UNIVERZITET U SARAJEVU

EKONOMSKI FAKULTET

AIDA KOZIĆ

PERCEPCIJE SIGURNOSTI I POVJERENJA KORISNIKA SISTEMA ELEKTRONSKOG PLAĆANJA

ZAVRŠNI RAD

SARAJEVO, JUNI 2023.

UNIVERZITET U SARAJEVU

EKONOMSKI FAKULTET

AIDA KOZIĆ

PERCEPCIJE SIGURNOSTI I POVJERENJA KORISNIKA SISTEMA ELEKTRONSKOG PLAĆANJA

ZAVRŠNI RAD

Mentor: Prof. dr. Aida Habul

Kandidat: Aida Kozić

Indeks: 5060-73362

Studij: Menadžment

Smjer: Menadžment informacione tehnologije

SARAJEVO, JUNI 2023.

Izjava o autorstvu

Izjavljujem da sam ovaj rad radila samostalno koristeći se navedenom literaturom. Ovaj završni rad je izrađen na Ekonomskom Fakultetu Univerziteta u Sarajevu pod mentorstvom Prof. dr. Aide Habul u akademskoj 2022/2023. godini.

SADRŽAJ

SAŽETAK

Prednosti plaćanja koje omogućava elektronski sistem plaćanja (EPS) za online transakcije doprinijela je poboljšanju ukupne kvalitete života ljudi. Literatura o e-kupovini već je dugo znala da su posljedice povjerenja i sigurnosti na korištenje EPS-a važne. Relativno mali broj istraživanja je istraživao ove dvije ideje iz perspektive potrošača. Uspostavljen je konceptualni model u svrhu ispitivanja faktora percipirane sigurnosti i povjerenja, kao i uticaja percipirane sigurnosti i povjerenja na korištenje elektronskih uređaja za sigurno plaćanje (EPS). Rezultati istraživanja su pokazala da i percipirana sigurnost i povjerenje imaju značajan uticaj na korištenje EPS-a. Pokazalo se da su uobičajeni prediktori percipirane sigurnosti i povjerenja su tehnička zaštita i prethodno iskustvo.

Ključne riječi: *EPS, sigurnost, povjerenje, banka, tehnička zaštita*

EXECUTIVE SUMMARY

The benefits of payment enabled by the Electronic Payment System (EPS) for online transactions have contributed to improving the overall quality of people's lives. The e-shopping literature has long known that the consequences of trust and security on the use of EPS are important. Relatively little research has explored these two ideas from a consumer perspective. A conceptual model was established for the purpose of examining the factors of perceived security and trust, as well as the impact of perceived security and trust on the use of electronic devices for secure payment (EPS). The results of the research showed that both perceived security and trust have a significant impact on the use of EPS. Common predictors of perceived safety and trust have been shown to be technical protection and previous experience.

Keywords: *EPS, security, trust, bank, technical protection*

1. UVOD

E-plaćanje se definiše kao prijenos elektronske vrijednosti plaćanja od platilaca do primalaca putem mehanizma elektronskog plaćanja. Usluge e-plaćanja korisnicima omogućavaju pristup i upravljanje svojim bankovnim računima i transakcijama (Weir et al. 2006, Lim 2008). Postoji veliki broj usluga e-plaćanja koje su razvijene unutar sistema plaćanja širom svijeta. To uključuje elektronske čekove, e-gotovinu, kreditne kartice i elektronske prijenose sredstava (Ma WK, 2003). Online plaćanje se može podijeliti u dvije vrste: jedno u svjetlu Internet Banking Payment Gateway (IBPG) i jedno u svjetlu platne platforme autsajdera. Prvi je svojevrsni izravni način plaćanja, gdje klijent podrazumijeva online plaćanje putem e-business frameworka koji je povezan s bankarskim okvirom. S druge strane, druga vrsta uključuje razmjenu novca s računa kupca na račun trgovca putem platforme za plaćanje izvana ili preko treće strane. IBPG se nalazi između sistema bankarskih procesa i interneta. To je sistem koji je posebno napravljen za upravljanje plaćanjima i autorizacije plaćanja. IBPG je poveznica koja povezuje kupca, trgovca i banku. Online način plaćanja koji se temelji na IBPG-u ne može postojati bez izvršitelja plaćanja (Yang Q et al., 2007).

Kada je Evropska komisija stvorila potrebu za uslugama e-plaćanja, tradicionalni instrumenti plaćanja zasnovani na gotovini i na računima korišteni su kao model. Istovremeno, novi posrednici kao što je PayPal uspjeli su ispuniti neke od novih potreba online trgovaca i potrošača (Dahlberg et al. 2008). U poređenju s tradicionalnim metodama plaćanja, tehnike e-plaćanja imaju nekoliko povoljnih karakteristika, uključujući sigurnost, pouzdanost, stabilnost, anonimnost, prihvatljivost, privatnost, učinkovitost i pogodnost (Chou et al. 2004, Stroborn et al. 2004, Tsiakis i Sthephanides 2005, Linck i et al., 2006, Cotteleer i et al., 2007, Kousaridas et al., 2008). Zahvaljujući tome sistem elektronskog plaćanja se koristi širom svijeta. Zapadne zemlje imaju potpuno razvijene sisteme elektronskog plaćanja, dok zemlje u tranziciji poput Bosne i Hercegovine nisu u potpunosti razvili sistem elektronskog plaćanja.

Sistem elektronskog plaćanja ima niz prednosti u odnosu na tradicionalne metode plaćanja (Hegarty et al. 2003, Linck et al. 2006). Međutim, grupacija Gartner izvještava da je 95% korisnika zabrinuto za privatnost ili sigurnost kada koriste kreditne kartice na Internetu. Također, u izvještaju od Harris interactive navedeno je da se šest od deset ispitanika boji krađe kreditne kartice. Transakcije se mogu odvijati bez prethodnog ljudskog kontakta ili uspostavljenih međuljudskih odnosa. Općenito, sigurnost je skup postupaka, mehanizama i računarskih programa za provjeru autentičnosti izvora informacija i garancija procesa transakcije (Theodosios i George 2005, Linck et al. 2006). Iako se postojeća literatura široko bavi tehničkim detaljima sigurnosti i povjerenja u EPS iz perspektive trgovaca ili pružaoca usluga EPS-a, percepcija potrošača o sigurnosti EPS-a nije dobro obrađena i nedostaju empirijske studije u ovom području (Linck et al. 2006).

Tehničke zaštite općenito se smatraju temeljem EPS sigurnosti. Niz specifičnih tehničkih mehanizama koriste se kako bi se osigurala sigurnost plaćanja tokom transakcijskog procesa na Internetu (Slyke i Belanger 2003, Linck et al. 2006, Kousaridas et al. 2008). U vezi s ovim konceptom, Chellappa i Pavlou (2002) tvrde da će tehnička zaštita, uključujući privatnost, integritet i stabilnost, povoljno uticati na percipiranu sigurnost i percipirano povjerenje. Ako sistem e-plaćanja može ponuditi garanciju u pogledu privatnosti, integriteta

i stabilnosti, tada se može poboljšati nivo percipirane sigurnosti potrošača i percipiranog povjerenja u EPS (Romdhane 2005, Tsiakis i Sthephanides 2005, Hwang et al. 2007).

Primarni cilj transakcijskih postupaka je olakšati potrošačima korištenje EPS-a i eliminisati njihovu zabrinutost oko sigurnosti EPS-a (Lawrence et al. 2002). Kako bi se ispunili sigurnosni zahtjevi potrošača, potrebno je pripremiti dobro definisane EPS procedure (Hwang et al. 2007). Obično se tokom procesa transakcije koriste tri glavne procedure:

(1) autentifikacija svakog sudionika prije transakcije;

(2) pružanje potrošačima nekoliko odvojenih koraka prema završetku transakcije e-plaćanja;

(3) slanje potvrde nakon svake transakcije kako bi se potrošači uvjerili da je sistem e-plaćanja uspješno izvršio zadatak (Tsiakis i Sthephanides 2005, Hwang et al. 2007).

Prema izvještaju Mukherjeeja i Natha (2003) sigurnosne izjave na web stranicama EPS-a ključni su faktor koji utiče na povjerenje potrošača u online aktivnostima. Informisanjem i uvjeravanjem potrošača u pogledu sigurnosti njihovih opcija plaćanja, bit će moguće uticati na percepciju potrošača o sigurnosti i povjerenju u EPS (Lim 2008). Ako normalni potrošači ne postanu svjesni nivoa sigurnosti koja je svojstvena njihovim transakcijama, nerado će se uključiti u e-plaćanja (Hegarty et al. 2003, Lim 2008). Na odluke potrošača da koriste bilo koji sistem e-plaćanja uveliko će uticati kvaliteta sigurnosnih izjava koje su im dostupne. Ovu ideju podupiru rezultati koje su iznijeli Miyazaki i Fernandez (2000), koji tvrde da će sigurnosne izjave koje su objavljene na web stranicama vjerojatno povećati šanse potrošača za kupovine putem Interneta.

Percipirana sigurnost odnosi se na korisnikovu subjektivnu procjenu sigurnosti sistema e-plaćanja (Linck et al. 2006). Budući da potrošači imaju različita iskustva i očekivanja, mogu imati različite stavove prema sigurnosti online transakcija. To vrijedi čak i ako sistemi e-plaćanja pružaju garanciju u pogledu svih aspekata sigurnosnih zahtjeva potrošača (Stroborn et al. 2004). Ako je nivo percipirane sigurnosti u transakcije e-plaćanja preniska, potrošači vjerojatno neće učestvovati u transakcijama dok se ne implementiraju rješenja koja će ublažiti njihove strahove (Tsiakis i Sthephanides 2005). Istraživanja pokazuju da percepcija potrošača o sigurnosti povezanoj s e-plaćanjem dominira njihovim odlukama o korištenju EPS-a. Sigurnost i pouzdanost glavne su brige za kupce koji koriste EPS i međusobno su blisko povezani (Guan i Hua 2003, Peha i Khamitov 2004, Linck i dr. 2006).

Percipirano povjerenje potrošača u EPS predstavlja uvjerenje potrošača da će transakcije e-plaćanja biti obrađene u skladu s njihovim očekivanjima (Tsiakis i Sthephanides 2005, Mallat 2007). Potrošači mogu donijeti racionalnu odluku na temelju saznanja o mogućim nagradama za povjerenje i nepovjerenje. Povjerenje omogućuje veće dobitke, dok nepovjerenje izbjegava potencijalne gubitke (Linck et al. 2006, Kousaridas et al. 2008). Stavovi potrošača prema EPS-u povezani su s njihovim percepcijama sigurnosti sistema. Drugim riječima, percepcije potrošača o načelima provedbe sigurnosti povećavaju njihova uvjerenja u sigurnost i zbog toga pridonose njihovoj percepciji povjerenja u elektronske transakcije. Kniberg (2002) tvrdi da je vjerojatnije da će korisnici i trgovci koristiti nesiguran sistem plaćanja trgovcu od povjerenja, nego siguran sistem plaćanja trgovcu kojem se ne vjeruje. Ovo je u skladu s rezultatima prethodnih istraživanja (Tsiakis i Sthephanides 2005, Mallat 2007), koji sugerišu da je povjerenje važnije od sigurnosti. Bez povjerenja kupaca, EPS-u bi bilo iznimno teško dobiti široku upotrebu.

1.1. Problem i predmet istraživanja

Brojni sistemi elektronskog plaćanja u zadnjih dvadeset godina su na internetu. Iako su različite sigurnosne mjere i mehanizmi dizajnirani za ove sisteme, mnogi sigurnosni problemi i dalje su prisutni (Hsieh 2001, Chou et al. 2004, Dai i Grundy 2007, Kousaridas et al. 2008). Zbog toga postoji potreba za smanjenjem rizika povezanih s transakcijskim procesima e-plaćanja (Tsiakis i Sthephanides 2005). Budući da je većina korisnika EPS-a relativno slabo upoznata s tehničkim detaljima EPS-a, skloni su procijeniti nivo sigurnosti EPS-a na osnovu svog iskustva s korisničkim okruženjima. Dakle, da bi se privukli i zadržali korisnici e-plaćanja, najvažnije je poboljšati percepciju potrošača o sigurnosti i održati povjerenje kupaca tokom transakcija e-plaćanja (Chellappa i Pavlou 2002, Stroborn et al. 2004, Tsiakis i Sthephanides 2005, Linck i dr. 2006, Kousaridas i dr. 2008).

Cilj ovog rada je istražiti efekte percipiranog povjerenja i sigurnosti na usvajanje EPS-a kupaca Kantona Sarajevo, na temelju informacija prikupljenih od kupaca u Kantonu Sarajevo. U obzir će biti uzeta briga korisnika o povjerenju i sigurnosti koja je kategorisana u tri dimenzije: tehničke i transakcijske procedure, pristup sigurnosnim smjernicama i upotrebljivost. Faktori su djelimično preuzeti i prilagođeni iz sličnih istraživanja (Sanayei i Noroozi, 2009; Kim et al., 2010; Goudarzi et al., 2013), dok su u obzir uzeti i novi, prethodno neistraženi faktori.

Empirijsko istraživanje pomoću strukturisanog upitnika provodit će se kako bi se ocijenili faktori iz perspektive kupaca. Rezultati će se analizirati korištenjem popularnih statističkih metoda kako bi se opravdala naša kategorizacija faktora, dok se ispituje učinak svakog faktora na percipiranu sigurnost i povjerenje potrošača. Pokušat ćemo proširiti prethodno izmjerene faktore i prikupiti statističke podatke od klijenata gotovo svih banaka na teritoriji Kantona Sarajevo. Naši rezultati pokazat će važnost tehničkih i transakcijskih procedura, te pristupa sigurnosnim smjernicama,. Rezultati ove studije pomoći će bankarskim organizacijama u Kantonu Sarajevo da razumiju klijentovu perspektivu povjerenja i sigurnosti i omogućiti im promicanje metoda i procesa za povećanje povjerenja svojih klijenata.

1.2. Ciljevi istraživanja

Na ovnovu problema i predmeta istraživanja, ciljevi ovog rada istaknuti su u nastavku:

1. Identificiranje učinkovitih faktora percipiranog povjerenja kupaca EPS-a.
2. Predlaganje modela kombinovane sigurnosti i povjerenja za usvajanje EPS-a.
3. Provođenje empirijske studije za procjenu modela na kupcima EPS-a u Kantonu Sarajevo.
4. Usporedba rezultata s rezultatima sličnih istraživanja.

1.3. Hipoteze istraživanja

Na osnovu ciljeva istraživanja, definisane su istraživačke hipoteze koje glase:

H1: Tehničke zaštite pozitivno su povezane s percipiranom sigurnošću potrošača u EPS-u.

H2: Transakcijski postupci pozitivno su povezani s percipiranom sigurnošću potrošača u EPS-u.

H3: Izjave o sigurnosti pozitivno su povezane s percipiranom sigurnošću potrošača u EPS-u.

H4: Percipirana sigurnost u EPS-u pozitivno je povezana s percipiranim povjerenjem potrošača u EPS.

H5: Percipirano povjerenje u EPS pozitivno je povezano s korištenjem EPS-a od strane potrošača.

1.1. Struktura rada

Završni rad će se sastojati iz teorijskog dijela i sistemskog pregleda, koji će dalje biti podijeljen na naslove i podnaslove. Strukturu rada činit će: uvod, teorijski dio, sistemski pregled literature i zaključak. U uvodu će biti prezentirana tematika rada, problem i predmet istraživanja, istraživački ciljevi i hipoteze i struktura rada. Nakon toga, u drugom poglavlju će se dati osnove o sistemu elektronskog plaćanja, definicijama elektronskog plaćanja i historiji elektronskog plaćanja. U nastavku ovog poglavlja prikazat će se tipovi elektronskog sistema. Treće poglavlje prezentirat će prednosti i nedostatke sistema elektronskog plaćanja. U četvrtom dijelu bit će prikazan pregled literature o percepciji sigurnosti i povjerenja korisnika sistema elektronskog plaćanja. Peto poglavlje se odnosi na metodologiju istraživanja, prezentaciju rezultata istraživanja, te na diskusiju. U petom dijelu rada će se iznijeti zaključci istraživanja i vlastiti osvrt na isto. Za navođenje literature bit će korišten APA stil.

