lančane mailove (npr. poruke o donacijama, sreći i sl.)*]. Druga se supskala (*k*=6) odnosi na održavanje osobnih računalnih sustava [npr. *Upotrebljavate različite lozinke za različite sustave, npr. za facebook jedna, za mail druga, za poslovni sustav treća lozinka itd.* ili *Održavate zaštitu svoga privatnog računala, odnosno radite li nadogradnju* (engl. *update*) *antispayware i antivirusnih programa*], dok se treća supskala (*k*=5) odnosi na posuđivanje pristupnih podataka [npr. *Otkrivate svoj pin (neskrivanjem, glasnim izgovaranjem prodavaču) kada plaćate karticom u*

trgovini ili *Posuđujete svojim prijateljima, rođacima, poznanicima svoje privatne pristupne podatke za pristup osobnoj/privatnoj e-mail adresi*]. Drugi se dio upitnika, koji mjeri znanje o informacijskoj sigurnosti, također sastoji od tri supskale. Prva supskala mjeri procjenu stupnja informacijske sigurnosti korisnika [*k*=5, npr. *Što mislite, koliko je sigurna komunikacija društvenim mrežama (npr. Facebook, Twitter)*]; druga subskala mjeri stupanj uvjerenja korisnika o informacijskoj sigurnosti podataka (*k*=5, npr. *Koliko ste uvjereni da postoji realna opasnost da će Vam netko ukrasti privatne podatke s Vašega kućnog računala*) te treća supskala, kojom se procjenjuje stupanj važnosti pravilnog čuvanja računalnih podataka (*k*=6, npr. *Prema Vašem mišljenju, koliko je važno provjeriti tuđi USB memorijski štapić od virusa prije učitavanja podataka*).

Za provjeru su kriterijske valjanosti kao vanjski kriteriji korištene sljedeće čestice: a) odavanje same lozinke od strane korisnika (je li korisnik napisao ili nije napisao svoju računalnu lozinku na Upitnik); b) korisnikova procjena broja osoba koje znaju njegovu lozinku; c) korisnikova procjena učestalosti obnavljanja sigurnosnih kopija, a sve su zadržane u Upitniku. Ove čestice predstavljaju jedan od mogućih aspekata rizičnog ponašanja računalnih korisnika za koje je bilo moguće prikupiti podatke.

Slika 1. *Prikaz skala i supskala Upitnik znanja i rizičnog ponašanja korisnika informacijskog sustava*



Za potrebe se istraživanja kao vanjski kriterij koristila adaptirana verzija *Upitnika samoiskaza rizičnog i delinkventnog ponašanja* (SRDP 2007; Ručević, Ajduković i Šincek, 2009). Originalni se upitnik sastoji od 42 čestice kojima se opisuju različita rizična i delinkventa ponašanja mladih i adolescenata. Upitnik (42 čestice) je podijeljen na sedam faktora: 1) Prekršajna i lakša delinkventna ponašanja (*k*=11); (2) Nepoželjna normativna ponašanja (*k*=7); (3) Rizična spolna ponašanja (*k*=4); (4) Korištenje ili zlouporaba psihoaktivnih tvari (*k*=6); (5) Nasilničko ponašanje u bliskim odnosima (*k*=5); (6) Teške krađe, provale i razbojništvo (*k*=6); i (7) Suicidalna i autoagresivna ponašanja (*k*=3). Ovi su faktori u međusobno niskim do umjereno pozitivnim korelacijama i tvore opći faktor rizičnog i delikventnog ponašanja. Rezultati se na pojedinim podljestvicama SRDP-a određuju kao zbroj umnožaka čestina pojedinih ponašanja (nikad, 1 – 2 puta, 3 – 5 puta i više od 5 puta) i pripadajućih indeksa težine (1 – 9) na svim česticama unutar pojedine podljestvice. Viši rezultat upućuje na izraženije rizično i delinkventno ponašanje. Za potrebe je našeg istraživanja odabrano 20 čestica iz prve četiri podljestvice (*Prekršajna i lakša delinkventna ponašanja, Nepoželjna normativna ponašanja, Rizična spolna ponašanja, Korištenje ili zlouporaba psihoaktivnih tvari*) koje su imale slabije indekse težine, odnosno ponašanja koja su manjeg stupnja rizičnosti i češće zastupljena u općoj populaciji, a ne samo tipičnih za populaciju mladih i adolescenata. Na temelju rezultata tako odabranih čestica formiran je ukupni rezultat, aritmetička sredina odabranih čestica, kao mjera blažih oblika rizičnog i delikventnog ponašanja. Viši rezultat upućuje i na viši stupanj rizičnog ponašanja i delikvencije. Pouzdanost adaptiranog SRDP-a se kretala između Cronbach α od .73 do .80.

Postupak

Validacija upitnika provedena je u tri koraka. U prvom je koraku primijenjena duža verzija upitnika (*k*=37) na studentima. Istraživanje je bilo upotpunosti dobrovoljno i anonimno. Podaci su prikupljeni grupno tijekom nastave na fakultetima, a popunjavanje je upitnika u prosjeku trajalo 30 minuta. U drugom je koraku skraćena i poboljšana verzija primijenjena na studentima na isti način kao i u prvom koraku, ali je u ovom koraku primijenjena i na odraslim zaposlenim osobama. Prikupljanje podataka među zaposlenim sudionicima odvijalo se na dobrovoljnoj bazi kolega i kolegica, na njihovu radnom mjestu, tijekom jednoga radnog dana. U trećem je koraku upitnik primijenjen i provjeren na odraslim zaposlenim osobama. Prikupljanje podataka zaposlenih sudionika odvijalo se unutar dva dana obilaženjem radnog mjesta zaposlenika. Nakon što su nadređeni obavijestili zaposlenike o provođenju ankete, istraživači su svakom zaposleniku ponaosob donijeli Upitnik te ih isti dan pred kraj radnog vremena i pokupili. Zaposlenici su imali vremena tijekom radnog dana popuniti Upitnik i odložiti na zajedničko mjesto (kartonska kutija) nakon što završe popunjavanje kako bi se osigurala anonimnost.

Rezultati

Konstruktna valjanost

U svrhu je provjere faktorske strukture prvog dijela UZPK (koji mjeri rizična ponašanja računalnih korisnika) te opravdanosti formiranja triju supskale na temelju skupa odabranih čestica (*k*=20) provedena eksploratorna faktorska analiza metodom glavnih komponenata uz oblimin kosokutnu rotaciju. Prema Guttman-Kaiserovu kriteriju (karakteristični korijen veći od 1) utvrđeno je postojanje čak osam faktora, no većina tih faktora objašnjavala je samo manji dio ukupne varijance (manji od 7%). Prema kriteriju *Scree*-testa jasno se mogu izdvojiti tri faktora, a ta tri faktora imaju svojstvenu vrijednost veću od dva i svaki objašnjava više od 10% ukupne varijance (ukupno 37.42% varijance). Zbog sadržaja čestica, koje se nisu smisleno ni interpretabilno raspodijelile u osam faktora, odlučeno je zadržati samo tri faktora, te izbaciti čestice koje imaju niska faktorska zasićenja tim faktorima (<.30). Ukupno su isključene tri čestice tako da se konačna verzija sastojala od 17 preostalih čestica. Nakon toga ponovljena je analiza glavnih komponenata uz oblimin-rotaciju. Prema Guttman-Kaiserovu kriteriju utvrđena su tri faktora sa svojstvenim vrijednostima većim od dva koji objašnjavaju 43.43% varijance dok se prema kriteriju *Scree*-testa jasno izdvajaju tri faktora. Prvi smo faktor nazvali *Supskala uobičajenih rizičnih ponašanja korisnika računala* (*k*=6), i on objašnjava 16.8% varijance. Drugi faktor *Supskala održavanja osobnih računalnih sustava* (*k*=6) objašnjava 14.8% varijance, a treći faktor *Supskala posuđivanja pristupnih podataka* (*k*=5) objašnjava 11.8% varijance.

