UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

Diplomsko delo

VARNOSTNI VIDIKI INFORMACIJSKIH SISTEMOV V JAVNI UPRAVI: POMEN GESEL

Adnan Dizdarević

Ljubljana, september 2014

UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

DIPLOMSKO DELO

VARNOSTNI VIDIKI INFORMACIJSKIH SISTEMOV V JAVNI UPRAVI: POMEN GESEL

Kandidat: Adnan Dizdarević
Vpisna številka: 04041535
Študijski program: univerzitetni študijski program Uprava 1. stopnja

Mentor: doc. dr. Mitja Dečman

Ljubljana, september 2014

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisan Adnan Dizdarević, študent univerzitetnega študijskega programa Uprava, z vpisno številko 04041535, sem avtor diplomskega dela z naslovom: VARNOSTNI VIDIKI INFORMACIJSKIH SISTEMOV V JAVNI UPRAVI: POMEN GESEL, ki sem ga napisal pod mentorstvom doc. dr. Mitje Dečmana.

S svojim podpisom zagotavljam, da:

- je priloženo delo izključno rezultat mojega lastnega raziskovalnega dela;
- sem poskrbel, da so dela in mnenja drugih avtorjev oz. avtoric, ki jih uporabljam v predloženem delu, navedena oz. citirana v skladu s fakultetnimi navodili;
- sem poskrbel, da so vsa dela in mnenja drugih avtorjev oz. avtoric navedena v seznamu virov, ki je sestavni element predloženega dela in je zapisan v skladu s fakultetnimi navodili;
- sem pridobil vsa dovoljenja za uporabo avtorskih del, ki so v celoti prenesena v predloženo delo, in sem to tudi jasno zapisal v predloženem delu;
- se zavedam, da je plagiatorstvo – predstavljanje tujih del, bodisi v obliki citata bodisi v obliki skoraj dobesednega parafraziranja bodisi v grafični obliki, s katerimi so tuje misli oz. ideje predstavljene kot moje lastne – kaznivo po zakonu (Zakon o avtorski in sorodnih pravicah, Uradni list RS, št. 21/95), kršitev pa se sankcionira tudi z ukrepi po pravilih Univerze v Ljubljani in Fakultete za upravo;
- se zavedam posledic, ki jih dokazano plagiatorstvo lahko predstavlja za predloženo delo in za moj status na Fakulteti za upravo;
- je elektronska oblika identična s tiskano obliko diplomskega dela ter soglašam z objavo dela v zbirki »Dela FU«.

Diplomsko delo je lektorirala: Marjanca Šoško, prof.

Ljubljana, 01. 09. 2014

Podpis avtorja:

POVZETEK

Tema diplomskega dela je varnost informacijskega sistema, pomen gesel in njihova varnost. Organizacije pri svojem delu za nemoteno delovanje uporabljajo informacijske sisteme, v katerih so shranjeni številni podatki. Prav tako v sodobnem svetu na e-poslovanju temelji vedno več storitev, kot so e-bančništvo, e-študent, e-uprava in druge e-storitve. V diplomskem delu smo se osredotočili na mehanizme zagotavljanja varnosti na različnih ravneh, in sicer normativni, organizacijski in tehnični. Diplomsko delo predstavi tudi varna gesla in razbijanje le-teh. V praktičnem delu smo analizirali gesla za dostop do e-študenta, ki jih uporabljajo študentje Fakultete za upravo. Poleg analize gesel smo opravili tudi anketo o ozaveščenosti glede varnosti in uporabe gesel med študenti Univerze v Ljubljani.

Ključne besede: informacijski sistem, e-poslovanje, e-uprava, varnostna politika, gesla

SUMMARY

SECURITY ASPECTS OF INFORMATION SYSTEM IN PUBLIC SECTOR: THE VALUE OF PASSWORD

The subject of the final paper is the safety of the information system, the importance of passwords and their safety. For a smooth performance, companies rely on information systems, which contain numerous data. In the modern world, more and more services like e-banking, e-student, e-administration and others are based on e-business. In the final paper we focused on safety mechanisms on different levels: normative, organisational and technical. The final paper also introduces secure passwords and ways to crack them. In the practical part we analysed the passwords for accessing the e-student platform used by students of the Faculty of administration. We also conducted a survey about the awareness of security and application of passwords among the students of the University of Ljubljana.

Key words: Information system, e-business, e-administration, security policy, paswords

KAZALO

KAZALO PONAZORITEV

KAZALO GRAFIKONOV

KAZALO SLIK

KAZALO TABEL

SEZNAM UPORABLJENIH KRATIC

IS	Informacijski sistem
IT	Informacijska tehnologija
IKT	Informacijsko-komunikacijska tehnologija
G2G	Poslovanje znotraj javne uprave
G2B	Poslovanje med upravo in podjetji
G2C	Poslovanje med upravo in občani

1 UVOD

Smo v času, ko vse temelji na razvoju in uporabi tehnologije, interneta in tudi e-poslovanja. Hkrati se je z razvojem in široko uporabo informacijskih sistemov povečalo tudi število nevarnosti glede zaščite in zavarovanja podatkov. Danes je varnost podatkov na prvem mestu, predvsem zaradi vseh vdorov in s tem morebitnih kraj osebnih podatkov posameznika ali pa kraj poslovnih, zaupnih in tajnih podatkov organizacij. Varnost podatkov dosežemo z različnimi mehanizmi; z ustrezno pravno podlago, internimi varnostnimi politikami, ki so podkrepljene s standardi, in ustrezno organizacijsko kulturo ter tehničnim varovanjem.

Organizacije delujejo s pomočjo informacijskih sistemov, ki zagotavljajo podatke, iz katerih lahko zaposleni v organizaciji pridobivajo informacije za svoje delo. Informacijski sistemi v javni upravi hkrati omogočajo sodelovanje med različnimi organizacijami javnega sektorja (pridobivanje, posredovanje, zbiranje podatkov).