2. SISTEM ELEKTRONSKOG PLAĆANJA

Prodavnica proizvoda i usluga između dvije strane seže od vremena prije početka poznate historije. S vremenom, kako se pokazalo da je razmjena dobara sve teža, jer su ljudi su predstavljali vrijednosti na apstraktan način, napredujući od sistema razmjene preko ovjerenih novčanica, čekova, naloga za plaćanje, debitnih i kreditnih kartica, te današnjeg elektronskog sistema plaćanja (ili e-platni sistemi). Neki dobro poznati problemi ili nedostaci nalaze se u uobičajenim metodama plaćanja: gotovina se može krivotvoriti, čekovi biti odbijeni, a potpisi krivotvoreni. Nasuprot tome, pravilno planirani elektronski sistem plaćanja zaista može pružiti idealnu sigurnost u odnosu na konvencionalne metode plaćanja, uz dodatnu prednost fleksibilnosti u korištenju (Sun et al., 2011; Aigbe i Akpojaro, 2014). Lakoća monetarne razmjene, te dodatno sigurniji i brži pristup kapitalnim resursima doveli su sistem e-plaćanja do velikog napretka u odnosu na sistem koji se zasniva na gotovinskoj valuti (Ayo et al., 2010; Oyewole et al., 2013). Uz nematerijalne transakcije koje postaju sve snažnije u privredi i njihov brži prijenos uz male troškove, konvencionalni sistemi plaćanja imaju tendenciju biti skuplji od današnjih strategija (Singh et al., 2012).

Sistem elektronskog plaćanja može se definisati kao vrsta međuorganizacionog informacijskog sistema (IOS) za novčane transakcije, koji povezuje brojne trgovce i pojedinačne klijente. Posebni atributi IOS-a također ga odvajaju od konvencionalnih internih informacionih sistema, i to tehnološki, relacijski i organizacijski, zamršeniji je i komplikovaniji (Boonstra et al., 2005), naglašavajući značaj saradnje i potrebu objedinjavanja svih aspekata (Briggs, 2011).

2.1. Historija sistema elektronskog plaćanja

Historija e-plaćanja može se pratiti od 1918. godine, kada je američka banka saveznih rezervi prvi put pokrenula elektronsku valutu u Sjedinjenim Američkim Državama (SAD) uz pomoć telegrafa. Međutim, ta tehnologija nije bila naširoko korištena u SAD-u sve do vremena kada je njihova automatizovana obračunska kuća osnovana 1972. Od tog vremena pokazalo se da je elektronski novac prilično popularan. To je omogućilo američkim komercijalnim bankama i centralnoj riznici da izađu s alternativom plaćanja čekom (Kabir MA et al., 2015). Također industrija kreditnih kartica se može pratiti od 1914. godine kada su robne kuće, naftne kompanije, Western Union i hoteli počeli izdavati kartice svojim kupcima kako bi im omogućili plaćanje roba i usluga. Nakon otprilike 40 godina evolucije kreditnih kartica, došlo je do povećanja broja korištenja kreditnih kartica jer su postale prihvatljivije ljudima kao sredstvo plaćanja, naročito u prijevozu. U početku su sve kreditne kartice bile papirne vrste plaćanja, sve do 1990-ih kada su takve kartice potpuno pretvorene u elektronske. Zbog sve većeg broja korištenja kreditnih kartica, industrija je brzo rasla što je dovelo i do uvođenja debitne kartice. Debitne i kreditne kartice sada se koriste u transakcijskim

plaćanjima za sve vrste kupovina ili usluga koje se pružaju širom svijeta (Al-Laham M et al., 2009).

2.2. Definicije sistema elektronskog plaćanja

Sistem elektronskog plaćanja sveobuhvatan je pojam koji opisuje različite isporuke elektronskim višekanalnim putem. E-plaćanje se može posmatrati iz različitih uglova, kao što su e-bankarstvo, m-plaćanje, e-gotovina, internet bankarstvo, e-broking, e-finance i tako dalje. Uzimajući sve u obzir, naučnici su kroz razna istraživanja pokušali definisati e-plaćanje (Oyewole et al., 2013).

Sistem e-plaćanja karakteriše (Abrazhevich, 2004) se kao vrsta finansijske obaveze koja uključuje kupca i trgovca, što je omogućeno korištenjem elektronskih infrastruktura. Osim toga, (Briggs i Brooks, 2011) e-plaćanje posmatra se kao vrsta međuodnosa između trgovaca i kupaca koja su potpomognuta bankama i interswitch kućama koje osnažuju finansijske transakcije elektronskim putem.

Drugo stajalište zastupa (Ogedebe et al., 2012) sistem e-plaćanja kao bilo koju vrstu razmjene novca putem interneta. Na sličan način sistem elektronskog plaćanja aludira na elektronsku metodu plaćanja za robu nabavljenu na webu ili na tržnicama i trgovačkim centrima. Druga definicija sugeriše da su sistemi e-plaćanja izvršena u uslovima elektronske razmjene kao razmjene novca putem elektronskih sredstava (Kaur i Pathak, 2015).

Osim toga, na elektronsko plaćanje se gleda kao na razmjenu novca koja se odvija online između trgovca i kupca (Kalakota i Whinston, 1997). Osim toga, elektronska plaćanja aludiraju na novac i srodne razmjene ostvarene korištenjem elektronskih sredstava. E-plaćanje se definiše i kao plaćanje putem elektronske razmjene podataka kreditnih kartica, izravnim kreditom ili nekim drugim elektronskim sredstvom osim plaćanja gotovinom i čekom (Agimo, 2017).

E-plaćanje se definiše kao plaćanje putem automatizirane klirinške kuće, sistema komercijalnih kartica i elektronskih prijenosa (Lin, 2011). E-plaćanje je okarakterisirano kao svaka kupovina novcem koja je započeta putem kanala elektronske korespondencije. E-plaćanje se također može definisati (Gans i Scheelings, 2017) kao plaćanje izvršeno korištenjem elektronskih signala povezanih s debitnim ili kreditnim računima (Hord, 2017). Još jedna definicija e-plaćanje smatra da je to plaćanje bilo kojom vrstom nenovčanog plaćanja koje ne uključuje papirni ček, odnosno novčanicu (Shon, 1998).

Također, je e-plaćanje smatrao bilo kojom razmjenom elektronske vrijednosti plaćanja od kupca do trgovca putem kanala e-plaćanja koji klijentima omogućuje daljinski pristup i

upravljanje njihovim finansijskim računima i razmjenama putem elektronskog sistema (Ming-Yen, 2013).

Općenito, sistem elektronskog plaćanja je aranžman novčane razmjene među kupcima i prodavačima na mrežnim uslovima koji je podržan digitalnim financijskim instrumentom (na primjer, elektronskim čekovima, kodiranim brojevima kreditnih kartica ili gotovinom u digitalnom obliku) od strane banke, posrednika ili zakonitog saradnika (Oh, 2006).

2.3. Vrste sistema elektronskog plaćanja

Postoji veliki broj usluga e-plaćanja koje su razvijene u sklopu sistema plaćanja širom svijeta. To uključuje elektroničke čekove, e-gotovinu, kreditne kartice i elektroničke prijenose sredstava (Ma, 2003). Općenito, online plaćanje može se podijeliti u dvije vrste: jedno kao Internet Banking Payment Gateway (IBPG) i drugo kao platne platforme autsajdera. Internet Banking Payment Gateway (IBPG) predstavlja svojevrsni izravan način plaćanja, a klijent podrazumijeva online plaćanje putem e-business frameworka koji je povezan s bankarskim okvirom. S druge strane, platne platforme autsajdera uključuju razmjenu novca s računa kupca na račun trgovca putem platforme za plaćanje izvana ili treće strane. IBPG se nalazi među sistemom bankarskih procesa i Internetom. To je sistem koji je posebno napravljen za upravljanje plaćanjem i autorizaciju plaćanja. IBPG je poveznica koja povezuje kupca, trgovca i banku. Online način plaćanja koji se zasniva na IBPG-u ne može postojati bez klijenta koji želi da izvrši plaćanje Yang, 2007).

Prema istraživanju (Yu, 2002), postoje četiri klasifikacije elektronskih sistema plaćanja koje vrijedi spomenuti: elektronska gotovina, online plaćanje kreditnom karticom, mala plaćanja i elektronski čekovi. Oni su naglasili da svaki od ovih sistema ima svoje prednosti i nedostatke. Također su naglasili da se svaki tip može procijeniti kroz ove četiri različite kvalitete, i to: tehnološki aspekt, ekonomski aspekt, društveni aspekt, te institucionalni i pravni aspekt. U stvarnosti se srećemo sa dvije različite vrste sistema plaćanja (Singh et al., 2016): internetski sistemi plaćanja i sistemi plaćanja baziran na elektronskim transakcijama

2.3.1. Internetski sistem plaćanja

2.3.1.1. Debitne kartice

Jedan od najčešće korištenih oblika e-plaćanja je debitna kartica. Tehnika debitne kartice objedinjuje elemente bankomata (ATM) s internetskim bankarstvom. Vlasnik debitne kartice plaća svoju kupovinu direktno putem banke zamjenjujući ček i fizički novac. U ovom

sistemu debitnih kartica klijenti unaprijed polažu novac u banku i podižu ga prilikom kupovine. U stvarnom svijetu postoje dvije vrste debitnih kartica (Kim et al., 2010):

- Online debitna kartica,
- Offline debitna kartica.

2.3.1.2. Kreditne kartice

Ovo je druga vrsta sistema e-plaćanja u kojem postoji korištenje kartice koju je izdala monetarna organizacija vlasniku kartice za plaćanje na webu ili putem elektronskog uređaja bez korištenja papirnatog novca (Singh, 2013). Najčešće korištena vrsta e-plaćanja je kreditna kartica. Za razliku od različitih EPS-a, nije prikladno koristiti kreditne kartice za transakcije malih vrijednosti, tj. razmjene koje ne uključuju samo jedan dolar (Kim et al., 2010).

2.3.1.3. Elektronski novac

Ova tehnika je nastala kao kontrastna opcija korištenju kreditnih kartica za kupovinu putem interneta. To je način elektronskog plaćanja u kojem se određena količina gotovine stavlja na korisnički račun i otvara za transakcije putem interneta. Na elektronski novac dalje možemo gledati kao na gotovinu u digitalnom obliku i koristi se softverom za e-gotovinu koji je instaliran na klijentovom mobitelu ili drugim elektronskim uređajima Istaknuta determinanta elektronske gotovine je njena niska cijena i zbog toga je među najpoticajnijim strategijama za plaćanja manjih transakcija (Singh i Asthi, 2013).

2.3.2. Sistem plaćanja baziran na elektronskim transakcijama

2.3.2.1. Sigurna elektronska transakcija (SET)

Sistem sigurnih elektronskih transakcija je aranžman za online plaćanja za obezbjeđivanje sigurnosti razmjene novca na webu. Određivanje SET-a je otvoren, tehnički standard za poslovanje, koji su stvorili Master Card i VISA. SET omogućava sigurne transakcije platnom karticom putem weba. Promjena povjerenja u cijelom sistemu stvara se pomoću digitalnog certifikata koji potvrđuje legitimitet izdavača kartice i vlasnika (Lu i Smolka, 1999).

2.3.2.2. Cyber novac

Cyber Cash je internetska usluga koja sama obrađuje i potvrđuje podatke o kreditnoj kartici klijenta, a zatim elektronskim putem tereti račun klijenta i polaže novac na račun trgovca. Korisnici cyber novca djeluju kao pristupnik između trgovca na webu i zaštićenog monetarnog sistema banke. Ovaj sistem koristi digitalne potpise kako bi održao sigurnost elektronskog plaćanja (Guttmann, 2002). Dok je novac u elektronskom obliku (e-novac) on je povezan na sve sisteme prijenosa sredstava koji su zasnovani na kompjuteru (ACH, debitne ili kreditne kartice) i hardveru koji je s njima uključen (prodajni terminali, bankomati), dok cyber gotovina stavlja poseban naglasak na sve sisteme za razmjenu novca koji se upravljaju putem weba. Teško je razlikovati elektronski novac od kibernetičkog novca, budući da je zadnji izveden iz prvog i trenutno se, malo po malo, objedinjuje u njega.

3. PREDNOSTI I NEDOSTACI SISTEMA ELEKTRONSKOG PLAĆANJA

3.1. Prednosti sistema elektronskog plaćanja

Po prvi put u historiji, pregled Odbora za politiku finansijskih usluga Federalne rezerve pokazuje da su razmjene elektronskih plaćanja u Sjedinjenim Američkim Državama nadmašile plaćanja čekovima. U 2003. godini je ukupan broj elektronskih razmjena iznosio 44,5 milijardi dolara, dok je količina plaćenih čekova iznosila 36,7 milijardi dolara. Očito se može prepoznati obrazac među kupcima, u kojem se vidi da su kupci spremniji raditi s elektronskim transakcijama i koristiti automatizovani medij za obavljanje svog poslovanja.

Kao što je navedeno u istraživanju, prodor weba doveo je do eksponencijalnog razvoja elektronskih plaćanja i razmjena. Kupci su mogli kupovati robu s interneta i slati brojeve kreditnih kartica u nešifriranom obliku preko sistema, što je transakcije činilo prilično pogodnim na prijetnje i prijevare (Fiallos, 2005). S razvojem sistema e-plaćanja pojavio se širok izbor novih sigurnih sistema plaćanja jer se pokazalo da korisnici više vode računa o svojoj zaštiti i sigurnosti. Kao što tvrdi, elektronska plaćanja imaju značajan broj finansijskih prednosti uz njihovu sigurnost i jednostavnost rada. Ove prednosti kada se prošire mogu znatno pridonijeti finansijskom poboljšanju zemlje (Hord, 2017).

Kompjuterizovana elektronska plaćanja pomažu u razvoju depozita u bankama i na taj način povećavaju rezerve dostupne za poslovne s kreditima, što se smatra pokretačem finansijskih postignuća. Povoljna i sigurna elektronska plaćanja sa sobom nose značajan obim finansijskih prednosti u punom kapaciteti.

EPS može biti od pomoći u iskorjenjivanju sivih ekonomija, uvođenju maskiranih razmjena u bankarski sistemima i pomoći u unošenju jednostavnosti, saradnje i povjerenja u ekonomski sistem. Također, postoji odnos između porasta depozita po viđenju i povećanja prodajnih volumena. Automatizovano elektronsko plaćanje djeluje kao ulaz u bankarski sektor i kao snažan pokretač rasta privrede (Humphrey, 2001). Takva plaćanja izvlače gotovinu iz opticaja i stavljaju je na bankovne račune, osiguravajući jeftina sredstva koja se mogu koristiti za podršku bankarskim zajmovima za ulaganja što predstavlja pokretač ukupne privredne aktivnosti. Proces stvara veću transparentnost i odgovornost, što dovodi do veće učinkovitosti i boljeg ekonomskog efekta.

Prema Hordu (2017), elektronsko plaćanje veoma je korisno za kupca. Većinu vremena od korisnika se traži da jednom unese podatke o svom računu, na primjer broj kreditne kartice i adresu za dostavu. Podaci se zatim čuvaju u bazi podataka web trgovca. Kada se klijent vrati na istu web stranicu, jednostavno se prijavljuje svojim korisničkim imenom i šifrom. Završetak transakcije je jednostavan jednom klikom miša. Sve što korisnik kartice treba da učiniti je da potvrditi svoju kupovinu i gotovo.