Analizom glavnih komponenata uz kosokutnu rotaciju na rezultatima drugog i trećeg uzorka (Tablica 2.), u kojima je primijenjena poboljšana verzija UZPK-a, prema *Scree*-test kriteriju također su utvrđena tri faktora koja su objašnjavala 46.23% i 43.43% varijance. Raspored čestica prema faktorima bio je jednak kao u prvom uzorku s razlikom da su supskale objašnjavale različite postotke varijanci u odnosu na prvi uzorak, odnosno mijenjao se redoslijed važnosti objašnjenih supskala.

U Tablici 2. prikazane su matrice faktorskih zasićenja za trofaktorske strukture Skale rizičnog ponašanja računalnih korisnika i Skale znanja o informacijskoj sigurnosti dok su deskriptivni podaci (koeficijenti pouzdanosti tipa unutarnje konzistencije (Cronbachov α), rezultati Kolmogorov-Smirnovljeva testa te aritmetičke sredine i standardne devijacije za sve čestice) prikazane u Tablici 3. Obje tablice prikazuju podatke za treći uzorak sudionika na kojem je rađena završna validacija Upitnika.

Tablica 2. *Matrica faktorskih zasićenja čestica UZPK za obje skale (Skala rizičnog ponašanja računalnih korisnika i Skala znanja o informacijskoj sigurnosti) za trofaktorske solucije na trećem uzorku zaposlenika (N=152)*

Supskala	Čestica	Komunalitet	Faktorsko zasićenje			Svojstvena vrijednost	Objašnjena varijanca
			1. faktor	2. faktor	3. faktor		
Skala rizičnog ponašanja računalnih korisnika							
Supskala posuđivanja pristupnih podataka PP (*k*=5)	PP1	.51		.55		2.43	14.27%
	PP2	.80		.68			
	PP3	.80		.80			
	PP4	.62	.30	.58			
	PP5	.59		.47			
Supskala održavanja osobnih računalnih sustava OS (*k*=6)	OS6	.60	.66			3.28	19.29%
	OS7	.81	.79				
	OS8	.75	.81				
	OS15	.69	.68				
	OS17	.51	.57				
	OS18	.71	.42				
Supskala uobičajnih rizičnih ponašanja korisnika računala RP (*k*=6)	RP9	.72	-.46		.36	1.68	9.88%
	RP11	.50			.60		
	RP12	.61			.77		
	RP13	.66			.75		
	RP14	.53			.50		
	RP16	.64	-.38		.36		
						ukupno	43.43%
Skala znanja o informacijskoj sigurnosti							
Supskala stupnja sigurnosti računalne komunikacije SS (*k*=5)	SS1	.64	-	.79	-	4.20	26.20%
	SS2	.69	-	.81	-		
	SS3	.79	-	.88	-		
	SS4	.71	-	.84	-		
	SS5	.76	-	.87	-		
Supskala uvjerenja o sigurnosti računalnih podataka US (*k*=5)	US1	.58	-	-	-.75	2.29	14.30%
	US2	.72	-	-	-.85		
	US3	.76	-	-	-.87		
	US4	.57	-	-	-.74		
	US5	.72	-	-	-.85		
Supskala važnosti pravilne pohrane računalnih podataka VP (*k*=6)	VP1	.64	.79	-	-	4.51	28.12%
	VP2	.73	.85	-	-		
	VP3	.69	.83	-	-		
	VP4	.63	.79	-	-		
	VP5	.68	.82	-	-		
	VP6	.70	.83	-	-		
						ukupno	68.69%

Tablica 3. *Deskriptivni podaci, pouzdanost i rezultati Kolmogorov-Smirnovljeva testa za UZPK za obje Skale (Skala rizičnog ponašanja računalnih korisnika i Skala znanja o informacijskoj sigurnosti) za trofaktorske solucije na trećem uzorku zaposlenika (N=152)*

Subskala	Čestica	*M*		*SD*		Raspon		Cronbach α	K-S
Subskala posuđivanja pristupnih podataka PP (*k*=5)	PP1	1.76	1.28	0.87	0.73	4	2.00	.66	0.28**
	PP2	1.27		0.61		3			
	PP3	1.15		0.43		2			
	PP4	1.17		0.48		3			
	PP5	1.09		0.44		3			
Subskala održavanja osobnih računalnih sustava OS (*k*=6)	OS6	1.92	1.77	1.51	0.85	4	4.00	.66	0.07**
	OS7	1.66		1.29		4			
	OS8	1.35		1.15		4			
	OS15	1.81		1.65		4			
	OS17	3.19		1.34		4			
	OS18	0.81		1.32		4			
Subskala uobičajnih rizičnih ponašanja korisnika računala RP (*k*=6)	RP9	1.54	1.39	0.77	0.40	4	2.00	.60	0.16**
	RP11	1.19		0.46		4			
	RP12	1.09		0.32		2			
	RP13	1.15		0.42		3			
	RP14	1.45		0.72		4			
	RP16	2.01		1.22		4			
Subskala stupnja sigurnosti računalne komunikacije SS (*k*=5)	SS1	2.72	2.42	1.03	0.86	4	3.60	.89	0.13**
	SS2	2.08		0.95		4			
	SS3	2.63		1.12		4			
	SS4	2.71		1.17		4			
	SS5	2.25		0.94		4			
Subskala uvjerenja o sigurnosti računalnih podataka US (*k*=5)	US1	1.16	1.06	1.09	0.80	4	4.00	.88	0.16**
	US2	0.91		0.92		4			
	US3	1.03		0.89		4			
	US4	1.01		1.07		4			
	US5	1.23		1.03		4			
Subskala važnosti pravilne pohrane računalnih podataka VP (*k*=6)	VP1	3.02	3.08	0.94	0.80	4	4.00	.86	0.20**
	VP2	3.14		0.98		4			
	VP3	3.24		0.97		4			
	VP4	2.90		1.00		4			
	VP5	2.95		0.96		4			
	VP6	3.21		0.93		4			

**$p<.01$.

U svrhu je provjere faktorske strukture drugog dijela UZPK (koji mjeri znanje o informacijskoj sigurnosti) te opravdanosti formiranja dviju pojedinačnih skala provedena eksploratorna faktorska analiza metodom glavnih komponenata uz kosokutnu rotaciju na prvom uzorku sudionika. Kako svaka supskala mjeri različit aspekt informacijske sigurnosti (stupanj sigurnosti komunikacije i stupanj uvjerenja o postojanju opasnosti koja ugrožava sigurnost računalnih podataka) očekivali smo dobivanje dvije jasno odvojene supskale.