V dobi informacijsko komunikacijske tehnologije lahko pride tudi do izgube podatkov. Pomemben razlog za izgubo podatkov so napake v strojni opremi in sistemske napake. Sledijo napake, ki jih povzroči človek, programske napake, računalniški virusi, kraja oz. tatvina in uničenje opreme. V tem delu smo se osredotočili na mehanizme zagotavljanja varnosti na različnih ravneh: normativni, organizacijski in tehnični. V diplomskem delu smo opisali te mehanizme in podrobneje opredelili področje gesel.

V empiričnem delu diplomskega dela smo s pomočjo analize gesel na Fakulteti za upravo želeli ugotoviti ustreznost gesel študentov, ki uporabljajo študentski informacijski sistem »e-študent«. S pomočjo anketnega vprašalnika smo želeli ugotoviti stopnjo ozaveščenosti študentov Univerze v Ljubljani glede varnosti in ustreznosti gesel. Tako smo si pri pisanju diplomskega dela postavili dve hipotezi, in sicer:

H1: Študentje na Fakulteti za upravo za svoj dostop do e-študenta, kjer so zabeleženi vsi njihovi pomembni in tudi zaupni osebni podatki, uporabljajo varna gesla.

H2: Študentje Univerze v Ljubljani so premalo ozaveščeni o sami uporabi, pomembnosti in varnosti gesel.

Da bi zgornji hipotezi dokazali, smo v praktičnem delu diplomskega dela analizirali ustreznost gesel študentov Fakultete za upravo. Ugotoviti smo želeli, kako varna oziroma ustrezna so gesla študentov na fakulteti. Opravili smo anketo o uporabi gesel študentov v njihovem širšem življenju, tako v okviru študija kot tudi izven njega. Anketa je bila anonimna in na voljo na spletu.

Ker se na področju javne uprave predvsem geslom redko posveča primerno raven pozornosti in ker na fakulteti, kot eni od organizacij javnega sektorja, še nikoli ni bila opravljena taka varnostna analiza, je diplomsko delo eno prvih na tem področju.

Cilj diplomskega dela je najprej opredeliti informacijski sistem in elektronsko poslovanje, nato pa bralca seznaniti z nevarnostmi, ki prežijo v sodobnem svetu interneta in e-poslovanja, predvsem z vidika poslovanja znotraj javne uprave (G2G), kot tudi poslovanja s strankami (G2C). Posebno pozornost nato delo posveti geslom ter njihovemu pomenu ter prednostim in slabostim gesel. Vključen je tudi vidik zakonodaje s področja e-poslovanja v javni upravi, vidik varnosti ter koncepti informacijske varnostne politike. Prav tako smo predstavili pomen standardov na tem področju in njihovo povezavo z delovanjem javne uprave.

2 INFORMACIJSKI SISTEMI IN JAVNA UPRAVA

2.1 OPREDELITEV INFORMACIJSKEGA SISTEMA

Pojem informacijski sistem lahko razčlenimo na dva dela, in sicer na informacijo in sistem. Pojem sistem se že dolgo uporablja, izhaja iz stare Grčije in predstavlja neko sestavljeno celoto. Definiramo ga lahko kot neko množico medsebojno povezanih elementov. Lahko ga členimo v posamezne sestavine, elemente, kar nam omogoča poznavanje sistema kot celote. Element je navadno predmet našega zanimanja.

Informacija je sporočilo, ki ga človek prejme in s tem se zmanjša njegova stopnja neznanja. Določi namreč nekaj, kar je bilo prej neznano. Človek se glede na količino prejete informacije ustrezno ali neustrezno odziva. Za dostop do informacij in njihovo obvladovanje človek uporablja računalniško in komunikacijsko tehnologijo ter informacijski sistem (Gradišar in Resinovič, 1998).

Informacijski sistem je organiziran in urejen sistem, ki uporabniku posreduje potrebne informacije za odločanje. Informacijski sistem opredelimo kot »sistem, v katerem se zbira, obdeluje, shranjuje, analizira in posreduje informacije za določen namen« (Gradišar, 2003, str. 104). Pomembno je, da so te informacije na pravem mestu, v pravem času in z minimalnimi stroški.

Sestavine informacijskega sistema so strojna oprema, programska oprema, podatki, postopki in ljudje, ki vedno sodelujejo v informacijskih sistemih. Udeleženci v informacijskih sistemih so notranji in zunanji uporabniki, katerim je informacijski sistem namenjen, in informatiki. Ti skrbijo, da se določen informacijski sistem razvije, izvaja in tudi vzdržuje. Tako informatiki kot tudi uporabniki informacijskih sistemov se morajo ravnati po določenih predpisanih postopkih v obliki organizacijskih predpisov. Podatki vstopajo in izstopajo iz sistema in so shranjeni v obliki baze podatkov. Strojna oprema so računalniki, ki omogočajo zajem, shranjevanje in tudi izpis/prikaz podatkov. Prav tako k strojni opremi prištevamo informacijsko infrastrukturo in telekomunikacijske naprave za delovanje omrežij in ožičenja. K programski opremi prištevamo različne programe, ki nadzirajo računalnike ali pa programe za pretvarjanje podatkov v različne formate, protivirusne programe in druge (Gradišar, 2003).

Informacijske sisteme lahko razdelimo na več načinov, in sicer glede na namembnost, nastanek ali pripadnost informacijskega sistema. Glede na namembnost informacijskega sistema poznamo informacijske sisteme za obveščanje, v katerega uvrščamo vse informacijske sisteme, ki zajemajo sredstva javnega obveščanja, kot so različni mediji. Njihov namen je, da posredujejo svojim uporabnikom informacije o stanjih in dogodkih v okolju ali sistemu. V to skupino spadajo tudi informacijski sistemi za upravljanje in odločanje, ki oskrbujejo uporabnike z informacijami za opravljanje matičnega sistema. Če je matični sistem neka organizacija, govorimo o informacijskem sistemu organizacije, ki oskrbuje uporabnike z informacijami o delovanju same organizacije in njenega okolja.