Također, elektronska plaćanja se koriste kako bi se smanjili troškovi organizacije (Appiah i Agyemang, 2006). Manje se novca troši na papir i poštarinu, uz sve veći broj elektronskih plaćanja. Predstavljanje mogućnosti elektronskog plaćanja također može pomoći organizacijama da poboljšaju očuvanje klijenata. Vjerojatnije je da će se kupac vratiti na istu stranicu e-kupovine gdje su njegovi ili njeni podaci već uneseni i pohranjeni.

Elektronska plaćanja mogu smanjiti transakcijske troškove, potaknuti veću potrošnju i BDP, povećati učinkovitost vlade, potaknuti financijsko posredovanje i poboljšati financijsku transparentnost. Ona dodatno navodi da vlade igraju veoma važnu ulogu u stvaranju okruženja u kojem se te koristi mogu postići na način koji je u skladu s njihovim vlastitim planovima privrednog razvoja (Nutham i Rashimi, 2014).

Isto tako, istraživanje od Humphreya i saradnika (2001) podupire realnost da korištenje elektronskih sistema plaćanja osigurava ogromnu prednost i trgovcima i kupcima, jer su troškovi smanjeni, veća je jednostavnost korištenja i veća sigurnost, pouzdana sredstva plaćanja i nemjerljiv raspon proizvoda i kompanija koji se nude širom svijeta putem weba ili drugih elektronskih sistema. Jedna takva prednost je da elektronski sistemi plaćanja omogućuju klijentima banke da obavljaju svoje svakodnevne novčane transakcije bez posjeta poslovnice banke. Elektronska plaćanja mogla bi trgovcu uštedjeti vrijeme i troškove u brizi o novcu.

Trošak imovine platnog okvira neke zemlje može predstavljati 3% njenog BDP-a. Budući da većina elektronskih sistema plaćanja košta samo oko 33% do 50% nenovčanog plaćanja zasnovanog na papiru, jasno je da bi društveni trošak okvira plaćanja mogao biti daleko manji ako je digitalizovan (Humphrey et al., 2000). Mehanizacija i preslagivanje elektronskih plaćanja proizvedenih korištenjem samouslužnih kanala, kao što su bankomati, sistemi prodajnih mjesta (POS) i terminala poslovnica, može smanjiti pogreške i troškove zasnovane na papiru.

Ispitivanje koje je dovršilo udruženje Visa Canada kao tim s Global Insightom otkrilo je da sistemi elektronskog plaćanja kupcima, trgovcima, bankama i privredama u cjelini pružaju vještinu u transakcijama. Elektronska plaćanja doprinijela su 107 milijardi dolara kanadskoj privredi od 1983. godine i čine oko 25% ukupnog razvoja kanadske privrede u navedenom periodu od 437 milijardi dolara. Tokom ista dva desetljeća, 60 milijardi USD ekspanzije troškova za ličnu potrošnju bilo je posebno moguće izvesti iz elektronskog plaćanja, pri čemu je kreditna kartica imala glavni udio u ovom razvoju (49,4 milijarde USD) u usporedbi s debitnim karticama (USD 10,4 milijarde) (Kumaga, 2012).

3.2. Nedostaci sistema elektronskog plaćanja

Uprkos brojnim prednostima elektronskih sistema plaćanja, oni imaju svoje poteškoće i izazove čak i u današnjem tehnološki naprednom svijetu. Izazovi koje su identifikovali prethodni istraživači su infrastrukturna, regulatorna, pravna i socio-kulturna pitanja.

3.2.1. Infrastruktura

Infrastruktura je osnova za učinkovito izvršenje elektronskog plaćanja. Odgovarajuća infrastruktura za elektronska plaćanja može predstavljati problem (Taddesse i Kidan, 2005). Da bi elektronska plaćanja bila uspješna, neophodno je imati finansijski potkovanu i pouzdanu infrastrukturu koju može koristiti veliki dio stanovništva. U zemljama u razvoju veliki dijelovi zemlje nemaju banke i nemaju pristup osnovnoj infrastrukturi koja pokreće elektronska plaćanja. S tim u vezi, istraživanje koje je proveo otkriva da u Nepalu električna energija i telekomunikacije nisu dostupni u cijeloj zemlji, što neosporno utiče na napredak e-plaćanja (Mishra, 2008).

3.2.2. Regulatorna i pravna pitanja

Nacionalno, pokrajinsko ili globalno uređenje države i zakona, standarda i raznih drugih smjernica neophodni su preduslovi za učinkovito izvršenje e-plaćanja. Značajan dio komponenti uključuje smjernice o utaji poreza, nadzoru organizacija e-novca i poslovnih banaka od strane stručnjaka za nadzor. Centralne banke trebale bi kontrolisati sisteme plaćanja, zaštitu kupaca i informacija, učestvovanje i pitanja rivalstva. Kao što je navedeno od naučnika (Taddesse i Kidan, 2005), virtualna priroda e-plaćanja dodatno otvara pravna pitanja, na primjer koji su zakoni relevantni u spornim slučajevima i koja će jurisdikcija biti nadležna, legitimnost digitalnih potpisa i elektronskih ugovora. Legitimna i administrativna struktura koja gradi samopouzdanje i pomaže u tehničkim naporima ključno je pitanje kojem se treba posvetiti u izvršavanju e-plaćanja.

3.2.3. Socio-kulturni izazovi

Društvene i kulturne razlike u pogledima i korištenju različitih vrsta gotovine (korištenje kreditnih kartica u Sjevernoj Americi i korištenje debitnih kartica u Europi) ometaju posao izgradnje elektronskog sistema plaćanja koji je relevantan na globalnom nivou. Kao što je naznačeno u (Taddesse i Kidan, 2005), razlika u nivou potrebne sigurnosti i produktivnosti među pojedincima u različitim društvima i stepenu napredovanja pogoršava problem.

Kupčevo povjerenje u uobičajene metode plaćanja čini klijente sklonijim prihvatanju novih inovacija. Nove inovacije neće vladati tržištem sve dok klijenti ne budu sigurni da je njihova privatnost osigurana i da je osigurana zadovoljavajuća potvrda sigurnosti (Taddesse i Kidan, 2005). Nova postignuća također moraju izdržati test vremena kako bi osigurala povjerenje ljudi, bez obzira na činjenicu da su jednostavnija za korištenje i jeftinija od standardnih tehnika (Kumaga, 2012).

3.3. Sigurnost sistema e-plaćanja

Nedostatak povjerenja, privatnosti i sigurnosti uvijek se u poslovnim analizama navodi kao jedan od značajnih faktora koji koče napredak sistema e-trgovine. S brzim usvajanjem sistema e-plaćanja povećavajući priliku za napad na internetu, privatnost i sigurnost postaju bitan faktor za svaki sistem e-plaćanja.

Budući da je Internet otvorena mreža bez izravne ljudske kontrole nad pojedinačnim transakcijama, tehnička infrastruktura koja podržava EC i EPS mora biti otporna na sigurnosne napade. Tehničke zaštite koje su osmišljene da smanje ovu vrstu rizika moraju se uzeti u obzir prije nego što se počne rješavati problem povjerenja potrošača. Kalakota i Whinston (1997) procjenjuju neka od pitanja povezanih sa sigurnošću EPS-a. Oni napominju da EPS treba ojačati protiv sigurnosnih proboja i da treba pažljivo razmotriti ranjivost EPS-a. Sigurnost transakcija e-plaćanja zavisi od nizu faktora, kao što su faktori sistema, tj. tehnička infrastruktura i implementacija (Laudon i Traver, 2001; Linck et al., 2006), faktori transakcije, tj. sigurno plaćanje u skladu sa specifičnim i dobro definisanim pravilima (Hwang et al., 2007; Lim, 2008), te pravni faktori, tj. pravni okvir za elektronske transakcije (Peha i Khamitov, 2004). Pregledavajući postojeće sigurnosne tehnologije za EPS, uključujući enkripciju i tehnike autentifikacije, Slyke i Belanger (2003) zaključuju da bi siguran sistem e-plaćanja trebao pružiti sigurnost od lažnih aktivnosti, te da mora štititi privatnost potrošača. Konačno, Romdhane (2005) govori o važnosti sigurnosne procjene za EPS i tvrdi da siguran sistem e-plaćanja mora sadržavati sljedeće komponente:

- Integritet - koji uključuje autentifikaciju, sprječavanje prijevara i privatnost;
- Djeljivost - prenosivost, sprječavanje dvostruke potrošnje, povjerljivost plaćanja, anonimnost plaćanja i sljedivost platitelja.

3.2.4. Sigurnosni zahtjevi u sistemima e-plaćanja

3.3.1.1. Integritet i ovlaštenje

Integritet se može okarakterisati kao valjanost, tačnost i potpunost podataka prema poslovnim kvalitetama i željama. U sistemima plaćanja, integritet podrazumijeva da se od klijenta ne uzima gotovina osim ako klijent odobri plaćanje. Trgovci ne moraju prihvatiti nikakvo plaćanje bez apsolutnog dopuštenja klijenata (Asokan et al., 1996).

3.3.1.2. Povjerljivost

Povjerljivost se može definisati kao sigurnost ličnih ili osjetljivih podataka od neodobrenog otkrivanja. Nekoliko uključenih organizacija možda će htjeti imati povjerljivost u svojim razmjenama. Povjerljivost podrazumijeva ograničenje znanja o različitim dijelovima podataka koji su povezani s transakcijom, kao što su provjera uplatitelja/primatelja, sadržaj kupovine, iznos itd. Obično uključeni članovi žele osigurati da su transakcije tajne (Asokan et al., 1996). Tamo gdje se traži neupadljivost ili anonimnost, preduslov može biti da se te informacije stave na raspolaganje samo određenim specifičnim podskupovima među učesnicima.

3.3.1.3. Dostupnost i pouzdanost

Dostupnost osigurava da su podatkovni okviri i informacije pripremljeni za korištenje kada su potrebni (Omotunde et al., 2013). Na primjer redovno se priopćava kao stopa vremena u kojem se okvir može koristiti za profitabilan rad. Svi dijelovi moraju imati kapacitet izvršiti ili primiti plaćanja kad god se za to ukaže potreba.

3.4.Poboljšanje sigurnosti e-plaćanja

Prema (Zandi et al., 2013), najpriznatija strategija za osiguranje e-plaćanja je korištenje inovacija zasnovanih na kriptografiji, na primjer digitalnih potpisa i enkripcije. Prilikom primjene, ove inovacije smanjuju brzinu i stručnost i zbog toga se mora napraviti kompromis između učinkovitosti i sigurnosti. Slijedi nekoliko načina za osiguranje e-plaćanja.

3.4.1. Sigurna elektronska transakcija (SET)

Ovo je otvoreni standard koji su izradile Visa i Master Card kako bi dale odgovor na sigurnosna pitanja za online sistem plaćanja koji uključuje kreditne kartice. To se postiže davanjem digitalnog certifikata i klijentu i trgovcu. Kao što je naznačio (Taddesse, 2005), ljudi to nisu podržali budući da je bilo složeno i da su i klijent i trgovac trebali preuzeti softver od 5 MB.

3.4.2. 3D Secure i Sigurnost pametne kartice

To je alternativa SET-u koji je izradila Visa SET i ne obavezuje posjedovanje certifikata za provjeru (Newstead, 2017). Informacije koje se nalaze na pametnoj kartici kodirane su po prirodi i ne mogu se koristiti bez PIN-a, te je stoga osigurana dobra sigurnost. Siyanbola (2013) tvrdi da chip kartice potiskuju kartice koje uključuju magnetske trake, tj. kreditne kartice, debitne kartice i tako dalje. Legitimni angažmani, metodologija i odgovarajući državni zakoni također bi trebali biti uspostavljeni kako bi se osigurao napredak, dajući najbolju moguću sigurnost (Oginni, 2013).

4. PRETHODNA ISTRAŽIVANJA O SIGURNOSTI I POVJERENJU KORISNIKA SISTEMA ELEKTRONSKOG PLAĆANJA

U ovom dijelu će se raspravljati o različitim vrstama postojećih metoda transakcije e-plaćanja koje su svojim radom uveli različiti istraživači. Ovo istraživanje u sklopu završnog rada će analizirati i ocijeniti te metode na osnovu njihove metrike izvedbe i dati kratak opis nakon istraživanja.

Od posljednja tri desetljeća do danas, kontinuirani je razvoj informacijskih i komunikacijskih tehnologija. Finansijske organizacije slijede politiku elektronskog posredovanja za transakcije fondova (Black et al., 2002). Prvi bankomat lansiran je 1970. godine, nakon čega su uslijedile usluge telefonskog bankarstva 1980-ih, usluge internetskog bankarstva 1990-ih, te m-banking 2000-ih (Barnes i Corbitt, 2003) Međutim, stopa usvajanja sistema e-plaćanja manja je od njegove stope razvoja (Hoele et al., 2012). Glavni izazovi su: sigurnost podataka, privatnost i sigurnost, curenje informacija od strane trgovaca i trećih strana. Takvi problemi imaju negativan uticaj direktno na usvajanje usluga e-bankarstva i povjerenje korisnika (Eastlick et al., 2006)

Cao i Zhu (2018) predstavili su shemu sigurne transakcije e-gotovine koja čuva privatnost za usluge prijevoza. Također, ovi autori su predstavili autentifikovani mehanizam lančanog raspršivanja kako bi e-plaćanje bilo djeljivo i ponovno upotrebljivo, što proširuje fleksibilnost transakcijskih sistema. Mehanizam mobilnog plaćanja prikazan je u (Abughazalah et al., 2014) primjenom sheme jednokratne lozinke. Dok su Qin i saradnici (2017) predložili novi okvir za sisteme m-plaćanja koji osiguravaju mobilni novčanik pomoću mehanizma digitalnog potpisa i metoda pseudoidentiteta.

Zahra i saradnici (2017) predstavili su istraživanje o faktorima koji utiču na povjerenje tokom online plaćanja u Iranu. Prikupili su faktore koji utiču na povjerenje i razvili sigurnosni model zasnovan na informacijama o transakcijama, dostupnosti i upotrebljivosti platnog sistema. Na kraju, autori su uporedili rezultate sa sličnim istraživanjima. Sličan pristup zastupaju Karmi i saradnici (2014), gdje je autor istraživao značajne faktore, tj. društvene web stranice, marketinške strategije, povjerenje, upotrebljivost, odnose s kupcima, pristupačnost koji utiču na sistem e-tržišta.

Danas je dostupno nekoliko sistema e-plaćanja koji rade na pametnim uređajima i omogućavaju bolju komunikaciju uz minimalne troškove. Ali anonimnost korisnika prilično je izazovna jer trenutni sistemi plaćanja pružaju samo privatnost transakcije, a značaj visoke sigurnosti nije na visini. Zbog toga je Breaken (2017) kao gledište anonimnosti korisnika, predstavio poboljšanu verziju sistema e-plaćanja za slijepe i slabovidne korisnike. Ovaj mehanizam također je primjenjiv za razvoj sistema plaćanja na maloprodajnim mjestima za kupce koji koriste mobilni telefon kao proxy. U Chaudhry i saradnici (2015) su riješili probleme anonimnosti korisnika i pokazali sigurnosne slabosti. Brzim usvajanjem načina e-plaćanja putem mobitela ili pametnih telefona, svakodnevni život i rad korisnika postaju

lakši, ali i praktičniji. E-plaćanje putem mobilnih telefona je sveprisutno u komercijalnim područjima u usponu (Ortiz-Yepes, 2016) Međutim, kod za brzi odgovor (tj. QR kod) relativno je nova komunikacijska tehnologija koja olakšava pohranu, prijenos i prepoznavanje podataka, a mobilni uređaj može prepoznati informacije s bilo kojeg mjesta (Subpratatsavee i Kuacharoen, 2015). Tehnologija QR kodova sve se više koristi u sigurnosno osjetljivim aplikacijskim područjima, na primjer kao što su sistemi plaćanja (Zhang et al., 2014).