U prvom je uzorku eksploratornom faktorskom analizom metodom glavnih komponenata uz kosokutnu rotaciju prema Guttman-Kaiserovu kriteriju (karakteristični korijen veći od 1) utvrđeno postojanje dvaju faktora koji objašnjavaju čak 56.33% varijance. Prema kriteriju *scree*-testa jasno se izdvajaju također dva faktora. Sva su faktorska zasićenja visoka (<.30). U skladu s aspektima koje mjere dodijelili smo i imena dvjema supskalama: *Supskala stupnja sigurnosti računalne komunikacije* (*k*=6), koja objašnjava 37.02% varijance i *Supskala uvjerenja o sigurnosti računalnih podataka* (*k*=5), koja objašnjava 19.32% varijance. Međutim, zbog izrazitog su narušavanja pouzdanosti dvije čestice iz *Supskale uvjerenja o sigurnosti računalnih podataka* izbačene. Ponovljena je eksploratorna faktorska analiza, metoda glavnih komponenata uz kosokutnu rotaciju, kojom je prema Guttman-Kaiserovu kriteriju utvrđeno postojanje dvaju faktora koji objašnjavaju čak 65.96% varijance. Prema kriteriju *scree*-testa jasno se izdvajaju također dva faktora. Sva su faktorska zasićenja visoka (<.30). *Supskala stupnja sigurnosti računalne komunikacije* (*k*=6) objašnjava 44.43% varijance dok *Subskala uvjerenja o sigurnosti računalnih podataka* (*k*=3) objašnjava 21.53% varijance.

U drugom i trećem uzorku došlo je do manjih promjena u obliku *Supskale stupnja sigurnosti računalne komunikacije* (*k*=6), gdje su dvije čestice zbog sličnosti smisla spojene u jednu, pa konačna verzija ima ukupno pet čestica. *Subskala uvjerenja o sigurnosti računalnih podataka* zadržala je jednak broj čestica (*k*=5), međutim dvije čestice koje su znatno narušavale pouzdanost te supskale su zamijenjene novim. U drugoj je fazi dodana i nova supskala nastala na temelju opisnih pitanja iz prve faze prikupljanja podatka, *Subskala važnosti pravilne pohrane računalnih podataka* (*k*=6), te je ona primijenjena u trećoj fazi prikupljanja podataka (Tablica 2. i 3.).

Analizom glavnih komponenata uz kosokutnu rotaciju na rezultatima drugog (Tablica 2.) i trećeg uzorka (Tablica 3.) dobiveni su vrlo slični rezultati. Prema Guttman-Kaiserovu kriteriju i *scree*-test kriteriju utvrđeno je postojanje triju faktora koji objašnjavaju 57.13% varijance, odnosno 68.69% varijance u trećem uzorku. Sve su čestice iz obaju uzoraka imale visoka faktorska zasićenja (>.60 za drugi uzorak, odnosno >.70 za treći uzorak).

Rezultati korelacijske analize pokazuju kako su dobivene statistički značajne niske korelacije (*r*=.22-.31) između supskala prvog dijela UZPK, koji mjeri rizična ponašanja računalnih korisnika te također statistički značajne niske korelacije (*r*=.15-.28) između supskala drugog dijela UZPK, koji mjeri znanja o informacijskoj sigurnosti.

Pouzdanost

Zadovoljavajuća je unutarnja pouzdanost UZPK dobivena na svim trima uzorcima studenata i zaposlenika (Tablica 4.).

Tablica 4. *Prikaz koeficijenata pouzdanosti (Cronbach α) za UZPK na svim trima uzorcima sudionika*

Upitnik znanja i rizičnog ponašanja korisnika informacijskog sustava (*k*=33)					
Skala rizičnog ponašanja računalnih korisnika (*k*=17); α_1=.63, α_2=.66, α_3=.56			Skala znanja o informacijskoj sigurnosti (*k*=16); α_1=.72, α_2=.80, α_3=.80		
Supskala uobičajnih rizičnih ponašanja korisnika računala RP (*k*=6); α_1=.61, α_2=.75, α_3=.60	Supskala održavanja osobnih računalnih sustava OS (*k*=6); α_1=.69, α_2=.77, α_3=.66	Supskala posuđivanja pristupnih podataka PP (*k*=5); α_1=.66, α_2=.82, α_3=.66	Supskala stupnja sigurnosti računalne komunikacije SS (*k*=5); α_1=.89, α_2=.90, α_3=.88	Supskala uvjerenja o sigurnosti računalnih podataka US (*k*=5); α_1=.76, α_2=.79, α_3=.86	Supskala važnosti pravilne pohrane računalnih podataka VP (*k*=6), α_1= / , α_2=.77, α_3=.89

α_1 – pouzdanosti prvog uzorka, α_2 – pouzdanosti drugog uzorka, α_3 – pouzdanosti trećeg uzorka

Osjetljivost

Osjetljivost je utvrđena rasponom dobivenih rezultata u ukupnom rezultatu za svaku skalu i supskalu UZPK. Dvije supskale koje mjere rizično ponašanje računalnih korisnika (*Supskala uobičajenih rizičnih ponašanja korisnika računala* i *Supskala posuđivanja pristupnih podataka*) nisu pokazale pun raspon odgovora iako razmatranjem pojedinačnih čestica na trima uzorcima primjećujemo da su, ovisno o uzorku, dobiveni puni rasponi odgovora za svaku česticu barem na jednom mjerenom uzorku, dok je jedna supskala (*Supskala održavanja osobnih računalnih sustava*) na sva tri uzorka pokazala pun raspon odgovora. Sve su tri skale koje mjere znanje o informacijskoj sigurnosti pokazale pun raspon odgovora.

Testiranjem je normalnosti distribucija u sva tri uzorka Kolmogorov-Smirnovljevim testom utvrđeno kako distribucije značajno odstupaju od normalne (Tablica 3.). Za tri su supskale koje mjere rizično ponašanje računalnih korisnika distribucije pozitivno asimetrične. Supskale koje mjere znanje o informacijskoj sigurnosti imaju različite distribucije: *Subskala stupnja sigurnosti računalne komunikacije* na jednom uzorku pokazuje normalnu distribuciju dok na ostala dva blažu asimetričnu distribuciju (na jednom pozitivno, a na drugom negativno asimetričnu); *Supskala uvjerenja o sigurnosti računalnih podataka* ima pozitivno asimetričnu distribuciju, dok *Supskala važnosti pravilne pohrane računalnih podataka* ima negativno asimetričnu distribuciju.

Razlike u rezultatima dobivenim na različitim supskalama Upitnika s obzirom na spol sudionika i grupu (zaposleni i studenti) provjerene su analizama varijance (2x2). Dobiveni su rezultati u skladu s očekivanjima (Tablica 5.). U drugom je uzorku dobiven značajni glavni efekt grupe na dvije supskale. Studenti se, u odnosu na zaposlenike, statistički značajno češće brinu o održavanju računalnih sustava dok zaposlenici procjenjuju komunikaciju računalom manje sigurnom, za razliku od studenata. Ni u jednoj provedenoj analizi nema značajnih interakcija, kao ni značajnoga glavnog efekta spola.