Glede na nastanek ločimo formalni in neformalni informacijski sistem. Formalen informacijski sistem je natančno načrtovan, nenehno deluje in se prilagaja vsem spremembam organizacije. Tak sistem je nujen za obstoj organizacije, saj sistematično spremlja vse, kar se pomembnega dogaja. Neformalen informacijski sistem je za razliko od formalnega brez trdne strukture, urejenega procesa in vnaprej določenih podatkov in informacij, ki se pojavijo in krožijo v njem. Pri pripadnosti informacijskega sistema lahko govorimo o javnem in zasebnem informacijskem sistemu. Javni oziroma uradni informacijski sistem zajema podatke in ustvarja informacije, ki so pomembne za celotni matični sistem. Podatki v uradnem informacijskem sistemu morajo zadovoljiti informacijske potrebe, ki so predpisane z zakoni ali sprejete z dogovori, zagotoviti informacije, ki so potrebne za upravljanje in odločanje v organizaciji, prav tako pa morajo omogočiti izdelavo različnih poročil izven organizacije. Zasebni informacijski sistem obsega podatke in informacije, ki imajo pomen le za del matičnega sistema oziroma za posameznike v njem (Gradišar in Vintar, 1998).

2.2 VARNOST INFORMACIJSKEGA SISTEMA

V informacijskem sistemu so shranjeni številni podatki, zato je varnost informacijskega sistema zelo pomembna. Potrebno je ločiti med zaščito in varovanjem podatkov. Medtem ko je cilj zaščite podatkov zavarovati podatke pred uničenjem, krajo ali nepooblaščeno spremembo, je cilj varovanja podatkov preprečiti razkritje podatkov nepooblaščeni osebi. Različne oblike računalniškega kriminala ter nesreče, kot so napačno ravnanje operaterja, strojne okvare, napake v programih, podatkih, poškodbe računalniške opreme, neprimerne tehnične karakteristike in neodgovornost, ogrožajo informacijske sisteme. Varnost IS lahko povečamo z različnimi dejavnostmi, kot so:

- fizična varnost;
- nadzor dostopa;
- nadzor obdelav;
- nadzor nad programi;
- pripravljenost na nesrečo;
- spremljanje delovanja sistema.

Vzdrževanje fizične varnosti je pomembno, saj se s tem zmanjšuje tveganje za nastanek okvar naprav in nesreč zaradi delovanja okolja. Povečanje fizične varnosti lahko dosežemo z dvema ukrepoma. Prvi ukrep zajema prepoved uživanja hrane, pijače in kajenja v prostorih, kjer je računalniška oprema. Drugi ukrep, ki prav tako povečuje fizično varnost, omejuje dostop nepooblaščenim osebam v prostore, kjer so računalniki in računalniška oprema, komunikacijski centri in podatki. Dostop je namreč dovoljen le pooblaščenim osebam. V okvir povečanja varnosti informacijskega sistema spada tudi nadzor dostopa, s katerim skušamo preprečiti vsak nepooblaščeni poseg. Poznamo 4 vidike nadzora dostopa, in sicer: dostop do ročno obdelanih podatkov, določanje pravice dostopa, uveljavljanje pravice dostopa in šifriranje podatkov. Pri ročno obdelanih podatkih velja pravilo, da se zaupnih podatkov ne pušča na delovni mizi, temveč se jih ustrezno shrani.

Enako velja tudi za odpadke, saj do njih navadno ni težko priti in lahko razkrijejo varovano vsebino. Prav zato morajo zaposleni odpaden papir uničiti s posebnimi stroji. Varnost informacijskega sistema dosežemo tudi z določanjem pravic dostopa. Primer določanja pravic dostopa je na primer, da računalniku posredujemo seznam vseh tistih, ki ga lahko uporabljajo, in vsakemu dodelimo pristopno geslo. S tem onemogočimo dostop ostalim, ki te pravice nimajo. Uporabniki so znotraj sistema razdeljeni na več skupin, vsaka izmed njih pa ima različne pravice dostopa do različnih datotek ali uporabe programov. Nekatere skupine nimajo dostopa, nekatere imajo dovoljeno branje, branje in kopiranje ter branje in spreminjanje itd.

Pri uveljavljanju pravic dostopa, bodisi v primeru nadzora fizičnega dostopa do računalnika, komunikacijskih naprav in podatkov bodisi uporabe računalnika in mreže, velja pravilo, da se identificiramo z enim izmed načinov identifikacije. Identifikacija je možna na osnovi tega, »kaj vemo«, ki predstavlja najenostavnejšo obliko identifikacije s pomočjo gesla. Identifikacija na osnovi tega, »kaj imamo« je možna na več načinov. Pogostejša načina sta dostop s ključem in identifikacijska kartica. Uporablja se jih pri nadzoru fizičnega dostopa, saj sta najenostavnejši in najcenejši rešitvi. V primeru identifikacije na osnovi tega, »kje smo«, pa se lahko prepreči dostop do računalnika in podatkov tistim, ki so prišli do gesla nekoga drugega, vendar pa jim je onemogočen fizični vstop na njegovo delovno mesto (povezava gesla s terminalom). Identifikacija na osnovi tega, »kdo smo«, velja za najzanesljivejši način izmed vseh naštetih. Pri tem pa velja omeniti, da je tudi najdražji. Potrebujemo različno opremo, ki zazna različne fizične značilnosti posameznika in ga s tem razlikuje od drugih ljudi. Naprave lahko zaznavajo: prstne odtise, barvo glasu in vzorec spleta krvnih žil na očesni mrežnici. Te tehnike zaznavanja imenujemo biometrične metode.

Nadzor obdelav podatkov je skupek treh metod, in sicer priprave podatkov, preverjanja podatkov in popravljanje morebitnih napak. Pri pripravi podatkov določimo, kdo je za podatke odgovoren in kateri podatki se bodo obdelali. Samo preverjanje podatkov lahko poteka ročno ali s pomočjo računalnika. Med pravilno in učinkovito obdelavo podatkov lahko ugotovimo morebitne napake in jih popravimo, za kar pa je potreben kakovosten uporabniški program in nadzor nad njim.

Pri nadzoru kakovosti uporabniških programov ugotavljamo vsebinsko ustreznost programa ter njihovo vzdrževanje. Pomembno je tudi preprečevanje programov z računalniškimi virusi.