Suryotrisongko i saradnici (2012) su predložili je novi sistem mobilnog plaćanja za zadružna trgovaca u zemljama u razvoju. Ovo istraživanje poboljšalo je prethodnu QR strategiju plaćanja smanjujući problem povezivanja s mrežom, jer se neke zemlje u razvoju suočavaju s poteškoćama s internetskom vezom. Uvedena su dva glavna faktora, tj. autentifikacija i QR šifrirane informacije za povećanje sigurnosti. Zbog toga predložena shema omogućuje više pogodnosti i jaku sigurnost za lakši prijenos novca pomoću mobilnog telefona. Tako autori zaključuju da se ovaj mehanizam odnosi na zemlje u razvoju.

Dey i saradnici (2015) uveli su alternativni pristup QR koda koji omogućuje korisničko suočavanje i iskoristio za ugradnju informacija u grafički format uz pomoć mobilnih aplikacija na pametnim telefonima. U drugom istraživačkom radu, Lu i saradnici koristili su sličan mehanizam QR koda zbog njegovih isplativih karakteristika posebno za sistem mobilnog plaćanja. Također je uvedena vizualna kriptografska metoda koja je pokazala izvedivost i sigurnosni faktor za autentifikaciju m-plaćanja.

Chitra i saradnici (2017) predstavili su modul digitalne kartice koji koristi biometrijski sistem koji je nazvan swing-pay metodom. Cilj predložene metode je korištenje otisaka prstiju korisnika za autentifikaciju. Ova metoda pruža učinkovit i siguran sistem plaćanja uz pomoć GSM-a, napojne jedinice, Cortex-M3, Bluetooth uređaja itd. Iz ove analize može se zaključiti da iz ove metode korisnik može dobiti transakciju primljenu porukom od poslužitelja za platitelja.

Među nekoliko aplikacija za e-plaćanje, usluge plaćanja u javnom prijevozu najčešće su korištene aplikacije za mobilne sisteme plaćanja. Aplikacija prethodne usluge prijevoza ne može obraditi informacije koje putnici predočavaju od organizacija, odnosno prijevozničkih agencija, bankarskih institucija, mobilnih operatera i davatelja pametnih kartica itd. Zbog toga su u istraživanju Kang i Nyang (2016) predložili jednostavan pristup sistema plaćanja koji čuva privatnost kako bi se sačuvale putničke informacije o masovnom prijevozu. Ovaj pristup olakšava pristup proaktivnog blokiranja za loše postupanje s putnicima, popust na transfer i postpaid uslugu.

Predloženo je više shema e-plaćanja gdje je primarni motiv povećati nivo sigurnosti tokom procesa e-transakcije. Ali neke tradicionalne metode ne nude zahtjev neporicanja od strane klijenta. Zbog toga napadač može lako odbiti e-transakciju i prodavač možda neće dobiti novac. Kako bi prevladali takvu vrstu izazova, Yang i Lin (2016) istražili su mehanizam

plaćanja anonimnosti za kompjuter u cloudu. Predložena metoda nudi zahtjev neporicanja od strane klijenta uz minimalne troškove. Iz komparativne analize autori zaključuju da je predloženi mehanizam e-plaćanja pravedniji, sigurniji i visoko učinkovit, te prikladan za računalstvo u cloudu u stvarnom vremenu.

U istraživačkom radu Kang i Xu (2016) predstavili su prilično sličan pristup anonimno sigurnom sistemu plaćanja e-gotovinom kako bi se osigurala privatnost korisnika. U ovom istraživanju autori ističu Chen et al. da je rad podložan nekim nedostacima. Doprinos je bio predstavljanje izvanmrežnog mehanizma e-gotovine s opozivom. Predložena studija osigurava značajno izbjegavanje prijevara trgovaca na malo. Sličnu istraživačku studiju o izvanmrežnom sistemu plaćanja e-gotovinom proveli su Fan i saradnici (2014). Autori su dizajnirali elektronski protokol obnove gotovine, gdje korisnici mogu zamijeniti svoje istekle i neiskorištene valute za druge.

Chitra i Kumar (2012, 2013) predstavili su pouzdan i siguran mehanizam mikro plaćanja. U radu (2012) autori su dizajnirali sigurnu arhitekturu sistema mikro plaćanja za bežičnu mrežu. Za sigurnosni proces autor je koristio pristup uvezivanja hash vrijednosti, a jednostavan kripto sistem s javnim ključem koji olakšava sigurno usmjeravanje tokom m-transakcija također nudi učinkovitu metodu za sistem digitalnih kovanica. U radu (2013) autori predstavili proširenu verziju prethodne studije koja se bavila sigurnosnim implikacijama sistema mikro plaćanja pomoću mobilnog agenta.

5. EMPIRIJSKO ISTRAŽIVANJE O VAŽNOSTI EMOCIONALNE INTELIGENCIJE

Od ukupno 987 ispitanika koji su pristupili ovom istraživanju, 58,7% su bile osobe ženskog spola (njih 579), dok je 41,3% bilo osoba muškog spola (njih 41,3%). To znači da su više od pola ispitanika pripadnice ženskog spola. Spolna struktura stanovnika prikazana je u tabeli 1.U nastavku su opisani instrument, uzorak, način provođenja istraživanja i obrada podataka.

Tabela 1 Spolna struktura ispitanika

Spolna struktura ispitanika		
	Broj ispitanika (N)	Procenat (%)
Muški	408	41.3
Ženski	579	58.7

5.1.Metodologija istraživanja

Istraživački dio rada podrazumijeva prikupljanje primarnih podataka, uz korištenje metode anketiranja, uz pomoć strukturisanog upitnika. Istraživački dio rada podrazumijeva prikupljanje primarnih podataka. Upitnik se sastoji od demografskih pitanja (spol, dob, mjesto rođenja), te pitanja prilagođenih iz upitnika koji su predložili Linck et al. (2006), koja ispituju percepciju korisnika o sigurnosti elektronskog plaćanja. Ovaj test se sastoji od 29 pitanja podijeljenih u 6 kategorija: transakcijski postupci u EPS-u, tehnička zaštita u EPS-u, sigurnosne izjave u EPS-u, percipirana sigurnost u EPS-u, percipirano povjerenje u EPS, obimu korištenja EPS-a. Ispitivanje se vrši uz pomoć Likertove skale, ocjenama od 1 do 5 pri čemu ocjena 1 znači da ispitanik se uopšte ne slaže sa tvrdnjom, a 5 znači da se potpunosti slaže sa navedenom tvrdnjom. Planirano istraživanje će obuhvatiti 1000 stanovnik Kantona Sarajevo koji pristanu popuniti anketu.

Prilikom testiranja definisanih hipoteza istraživanja koristit će se višestruka regresiona analiza. Podaci će biti prikupljeni korištenjem „Google Forms“ platforme. Za statističku obradu podataka planirano je koristiti „Statistical Package for the Social Sciences, 26.0 (SPSS)“ program.

Nakon što se sprovede istraživanje, analiza i obrada podataka vršit će se korištenjem različitih metoda:

- metodom deskripcije opisati će se pojave i predmeti, kao i njihove veze i odnosi, ali bez naučnog objašnjavanja i tumačenja.
- Zatim koristit metodu analize dokumentacije koja obuhvata prikupljanje i proučavanje stručne literature, članaka kao i obradu prikupljenih podataka.
- Induktivnom metodom doći će se do općih zaključaka polazeći od pojedinačnih premisa.
- Metodom sinteze izvršiti će se spajanje dijelova ili elemenata u cjelinu, tj. sastavljanje jednostavnih misaonih tvorevina u složenije.
- Komparativnom metodom usporediti će se iste ili slične pojave, te će se istaći njihova zajednička obilježja ili razlike.
- Metodom kompilacije predstaviti preuzete tuđe rezultate naučnoistraživačkog rada, odnosno tuđih spoznaja, zaključaka, stavova i opažanja.

5.2.Rezultati istraživanja

Što se tiče nivoa obrazovanja ispitanika, najviše odgovora je stiglo od ispitanika koji studiraju ili su završili drugi ciklus obrazovanja (njih 34,9%), zatim osobe koje završavaju ili imaju završenu srednju stručnu spremu (njih 24,6%). Nakon njih su osobe sa visokom stručnom spremom (20%), onda ispitanici koji studiraju ili su završili prvi ciklus obrazovanja (18%), i na kraju osobe trećeg ciklusa studija (2,5%). Obrazovna struktura ispitanika prikazana je u tabeli 2.

Tabela 2 Demografska statistika – zastupljenost ispitanika prema nivou obrazovanja

Nivo obrazovanja ispitanika		
	Broj ispitanika (N)	Procenat (%)
Drugi ciklus visokog obrazovanja	344	34.9
Prvi ciklus visokog obrazovanja	178	18.0
SSS	243	24.6
Treći ciklus visokog obrazovanja	25	2.5
VSS	197	20.0

Na pitanje o nazivu banke čije usluge koriste, najviše odgovora je stiglo od korisnika UniCredit Banke (31,6%), zatim nešto malo manje od korisnika Raiffeisen Banke (24,6%), onda Intesa San Paolo Banke (20,5%). Ostale navede banke ne prelaze postotak od 10% zastupljenosti. Od preostalih najbrojnija ja ASA Banka (7,2%), BBI Banka (4,8%), Addiko Banka (3,6%), NLB Banka (2,2%), Ziraat Banka i Sparkasse banka (obje po 1,9%), te najmanje odgovora je stiglo od ispitanika Nove banke (1,6%). Zastupljenost banaka čije usluge koriste ispitanici prikazana je u tabeli 3.

Tabela 3 Odgovori na tvrdnju "EPS uvijek traži korisničko ime i šifru kada se prijavljujete."

EPS uvijek traži korisničko ime i šifru kada se prijavljujete.		
	Broj ispitanika (N)	Procenat (%)
1	131	13.3
2	19	1.9
3	176	17.8
4	166	16.8
5	495	50.2

Na pitanje "EPS uvijek traži korisničko ime i šifru kada se prijavljujete." 50,2% ispitanika je odgovorilo da se u potpunosti slaže s navedenom tvrdnjom, dok samo 1,9% ispitanika tvrdi da se ne slaže s navedenom tvrdnjom. Rezultati odgovora prikazani su u tabeli 4.

Tabela 4 Odgovori na tvrdnju "EPS pruža različite mjere za provjeru autentičnosti."

EPS pruža različite mjere za provjeru autentičnosti.		
	Broj ispitanika (N)	Procenat (%)
1	69	7.0

2	47	4.8
3	265	26.8
4	190	19.3
5	416	42.1

Naredno pitanje u anketi se odnosilo na pružanje različitih mjera za provjeru autentičnosti. Najviše odgovora, njih 42,1%, smatra da njihov EPS u potpunosti pruža različite mjere za provjeru autentičnosti, dok samo 4,8% ispitanika smatra da ne pruža. Rezultati odgovora prikazani su u tabeli 5.

Tabela 5 Odgovori na tvrdnju "Stranice na kojima plaćate putem EPS-a Vam nudi priliku da promijenite bilo koji podatak o plaćanju prije završne faze procesa plaćanja."

Stranice na kojima plaćate putem EPS-a Vam nudi priliku da promijenite bilo koji podatak o plaćanju prije završne faze procesa plaćanja.		
	Broj ispitanika (N)	Procenat (%)
1	74	7.5
2	71	7.2
3	258	26.1
4	219	22.2
5	365	37.0

37% ispitanika u potpunosti smatra da im stranice na kojima plaćaju putem EPS-a Vam nude priliku da promijene bilo koji podatak o plaćanju prije završne faze procesa plaćanja, dok njih 7,5% se uoće ne slaže s navedenom tvrdnjom. Rezultati odgovora prikazani su u tabeli 6.

Tabela 6 Odgovori na tvrdnju "Stranice na kojima plaćate putem EPS-a Vam nudi korak za provjeru plaćanja prije finaliziranja stvarnog plaćanja."

Stranice na kojima plaćate putem EPS-a Vam nudi korak za provjeru plaćanja prije finaliziranja stvarnog plaćanja.		
	Broj ispitanika (N)	Procenat (%)
1	79	8.0
2	68	6.9
3	165	16.7
4	153	15.5
5	522	52.9

Najviše ispitanika (52,9%) je odgovorilo da se u potpunosti slaže s tvrdnjom da im stranice na kojima plaćaju putem EPS-a nude korak za provjeru plaćanja prije finaliziranja stvarnog plaćanja. Samo 6,9% ispitanika se ne slaže s tom tvrdnjom. Rezultati odgovora prikazani su u tabeli 7.

Tabela 7 Odgovori na tvrdnju "Stranice na kojima plaćate putem EPS-a obično prikazuju sažetak podataka o plaćanju (trošak, primalac...) i konačni iznos plaćanja."

Stranice na kojima plaćate putem EPS-a obično prikazuju sažetak podataka o plaćanju (trošak, primalac...) i konačni iznos plaćanja.		
	Broj ispitanika (N)	Procenat (%)
1	51	5.2
2	43	4.4
3	137	13.9

4	206	20.9
5	550	55.7

Najveći broj ispitanika (55,7%) smatra da je tvrdnja "Stranice na kojima plaćate putem EPS-a obično prikazuju sažetak podataka o plaćanju (trošak, primalac...) i konačni iznos plaćanja." u potpunosti tačna. Samo 4,4% ispitanika se ne slaže s tom tvrdnjom. Rezultati odgovora prikazani su u tabeli 8.

Tabela 8 Odgovori na tvrdnju "Potvrda Vam se šalje putem jednog od nekoliko dostupnih načina (e-mailom, notifikacijama, itd) kako bi Vas uvjerili da je uplata zaista primljena."

Potvrda Vam se šalje putem jednog od nekoliko dostupnih načina (e-mailom, notifikacijama, itd) kako bi Vas uvjerili da je uplata zaista primljena.		
	Broj ispitanika (N)	Procenat (%)
1	60	6.1
2	69	7.0
3	140	14.2
4	216	21.9
5	502	50.9

Čak 50,9% ispitanika od banke dobiva potvrdu putem jednog od nekoliko dostupnih načina (e-mailom, notifikacijama, itd) kako bi ih uvjerili da je uplata zaista primljena. Dok samo 6,1% ispitanika isto ne dobiva. Rezultati odgovora prikazani su u tabeli 9.

Tabela 9 Transakcijski postupci u EPS-u (grupa)

Transakcijski postupci u EPS-u (grupa)		
	Broj ispitanika (N)	Procenat (%)
1 – 2	60	6.1
2 – 3	76	7.7
3 - 4	223	22.6
4 – 5	490	49.6
5	138	14.0

Najveći broj ispitanika (49,6%) je transakcijski postupak u EPS-u je ocijenio ocjenama u rasponu od 4 do 5. Rezultati odgovora prikazani su u tabeli 10.

Tabela 10 Odgovori na tvrdnju "Vaši lični podaci, poput podataka za kontakt ili podataka o plaćanju, nikada nisu ukradeni zbog korištenja EPS-a."

Vaši lični podaci, poput podataka za kontakt ili podataka o plaćanju, nikada nisu ukradeni zbog korištenja EPS-a.		
	Broj ispitanika (N)	Procenat (%)
1	74	7.5
2	52	5.3
3	119	12.1
4	75	7.6
5	667	67.6

Na konstataciju "Vaši lični podaci, poput podataka za kontakt ili podataka o plaćanju, nikada nisu ukradeni zbog korištenja EPS-a." najviše odgovora je došlo od ispitanika koji se u potpunosti slažu s tvrdnjom (njih 67,7%), dok je najmanje ispitanika koji se ne slažu s tvrdnjom, njih 5,3%. Rezultati odgovora prikazani su u tabeli 11.