Tablica 5. *ANOVA (2x2) za sve skale UZPK s obzirom na spol i grupu (zaposlenici i studenti) za drugi uzorak (N=211)*

UZPK		*M*	*SD*	$F_{(1,210)}$
rizična ponašanja korisnika računala (RP)	mladići	1.81	0.47	0.18
	djevojke	1.80	0.59	
	zaposleni	1.82	0.60	0.27
	studenti	1.80	0.43	
održavanje osobnih računalnih sustava (OS)	mladići	2.78	0.98	0.75
	djevojke	3.03	0.96	
	zaposleni	3.26	1.04	29.19**
	studenti	2.54	0.81	
posuđivanje pristupnih podataka (PP)	mladići	1.40	0.43	0.39
	djevojke	1.51	0.45	
	zaposleni	1.52	0.52	3.59
	studenti	1.36	0.34	
sigurnost računalne komunikacije (SS)	mladići	2.88	0.98	0.00
	djevojke	2.65	0.87	
	zaposleni	2.60	0.92	9.75**
	studenti	2.97	0.95	
uvjerenje o sigurnosti računalnih podataka (US)	mladići	1.01	0.76	3.70
	djevojke	1.26	0.70	
	zaposleni	1.16	0.73	0.80
	studenti	1.04	0.77	
važnost pravilne pohrane računalnih podataka (VP)	mladići	2.90	0.65	3.22
	djevojke	3.15	0.52	
	zaposleni	3.08	0.59	2.14
	studenti	2.89	0.63	

**$p<.01$.

Analizom je varijance na trećem uzorku zaposlenika dobivena samo jedna statistički značajna razlika (Tablica 6.). Muškarci, za razliku od žena, smatraju da je komunikacija računalom sigurnija.

Tablica 6. *ANOVA za sve skale s obzirom na spol za treći uzorak zaposlenika (N=152; Nm=50, Nž=152)*

UZPK	spol	*M*	*SD*	$F_{(1,151)}$
rizična ponašanja korisnika računala (RP)	m	1.48	0.44	3.11
	ž	1.36	0.38	
održavanje osobnih računalnih sustava (OS)	m	2.97	0.88	3.85
	ž	2.69	0.80	
posuđivanje pristupnih podataka (PP)	m	1.32	0.45	0.35
	ž	1.28	0.34	
sigurnost računalne komunikacije (SS)	m	2.63	0.81	4.36*
	ž	2.32	0.87	
uvjerenje o sigurnosti računalnih podataka (US)	m	0.96	0.77	1.08
	ž	1.11	0.81	
važnost pravilne pohrane računalnih podataka (VP)	m	3.12	0.78	0.22
	ž	3.05	0.80	

*p<.05.

Kriterijska valjanost

Za moguću je provjeru kriterijske valjanost UZPK-a primijenjena analiza varijance kojom smo provjerili razlikuju se rezultati na svim skalama i supskalama UZPK-a s obzirom na otkrivanje stvarne lozinke sudionika istraživanja (odnosno, jesu li sudionici istraživanja na Upitnik napisali svoju stvarnu lozinku ili nisu). Statistički su značajne razlike dobivene za sva rizična ponašanja korisnika računala u trećem uzorku te za supskalu posuđivanja pristupnih podataka, ali ne i za supskale znanja (Tablica 7.). Sudionici koji su napisali svoju lozinku pokazivali su rizičnija ponašanja pri korištenju računala, odnosno rizičnija ponašanja pri održavanju osobnih računalnih sustava i posuđivanju pristupnih podataka.

Tablica 7. *ANOVA za sve skale UZPK s obzirom na davanje lozinke za drugi i treći uzorak*

		drugi uzorak (*N*=211)			treći uzorak (*N*=152)		
UZPK	lozinka	*M*	*SD*	$F_{(1,209)}$	*M*	*SD*	$F_{(1,150)}$
rizična ponašanja korisnika računala (RP)	NE	1.80	0.48	0.49	1.32	0.39	4.53*
	DA	1.85	0.60		1.46	0.40	
održavanje osobnih računalnih sustava (OS)	NE	2.75	0.95	2.03	2.63	0.85	3.91*
	DA	3.18	0.99		2.90	0.82	
posuđivanje pristupnih podataka (PP)	NE	1.41	0.43	7.52**	1.21	0.31	6.09*
	DA	1.51	0.46		1.36	0.42	
sigurnost računalne komunikacije (SS)	NE	2.84	0.98	0.46	2.46	0.94	0.29
	DA	2.73	0.87		2.38	0.77	
uvjerenje o sigurnosti računalnih podataka (US)	NE	2.13	0.80	2.63	1.29	0.83	0.15
	DA	1.94	0.56		1.04	0.77	
važnost pravilne pohrane računalnih podataka (VP)	NE	2.93	0.63	1.57	3.13	0.76	0.73
	DA	3.07	0.58		3.02	0.83	

*p<.05; **p<.01.

Nadalje, za provjeru su kriterijske valjanosti provedene i korelacijske analize (Pearsonovi koeficijenti korelacije), odnosno utvrđena je povezanost vanjske kriterijske varijable (blaže rizično i delikventno ponašanje) s procjenom rizičnog ponašanja računalnih korisnika u očekivanom smjeru (Tablica 8.). Također smo provjerili razlikuju li se te povezanosti s obzirom na spol. Fisherovim *z*-testom razlika u korelacijama nisu dobivene spolne razlike u povezanosti ni u jednoj supskali UZPK i blažega rizičnog i delikventnog ponašanja.

Tablica 8. *Matrica korelacija UZPK s rizičnim i delikventnim ponašanjem mladih za drugi (N=211, Nm=148, Nž=63) i treći uzorak (N=152, Nm=50, Nž=102) te testiranje značajnosti spolnih razlika u korelacijama za oba uzorka*

UZPK	Rizično i delikventno ponašanje drugi uzorak (*N*=211)	Fisherov *z*-test razlika u korelacijama	Rizično i delikventno ponašanje treći uzorak (*N*=152)	Fisherov *z*-test razlika u korelacijama
rizična ponašanja	**.24****		**.37****	
korisnika računala (RP)		.12		-.87
m	.26**		.38**	
ž	.25		.50**	
održavanje osobnih	**.18****		**.20***	
računalnih sustava (OS)		-1.29		.21
m	.11		.19*	
ž	.30**		.15	
posuđivanje pristupnih	.07		**.21****	
podataka (PP)		1.17		-.40
m	.17*		.21*	
ž	-.01		.28**	
sigurnost računalne	-.02		.10	
komunikacije (SS)		-1.08		-.09
m	-.10		.10	
ž	.07		.12	
uvjerenje o sigurnosti	.02		.03	
računalnih podataka (US)		-.25		.25
m	-.03		-.00	
ž	-.07		.04	
važnost pravilne pohrane	**.16***		-.01	
računalnih podataka (VP)		-1.22		.08
m	.07		-.05	
ž	.25**		-.03	

Napomene: m – muški spol; ž – ženski spol.

$^{*}p<.05$; $^{**}p<.01$.