Pripravljenost na nesrečo zajema načrt dejanj, ki zmanjšajo ali odpravijo posledice odpovedi informacijskega sistema. Od vloge, ki jo ima informacijski sistem v organizaciji, je odvisna natančnost in obsežnost tega načrta. Načrt ima pomembno vlogo predvsem v organizacijah, kot so banke, zavarovalnice itd. Te organizacije se pred takšnimi nesrečami zavarujejo tudi z dvema enakima bazama podatkov.

Spremljanje delovanja informacijskega sistema zajema splošen nadzor nad računalniško opremo in njeno uporabo. Cilj je zagotavljanje pravilnega izvajanja postopkov vnosa, obdelave in izpisa podatkov (Gradišar in Resinovič, 1998).

2.3 INFORMACIJSKI SISTEMI V JAVNI UPRAVI

V tem poglavju bomo najprej opredelili pojem javna uprava. »Javna uprava je del oblastnega dela javnega sektorja, ki obsega državno upravo, lokalno samoupravo in nosilce javnih pooblastil. Gre za upravo v javnih zadevah, kjer vsakokratna oblast oceni, ali je določene zadeve treba opravljati v javnem interesu. V ta sklop uvrščamo vse zadeve, ki so skupnega pomena za vse prebivalce in organizacije na določenem območju« (Kavčič, 2011, str. 4).

Organizacije v javni upravi delujejo s pomočjo informacijskih sistemov. Informacijski sistemi v javni upravi omogočajo sodelovanje med različnimi organizacijami javnega sektorja. Med sodelovanje prištevamo pridobivanje, posredovanje in zbiranje podatkov. Nekateri informacijski sistemi v upravi so: pravni informacijski sistem, statistični informacijski sistem, geografski informacijski sistem, sistem za obravnavo dokumentov in drugi. Pomemben segment pa so različni registri in zbirke podatkov, ki delovanje teh sistemov podpirajo. Omeniti velja Centralni register prebivalstva, Kataster, Zemljiško knjigo in Poslovni register.

Pravno-informacijski sistem je izoblikovan iz posameznih podatkovnih baz in omogoča brezplačen dostop do zakonodajnih in drugih javnih dokumentov državnih organov in nosilcev javnih pooblastil v Republiki Sloveniji ter dokumentov, ki jih izdajajo institucije Evropske unije in Sveta Evrope. Pravno-informacijski sistem upravlja in vodi Služba vlade Republike Slovenije za zakonodajo. Cilj pravno-informacijskega sistema je zagotavljanje evidence vseh pravnih aktov, enotna uporaba pravnih predpisov, dostop do pravnih predpisov, javnost sodnih odločb ter enostavnost uporabe (Služba vlade RS za zakonodajo, 2013).

Statistični urad RS je specializirana informacijska služba, ki uporablja statistični informacijski sistem. Državnim organom in gospodarstvu zagotavljajo osnovne podatke za odločanje na strateški ravni. Sam statistični informacijski sistem pa obravnava podatke, ki jih lahko statistično obravnavamo (popis prebivalstva, starost idr.). Za statistični sistem je značilno, da podatke, ki jih pridobimo, lahko primerjamo z drugimi državami.

Uporablja se tudi geografski informacijski sistem, ki je definiran kot »sistem, ki združuje računalniško, strojno in programsko opremo ter postopke, oblikovane v podporo zbiranju, upravljanju, manipulaciji, analizi, modeliranju in prikazovanju prostorsko opredeljenih podatkov za reševanje zapletenega načrtovanja in upravljavskih problemov« (Korte v: Kotnik, 2003, str. 12). Pomemben segment pa so tudi različni registri in zbirke podatkov, ki delovanje teh sistemov podpirajo. Omeniti velja Centralni register prebivalstva, Kataster, Zemljiško knjigo, Poslovni register in druge.

2.4 OPREDELITEV E-POSLOVANJA

S pojavom interneta se je začelo e-poslovanje, ki po svoji naravi globalno in teoretično odpravlja tako časovne kot tudi geografske ovire.

Izvor pojma elektronsko poslovanje izhaja iz angleščine. V angleščini se za elektronsko poslovanje uporabljata dva pojma, in sicer »electronic business« ter »electronic commerce« Slednji obsega način dela, ki je elektronsko izmenjevanje podatkov ter skoraj neomejene vsebine poslovanja, kot so blago, storitve, plačevanje, delovanje državnih organov in javnih služb itd. (Toplišek, 1998) (Gradišar, 2003). Evropska komisija opredeljuje e-poslovanje kot »katero koli obliko poslovne transakcije, v kateri stranke delujejo elektronsko, namesto da bi si pošiljale »telesna« sporočila (physical exchanges) ali da bi bile v neposrednem stiku« (European Commision v: Toplišek, 1998, str. 4). Tako lahko tudi na področju poslovanja javne uprave govorimo o e-poslovanju, pri katerem se uporabniki poslužujejo informacijske tehnologije.

Uporabnike razdelimo v tri skupine:

- podjetja in poslovni, gospodarski subjekti (business – B);
- državljani (citizen – C);
- javna uprava (government – G).

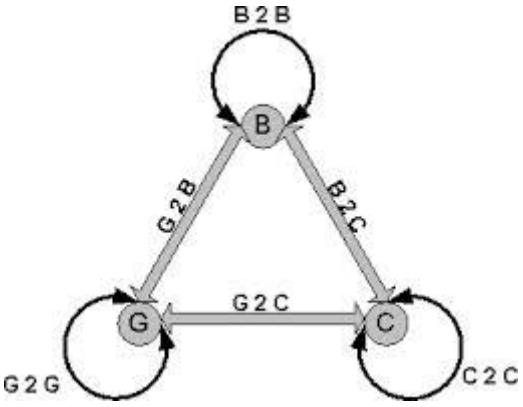
Glede na vrsto uporabnikov so razvrščene tudi e-storitve. Te so: G2C (»Government to Citizen«), G2B (»Government to Business«) in G2G (»Government to Government«).