Tabela 11 Odgovori na tvrdnju "EPS pružaoci usluga nisu dali Vaše lične podatke drugim stranama u bilo koje druge svrhe."

EPS pružaoci usluga nisu dali Vaše lične podatke drugim stranama u bilo koje druge svrhe.		
	Broj ispitanika (N)	Procenat (%)
1	69	7.0
2	67	6.8
3	196	19.9
4	83	8.4
5	572	58.0

Najveći broj ispitanika (58%) smatra da je tvrdnja "EPS pružaoci usluga nisu dali Vaše lične podatke drugim stranama u bilo koje druge svrhe." u potpunosti tačna. 6,8% ispitanika se ne slaže s tom tvrdnjom. Rezultati odgovora prikazani su u tabeli 12.

Tabela 12 Odgovori na tvrdnju "Iznos plaćanja ili podaci o transakciji koji su prikazani na EPS-u uvijek su tačni."

Iznos plaćanja ili podaci o transakciji koji su prikazani na EPS-u uvijek su tačni.		
	Broj ispitanika (N)	Procenat (%)
1	46	4.7

2	19	1.9
3	120	12.2
4	230	23.3
5	572	58.0

Na pitanje da li su iznosu plaćanja ili podaci o transakciji koji su prikazani na EPS-u uvijek tačni, najviše odgovora je stiglo za odgovor da se u potpunosti slažu s tvrdnjom (58%), dok je najmanje stiglo za odgovor da se ne slažu s ovom tvrdnjom (1,9%). Rezultati odgovora prikazani su u tabeli 13.

Tabela 13 Odgovori na tvrdnju "Smatrate da su podaci o transakcijama EPS-a koji se prenose putem interneta sigurni i zaštićeni."

Smatrate da su podaci o transakcijama EPS-a koji se prenose putem interneta sigurni i zaštićeni.		
	Broj ispitanika (N)	Procenat (%)
1	67	6.8
2	92	9.3
3	309	31.3
4	281	28.5
5	238	24.1

Najviše ispitanika (31,3%) je odgovorilo da se niti slaže niti ne slaže s tvrdnjom "Smatrate da su podaci o transakcijama EPS-a koji se prenose putem interneta sigurni i zaštićeni.", a najmanje odgovora je stiglo za odgovor da se ne slaže s tvrdnjom (6,8%). Rezultati odgovora prikazani su u tabeli 14.

Tabela 14 Odgovori na tvrdnju "Usluge plaćanja uvijek su dostupne u bilo koje vrijeme u toku dana."

Usluge plaćanja uvijek su dostupne u bilo koje vrijeme u toku dana.		
	Broj ispitanika (N)	Procenat (%)
1	50	5.1
2	67	6.8
3	184	18.6
4	257	26.0
5	429	43.5

43,5% ispitanika su usluge plaćanja uvijek dostupne u bilo koje vrijeme u toku dana, dok njih 5% nema uvijek dostupnu tu uslugu. Broj odgovora prikazan je u tabeli 15.

Tabela 15 Odgovori na tvrdnju "Privremene ili iznenadne pogreške često se događaju tokom EPS transakcije."

Privremene ili iznenadne pogreške često se događaju tokom EPS transakcije.		
	Broj ispitanika (N)	Procenat (%)
1	205	20.8
2	228	23.1
3	278	28.2
4	195	19.8
5	81	8.2

Najveći broj ispitanika (28,2%) se niti slaže niti ne slaže s tvrdnjom "Privremene ili iznenadne pogreške često se događaju tokom EPS transakcije." , a 8,2% ispitanika se u potpunosti slaže s tom tvrdnjom. Rezultati odgovora prikazani su u tabeli 16.

Tabela 16 Tehnička zaštita u EPS-u (grupa)

Tehnička zaštita u EPS-u (grupa)		
	Broj ispitanika (N)	Procenat (%)
1 – 2	35	3.5
2 – 3	83	8.4
3 - 4	334	33.8
4 – 5	521	52.8
5	14	1.4

Najveći broj ispitanika (52,8%) je tehničku zaštitu u EPS-u ocijenio ocjenama u rasponu od 4 do 5. Broj odgovora prikazan je u tabeli 17.

Tabela 17 Odgovori na tvrdnju "Stranice na kojima koristite EPS Vam nude detaljna objašnjenja o tome kako pregledati, poništiti, izmijeniti ili izvršiti plaćanje."

Stranice na kojima koristite EPS Vam nude detaljna objašnjenja o tome kako pregledati, poništiti, izmijeniti ili izvršiti plaćanje.		
	Broj ispitanika (N)	Procenat (%)
1	87	8.8
2	115	11.7
3	236	23.9
4	259	26.2
5	290	29.4

Na pitanje da li stranice na kojima koriste EPS nude detaljna objašnjenja o tome kako pregledati, poništiti, izmijeniti ili izvršiti plaćanje, najveći broj odgovora je stigao za odgovor da se u potpunosti slažu s tvrdnjom (29,4%), dok je najmanje stiglo za odgovor da se u potpunosti ne slažu s ovom tvrdnjom (8,8%). Rezultati odgovora prikazani su u tabeli 18.

Tabela 18 Odgovori na tvrdnju "Stranica na kojima koristite EPS Vam nude sigurnosne izjave o sigurnosnoj politici, podatke za kontakt u hitnim slučajevima, tehničke opise i funkcionalnosti EPS-a."

Stranica na kojima koristite EPS Vam nude sigurnosne izjave o sigurnosnoj politici, podatke za kontakt u hitnim slučajevima, tehničke opise i funkcionalnosti EPS-a.		
	Broj ispitanika (N)	Procenat (%)
1	61	6.2
2	94	9.5
3	221	22.4
4	252	25.5
5	359	36.4

Najviše ispitanika (36,4%) je odgovorilo da se u potpunosti slaže s tvrdnjom da im stranica na kojima koriste EPS nude sigurnosne izjave o sigurnosnoj politici, podatke za kontakt u hitnim slučajevima, tehničke opise i funkcionalnosti EPS-a. Samo 6,2% ispitanika se ne slaže s ovom tvrdnjom. Broj odgovora prikazan je u tabeli 19.

Tabela 19 Odgovori na tvrdnju "Ne trebate ulagati nikakve posebne napore da pronađete izjave vezane za sigurnost."

Ne trebate ulagati nikakve posebne napore da pronađete izjave vezane za sigurnost.		
	Broj ispitanika (N)	Procenat (%)
1	87	8.8
2	86	8.7
3	235	23.8
4	290	29.4
5	289	29.3

Najveći broj ispitanika na konstataciju o (ne)ulaganju nikakvih posebnih napora da se pronađu izjave vezane za sigurnost.,29,4% se slaže, dok 29,3% se u potpunosti slaže, dok njih 8,8% se u potpunosti ne slaže s tom tvrdnjom, dok se 8,8% ne slaže. Rezultati odgovora prikazani su u tabeli 20.

Tabela 20 Odgovori na tvrdnju "Izjave koje se odnose na sigurnost sastavljene su na lako razumljiv način i uglavnom bez tehničkih riječi."

Izjave koje se odnose na sigurnost sastavljene su na lako razumljiv način i uglavnom bez tehničkih riječi.		
	Broj ispitanika (N)	Procenat (%)
1	62	6.3
2	98	9.9
3	268	27.2

4	304	30.8
5	255	25.8

Na izjave koje se odnose na sigurnost sastavljene su na lako razumljiv način i uglavnom bez tehničkih riječi se slaže 30,8% ispitanika, dok je najmanje odgovora stiglo od ispitanika koji se u potpunosti ne slažu s ovom tvrdnjom (6,3%). Rezultati odgovora prikazani su u tabeli 21.

Tabela 21 Odgovori na tvrdnju "Izjave koje se odnose na sigurnost sastavljene su na način koji privlači Vašu pažnju."

Izjave koje se odnose na sigurnost sastavljene su na način koji privlači Vašu pažnju.		
	Broj ispitanika (N)	Procenat (%)
1	125	12.7
2	137	13.9
3	326	33.0
4	232	23.5
5	167	16.9

33% ispitanika se niti slaže niti ne slaže s izjavama koje se odnose na sigurnost koje su sastavljene na način koji privlači pažnju, dok se najmanje ispitanika u potpunosti ne slaže s tvrdnjom (12,7%). Rezultati odgovora prikazani su u tabeli 22.

Tabela 22 Sigurnosne izjave u EPS-u (grupa)

Sigurnosne izjave u EPS-u (grupa)		
	Broj ispitanika (N)	Procenat (%)
1 – 2	75	7.6
2 – 3	161	16.3
3 - 4	359	36.4
4 – 5	289	29.3
5	103	10.4

Najveći broj ispitanika (36,4%) je sigurnosne izjave u EPS-u ocijenio ocjenama u rasponu od 3 do 4. Rezultati odgovora prikazani su u tabeli 23.

Tabela 23 Odgovori na tvrdnju "EPS smatram sigurnim."

EPS smatram sigurnim.		
	Broj ispitanika (N)	Procenat (%)
1	58	5.9
2	60	6.1
3	166	16.8
4	412	41.7
5	291	29.5

Najveći broj ispitanika (41,7%) smatra da je EPS siguran, dok samo 5,9% ispitanika se u potpunosti ne slaže s tim. Rezultati odgovora prikazani su u tabeli 24.

Tabela 24 Odgovori na tvrdnju "Informacije koje se odnose na korisničke i EPS transakcije smatram sigurnim."

Informacije koje se odnose na korisničke i EPS transakcije smatram sigurnim.		
	Broj ispitanika (N)	Procenat (%)
1	58	5.9
2	56	5.7
3	223	22.6
4	327	33.1
5	323	32.7

33% ispitanika smatra da su informacije koje se odnose na korisničke i EPS transakcije sigurne, dok se samo 5,7% ispitanika s tim ne slaže. Rezultati odgovora prikazani su u tabeli 25.

Tabela 25 Odgovori na tvrdnju "Informacije koje sam naveo ranije prilikom korištenja EPS-a korisne su za sigurne naredne transakcije plaćanja."

Informacije koje sam naveo ranije prilikom korištenja EPS-a korisne su za sigurne naredne transakcije plaćanja.		
	Broj ispitanika (N)	Procenat (%)
1	58	5.9
2	24	2.4
3	228	23.1
4	322	32.6
5	355	36.0

36% ispitanika smatra da su informacije koje su naveli ranije prilikom korištenja EPS-a korisne za sigurne naredne transakcije plaćanja, dok se samo 2,4% ispitanika s tim ne slaže. Rezultati odgovora prikazani su u tabeli 26.

Tabela 26 Odgovori na tvrdnju "Ne bojim se hakerskih napada na EPS."

Ne bojim se hakerskih napada na EPS.		
	Broj ispitanika (N)	Procenat (%)
1	122	12.4
2	172	17.4
3	351	35.6
4	208	21.1
5	134	13.6

Na izjavu da se ne boje hakerskih napada na EPS 35,6% ispitanika se niti slaže niti ne slaže. Njih 13,6% se u potpunosti slažu, a 12,4% se u potpunosti ne slažu s ovom izjavom. Rezultati odgovora prikazani su u tabeli 27.

Tabela 27 Percipirana sigurnost u EPS-u (grupa)

Percipirana sigurnost u EPS-u (grupa)		
	Broj ispitanika (N)	Procenat (%)
1 – 2	66	6.7
2 – 3	115	11.7
3 - 4	374	37.9
4 – 5	318	32.2
5	114	11.6

Najveći broj ispitanika (37,9%) je percipiranu sigurnost u EPS-u ocijenio ocjenama u rasponu od 3 do 4. Broj odgovora prikazan je u tabeli 28.

Tabela 28 Odgovori na tvrdnju "Vjerujem svakom učesniku, poput trgovca i kupca, koji su uključeni u EPS."

Vjerujem svakom učesniku, poput trgovca i kupca, koji su uključeni u EPS.		
	Broj ispitanika (N)	Procenat (%)
1	92	9.3
2	205	20.8
3	223	22.6
4	312	31.6
5	155	15.7

Najviše ispitanika (31,6%) je odgovorilo da u potpunosti vjeruju svakom učesniku, poput trgovca i kupca, koji su uključeni u EPS. Njih 9,3% se u potpunosti ne slaže s ovom tvrdnjom. Broj odgovora prikazan je u tabeli 29.

Tabela 29 Odgovori na tvrdnju "Vjerujem sigurnosnim mehanizmima EPS-a."

Vjerujem sigurnosnim mehanizmima EPS-a.		
	Broj ispitanika (N)	Procenat (%)
1	68	6.9
2	61	6.2
3	320	32.4
4	259	26.2
5	279	28.3

32,4% ispitanika niti vjeruje niti ne vjeruje u sigurnosni mehanizam EPS-a. 6,2% ispitanika se u potpunosti ne slaže, dok 28,3% se u potpunosti slaže. Broj odgovora prikazan je u tabeli 30.

Tabela 30 Odgovori na tvrdnju "Vjerujem EPS uslugama."

Vjerujem EPS uslugama.		
	Broj ispitanika (N)	Procenat (%)
1	66	6.7
2	38	3.9
3	205	20.8
4	343	34.8
5	335	33.9

Na izjavu da vjeruju EPS uslugama 34,8% ispitanika se slaže, dok se 3,9% ispitanika ne slaže. Broj odgovora prikazan je u tabeli 31.

Tabela 31 Odgovori na tvrdnju "Vjerujem informacijama dobivenim tokom postupka EPS-a."

Vjerujem informacijama dobivenim tokom postupka EPS-a.		
	Broj ispitanika (N)	Procenat (%)
1	44	4.5
2	22	2.2
3	204	20.7
4	384	38.9
5	333	33.7

Na izjavu da vjeruju informacijama dobivenim tokom postupka EPS-a 38,9% ispitanika se slaže, dok se 2,2% ispitanika ne slaže. Broj odgovora prikazan je u tabeli 32.

Tabela 32 Percipirano povjerenje u EPS (grupa)

Percipirano povjerenje u EPS (grupa)		
	Broj ispitanika (N)	Procenat (%)
1 – 2	68	6.9
2 – 3	88	8.9
3 - 4	366	37.1

4 – 5	336	34.0
5	129	13.1

Najveći broj ispitanika (37,1%) je percipirano povjerenje u EPS-u ocijenio ocjenama u rasponu od 3 do 4. Broj odgovora prikazan je u tabeli 33.

Tabela 33 Odgovori na tvrdnju "Koristim EPS češće od drugih iz svoje okoline."

Koristim EPS češće od drugih iz svoje okoline.		
	Broj ispitanika (N)	Procenat (%)
1	87	8.8
2	152	15.4
3	167	16.9
4	237	24.0
5	344	34.9

35% ispitanika koristi EPS češće od drugih iz svoje okoline, a 8,8% ispitanika se ne slaže s tim. Broj odgovora prikazan je u tabeli 34.

Tabela 34 Odgovori na tvrdnju "Trenutno koristim i nastavit ću koristiti EPS."

Trenutno koristim i nastavit ću koristiti EPS.		
	Broj ispitanika (N)	Procenat (%)
1	75	7.6
2	80	8.1
3	140	14.2
4	274	27.8
5	418	42.4

Najveći broj ispitanika (42,4%) trenutno koristi i nastavit će koristiti EPS, a njih 7,6% se ne slaže s tim. Broj odgovora prikazan je u tabeli 35.

Tabela 35 Odgovori na tvrdnju "Vjerujem da će se upotreba EPS-a u budućnosti povećati."