Također, i korelacije UZPK-a s ostalim vanjskim varijablama, korisnikova procjena učestalosti obnavljanja sigurnosnih kopija i procjena broja osoba koje znaju korisnikovu lozinku su očekivane (Tablica 9.). Dobivena je samo jedna

spolna razlika u povezanosti, pri čemu zaposlenice koje su dale svoju lozinku većem broju osoba češće posuđuju korisničke podatke drugim korisnicima, dok takva povezanost nije dobivena za zaposlenike.

Tablica 9. *Matrica korelacija UZPK s vanjskim kriterijima (procjena broja osoba koje znaju lozinku i procjena učestalosti obnavljanja sigurnosnih kopija) te testiranje značajnosti spolnih razlika u korelacijama za oba kriterija na trećem uzorku sudionika (N=152, Nm=50, Nž=102)*

UZPK		procjena učestalosti obnavljanja sigurnosnih kopija		Fisherov z-test razlika u korelacijama	procjena broja osoba koje znaju lozinku		Fisherov z-test razlika u korelacijama
rizična ponašanja korisnika računala (RP)		**-.29****		-.90	.15		.44
m	ž	-.19	-.34**		.17	.09	
održavanje osobnih računalnih sustava (OS)		**-.45****		-1.91	**.34****		.58
m	ž	-.27	-.54**		.36**	.27**	
posuđivanje pristupnih podataka (PP)		**-.18***		.68	.04		.29*
m	ž	-.24	- .12		.16	**-.24***	
sigurnost računalne komunikacije (SS)		-.06		-1.52	**.28****		1.12
m	ž	-.09	-.34		.39**	.21*	
uvjerenje o sigurnosti računalnih podataka (US)		-.12		-.08	.02		.99
m	ž	-.12	-.13		-.83	.92	
važnost pravilne pohrane računalnih podataka (VP)		**-.39****		1.07	**.21***		.31
m	ž	-.49**	-.33**		.24	.19	

Napomene: m – muški spol; ž – ženski spol.

$^{*}p<.05$; $^{**}p<.01$.

Rasprava

Dosadašnja su se istraživanja (koja se bave čovjekom kao faktorom koji narušava informacijsku sigurnost sustava) pokazala nedostatnim te su upućivala na potrebu razvoja univerzalnoga mjernog instrumenta ili protokola koji bi omogućio

standardizirano mjerenje rizičnog ponašanja računalnih korisnika (Choo, 2011; Crossler i sur., 2013). Budući da je utjecaj korisnika na cjelokupnu sigurnost informacijskog sustava značajan (Sasse i sur., 2001; Thompson, 2013), potrebna su daljnja istraživanja koja će dovesti do novih općih saznanja o razini znanja i rizičnosti ponašanja općenitog korisnika informacijskih sustava. Nova bi saznanja o korisnicima trebala potaknuti poboljšanja u postojećim rješenjima te razvoj novih sigurnosnih rješenja temeljenih na edukaciji korisnika.

U skladu s tim, javila se potreba za razvojem validiranog upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava, koji će biti prilagođen za populaciju zaposlenika, te čija će primjena biti relativno jednostavna i brza.

Konstruktna je valjanost Upitnika provjeravana faktorskom analizom, metodom glavnih komponenata uz kosokutnu rotaciju, pri čemu su na sva tri uzorka sudionika dobiveni slični rezultati. Prvo je provjeravana konstruktna valjanost prvog dijela Upitnika, odnosno *Skale rizičnog ponašanja računalnih korisnika*. U sva tri uzorka dobivena je jasna trofaktorska struktura *Skale rizičnog ponašanja računalnih korisnika*, te također u sva tri uzorka tri supskale objašnjavaju približno jednak postotak varijance (oko 45%). Zanimljivo je da, ovisno o uzorku, ista supskala objašnjava različit postotak varijance (iako je ukupna objašnjena varijanca podjednaka za sva tri uzorka), što nam govori u prilog dobroj konstruktnoj valjanosti ove Skale. Nadalje, provjeravana je i faktorska struktura drugog dijela UZPK, odnosno *Skale znanja o informacijskoj sigurnosti*. Faktorskom analizom, metodom glavnih komponenata na rezultatima drugih dvaju uzoraka dobivena je jasna trofaktorska struktura *Skale znanja o informacijskoj sigurnosti*, visok postotak objašnjene varijance, kao i izrazito visoka faktorska zasićenja (>.60). Također, supskale objašnjavaju različit postotak varijance ovisno o uzorku. Mijenjanje važnosti faktora (supskala), odnosno postotka objašnjenje varijance, koje varira od uzorka do uzorka, govori nam u prilog o podjednakoj važnosti svih triju supskala.

Osim toga, i rezultati korelacijske analize, gdje su utvrđene statistički značajne niske korelacije između supskala pripadajućih skala UZPK govore u prilog opravdanoj podjeli UZPK na dva nezavisna dijela, kao i o opravdanoj upotrebi zasebnih supskala pri mjerenju. Zadovoljavajući koeficijenti pouzdanosti tipa unutarnje konzistencije različitih supskala Upitnika potkrepljuju rezultate faktorske analize i podržavaju opravdanost formiranja različitih skala i supskala UZPK-a. Premda se može zamijetiti kako je pouzdanost supskala rizičnog ponašanja računalnih korisnika nešto niža u uzorku gdje su zastupljeni samo studenti i samo zaposlenici, ona je idalje zadovoljavajuća, dok je za ostale skale bez obzira na uzorak pouzdanost visoka.

Osjetljivost UZPK-a provjeravana je rasponom dobivenih rezultata u ukupnom rezultatu za svaku skalu i supskalu UZPK. Raspon ukupnih rezultata u grubim crtama pokazuje možemo li pomoću upitnika razlikovati i male razlike u procjenama rizičnih ponašanja korisnika računala i procjenama znanja o sigurnosti

računalnih sustava. Dvije supskale koje pripadaju *Skali rizičnog ponašanja računalnih korisnika* nisu pokazale puni raspon odgovora, međutim, ovisno o uzorku, dobiveni su puni rasponi odgovora za svaku česticu barem na jednom mjerenom uzorku, dok je jedna supskala na sva tri uzorka pokazala puni raspon odgovora. Sve su tri supskale koje pripadaju *Skali znanja o informacijskoj sigurnosti* pokazale puni raspon odgovora. Može se zaključiti kako UZPK uspješno ispituje i manje razlike u procjeni rizičnog ponašanja računalnih korisnika.