G2C predstavlja e-storitve za državljane oziroma povezavo med javno upravo in državljani. To državljanom omogoča oddajo elektronskih vlog, plačevanje na spletu, iskanje zaposlitve, oddajo dohodninske napovedi, e-volitve, prijavo/odjavo stalnega bivališča, sprememba osebnega imena polnoletne osebe, spletno podaljšanje vozniškega dovoljenja, e-opomnik, e-gradiva itd.

G2B opredeli odnos med javno upravo in poslovnimi, gospodarskimi subjekti. Zajema prijavo davka na dodano vrednost (DDV), sodelovanje pri javnih naročilih itd.

G2G predstavlja e-storitve znotraj organizacij javne uprave in njihovo medsebojno sodelovanje, kar omogoča lažje in učinkovitejše poslovanje znotraj uprave. Omogoča pridobivanje in posredovanje podatkov med organi javne uprave (med oddelki, referenti, ministrstvi) (Kričej, 2002).

Slika 1: Prikaz poslovanja e-uprave



Vir: Lesjak (2003, str. 77)

Ker je e-poslovanje širok pojem, je za določene vrste e-poslovanja bolje uporabiti izraze, ki to poslovanje opredelijo bolj funkcionalno. Primeri takšnih poslovanj so e-trgovanje, e-bančništvo, e-plačevanje, delo na daljavo, e-založništvo, e-vloge, e-zavarovalništvo, e-naročanje idr. (Toplišek, 1998).

2.5 PRAVNA OPREDELITEV E-POSLOVANJA

Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP – Ur. l. RS, št. 57/2000) je bil prvič sprejet leta 2000 in je istega leta stopil v veljavo. S tem se je začela tudi slovenska pot v e-upravo. Zakon je razdeljen na 5 poglavij. V prvem poglavju najdemo splošne določbe in opredelitev elektronskega poslovanja, ki zajema »poslovanje v elektronski obliki z uporabo informacijske in komunikacijske tehnologije in uporabo elektronskega podpisa v pravnem prometu, kar vključuje tudi elektronsko poslovanje v sodnih, upravnih in drugih podobnih postopkih, če zakon ne določa drugače« (ZEPEP-UPB1, 1. člen). Drugo poglavje se nanaša na samo elektronsko poslovanje in je razdeljeno na tri oddelke. Prvi oddelek ureja elektronsko sporočilo, drugi podatke v elektronski obliki in tretji odgovornost ponudnikov storitev informacijske družbe. Elektronsko sporočilo je »niz podatkov, ki so poslani ali prejeti na elektronski način, kar vključuje predvsem elektronsko izmenjavo podatkov in elektronsko pošto« (ZEPEP-UPB1, 2. člen). Elektronski podpis najdemo v tretjem poglavju, ki je razdeljen na osem oddelkov. Zakonsko je elektronski podpis definiran kot »niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki in je namenjen preverjanju pristnosti teh podatkov in identifikaciji« (ZEPEP-UPB1, 2. člen). Pri uporabi elektronskega podpisa je pomembna njegova varnost. Varen elektronski podpis mora biti povezan izključno s podpisnikom, iz njega se lahko zanesljivo ugotovi podpisnika, ustvarjen s sredstvi za varno elektronsko poslovanje, povezan s podatki, na katere se nanaša, kar omogoča vpogled v vsako spremembo podatkov. Četrto poglavje ureja kazenske določbe. V tem poglavju so navedeni prekrški in sankcije. V petem poglavju pa najdemo prehodne in končne odločbe.

2.6 SWOT ANALIZA E-POSLOVANJA JAVNE UPRAVE

V SWOT analizi e-poslovanja bomo prikazali 4 aspekte, in sicer: **s**trenght – prednosti, **w**eaknesses – slabosti, **o**pportunities – priložnosti in **t**hreats – nevarnosti. SWOT analiza je ena najpogostejših analiz in jo lahko apliciramo na katero koli področje. Po analizi lahko gradimo na prednostih, odpravljamo pomanjkljivosti, izkoristimo priložnosti ter se izognemo nevarnostim. V spodnji tabeli 1 so predstavljene nekatere prednosti in slabosti ter priložnosti in nevarnosti e-poslovanja.

Tabela 1: SWOT analiza e-poslovanja javne uprave

PREDNOSTI	**SLABOSTI**	**PRILOŽNOSTI**	**NEVARNOSTI**
Pridobivanje trgov, kjer koli in kadar koli.	Sledenje in povezovanje uporabniških profilov.	Informacijska družba lahko postane bolj demokratična.	Propad številnih »klasičnih« dejavnosti.
Neposreden dostop do kupca.	Zasebnost, nadlegovanje s sporočili.	Možnost za razvijalce programske in strojne opreme.	Manj delovnih mest, izguba starih delovnih mest.
Globalna dosegljivost.	Pomanjkanje standardov varnosti, kakovosti, zasebnosti.	Hitrejši razvoj.	Kraja oz. odtujitev podatkov.
Zmanjšanje stroškov.	Draga uporaba interneta.	Učinkovitejše poslovanje.	Prevare.
Povečanje časovnega in geo. obsega poslovanja.	Dosegljivost interneta.		
Cenejši in več izdelkov in storitev, dostava po želji.	Nezaupanje v brezpapirno e-poslovanje.		
Dosegljive informacije, višji življenjski standard.	Pomanjkanje varnosti in zasebnosti podatkov.		
Na voljo so storitve javne uprave.	Internetno poslovanje zahteva stalno posodabljanje, nujni so hitri odzivi.		

Vir: Toplišek (1998, str. 22–23) (Možina et al., 2002)

2.7 E-UPRAVA

Težnja k razvoju e-uprave se je pojavila zaradi nekaterih slabosti »klasične« uprave, kot so nepreglednost in slaba dostopnost storitev, parcialnost, dolgi čakalni časi, zbirokratiziranost postopkov in netransparentnost delovanja upravnih organov. Vse to namreč ne zadovoljuje potrebe uporabnikov.