Vjerujem da će se upotreba EPS-a u budućnosti povećati.		
	Broj ispitanika (N)	Procenat (%)
1	36	3.6
2	50	5.1
3	52	5.3
4	209	21.2
5	640	64.8

Na izjavu da vjeruju da će se upotreba EPS-a u budućnosti povećati se u potpunosti slaže čak 63% ispitanika, a samo njih 3,6% se u potpunosti ne slažu s ovom izjavom. Broj odgovora prikazan je u tabeli 36.

Tabela 36 Opseg korištenja EPS-a (grupa)

Opseg korištenja EPS-a (grupa)		
	Broj ispitanika (N)	Procenat (%)
1 – 2	58	5.9
2 – 3	95	9.6
3 - 4	176	17.8
4 – 5	362	36.7
5	296	30.0

Najveći broj ispitanika (36,7%) je opseg korištenja EPS-a ocijenio ocjenama u rasponu od 4 do 5. Broj odgovora prikazan je u tabeli 37.

5.3. Testiranje hipoteza istraživanja

U narednom dijelu su tabelarno predstavljeni rezultati istraživanja sprovedenom među korisnicima EPS usluga iz Kantona Sarajevo.

Tabela 37 Rezultati poređenja spola i kategorija

Transakcijski postupci u EPS-u (grupa)					
	1.00	2.00	3.00	4.00	5.00
Muški	38.3%	46.1%	36.3%	44.3%	37.7%
Ženski	61.7%	53.9%	63.7%	55.7%	62.3%
$X^2(4, N=987)=5.750, p=0.219$					
Tehnička zaštita u EPS-u (grupa)					
	1.00	2.00	3.00	4.00	5.00
Muški	28.6%	47.0%	41.0%	41.8%	28.6%
Ženski	71.4%	53.0%	59.0%	58.2%	71.4%
$X^2(4, N=987)=4.455, p=0.348$					
Sigurnosne izjave u EPS-u (grupa)					
	1.00	2.00	3.00	4.00	5.00
Muški	36.0%	40.4%	42.9%	40.5%	43.7%
Ženski	64.0%	59.6%	57.1%	59.5%	56.3%
$X^2(4, N=987)=1.625, p=0.804$					
Percipirana sigurnost u EPS-u (grupa)					

	1.00	2.00	3.00	4.00	5.00
Muški	36.4%	43.5%	39.8%	43.4%	41.2%
Ženski	63.6%	56.5%	60.2%	56.6%	58.8%
$X^2(4, N=987)=1.793, p=0.774$					
Percipirano povjerenje u EPS (grupa)					
	1.00	2.00	3.00	4.00	5.00
Muški	35.3%	45.5%	40.7%	43.5%	38.0%
Ženski	64.7%	54.5%	59.3%	56.5%	62.0%
$X^2(4, N=987)=2.916, p=0.572$					
Opseg korištenja EPS-a (grupa)					
	1.00	2.00	3.00	4.00	5.00
Muški	36.2%	42.1%	44.9%	39.8%	41.9%
Ženski	63.8%	57.9%	55.1%	60.2%	58.1%
$X^2(4, N=987)=1.967, p=0.742$					

Spol ispitanika nema signifikantnog značaja za svih šest kategorija. Rezultate poređenja spola i kategorija možemo vidjeti prikazane u tabeli 38.

Tabela 38 Rezultati poređenja nivoa obrazovanja i kategorija

Transakcijski postupci u EPS-u (grupa)					
	1.00	2.00	3.00	4.00	5.00
Drugi ciklus visokog obrazovanja	21.7%	30.3%	36.8%	37.6%	30.4%
Prvi ciklus visokog obrazovanja	25.0%	21.1%	15.7%	17.3%	19.6%
SSS	30.0%	28.9%	25.6%	22.4%	26.1%
Treći ciklus visokog obrazovanja	0.0%	0.0%	2.7%	2.7%	4.3%
VSS	23.3%	19.7%	19.3%	20.0%	19.6%
$X^2(16, N=987)=16.585, p=0.413$					
Tehnička zaštita u EPS-u (grupa)					
	1.00	2.00	3.00	4.00	5.00
Drugi ciklus visokog obrazovanja	20.0%	39.8%	36.5%	34.4%	21.4%
Prvi ciklus visokog obrazovanja	28.6%	16.9%	16.5%	18.4%	21.4%
SSS	31.4%	24.1%	23.7%	24.4%	42.9%
Treći ciklus visokog obrazovanja	0.0%	1.2%	2.4%	3.1%	0.0%
VSS	20.0%	18.1%	21.0%	19.8%	14.3%
$X^2(16, N=987)=12.313, p=0.722$					

Sigurnosne izjave u EPS-u (grupa)					
	1.00	2.00	3.00	4.00	5.00
Drugi ciklus visokog obrazovanja	42.7%	37.3%	34.5%	30.4%	38.8%
Prvi ciklus visokog obrazovanja	16.0%	18.6%	17.5%	19.7%	15.5%
SSS	24.0%	23.0%	24.8%	24.6%	27.2%
Treći ciklus visokog obrazovanja	2.7%	1.9%	2.8%	2.4%	2.9%
VSS	14.7%	19.3%	20.3%	22.8%	15.5%
$X^2(16, N=987)=8.983, p=0.914$					
Percipirana sigurnost u EPS-u (grupa)					
	1.00	2.00	3.00	4.00	5.00
Drugi ciklus visokog obrazovanja	33.3%	38.3%	35.6%	32.1%	37.7%
Prvi ciklus visokog obrazovanja	15.2%	20.0%	18.2%	19.2%	14.0%
SSS	27.3%	20.0%	21.9%	27.7%	28.1%
Treći ciklus visokog obrazovanja	6.1%	0.9%	2.1%	2.8%	2.6%
VSS	18.2%	20.9%	22.2%	18.2%	17.5%
$X^2(16, N=987)=14.030, p=0.596$					
Percipirano povjerenje u EPS (rupa)					

	1.00	2.00	3.00	4.00	5.00
Drugi ciklus visokog obrazovanja	36.8%	39.8%	35.5%	31.8%	36.4%
Prvi ciklus visokog obrazovanja	16.2%	17.0%	18.3%	18.8%	17.1%
SSS	23.5%	17.0%	23.2%	26.5%	29.5%
Treći ciklus visokog obrazovanja	4.4%	3.4%	1.9%	2.7%	2.3%
VSS	19.1%	22.7%	21.0%	20.2%	14.7%
$X^2(16, N=987)=10.304, p=0.850$					
Opseg korištenja EPS-a (grupa)					
	1.00	2.00	3.00	4.00	5.00
Drugi ciklus visokog obrazovanja	36.2%	36.8%	30.1%	33.7%	38.2%
Prvi ciklus visokog obrazovanja	17.2%	22.1%	19.3%	18.2%	15.9%
SSS	24.1%	20.0%	26.1%	25.4%	24.3%
Treći ciklus visokog obrazovanja	3.4%	5.3%	1.7%	1.9%	2.7%
VSS	19.0%	15.8%	22.7%	20.7%	18.9%
$X^2(16, N=987)=11.078, p=0.805$					

Nivo obrazovanja ispitanika nema signifikantnog značaja za svih šest kategorija. Rezultate poređenja nivoa obrazovanja i kategorija možemo vidjeti prikazane u tabeli 39.

Tabela 39 Rezultati poređenja naziva banke ispitanika i kategorija: transakcijski postupci u EPS-u i tehnička zaštita u EPS-u

Transakcijski postupci u EPS-u (grupa)					
	1.00	2.00	3.00	4.00	5.00
ADDIKO	3.3%	3.9%	5.8%	3.5%	0.7%
ASA	11.7%	10.5%	9.0%	7.1%	0.7%
BBI	6.7%	11.8%	2.2%	5.9%	0.0%
ISPB	23.3%	25.0%	30.0%	19.2%	5.8%
NLB	6.7%	2.6%	3.6%	1.6%	0.0%
NOVA	3.3%	6.6%	0.4%	1.4%	0.7%
RFB	35.0%	22.4%	19.3%	22.9%	36.2%
SPARKASSEKASSE	1.7%	2.6%	2.7%	2.0%	0.0%
UCB	1.7%	13.2%	24.2%	34.9%	55.1%
ZIRAAT	6.7%	1.3%	2.7%	1.4%	0.7%
$X^2(36, N=987)=171.100, p=0.000$					
Tehnička zaštita u EPS-u (grupa)					
	1.00	2.00	3.00	4.00	5.00
ADDIKO	2.9%	6.0%	4.2%	3.1%	0.0%
ASA	11.4%	8.4%	8.7%	5.8%	7.1%
BBI	5.7%	10.8%	3.3%	4.6%	7.1%

ISPB	28.6%	26.5%	26.0%	15.7%	7.1%
NLB	8.6%	3.6%	1.5%	1.7%	14.3%
NOVA	2.9%	2.4%	2.1%	1.2%	0.0%
RFB	25.7%	26.5%	24.6%	24.2%	28.6%
SPARKASSE	2.9%	3.6%	2.1%	1.5%	0.0%
UCB	2.9%	7.2%	26.3%	40.7%	35.7%
ZIRAAT	8.6%	4.8%	1.2%	1.5%	0.0%
$X^2(36, N=987)=105.564, p=0.000$					

Naziv banke koju ispitanici koriste ima signifikantnog značaja za dvije kategorija: transakcijski postupci u EPS-u i tehnička zaštita u EPS-u. Rezultate poređenja naziva banke ispitanika i kategorija možemo vidjeti prikazane u tabeli 40.

Tabela 40 Rezultati poređenja naziva banke ispitanika i kategorije sigurnosne izjave u EPS-u

Sigurnosne izjave u EPS-u (grupa)					
	1.00	2.00	3.00	4.00	5.00
ADDIKO	0.0%	5.6%	3.9%	4.2%	1.0%
ASA	6.7%	7.5%	9.7%	4.2%	6.8%
BBI	2.7%	6.2%	5.0%	4.5%	3.9%
ISPB	24.0%	25.5%	23.4%	14.2%	17.5%
NLB	2.7%	1.9%	2.5%	2.4%	1.0%

NOVA	1.3%	1.9%	2.2%	1.0%	1.0%
RFB	22.7%	18.0%	25.3%	24.9%	33.0%
SPARKASSE	2.7%	0.6%	1.7%	2.4%	2.9%
UCB	34.7%	29.8%	24.8%	40.1%	32.0%
ZIRAAT	2.7%	3.1%	1.4%	2.1%	1.0%
$X^2(36, N=987)=51.598, p=0.044$					

Naziv banke koju ispitanici koriste nema signifikantnog značaja za kategoriju sigurnosne izjave u EPS-u. Rezultate poređenja naziva banke ispitanika i ove kategorije možemo vidjeti prikazane u tabeli 41.

Tabela 41 Rezultati poređenja naziva banke ispitanika i kategorije percipirane sigurnosti u EPS-u

Percipirana sigurnost u EPS-u (grupa)					
	1.00	2.00	3.00	4.00	5.00
ADDIKO	0.0%	4.3%	4.8%	3.5%	1.8%
ASA	6.1%	4.3%	9.9%	6.0%	5.3%
BBI	9.1%	4.3%	4.5%	4.4%	4.4%
ISPB	19.7%	20.9%	25.4%	15.7%	17.5%
NLB	4.5%	1.7%	2.1%	1.9%	2.6%
NOVA	0.0%	1.7%	1.1%	2.5%	1.8%
RFB	25.8%	17.4%	23.8%	26.1%	29.8%

SPARKASSE	0.0%	2.6%	1.9%	2.8%	0.0%
UCB	30.3%	37.4%	25.9%	34.6%	36.8%
ZIRAAT	4.5%	5.2%	0.5%	2.5%	0.0%
X^2(36, N=987)=59.657, p=0.008					

Naziv banke koju ispitanici koriste ima signifikantnog značaja za kategoriju percipirane sigurnosti u EPS-u. Rezultate poređenja naziva banke ispitanika i kategorije možemo vidjeti prikazane u tabeli 42.

Tabela 42 Rezultati poređenja naziva banke ispitanika i kategorije percipirano povjerenje u EPS-u

Percipirano povjerenje u EPS (grupa)					
	1.00	2.00	3.00	4.00	5.00
ADDIKO	2.9%	1.1%	4.4%	3.9%	3.1%
ASA	5.9%	8.0%	9.0%	5.1%	7.8%
BBI	8.8%	0.0%	5.7%	3.6%	6.2%
ISPB	20.6%	18.2%	25.7%	17.0%	16.3%
NLB	2.9%	2.3%	2.7%	2.1%	0.8%
NOVA	0.0%	2.3%	1.4%	1.8%	2.3%
RFB	22.1%	27.3%	19.9%	28.9%	26.4%
SPARKASSE	1.5%	0.0%	3.0%	1.2%	2.3%
UCB	30.9%	38.6%	25.7%	35.7%	33.3%
ZIRAAT	4.4%	2.3%	2.5%	0.9%	1.6%
X^2(36, N=987)=50.645, p=0.054					

Naziv banke koju ispitanici koriste nema signifikantnog značaja za kategoriju percipiranog povjerenja u EPS-u. Rezultate poređenja naziva banke ispitanika i kategorije možemo vidjeti prikazane u tabeli 43.

Tabela 43 Rezultati poređenja naziva banke ispitanika i kategorije opsega korištenja EPS-a

Opseg korištenja EPS-a (grupa)					
	1.00	2.00	3.00	4.00	5.00
ADDIKO	3.4%	2.1%	3.4%	4.1%	3.7%
ASA	5.2%	6.3%	10.2%	5.5%	8.1%
BBI	3.4%	8.4%	3.4%	4.1%	5.4%
ISPB	24.1%	24.2%	26.7%	19.3%	16.2%
NLB	5.2%	0.0%	2.3%	2.2%	2.4%
NOVA	0.0%	1.1%	0.0%	2.2%	2.4%
RFB	19.0%	22.1%	25.0%	24.6%	26.4%
SPARKASSE	1.7%	3.2%	2.3%	2.2%	1.0%
UCB	34.5%	24.2%	26.7%	34.3%	33.1%
ZIRAAT	3.4%	8.4%	0.0%	1.4%	1.4%
$X^2(36, N=987)=60.611, p=0.006$					

Naziv banke koju ispitanici koriste ima signifikantnog značaja za kategoriju opsega korištenja EPS-a. Rezultate poređenja naziva banke ispitanika i kategorije možemo vidjeti prikazane u tabeli 44.

Tabela 44 Rezultati poređenja sigurnosnih izjava u EPS-u i kategorija

Opseg korištenja EPS-a (grupa)					
	1 - 2	2 - 3	3 - 4	4 - 5	5
1 – 2	65.5%	6.3%	0.0%	0.0%	10.5%
2 – 3	34.5%	35.8%	11.9%	17.1%	8.1%
3 – 4	0.0%	42.1%	69.3%	19.3%	42.9%
4 – 5	0.0%	6.3%	10.2%	61.0%	14.9%
5	0.0%	9.5%	8.5%	2.5%	23.6%
$X^2(16, N=987)=735.342, p=0.000$					
Percipirano povjerenje u EPS (grupa)					
	1 - 2	2 - 3	3 - 4	4 - 5	5
1 – 2	47.1%	22.7%	6.3%	0.0%	0.0%
2 – 3	41.2%	35.2%	22.4%	6.0%	0.0%
3 – 4	11.8%	42.0%	50.3%	26.8%	31.0%
4 – 5	0.0%	0.0%	19.4%	56.0%	23.3%
5	0.0%	0.0%	1.6%	11.3%	45.7%
$X^2(16, N=987)=678.438, p=0.000$					
Percipirana sigurnost u EPS-u (grupa)					
	1 - 2	2 - 3	3 - 4	4 - 5	5
1 – 2	57.6%	12.2%	0.0%	7.2%	0.0%

2 – 3	30.3%	50.4%	20.1%	2.5%	0.0%
3 – 4	12.1%	14.8%	63.9%	15.4%	40.4%
4 – 5	0.0%	22.6%	14.4%	62.9%	7.9%
5	0.0%	0.0%	1.6%	11.9%	51.8%
X^2(16, N=987)=972.187, p=0.000					

Sigurnosne izjave u EPS-u ima signifikantnog značaja za tri kategorije: opseg korištenja, percipirano povjerenje i percipirana sigurnost. Rezultate poređenja sigurnosne izjave u EPS-u i kategorija možemo vidjeti prikazane u tabeli 45.