Distribucija ukupnih rezultata također je jedan od indikatora osjetljivosti UZPK-a, a testiranjem je normalnosti distribucija u sva tri uzorka Kolomogorov-Smirnovljevim testom utvrđeno kako distribucije značajno odstupaju od normalne. Sve su tri supskale koje pripadaju *Skali rizičnog ponašanja računalnih korisnika* pozitivno asimetrične. Takva distribucija pokazuje kako rezultati imaju tendenciju grupiranja prema nižim vrijednostima koje upućuju na procjenu manje rizičnog ponašanja računalnih korisnika. Ovakva raspodjela rezultata nije neočekivana jer se pretpostavlja da većina studenata i zaposlenika zna barem osnovna pravila korištenja računala. Supskale koje pripadaju *Skali znanja o informacijskoj sigurnosti* imaju različite distribucije. *Supskala stupnja sigurnosti računalne komunikacije* na jednom uzorku pokazuje normalnu distribuciju dok na ostala dva blažu asimetričnu distribuciju (na jednom pozitivno, a na drugom negativno asimetričnu), što govori u prilog o normalnoj distribuciji odgovora, odnosno da je podjednak broj onih koji vjeruju da je komunikacija internetom sigurna kao i onih koji su uvjereni da je takav vid komunikacije nesiguran. *Supskala uvjerenja o sigurnosti računalnih podataka* ima pozitivno asimetričnu distribuciju. Takva distribucija pokazuje kako rezultati imaju tendenciju grupiranja prema nižim vrijednostima koje upućuju na procjenu manje sigurnosti računalnih podataka. Ovakva raspodjela rezultata nije neočekivana jer se pretpostavlja da većina studenata i zaposlenika zna osnovne sigurnosne postavke pri radu s računalnim podacima. *Supskala važnosti pravilne pohrane računalnih podataka* ima negativno asimetričnu distribuciju, odnosno rezultati imaju tendenciju grupiranja prema višim vrijednostima što pokazuje da sudionici iako posjeduju određena znanja o informacijskoj sigurnosti, ne smatraju važnim pravilno pohranjivati i održavati računalne podatke. Ovaj je rezultat i odraz stvarne situacije, kada osobe unatoč visokoj stručnosti i znanju, nisu u stanju pravilno postupati s prikupljenim podacima što nerijetko dovodi do zastoja i problema u informacijskom sustavu (Šolić i Ilakovac, 2009).

Nadalje, proveli smo i nekoliko analiza varijance kako bismo utvrdili razlikuju li se rezultati na različitim subskalama Upitnika s obzirom na neke karakteristike sudionika istraživanja, odnosno kako bismo utvrdili možemo li na temelju rezultata pojedinih supskala Upitnika razlikovati različite grupe sudionika istraživanja. Pretpostavili smo da prosječni studenti u odnosu na prosječne zaposlenike iz našeg uzorka bolje održavaju računala i više se njime koriste u svrhu komunikacije (npr. češće su članovi društvenih grupa, koriste se različitim internetskim alatima u

komuniciranju s nastavnicima, npr. Moodle, Loomen i sl.). Dobiveni su rezultati u skladu s očekivanjima i govore u prilog dobroj osjetljivosti Upitnika. Studenti, u odnosu na zaposlenike, statistički značajno češće brinu o održavanju računalnih sustava, što je i očekivano jer se radi o studentima Elektrotehničkog fakulteta, kojima je to sastavni dio obrazovanja. Očekivano, zaposlenici procjenjuju komunikaciju računalom manje sigurnom za razliku od studenata, koji komunikaciju putem računala vjerojatno koriste u različite svrhe (npr. upoznavanje, druženje, razmjena informacija i sl.) i ne uzimaju u obzir sve potencijalne opasnosti, već su usmjereni na prednosti elektroničke komunikacije. Također je moguće da posjeduju i dodatna znanja kako zaštiti svoj računalni sustav, pa stoga ovu vrstu komunikacije smatraju sigurnijom. Na trećem je uzorku zaposlenika dobivena i jedna statistički značajna razlika između muškaraca i žena. Muškarci, za razliku od žena, smatraju da je komunikacija računalom sigurnija. Moguće da je dobivena razlika odraz društva u kojem živimo, ali i stvarnih situacija u kojima su žene češće žrtve zlouporabe i internetskoga nasilja (West, 2014), pa ne iznenađuje da one procjenjuju komunikaciju internetom manje sigurnom.

U sklopu su provjere kriterijske valjanosti UZPK-a provjerene razlike u rezultatima ispitanika na Upitniku između onih sudionika koji su otkrili i onih koji nisu otkrili lozinku. Također je provjerena povezanost Upitnika s vanjskim varijablama (blaže rizično i delikventno ponašanje, učestalost obnavljanja sigurnosnih kopija, broj osoba koje posjeduju korisnikovu lozinku), odnosno sklonosti onim ponašanjima koje ugrožavaju informacijsku sigurnost (CERT, 2010). Pretpostavili smo da će osobe koje su sklone napisati svoju lozinku (koju upotrebljavaju za bankovni račun, poslovnu e-adresu ili sl.) na anonimnom upitniku i predati je istraživaču s kojim se prvi put susreću biti sklonije i ostalim rizičnim ponašanjima računalnih korisnika kojima ugrožavaju informacijsku sustav. Prema dobivenim rezultatima, sva rizična ponašanja računalnih korisnika (uobičajena rizična ponašanja računalnih korisnika, slabije održavanje računalnih sustava i posuđivanje pristupnih podataka drugim osobama) češće su u osoba koje su napisale svoju lozinku u odnosu na osobe koje nisu dale svoje lozinku. Posjedovanje znanja o informacijskoj sigurnosti nije se razlikovalo kod sudionika koji su napisali i onih koji nisu napisali svoju lozinku. Ovi rezultati govore u prilog tezi da iako većina osoba posjeduje određena znanja, prijenos tih znanja u područje sigurnosnih ponašanja pri korištenju računala očito nije uspješan, što se vidi iz podatka da je većina njih spremna dati lozinku nepoznatoj osobi koja je lako može zloupotrijebiti. U drugom uzorku, u kojem su sudjelovali studenti, čak 75.8% (N=160) osoba je dalo svoje lozinke, dok je u trećem uzorku u kojem su sudjelovali samo zaposlenici ipak manji broj osoba dao lozinku, 51.9% (N=79), što je idalje više od polovice sudionika. Nadalje, dobivene su očekivane povezanosti između rizičnog ponašanja računalnih korisnika (za sve supskale) i blažeg rizičnog i delikventnog ponašanja. Rezultati korelacijske analize govore u prilog dobroj kriterijskoj valjanosti UZPK. Iako dobivene korelacije nisu visoke, one su statistički značajne i u očekivanom smjeru te se kreću u rangu vrijednosti od .16 do