Obstaja več definicij e-uprave, odvisno od tega, kako avtor sam vidi e-upravo. Sami smo mnenja, da lahko e-upravo definiramo preprosto kot poslovanje z državo po elektronski poti. Delovanje e-uprave torej temelji na uporabi interneta, e-poslovanja in elektronskih dokumentov. E-uprava se nanaša na zakonodajno, izvršilno in sodno vejo oblasti, posluje na nadnacionalni, nacionalni, regionalni in lokalni ravni. Obsega poslovanje znotraj organizacij javne uprave (G2G), med upravo in podjetji (G2B, B2G), med upravo in občani (G2C, C2G) (Dečman, 2014).

E-uprava je usmerjena k uporabnikom. Njen namen je, da informira uporabnike, saj so vse potrebne informacije zbrane na enem mestu. S tem se zmanjša poraba časa uporabnikov pri urejanju in reševanju upravnih zadev. Uporabnikom tako ni potrebno kontaktirati uradnikov za splošna in ponavljajoča se vprašanja. Prav tako so uporabniki lahko bolj informirani, kar vodi do zmanjšanja obiskov v upravni enoti. Z e-upravo so upravne storitve postale celovite in bolj pregledne, delovanje e-uprave pa je bolj transparentno (Pintarič in Svete, 2007).

3 VARNOSTNA POLITIKA

3.1 ZAGOTAVLJANJE VARNOSTI V E-POSLOVANJU (VIDIK ORGANIZACIJE, TEHNOLOGIJ, PRAVNIH NORM)

Varnost v e-poslovanju temelji na diagramu zagotavljanja varnosti. Diagram zagotavljanja varnosti je cikel štirih elementov, in sicer: reagiranje, reševanje in blaženje, preprečevanje in zaznavanje. Najbolje je izvajati le preprečevanje.

Slika 2: Diagram zagotavljanja varnosti

Vir: Vintar in Grad (2004, str. 222)

Varnost v e-poslovanju dosežemo z različnimi elementi, kot so: varnostne politike, zavedanje o nevarnosti, varovanje IT, fizična varnost, varnost organizacije, načrtovanje kriznih situacij, varnost pred vplivi zaradi človeškega faktorja. Predvsem je pomembno tudi izobraževanje in osveščanje vseh sodelujočih v e-poslovanju o varnosti. Pomembno je ohraniti ustrezne podatke tajne in uporabljati šifrirana sporočila (Vintar in Grad, 2004).

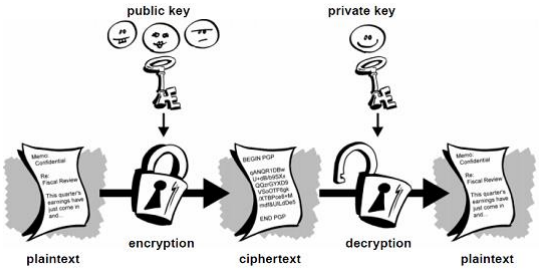
Pri tehničnem vidiku varnosti e-poslovanja se lahko uporablja različne metode, katerih uporaba je odvisna od zahtevane stopnje zaščite in tudi oblike sistema. Te metode so šifriranje, digitalni podpis in požarni zid. Z uporabo požarnega zidu preprečimo, da bi neavtoriziran uporabnik dobil dostop do omrežja. S postavitvijo požarnega zidu namreč omejimo možnosti za vdor v sistem ter omogočimo bolj varno uporabo uporabnikom interneta. Požarni zid je potrebno z veliko natančnostjo konfigurirati, namestiti in vzdrževati, saj nepravilno konfigurirana, nenadzorovana in slabo vzdrževana oprema poleg dejanske nevarnosti, povzroča tudi lažen občutek varnosti. Najbolj znani izdelovalci požarnih zidov na tržišču so Microsoft, Cisco, Checkpoint, Nortel in drugi. Šifriranje prepreči ponarejanje podatkov, če ti pridejo v napačne roke. Osnovno sporočilo, ki ga pošiljamo, je čistopis, šifropis pa je zašifrirano osnovno sporočilo. Sporočilo se spremeni v

šifrirano sporočilo po nekem postopku oziroma algoritmu, ki vključuje ključ. V elektronskem poslovanju se pogosto uporablja digitalni podpis, ki omogoča preverjanje identitete podpisnika, s čimer se prepreči goljufije in uporabo tuje identitete. Potrebno je ločiti med digitalnim podpisom in šifriranjem. Šifrira se vsebino sporočila, s čimer se zagotavlja predvsem zasebnost. Digitalni podpis pa dokaže verodostojnost sporočila. Prav tako pa je potrebno digitalni podpis ločiti od elektronskega podpisa. Medtem ko je elektronski podpis vsaka oblika podpisa, dobljena z elektronsko tehnologijo, je digitalni podpis pridobljen s šifrirnimi postopki. Za šifriranje se lahko uporablja dva šifrirna postopka, enojni/simetrični ali dvojni/asimetrični ključ (dvojni se uporablja pri digitalnem podpisovanju). Enojni ključ je manj varen kot dvojni ključ, saj je pri simetričnem sistemu potrebno ključ prenesti do druge stranke. Tako prejemnik kot pošiljatelj uporabljata enak ključ za šifriranje in dešifriranje. Ključ mora ostati tajen, prav zato se pogosto pojavi varnostni problem, saj bi lahko s poznavanjem tega ključa vsak dešifriral vsebino sporočila. Z uporabo sistema dvojnega ključa ima vsak pošiljatelj svoj zasebni ključ, ki ga pozna le on in ga lahko zavaruje tudi z geslom. Ima pa tudi javni ključ, ki ga mora poznati tudi prejemnik, da lahko dešifrira sporočilo.

Slika 3: Simetrično šifriranje/dešifriranje

Vir: (Križanovski, 2013)

Slika 4: Asimetrično šifriranje/dešifriranje



Vir: (Križanovski, 2013)

Poznamo tudi skupinski javni ključ, kadar hkrati podpisuje več oseb, kar tvori skupinski podpis. Da bi prejemnik sporočila ugotovil, ali uporabljeni javni ključ pripada podpisniku, se uporablja digitalno potrdilo. Digitalno potrdilo vključuje osebne in identifikacijske podatke lastnika, javni ključ in dodatne tehnične podatke. Digitalno potrdilo prav tako vsebuje podpis s strani overitelja digitalnih potrdil. To je identifikacijski dokument elektronskega okolja. V Sloveniji poznamo več overiteljev digitalnih potrdil. Nekateri izmed njih so: SIGEN-CA, SIGOV-CA, HALCOM-CA in drugi, ki delujejo v skladu z ZEPEP (Toplišek, 1998) (Vintar in Grad, 2004) (Bratuša in Verdonik, 2005).