Tabela 45 Rezultati poređenja tehničke zaštite u EPS-u i kategorija

Opseg korištenja EPS-a (grupa)					
	1 - 2	2 - 3	3 - 4	4 - 5	5
1 – 2	24.1%	5.3%	2.8%	1.4%	2.0%
2 – 3	27.6%	12.6%	4.0%	9.1%	5.1%
3 – 4	34.5%	36.8%	30.1%	26.8%	43.6%
4 – 5	13.8%	45.3%	63.1%	61.6%	45.9%
5	0.0%	0.0%	0.0%	1.1%	3.4%
X^2(16, N=987)=169.464, p=0.000					
Percipirano povjerenje u EPS (grupa)					
	1 - 2	2 - 3	3 - 4	4 - 5	5

1 – 2	17.6%	3.4%	2.2%	1.8%	4.7%
2 – 3	30.9%	8.0%	7.4%	5.7%	7.0%
3 – 4	30.9%	34.1%	38.5%	34.8%	19.4%
4 – 5	20.6%	54.5%	51.1%	56.8%	62.8%
5	0.0%	0.0%	0.8%	0.9%	6.2%
$X^2(16, N=987)=140.411, p=0.000$					
Percipirana sigurnost u EPS-u (grupa)					
	1 - 2	2 - 3	3 - 4	4 - 5	5
1 – 2	21.2%	3.5%	1.6%	2.5%	2.6%
2 – 3	31.8%	15.7%	4.8%	6.3%	5.3%
3 – 4	27.3%	27.8%	43.9%	29.6%	22.8%
4 – 5	19.7%	53.0%	49.5%	60.1%	62.3%
5	0.0%	0.0%	0.3%	1.6%	7.0%
$X^2(16, N=987)=192.147, p=0.000$					

Tehnička zaštita u EPS-u ima signifikantnog značaja za tri kategorije: opseg korištenja, percipirano povjerenje i percipirana sigurnost. Rezultate poređenja tehničke zaštite u EPS-u i kategorija možemo vidjeti prikazane u tabeli 46.

Tabela 46 Rezultati poređenja transakcijskih postupaka u EPS-u i kategorija

Opseg korištenja EPS-a (grupa)					
	1 - 2	2 - 3	3 - 4	4 - 5	5
1 – 2	22.4%	4.2%	4.5%	6.6%	3.7%
2 – 3	13.8%	6.3%	2.8%	11.0%	5.7%
3 – 4	8.6%	32.6%	28.4%	20.4%	21.3%
4 – 5	37.9%	54.7%	57.4%	47.8%	48.0%
5	17.2%	2.1%	6.8%	14.1%	21.3%
X^2(16, N=987)=90.026, p=0.000					
Percipirano povjerenje u EPS (grupa)					
	1 - 2	2 - 3	3 - 4	4 - 5	5
1 – 2	16.2%	4.5%	4.6%	4.8%	9.3%
2 – 3	11.8%	0.0%	9.6%	8.0%	4.7%
3 – 4	11.8%	35.2%	29.2%	18.8%	10.9%
4 – 5	50.0%	55.7%	45.6%	52.7%	48.8%
5	10.3%	4.5%	10.9%	15.8%	26.4%
X^2(16, N=987)=80.680, p=0.000					
Percipirana sigurnost u EPS-u (grupa)					
	1 - 2	2 - 3	3 - 4	4 - 5	5
1 – 2	19.7%	7.0%	2.9%	6.3%	7.0%

2 – 3	12.1%	1.7%	10.4%	7.2%	3.5%
3 – 4	12.1%	28.7%	30.5%	18.9%	7.0%
4 – 5	40.9%	60.9%	44.9%	49.7%	58.8%
5	15.2%	1.7%	11.2%	17.9%	23.7%
$X^2(16, N=987)=102.563, p=0.000$					

Transakcijski postupci u EPS-u ima signifikantnog značaja za tri kategorije: opseg korištenja, percipirano povjerenje i percipirana sigurnost. Rezultate poređenja transakcijskih postupaka u EPS-u i kategorija možemo vidjeti prikazane u tabeli 47.

Tabela 47 Korelaciona analiza

	Transakcijski postupci u EPS-u	Tehnička zaštita u EPS-u	Sigurnosne izjave u EPS-u	Percipirana sigurnost u EPS-u	Percipirano povjerenje u EPS	Obim korištenja EPS-a
Transakcijski postupci u EPS-u	1					
Tehnička zaštita u EPS-u	.773**	1				
Sigurnosne izjave u EPS-u	.138**	.317**	1			
Percipirana sigurnost u EPS-u	.170**	.329**	.722**	1		

Percipirano povjerenje u EPS	.131**	.260**	.736**	.865**	1	
Obim korištenja EPS-a	.160**	.271**	.487**	.683**	.653**	1

Transakcijski postupci u EPS-u imaju signifikantan značaj za tehničku zaštitu u EPS-u, zatim za sigurnosne izjave u EPS-u, za percipiranu sigurnost u EPS-u, za percipirano povjerenje u EPS i u obim korištenja EPS-a. Tehnička zaštita u EPS-u ima signifikantan značaj za transakcijske postupke u EPS-u, zatim za sigurnosne izjave u EPS-u, za percipiranu sigurnost u EPS-u, za percipirano povjerenje u EPS i u obim korištenja EPS-a. Sigurnosne izjave u EPS-u imaju signifikantan značaj za transakcijske postupke u EPS-u, tehničku zaštitu u EPS-u, zatim za percipiranu sigurnost u EPS-u, za percipirano povjerenje u EPS i u obim korištenja EPS-a. Percipirana sigurnost u EPS-u ima signifikantan značaj za transakcijske postupke u EPS-u, zatim za tehničku zaštitu u EPS-u, za sigurnosne izjave u EPS-u, za percipirano povjerenje u EPS i u obim korištenja EPS-a. Percipirano povjerenje u EPS-u ima signifikantan značaj za transakcijske postupke u EPS-u, zatim za tehničku zaštitu u EPS-u, za sigurnosne izjave u EPS-u, za percipiranu sigurnost u EPS i u obim korištenja EPS-a. Obim korištenja EPS-u ima signifikantan značaj za transakcijske postupke u EPS-u, zatim za tehničku zaštitu u EPS-u, za sigurnosne izjave u EPS-u, za percipiranu sigurnost u EPS i za percipirano povjerenje u EPS.

5.3. Diskusija dobijenih rezultata istraživanja

Prema analizi dobijenih rezultata dolazimo do zaključka da su svi rezultati signifikantni i da se svih 5 hipoteza ovog istraživanja (H1: Tehničke zaštite pozitivno su povezane s percipiranom sigurnošću potrošača u EPS-u.; H2: Transakcijski postupci pozitivno su povezani s percipiranom sigurnošću potrošača u EPS-u.; H3: Izjave o sigurnosti pozitivno su povezane s percipiranom sigurnošću potrošača u EPS-u.; H4: Percipirana sigurnost u EPS-u pozitivno je povezana s percipiranim povjerenjem potrošača u EPS.; H5: Percipirano povjerenje u EPS pozitivno je povezano s korištenjem EPS-a od strane potrošača.) prihvata.

U sprovedenom istraživanju su se pokušali utvrditi faktori koji određuju percipiranu sigurnost i percipirano povjerenje, kao i efekat koji ti faktori imaju na korištenje EPS-a. Koncepti sigurnosti i povjerenja istraženi su iz perspektive korisnika EPS-a kako bi se omogućilo bolje razumijevanje ovih konstrukata budući da pokazuju prošireno viđenje korisnika EPS-a. Prema rezultatima našeg istraživanja, osjećaji percipirane sigurnosti i

percipiranog povjerenja imaju pozitivan i značajan efekat na korištenje EPS-a. Drugim riječima, kada korisnici imaju osjećaj da je EPS pouzdan i siguran, veća je vjerovatnoća da će svoje transakcije izvršiti elektronsnkim putem. Ovi rezultati su u skladu s prethodnim istraživanjima (Culnan i Armstrong, 1999; Kim et al., 2010). Dobijeni rezultati su također pokazali da je osigurani nivo tehničke zaštite najvažniji faktor u smislu određivanja povjerenja u kompaniju. Ovaj rezultat je u skladu s rezultatima iz ranijih istraživanja (Kim et al., 2010). Zbog toga rezultati pokazuju da pružanje tehničke zaštite korisnicima EPS-a može povećati osjećaj sigurnosti i povjerenja kod kupaca.

sRezultati koje smo dobili u ovom istraživanju, kao i oni koje je dobio Romdhane (2005), pokazuju da postoji značajan efekat koji procedura transakcije ima na percipiran nivo povjerenja i sigurnosti. Na osnovu ovog rezultata možemo zaključiti da je transakcijski postupak parametar za sigurnost i pouzdanost EPS-a. Također, postupak transakcije može povremeno za rezultat imati neugodnosti za korisnike i rezultirati smanjenjem povjerenja korisnika u EPS kao i njihove procjene vrijednosti. Otkriveno je da je lično iskustvo s EPS-om povezano s osjećajem sigurnosti i povjerenja u sistem elektronske kupovine. Ovaj rezultat se podudara s onim što su Pavlou i Gefen (2004) pronašli u svom istraživanju. Također, ovaj rezultat sugeriše da pojedinci grade svoj osjećaj sigurnosti i povjerenja na osnovu iskustava koja su imali u prošlosti. Kao rezultat toga, razumno je istaknuti da sigurnost i povjerenje proizlaze iz iskustava koja su stečena u prošlosti tokom određenog vremenskog perioda i sazrijevaju kao funkcija iskustava koja su stečena u prošlosti.

6. ZAKLJUČAK

Elektornsko plaćanje (EPS) je elektronski prijenos vrijednosti od platioca do primaoca. Sistemi e-plaćanja omogućavaju korisnicima da upravljaju svojim bankovnim računima i transakcijama. Globalni sistemi plaćanja pružaju nekoliko usluga e-plaćanja. Elektronski čekovi, e-gotovina, kreditne kartice i EFT. Postoje internet plaćanja zasnovana na Internet Banking Payment Gateway (IBPG) i vanjska platna platforma. Prvo je tehnika izravnog plaćanja gdje korisnik plaća putem interneta koristeći arhitekturu e-poslovanja povezanog s bankarstvom. Druga vrsta prenosi novac s računa kupca na račun trgovca putem pružaoca usluga plaćanja treće strane. Između bankarstva i interneta je IBPG. Upravljanje plaćanjem i autorizacijom je specijalnost IBPG-a. IBPG je veza klijent-trgovac-banka. Online plaćanja zasnovana na IBPG-u trebaju kupca.

Od 987 ispitanika 58,7% (579) bile su žene, a 41,3% (41,3%) muškarci. Najviše ispitanika bilo je u drugom ciklusu školovanja (34,9%) ili srednjem stručnom obrazovanju (24,6%). Slijede diplomirani studenti (20%), studenti prvog ciklusa (18%) i studenti trećeg ciklusa (2,5%). Klijenti UniCredit Banke (31,6%) najčešće su spominjali svoju banku, zatim Raiffeisen (24,6%) i Intesa Sanpaolo (20,5%). Ostale navedene banke čine 10%. Ostale banke su: ASA Banka (7,2%), BBI Banka (4,8%), Addiko Banka (3,6%), NLB Banka (2,2%), Ziraat Banka (1,9%) i Nova Banka (1,6%). S tvrdnjom "EPS uvijek treba prijavu i lozinku za prijavu." se u potpunosti slaže 50,2% ispitanika, a ne slaže se 1,9%. 42,1% ispitanika smatra da njihov EPS u potpunosti podržava različite postupke provjere autentičnosti, dok 4,8% ne podržava. 37% ispitanika u potpunosti se slaže da im EPS stranice omogućuju izmjenu podataka o plaćanju prije posljednjeg koraka postupka plaćanja, dok se 7,5% u potpunosti ne slaže. Većina ispitanika (52,9%) slaže se da stranice koje prihvaćaju EPS plaćanja trebaju korak provjere prije obrade plaćanja. 6,9% se ne slaže. "Stranice na kojima plaćate putem EPS-a općenito nude sažetak podataka o plaćanju (trošak, primatelj...) i konačni iznos plaćanja", smatra 55,7% ispitanika. 4,4% se ne slaže. 50,9% ispitanika dobiva bankovnu potvrdu (e-mail, obavijest i sl.) za potvrdu plaćanja. Većina ispitanika (49,6%) metodi EPS transakcije dala je ocjenu 4 ili 5. Većina ispitanika (67,7%) složila se s tvrdnjom "Vaši osobni podaci, kao što su kontakt informacije ili podaci o plaćanju, nikada nisu ukradeni zbog korištenja EPS-a", dok se 5,3% ne slaže. Većina ispitanika (58%) smatra da "davatelji EPS usluga nisu podijelili vaše osobne podatke s trećim stranama iz bilo kojeg drugog razloga." je istina. 6,8% se ne slaže. Većina ispitanika (58%) slaže se da su iznosi plaćanja i podaci o transakcijama na EPS-u uvijek točni, dok se najmanje ne slaže. 1,9 posto. Većina ispitanika (31,3%) niti se slaže niti ne slaže s izjavom "Smatrate da su podaci koji se tiču EPS transakcija komuniciranih putem interneta sigurni i zaštićeni." Najmanje ispitanika (6,8%) se ne slaže. 43,5% ispitanika ima 24/7 pristup uslugama plaćanja, dok 5% nema. Većina ispitanika (28,2%) niti se slaže niti ne slaže s tvrdnjom "Privremene ili neočekivane greške obično se događaju tijekom EPS transakcija", dok se 8,2% apsolutno slaže. Većina ispitanika (52,8%) dala je EPS tehničkoj zaštiti ocjenu 4 ili 5. Na pitanje pružaju li stranice na kojima koriste EPS eksplicitne upute o tome kako vidjeti, otkazati, promijeniti ili izvršiti plaćanje, 29,4% ispitanika se nije složilo, dok se 8,8% složilo. Većina ispitanika (36,4%)

izjavila je da im je potpuno drago što web stranica na kojoj koriste EPS sadrži sigurnosne izjave u vezi sa sigurnosnom politikom, podatke za kontakt u hitnim slučajevima, tehničke detalje i funkcije EPS-a. 6,2% se ne slaže. S tvrdnjom o (ne)polaganju posebnog truda u prepoznavanje sigurnosnih komentara slaže se 29,4% ispitanika, dok se 29,3% slaže, a 8,8% ne slaže. 8,8% se ne slaže. 30,8% ispitanika smatra da su sigurnosne poruke razumljive i općenito bez tehničke terminologije, dok se 6,3% ne slaže s tim. 33% ispitanika niti se slaže niti ne slaže sa sigurnosnim izrazima koji privlače pozornost, dok ih 12,7% to izrazito ne odobrava. Većina ispitanika (36,4%) ima povjerenje u EPS s ocjenama od 3 do 4. Većina (41,7%) misli da je EPS siguran, dok se 5,9% ne slaže s tim. 33% smatra da su podaci o korisniku i EPS transakcijama sigurni, dok se 5,7% ne slaže. 36% ispitanika smatra da EPS znanje pomaže u osiguravanju budućih plaćanja, dok se 2,4% ne slaže s tim. 35,6% ispitanika ne boji se EPS hakerskih napada. 13,6% se slaže, 12,4% se ne slaže. Većina ispitanika (31,6%) vjeruje svim sudionicima EPS-a, uključujući trgovce i kupce. 9,3% se ne slaže. 32,4% ispitanika je neodlučno o EPS sigurnosti. Apsolutno se slaže 28,3%, dok se ne slaže 6,2%. 34,8% ispitanika vjeruje uslugama EPS-a, dok 3,9% ne kaže ništa. 38,9% ispitanika želi izjavu za provjeru EPS podataka, dok je 2,2% ne može pronaći. Većina ispitanika (37,1%) procijenila je svoje percipirano povjerenje u EPS između 3 i 4. 35% ispitanika koristi EPS češće od ostalih u svojoj okolini, dok se 8,8% s tim ne slaže.