.45. Kako dosad nisu rađena slična istraživanja, pretpostavku smo općenito temeljili na sklonosti rizičnom ponašanju, koja je očekivano povezana za različite aspekte rizičnog ponašanja. Osobe koje su sklonije blažim oblicima rizičnog i delikventnog ponašanja sklonije su i uobičajenim rizičnim ponašanjima pri korištenju računala, ne održavanju računalnih sustava i posuđivanju pristupnih podataka drugim osobama, što može biti i odraz životnog stila. Također je dobivena i pozitivna povezanost između blažega rizičnog i delikventnog ponašanja i jedne skale znanja o informacijskoj sigurnosti. Osobe koje procjenjuju da su sklonije blažem rizičnom i delikventom ponašanju također procjenjuju kako im nije važna pravilna pohrana računalnih podataka. Nisu dobivene spolne razlike u povezanosti ni jedne subskale UZPK i blažega rizičnog i delikventnog ponašanja, što govori u prilog dobroj vanjskoj valjanosti UZPK-a. Korelacije s ostalim vanjskim kriterijima (samoprocjena učestalosti obnavljanja sigurnosnih kopija te procjena broja osoba koje znaju korisnikovu računalnu lozinku) također su očekivane. Procjena češćeg obnavljanja sigurnosnih kopija povezana je s manje rizičnog ponašanja korisnika računala, s boljim održavanjem računalnih sustava, kao i s manje posuđivanja pristupnih podataka drugim korisnicima te s većom važnošću pravilne pohrane računalnih podataka. Osobe koje češće rade sigurnosne kopije (engl. *backup*) osobnih podataka pokazuju općenito manje svih vrsta rizičnih ponašanja pri korištenju računala kao i bolje shvaćanje važnosti pravilne pohrane računalnih podataka. Nadalje, procjena je većeg broja osoba koje znaju lozinku povezana sa slabijim održavanjem računalnih sustava, s procjenom veće sigurnosti računalne komunikacije i s manjom važnošću pravilne pohrane računalnih podataka. Osobe koje većem broju ljudi daju svoju lozinku pokazuju rizična ponašanja u vidu slabog održavanja računalnih sustava te smatraju kako je internetska komunikacija sigurna te ne znaju kako pravilno pohraniti i čuvati računalne podatke. Dobivena je i samo jedna spolna razlika. Naime, zaposlenice koje su dale svoju lozinku većem broju osoba češće posuđuju korisničke podatke drugim korisnicima (iako je povezanost mala), dok takva povezanost nije dobivena za zaposlenike. Moguće je da u ovom uzorku, gdje su sudjelovali samo zaposlenici, i to veći broj žena (oko 67%), možda zbog potreba posla su žene sklonije posuđivati svoju lozinku većem broju osoba (npr. medicinske sestre koje imaju zajedničke pristupne zaporke za računala na poslu). Bez obzira na moguća uzročno-posljedična objašnjenja, jasne povezanosti vanjskih varijabli s rizičnim ponašanjem računalnih korisnika u očekivanim smjerovima govore u prilog dobroj valjanosti UZPK.

Provedena validacija UZPK upućuje na njegove zadovoljavajuće metrijske karakteristike. Poželjno bi bilo UZPK validirati na većem broju različitih skupina zaposlenika radi njegove praktične primjene. U tu je svrhu planirano i određivanje normi hrvatskih zaposlenika na mjerama rizičnog ponašanja korisnika računala kako bi praktičari i istraživači mogli bolje usporediti različite stupnjeve rizičnog ponašanja računalnih korisnika s ciljem organiziranja dodatnih edukacija i poboljšanja u području sigurnosti rada s računalnim podacima za pojedine skupine

zaposlenika. Nadalje, potrebna je i dodatna provjera strukture samog upitnika konfirmatornom faktorskom analizom putem strukturalnog modeliranja kako bi potvrdili podjelu Upitnika na pretpostavljene skale i supskale. Također se preporuča provjera povezanosti UZPK s nekim drugim provjerenim i pouzdanim vanjskim mjerama, kao što su npr. stvarno odavanje osobnih podataka ili kršenje sigurnosnih mjera na poslu i slično, kao i prijevod Upitnika na druge strane jezike uz validaciju za svaki pojedini prijevod. Prijevodom bi se upitniku znatno povećala njegova korisnost i uporabljivost.

Dosadašnja primjena UZPK upitnika obuhvaća kako znanstvene radove, tako i stručnu odnosno praktičnu primjenu. Iz razloga što ne postoji sličan, odnosno usporediv mjerni instrument, napravljeno je empirijsko istraživanje na kontroliranom većem uzorku, a rezultati su objavljeni na konferencijama (Šolić, Velki i Galba, 2015) i u radovima (Galba, Šolić i Lukić, u tisku). U sklopu tih radova definirane su prosječne ocjene supskala koje predstavljaju referentne vrijednosti za internetsko rješenje nazvano "Sustav za samoprocjenu ponašanja korisnika Interneta" koji će biti integriran s "Kalkulatorom privatnosti" (Vuković i sur., 2015) te uskoro dostupan besplatno na stranicama regulatorne agencije HAKOM (www.hakom.hr) cjelokupnoj populaciji korisnika interneta u Hrvatskoj. Sustav je detaljno opisan u radu Galba i sur. (u tisku), a probni je link dostupan na stranicama Elektrotehničkog fakulteta Osijek (http://vns.etfos.hr/Samoprocjena/).

Literatura

CERT (2010). *Upute za laike "Sigurnije na Internetu"*. Preuzeto s http://www.cert.hr/dokumenti/sigurnije_na_internetu.

CERT (2014). *Croatian national computer emergency response team. Preporuke*. Preuzeto s http://www.cert.hr/preporuke

Chan, Y., Shoniregun, C.A., Akmayeva, G.A. i Al-Dahoud, A. (2009). Applying semantic web and user behavior analysis to enforce the intruder detection system. *Proceedings of Institute of Electrical and Electronics Engineers International Conference for Internet Technology and Secured Transactions*, 1-5.

Choo, K.K.R. (2011). The cyberthreat landscape: Challenges and future research directions. *Compures & Security*, *30*(8), 719-731.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. i Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*(1), 90-101.

Dell'Amico, M., Michiardi, P. i Roudier, Y. (2010). Password strength: An empirical analysis. *Proceedings Institute of Electrical and Electronics EngineersINFOCOM, (San Diego, CA)*, 1-9.

ENISA (2010). *The new users' guide: How to raise information security awareness*. Preuzeto s http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2010/new-users-guide

Furman, S., Theofanos, M., Choong, Y. i Stanton, B. (2011). Basing cybersecurity training on user perceptions. *IEEE Security & Privacy*, *2*(10), 40-49.

Galba, T., Šolić, K. i Lukić, I. (u tisku). Towards Information security and privacy self-assessment (ISPSA) tool for Internet users. *Acta Polytechnica Hungarica.*

Groš, S., Golub, M. i Glavinić, V. (2008). Using trust on the Internet. *Proceedings of Institute of Electrical and Electronics Engineers MIPRO*, 118-123.

Haley, K. (2011). *Information robbery - The 2011 Internet security threat report. InfoSecToday*. Preuzeto s http://www.infosectoday.com/Articles/Information_Robbery.htm.

Horcher, A.M. i Tejay, G.P. (2009). Building a better password: The role of cognitive load in information security training. *Proceedings Institute of Electrical and Electronics Engineers ISI*, 113-118.

Johnson, M.E. i Pfleger S.L. (2011). The human side of risk management. *Institute of Electrical and Electronics Engineers Security & Privacy*, *9*(1), 51.

Kelley, P.G., Komanduri, S., Mazurek, M.L., Shay, R., Vidas, T., Bauer L., Christin, N., Cranor, L.F. i Lopez, J. (2012). Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. *Institute of Electrical and Electronics Engineers Symposium on Security and Privacy, (San Francisco, CA)*, 523-537.

Liqin, T., Chuang, L. i Sunjinxia (2006). A kind of prediction method of user behaviour for future trustworthy network. *Proceedings Institute of Electrical and Electronics Engineers International Conference on Communications and Technology*, 1-4.

Lukasik, S.J. (2011). Protecting users of the cyber commons. *Communications of the Association for Computing Machinery, 54*(9), 54-61.

Mitnick, K.D., Simon, W.L. i Wozniak S. (2002). *The art of deception: Controlling the human element of security*. Indianapolis, Indiana, USA: Wiley Publishing, Inc.