Pri zagotavljanju varnosti v e-poslovanju je treba upoštevati tudi pravne norme. Pri e-poslovanju je treba upoštevati splošne in posebne predpise, ki urejajo varstvo osebnih podatkov. Zakon in predpisi o telekomunikacijah urejajo povezovanje z internetom in obravnavajo javna in zaprta omrežja ter telekomunikacijske javne in tržne storitve.

3.2 VARNOSTNA POLITIKA

Varnostna politika je proces, ki poteka stalno, temelji na stvarnih rešitvah in predstavlja nek formalni zapis vseh varnostnih mehanizmov in pravil, katerih se morajo pri svojem delu držati vsi posamezniki z dostopom do opreme in informacij (Golčman, 2008). Navadno je sestavljena iz treh delov. Tehnološki del zajema strojno, programsko in omrežno opremo, komunikacijski del vsebuje kriptografijo in protokole, organizacijsko-pravni del pa zajema delovne postopke in zakonodajno podlago.

Varnostna politika ima pomembno vlogo pri zagotavljanju celovite varnosti v organizaciji in omogoča pravilno postopanje glede pravne odgovornosti v primeru varnostnih nesreč. Pomembni so varnostni mehanizmi, kot so fizična zaščita, kriptografija, kontrola dostopa, beleženje aktivnosti, zaposlovalna politika, podvajanje, požarni zid, protivirusna zaščita in druge. Dobra varnostna politika je vpeljana skozi skrbniške postopke, smiselne smernice in druge primerne metode. Predstavljena mora biti vsem v organizaciji, prilagodljiva spremembam okolja in opredeliti mora vsa področja odgovornosti uporabnikov, skrbnikov in vodilnih. Prav tako dobra varnostna politika preprečuje nepooblaščeno dostopanje do informacij (Golčman, 2008).

3.3 VARNOSTNA POLITIKA V SLOVENSKI JAVNI UPRAVI

Varnostna politika javne uprave je dokument, ki je odsev politike, s katero javna uprava varuje informacijsko premoženje. Delo vseh zaposlenih, tako vodstva, kot tudi tistih, ki imajo dostop do informacij v sistemu javne uprave, mora temeljiti na tem dokumentu. Cilji varnostne politike v javni upravi so raznoliki. Med drugim je cilj postaviti skupno informacijsko varnostno politiko za celoten javni sektor. Temu sledi vzpostavitev standardov in sama skladnost s standardi. Cilj varnostne politike je tudi vzpostavitev kulture ter ozaveščanje uporabnikov o nevarnostih, ki pretijo v informacijskih sistemih. Vsi cilji so postavljeni z namenom, da se zagotavlja zaščita informacijskih sredstev pred vsemi nevarnostmi. Varnostna politika vključuje fizično varovanje, ki zajema kontrolo vstopov, dnevnike obiskov, video nadzor, varovanje opreme, varnostna območja, požarno varnost

in tudi seznam inventarja. Fizični zaščiti sledi varnostna politika na področju primerne rabe informacijskih sistemov. Ta določa uporabo elektronske pošte in interneta ter omejuje dostop do IS, kar pomeni, da lahko nekdo upravlja s podatki v IS samo s pridobljeno pravico, s tem pa sprejema tudi odgovornost za te podatke. Varnostna politika narekuje tudi šifriranje podatkov in varovanje občutljivih podatkov ter sankcije v primeru kršitev tega dokumenta. Določa tudi, kako se upravlja z dokumenti v javni upravi, samo klasificiranje podatkov, hranjenje in arhiviranje podatkov. Pomembna je vzpostavitev varnostnih kopij, zagotavljanje varnosti v omrežjih in IS ter postavitev neprekinjenega poslovanja in storitev. Vse storitve v slovenski e-upravi, v okviru poslovanja C2G in B2G, morajo torej biti varne. Varnost dosežejo tudi z uporabo kvalificiranega digitalnega potrdila različnih overiteljev. V Sloveniji imamo več overiteljev, in sicer SIGEN-CA, SIGOV-CA, podjetje Halcom informatika, d. o. o., Nova ljubljanska banka, d. d., in Pošta Slovenije d. o. o. SIGEN-CA izdaja kvalificirana digitalna potrdila za fizične in pravne osebe, overitelj SIGOV-CA pa za institucije v upravi. Služba HALCOM-CA pri podjetju Halcom Informatika, d. o. o., izdaja spletna digitalna potrdila za pravne osebe in fizične osebe. Prav tako za fizične ter zaposlene pravne in fizične osebe izdaja digitalna potrdila NLB-CA pri Novi Ljubljanski banki, d. d., in POŠTA®CA pri Pošti Slovenije, d. o. o. Storitve, ki jih lahko opravijo fizične in pravne osebe s kvalificiranim digitalnim potrdilom so oddajanje vlog, personalizacija portala e-uprava, e-zaposlitve, e-dohodnina, e-davki, naročanje izpisov iz matičnih knjig, vpogled v lastne osebne podatke in tudi elektronske storitve notarjev (Vintar in Grad, 2004; MJU, 2010; Marinšek, 2009).