U ovom istraživanju je predložen, a onda i testiran istraživački model koji je istraživao determinante percipirane sigurnosti i percipiranog povjerenja, kao i efekat ove dvije varijable na korištenje EPS-a. Prema rezultatima, lični historijat pojedinca kao i njihova izloženost tehnološkim zaštitnim mjerama važni su faktori koji utiču na njihov osjećaj povjerenja i sigurnosti. Također, izjava o sigurnosti prepoznata je kao faktori koji određuje koliko se osoba osjeća sigurnom. Posljednje, ali ne i najmanje važno, otkriveno je da su percipirano povjerenje i percipirana sigurnost važne odrednice korištenja EPS-a. Ovi rezultati su u skladu s rezultatima prethodnih istraživanja (Miyazaki i Fernandez, 2000; Pavlou i Gefen, 2004; Kim et al., 2010). Prema rezultatima ovog istraživanja, postoji dokaza o statistički značajnoj povezanosti između percipiranog povjerenja i sigurnosti potrošača u korištenje EPS-a i transakcijskih procedura koje se koriste. Pretpostavljamo da je ovaj rezultat postignut iz niza razloga, od kojih je jedan taj što klijenti sada transakcijske postupke smatraju jednostavnijim i bržim nego ranije, što posljedično može imati pozivan uticaj na njihovu percepciju sigurnosti i povjerenja. Ovaj rezultat pokazuje da korisnici uzimaju u obzir ne samo sigurnost postupaka, već i praktičnost postupaka kada je u pitanju EPS.

Ovo istraživanje ima neka specifična ograničenja. Za početak, korištenje određenog uzorka ograničava rezultate istraživanja na sam uzorak, što znači da se ti rezultati ne mogu odnositi na veću populaciju i zbog toga se ne mogu smatrati krajnjim (Hair et al., 1998). Također, postoji mogućnost da rezultati istraživanja nisu reprezentativni, jer su uzorak činili studenti. Međutim, prema Lightneru i saradnicima (2002), studenti su reprezentativni uzorak tipičnih online kupaca u svijetu elektronske kupovine. To je prije svega zbog poznavanja rada na računarima.

U završnom dijelu ovog istraživanja istraženi su nezavisni efekti percipiranog povjerenja i percipirane sigurnosti na korištenje EPS-a. U kasnijim istraživanjima, regresiona analiza može se koristiti za istraživanje kombinovanog uticaja ovih faktora na potrošnju EPS-a. Ova metoda može pokazati kako se različite kombinacije ove dvije varijable predviđanja (percipirana sigurnost i percipirano povjerenje) odnose na korištenje EPS-a.

6.1.Doprinosi istraživanja

Ovo istraživanje ima različite važne posljedice za menadžere općenito, a poseban akcenat je na odnosu između upotrebe EPS-a i sigurnosti potrošača u Sarajevu. Ovo je posebno važno obzirom da korisnici u Sarajevu sve više učestvuju u elektronskim sistemima plaćanja (EPS). Kompanije su uočile da će vjerovatnost njihovog uspjeha porasti ako komuniciraju s kupcima elektronski (koristeći EPS). S druge strane, stepen percipirane sigurnosti i povjerenja faktor je u ovoj uključenosti. Dakle, potrebno je da menadžeri razumiju efekte faktora koji utiču na situaciju. Za početak, rezultati ovog istraživanja pokazuju da je povećana upotreba EPS-a povezana s većim nivoom osjećaja sigurnosti i povjerenja. Menadžeri kompanija bi trebali tražiti nekoliko pristupa kako bi povećali osjećaj povjerenja i sigurnosti kod potrošača. Empirijski dokazi koji su traženi u svrhu ovog istraživanja usmjereni su na metode aktiviranja osjećaja sigurnosti i povjerenja korisnika, budući da podaci pokazuju da su percipirana sigurnost i povjerenje određeni tehnološkom zaštitom. Zbog toga bi naglasak upravljanja trebao biti na osiguravanju najviše moguće tehnološke zaštite i osiguranju da korisnici imaju pristup sigurnom sistemu elektronske kupovine. EPS bi trebao osigurati da lični podaci korisnika, kao što su njihova imena, adrese, telefonski brojevi i brojevi kreditnih kartica budu tajni, te da su prijenosi brzi i pouzdani.

Također, prethodno iskustvo značajan je faktor u određivanju stepena do kojeg se neko osjeća sigurno i može vjerovati u elektronsku kupovinu. Korisnici će se s vremenom bolje upoznati s EPS-om, ali u međuvremenu menadžment kompanija treba osigurati da su korisnici zadovoljni svojim učestvovanjem u kupovini. Kada kupci imaju pozitivna iskustva u prošlosti, to pomaže u njihovoj vjeri u kompaniju i osjećaju sigurnosti prema EPS-u. Kao rezultat toga, za kompanije je ključno da prate iskustva svojih kupaca i da poduzimaju odgovarajuće mjere za nezadovoljstvo kupaca.

Literatura

1. Adeniji, A.A., Osibanjo, A. O. (2012). Human Resource Management: Theory & Practice. Pumark Nigeria Limited

2. Bersin, J. (2011). The Agile Model comes to Management, Learning, and Human Resources. Preuzeto 01.12.2020. s https://joshbersin.com/2011/09/the-agile-model-comes-to-management-learning-and-human-resources/

3. Bodrožić, Z., Adler S.P. (2017). The Evolution of Management Models: A Neo-Schumpeterian Theory. Administrative Science Quarterly, pp. 85-129

4. Bratton, J., & Gold, J. (1999). Human resource management: Theory and practice. Hampshire, UK: MacMillan Business.

5. Byars, L.L., Rue, L.W. (2004). Human Resource Management, International edition, McGraw – Hill

6. Calamai, J.B., Hill, A., Johnsen, G., Mazor, A., Moen, B., Stephane, J. (2019). Exponential HR: Break Away from traditional operating models to achieve work outcomes. Deloitte Development LLC

7. Cappelli, P., Travis, A. (2018). HR Goes Agile (Harvard Business Review)

8. Centre for Change, Entrepreneurship and Innovation Management pp. 193-201

9. Conboy, K., Coyle, S. (2011). People Over Process: Key Challenges in Agile Development

10. Denning, S. (2018). The Emergence of Agile People Management

11. Devanna, M., Fombrun, C. & Warren, L. (1982). Strategic Planning and Human Resource Management. Human Resource Management

12. Doshi, C., Doshi, D. (2009). A Peek into an Agile Infected Culture

13. Duke II, J., Udono, E.N. (2012). A New Paradigm in Traditional Human Resource Management Practices, pp. 158-162

14. Francis, D. (2001). Managing People in Agile Organisations. University of Brighton

15. Goebel III, C.J. (2009). How Being Agile Changed Our Human Resources Policies

16. Howey, J. (2016). Practicing Agility in Human Resources

17. https://agilemanifesto.org/

18. https://modernagile.org/

19. https://www.agilealliance.org/agile101/agile-glossary/ pristupljeno 03.01.2021

20. https://www.agilehrmanifesto.org/ pristupljeno 03.01.2021

21. Maples, C. (2009). Enterprise Agile Transformation: The Two-Year Wall

22. McMackin, J., Heffernan M. (2020). Agile for HR: Fine in practice, but will it work in theory?

23. Milkovich, G. T., & Boudreau, J. W. (2004). Personnel/Human Resource Management: A diagnostic approach (5th ed.)

24. Moreira, M.E. (2017). The Agile Enterprise: Building and Running Agile Organizations, pp. 245-256

25. Nerur, S., Mahapatra, R., Mangalaraj, G. (2005). Challenges of Migrating to Agile Methodologies, pp. 72-78

26. Noe, R. A., Hollenbeck, J. R., Gerhart, B., & Wright, P. M. (2004). Fundamentals of human resource management. Boston: McGraw-Hill.

27. Oyesola, A. (2011, June 20). Managing health and safety in workplace: Employee's perspective. Daily Sun, pp. 31 & 33.

28. Peters, G., Dijk, W. (2020). 1st State of Agile HR 2020

29. Rahimić, Z. (2010). Menadžment ljudskih resursa. Ekonomski fakultet u Sarajevu

30. Rigby, D.K., Sutherland, J., Noble, A. (2018). Agile at Scale. Harvard Business Review

31. Rousseau, D. M. & Greller, M. M. (1994). Human Resource Practices: Administrative Contract Makers. Human Resource Management, pp. 385-401.

32. Schuh, P. (2004). Integrating Agile Development in the Real World, Charles River Media

33. Storey, J. (1995). Is HRM catching on? International journal of manpower. Vol,16.No.4

34. Ulrich, D. (1996). Human Resource Champions: The Next Agenda for Adding Value and Delivering Results. Harvard Business Press

35. Ulrich, D., Allen, J., Brockbank, W., Younger, J., Nyman, M. (2009). HR Transformation: Building Human Resources from the Outside In. RBL Insistitute

36. Vulpen, E. v. (2019). 15 Key Human Resoruces Roles. Preuzeto 13.12.2020. s https://www.digitalhrtech.com/human-resources-roles/

37. Wright, C., 2008. Reinventing human resource management: Business partners, internal consultants and the limits to professionalization. Human Relations, pp. 1063–1086.

38. Zheltoukhova, K. (2014). HR: Getting smart about agile working. Chartered Institute of Personnel and Development (CIPD)

Prilozi

Prilog 1. - Anketni upitnik

Poštovani,

anketa kojoj ste upravo pristupili dio je istraživanja koje se provodi u okviru završnog rada na Ekonomskom fakultetu Univerziteta u Sarajevu, na temu „Percepcije sigurnosti i povjerenja korisnika sistema elektronskog plaćanja“, pod mentorstvom prof. dr. Aida Habul. Anketa je anonimna, što znači da je ne potpisujete i da niko neće provjeravati Vaše odgovore. Sve što ćete reći ostaje strogo povjerljivo i koristit će se isključivo kao skupina podataka za statističku obradu. U narednom odjeljku ukratko će Vam biti predstavljeno šta se podrazumijeva pod sistemom elektronskog plaćanja.

Molimo Vas da odvojite malo vremena i iskreno odgovorite na pitanja ankete.

Unaprijed se zahvaljujem i srdačno Vas pozdravljam!

Aida Kozić

E-plaćanje se definiše kao prijenos elektronske vrijednosti plaćanja od platilaca do primalaca putem mehanizma elektronskog plaćanja. Usluge e-plaćanja korisnicima omogućavaju pristup i upravljanje svojim bankovnim računima i transakcijama. Međunarodna bankarska statistika Banke za međunarodna poravnanja i Evropske središnje banke pokazuje da popularni instrumenti plaćanja koji se koriste za plaćanje svakodnevnih kupovina uključuju gotovinu, čekove, debitne kartice i kreditne kartice. Općenito, EPS (sistem elektronskog plaćanja) se može klasifikovati u pet kategorija, koje su navedene u nastavku:

1. Elektronska gotovina: transakcije se namiruju putem razmjene elektronske valute.

2. Pre-paid kartica: korisnici koriste pre-paid karticu za određeni iznos unosom jedinstvenog broja kartice na trgovačke stranice. Vrijednost kartice umanjuje se za iznos uplaćen trgovcu.

3. Kreditne kartice: server provjerava autentičnost potrošača i provjerava kod banke jesu li dostupna odgovarajuća sredstva prije kupovine, troškovi se knjiže na račun kupca, a klijentu se naknadno naplaćuju troškovi.

4. Debitne kartice: korisnik održava pozitivno stanje na računu, a novac se skida s računa prilikom izvršenja terećenja.

5. Elektronski čekovi: institucija elektronski namiruje transakcije između banke kupca i banke trgovca u obliku elektronskog čeka.

U narednom odjeljku nalazi se upitnik koji je podijeljen na 6 grupa pitanja:

1. Stavke ankete za transakcijske postupke u EPS-u.

1.1. EPS uvijek traži korisničko ime i lozinku kada se prijavljujete.

1.2. EPS pruža različite mjere za provjeru autentičnosti.

1.3. Stranica vam nudi priliku da promijenite bilo koji podatak o plaćanju prije završne faze procesa plaćanja.

1.4. Stranica nudi korak za provjeru plaćanja prije finalizacije stvarnog plaćanja.

1.5. Stranica obično prikazuje sažetak podataka o plaćanju (trošak, primalac...) i konačni iznos plaćanja.

1.6. Potvrda Vam se šalje putem jednog od nekoliko dostupnih načina (online, e-poštom, itd.) kako bi Vas uvjerili da je uplata zaista primljena.

2. Stavke ankete za tehničku zaštitu u EPS-u.

2.1. Vaši lični podaci, poput podataka za kontakt ili podataka o plaćanju, nikada nisu ukradeni zbog korištenja EPS-a.

2.2. EPS pružaoci usluga nisu dali Vaše lične podatke drugim stranama u bilo koje druge svrhe.

2.3. Iznos plaćanja ili podaci o transakciji koji su prikazani na EPS-u uvijek su tačni.

2.4. Smatrate da su podaci o transakcijama EPS-a koji se prenose putem interneta sigurni i zaštićeni.

2.5. Usluge plaćanja uvijek su dostupne u bilo koje vrijeme u toku dana.

2.6. Privremene ili iznenadne pogreške često se događaju tokom EPS transakcije.

3. Stavke ankete za sigurnosne izjave u EPS-u.

3.1. Stranica nudi detaljna objašnjenja o tome kako pregledati, poništiti, izmijeniti ili izvršiti plaćanje.

3.2. Stranica nudi sigurnosne izjave o sigurnosnoj politici, podatke za kontakt u hitnim slučajevima, tehničke opise i funkcionalnosti EPS-a.

3.3. Ne trebate ulagati nikakve posebne ili izvanredne napore da pronađete izjave vezane za sigurnost.

3.4. Svoje brige o sigurnosnim pitanjima možete lako pronaći u često postavljanim pitanjima (FAQ) ili u odjeljku za pomoć.

3.5. Izjave koje se odnose na sigurnost sastavljene su na lako razumljiv način i uglavnom bez tehničkih riječi.

3.6. Izjave koje se odnose na sigurnost sastavljene su na način koji privlači Vašu pozornost.

4. Stavke ankete za percipiranu sigurnost u EPS-u.

4.1. EPS smatram sigurnim.

4.2. Informacije koje se odnose na korisničke i EPS transakcije smatram sigurnim.

4.3. Informacije koje sam naveo u prethodnom EPS-u korisne su za sigurne naredne transakcije plaćanja.

4.4. Ne bojim se hakerske invazije na EPS.

5. Stavke ankete za percipirano povjerenje u EPS.

5.1. Vjerujem svakom učesniku, poput trgovca i kupca, koji su uključeni u EPS.

5.2. Vjerujem sigurnosnim mehanizmima EPS-a.

5.3. Vjerujem EPS uslugama.

5.4. Vjerujem informacijama dobivenim tokom postupka EPS-a.

6. Stavke ankete o obimu korištenja EPS-a.

6.1. Koristim EPS češće od drugih iz svoje okoline.

6.2. Trenutno koristim i nastavit ću koristiti EPS.

6.3. Vjerujem da će se upotreba EPS-a u budućnosti povećati.

Prilog 2. - Lista tabela