Narodne novine (79/07). *Zakon o informacijskoj sigurnosti, Osnovne odredbe*. Preuzeto s http://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti

Ručević, S., Ajduković, M. i Šincek, D. (2009). Upitnik samoiskaza rizičnog i delinkventnog ponašanja. *Kriminologija i socijalna integracija, 17*(1), 1-11.

Saleh, K. i Habil, M. (2008). Security requirements behavior model for trustworthy software. *Proceedings Institute of Electrical and Electronics Engineers Multidisciplinary Conference on e-Technologies*, 235-238.

Sasse, M.A., Brostoffand, S. i Weirich, D. (2001). Transforming the 'weakest link' – a human/ computer interaction approach to usable and effective security. *British Telecom Technology Journal, 19*(3), 122-131.

Šolić, K. i Ilakovac, V. (2009). Security perception of a portable PC user (The difference between medical doctors and engineers): A pilot study. *Medicinski glasnik Dobojsko-Tuzlanskog kantona, 6*(2), 261-264.

Šolić, K., Jović, F. i Blažević, D. (2013). An approach to the assessment of potentially risky behavior of ICT system's users. *Technical Gazette, 20*(2), 335-342.

Šolić, K., Sebo, D., Jović, F. i Ilakovac, V. (2011). Possible decrease of spam in the email communication. *Institute of Electrical and Electronics Engineers MIPRO,* 170-173.

Šolić K., Velki, T. i Galba, T. (2015). Empirical study on ICT system's users' risky behavior and security awareness. *IEEE MIPRO / ISS*, 1623-1627.

Symantec (2010). *State of spam & phishing – A monthly report.* Preuzeto s http://www.symantec.com/content/en/us/enterprise/other_resources/b-state_of_spam_and_phishing_report_12-2010.en-us.pdf.

Tang, K., Zhou, M.T. i Wang W.Y. (2009). Insider cyber threat situational awareness framework using dynamic Bayesian network. *Proceedings of Institute of Electrical and Electronics Engineers of International Conference on Computer Science and Education*, 1146-1150.

Thompson, H. (2013). The human element of information security. *Institute of Electrical and Electronics Engineers Security & Privacy, 11*(1), 32-35.

Velki, T., Šolić, K. i Očević, H. (2014). Development of Users' information security awareness questionnaire (UISAQ) - Ongoing work. *Institute of Electrical and Electronics Engineers Proceedings 37th MIPRO Information System Security*, 1564-1568.

Voyiatzis, A.G., Fidas, C.A., Serpanos, D.N. i Avouris, N.M. (2011). *An empirical study on the web password strength in Greece*. 15th Panhellenic Conference on Informatics, (Kastonija Greece).

Vuković, M., Katušić, D., Skocir, P., Jevtić, D., Delonga, L. i Trutin, D. (2014). User privacy risk calculator. *Proceedings of Softver, Telecommunicatins and Computer Networks,* 1709.

Vuković, M., Katušić, D., Skocir, P., Jevtić, D., Trutin, D. i Delonga, L (2015). Estimating real world privacy risk scenarios. *Proceedings of Softver, Telecommunicatins and Computer Networks*, 1-7.

Wanli, M., Campbell, J., Tran, D. i Kleeman, D. (2010). *Password entropy and password quality*. 4th International Conference on Network and System Security, (Melbourne, VIC).

West, J. (2014). *Cyber-violence against women*. Vancouver, BC Canada: Battered Women's Support Services.

Development and Validation of Users' Information Security Awareness Questionnaire (UISAQ)

Abstract

Previous researches have shown that information systems' users are still the weakest link in information security area. Scientists did not yet develop some reliable instruments that measure the level of user's influence on information systems' security. The aim of the research was to develop a reliable and valid instrument for measuring a level of users' security awareness and its potentially

risky behaviour. For research purposes, Users' Information Security Awareness Questionnaire (UISAQ; Velki & Solic, 2014; according to Velki, Šolić, & Očević, 2014) was developed and with that questionnaire data were collected in three waves. Participants in the first wave were 135 second-year students of undergraduate study on who we tested the construct validity, reliability and sensitivity of individual subscales, and from which we choose items. In the second wave, we had a sample of 211 both students and employees. In this wave, metric characteristics of improved version of UISAQ have been examined. Result was final version of UISAQ (*k*=33) split into two scales: Scale of computer users' potentially risky behaviour (*k*=17) [split into three subscales: Subscale of computer users' usual behaviour (*k*=6), Subscale of personal computer systems' maintenance (*k*=6) and Subscale of access data lending (*k*=5)] and Scale of information security knowledge (*k*=16) [split into three subscales: Subscale of level of security in communications (*k*=5), Subscale of belief into data security status (*k*=5) and Subscale of backup importance (*k*=6)]. The third wave was conducted on 152 employees and in this wave validation was concluded. We obtained good constructive validity, where all scales and subscales have good metric characteristics, and good criterion validity. This newly developed questionnaire has proved to be a reliable and valid instrument with proper psychometric characteristics.

Keywords: validation, users' information security awareness, information security area, UISAQ

Desarrollo y validación del Cuestionario sobre el saber y la conducta de riesgo de los usuarios del sistema de informaciones (CSCU)

Resumen

Las investigaciones anteriores han mostrado que el hombre es el vínculo más débil del sistema de seguridad y que no existe una manera fiable de medir el riesgo de la conducta humana para no romper la seguridad del sistema de informaciones. El objetivo de esta investigación fue desarrollar un instrumento válido y fiable que mediría la influencia que tiene el usuario sobre la seguridad del sistema de informaciones. Con este fin fue creado el Cuestionario sobre el saber y la conducta de riesgo de los usuarios del sistema de información (CSCU; Velki i Šolić, 2014). La investigación fue realizada en tres fases de recolección de datos. La primera muestra constaba de 135 estudiantes del 2º año de estudios de grado y en ella se controlaba la validez de constructo, fiabilidad y sensibilidad de ciertas subescalas. También fueron elegidas partículas correspondientes. La segunda muestra constaba de 211 estudiantes y empleados. En ella se comprobaban características métricas del instrumento mejorado y se obtuvo la versión final del CSCU *(k=33)* que se divide en dos escalas: la Escala de conducta de riesgo de los usuarios *(k=17)* [consta de tres subescalas: la Subescala de conductas de riesgo habituales *(k=6)*, la Subescala de mantenimiento de los sistemas de ordenadores personales *(k=6)* y la Subescala de prestación de datos de acceso *(k=5)*] y la Escala del saber sobre la seguridad de informaciones *(k=16)* [que también consta de tres subescalas: la Subescala de grado de seguridad de la comunicación *(k=5)*, la Subescala de creencia sobre la seguridad de datos *(k=5)* y la Subescala de importancia del almacenamiento correcto de datos *(k=6)*]. La tercera muestra constaba de 152 empleados y en ella se validó el CSCU. Se obtuvo una validez de constructo muy buena, todas las escalas y subescalas tienen características métricas satisfactorias (fiabilidad y sensibilidad) y se obtuvo buena validez de criterio. Se puede concluir que el Cuestionario recién desarrollado representa un instrumento métrico válido y fiable, con características psicométricas satisfactorias.

Palabras claves: validación, conducta de riesgo de los usuarios, seguridad del sistema de informaciones, CSCU

Primljeno: 11.11.2014.