3.4 STANDARDI NA PODROČJU VARNOSTI IN VARNOSTNIH POLITIK

Varnostna politika temelji na različnih zakonih, pravilnikih in standardih. Pomembno vlogo ima serija standardov ISO/IEC 27000, katerih cilj je doseganje visoke kakovosti varovanja informacij v organizacijah. Standard ISO/IEC 27000 usklajuje ustrezne strokovne pojme, principe in definicije. Osnova standarda je ISO 9000. Standard ISO/IEC 27000 vsebuje standarde:

- ISO/IEC 27001 – zahteve za gradnjo, upravljanje, vzdrževanje in izboljšanje sistema za upravljanje varovanja informacij (SUVI);
- ISO/IEC 27002 – vpeljava, izvajanje in vzdrževanje SUVI;
- ISO/IEC 27003 – vodenje standardizacije po ISO/IEC 27001;
- ISO/IEC 27004 – smernice za vrednotenje in poročanje o učinkovitosti informacijskih sistemov za zagotavljanje zanesljivosti;
- ISO/IEC 27005 – navodila za obravnavo, ocenjevanje in vrednotenje tveganj na področju informacijske varnosti;
- ISO/IEC 27006 – zahteve za organe, ki zagotavljajo smernice za revizijo in certificiranje varnosti informacijskih sistemov;
- ISO/IEC 27007 – smernice za organe, ki certificirajo, ter notranjo in zunanjo revizijo.

ISO/IEC 27002 ni formalni standard s specifikacijami, vendar se uporablja za usmerjanje certifikacije v skladu z ISO/IEC 27001. Predlaga dobre prakse s področja informacijske varnosti. Sam standard ISO/IEC 27001 navaja, kako graditi, upravljati, vzdrževati in izboljševati SUVI v organizaciji. Vsebuje 4 faze za upravljanje varovanja informacij, in sicer: vzpostavitev SUVI, izvajanje ter delovanje SUVI-ja, spremljanje in pregledovanje SUVI-ja in ne nazadnje vzdrževanje ter izboljševanje SUVI-ja. V prvem koraku je potrebno vzpostaviti politiko, cilje, procese ter postopke SUVI. V tej fazi načrtovanja mora biti vse dokumentirano. Drugi korak izvajanja ter delovanja SUVI-ja zajema vpeljavo in delovanje politik, ciljev, procesov in postopkov. V tem koraku se izvajajo vse načrtovane aktivnosti, ki so bile določene v prvem koraku. Sledi spremljanje in pregledovanje, kjer poteka ocenjevanje in tudi merjenje delovanja procesov glede na politiko in cilje SUVI. V tej fazi vodstvo organizacije pregleda rezultate na podlagi pridobljenih poročil. Vsi zbrani podatki v tretjem koraku služijo za merjenje uspešnosti pri doseganju poslovnih ciljev podjetja. V zadnjem koraku gre predvsem za sprejemanje popravnih in preventivnih ukrepov na podlagi rezultatov. Za izvajanje SUVI so odgovorni vsi zaposleni, vodilni v organizaciji, pooblaščenec za informacijsko varnost, stranke in drugi (Košćak, 2011).

4 GESLO

4.1 OPREDELITEV GESLA

Vse hitrejši razvoj tehnologije in informatizacije družbe od uporabnika zahteva pomnjenje uporabniških imen in gesel, ki jih potrebuje za dostop do različnih virov.

Gesla so ena izmed najstarejših metod zaščite, poznamo jih že iz Antike, kjer je bilo potrebno za dostop do mesta ali zgradbe poznati frazo – geslo. Gesla so uporabljali tudi v vojnah za razločevanje med sovražniki in prijatelji.

Danes geslo velja za najlažjo in verjetno najcenejšo zaščito bodisi informacijskega sistema, računalnika, telefona, e-poštnega strežnika za prebiranje pošte, raznih zbirk podatkov, forumov in spletnih strani. Kot je omenjeno v drugem poglavju diplomskega dela gre pri geslu za področje identifikacije na osnovi tega, »kaj vemo«. Kljub temu da poznamo številne tehnike overjanja, kot so biometrija, pametne kartice idr., je kombinacija gesla in uporabniškega imena še vedno prevladujoč pristop. Geslo lahko definiramo kot niz znakov. Sestavljajo ga črke, številke, drugi znaki, med katere spadajo tudi ločila ter ostali posebni znaki, ki določajo kakovost gesel (Hölbl, 2007).

4.2 ŠIBKA IN MOČNA GESLA

Šibka gesla so gesla, pri katerih potencialni napadalec nima pretiranega dela z ugotavljanjem le-teh. Šibka gesla so po navadi sestavljena iz kratkih, pogostih in lahko določljivih besed. Prav tako za šibka gesla veljajo privzeta gesla nekaterih naprav in omrežij. Šibka gesla se lahko ugotovijo z uporabo slovarja ali pa z grobo silo. Takšna gesla večinoma sestavljajo besede iz slovarjev, razna imena, izrazi, izpeljani iz uporabniškega imena ter imena domačih živali, datumi rojstev in podobni podatki, povezani z oškodovano osebo. Torej, šibka gesla so sestavljena iz črk in števil in so krajša, saj vsebujejo manj kot 8 znakov. Kot je omenjeno zgoraj, pogosto uporabniki svojih privzetih gesel ne zamenjajo, kar spletnim goljufom omogoča hitro ugotovitev gesel, saj je na spletu na razpolago veliko seznamov privzetih gesel.

Glede močnih gesel viri navajajo različno število znakov, ki naj bi veljali za dolžino močnega gesla. Niz znakov naj bi vseboval vsaj 8 znakov. Sestavljeni morajo biti tako iz črk, številk, ločil kot tudi posebnih znakov oziroma simbolov in morajo biti bolj »naključna«, saj s tem nepridipravom otežimo delo. Ker so močnejša gesla po navadi daljša in si jih je posledično težje zapomniti, lahko uporabimo mnemotehniko. To je tehnika, s katero si poenostavimo pomnjenje gesla. Pri mnemotehniki posamezne črke iz gesla povežemo z besedami, ki imajo določen pomen (Kodermac, 2011).

4.3 TEHNIKE OBLIKOVANJA GESEL

Problem oblikovanja gesel se pojavi takrat, ko si je izbrano geslo potrebno zapomniti. Vsi tisti, ki uporabljamo internet, uporabljamo bodisi eno geslo, bodisi več gesel za različne

namene. Temeljno pravilo oblikovanja gesel je, da je le-te potrebno razvrstiti po namenu uporabe. Nekateri uporabniki uporabljajo tako enako vrsto gesel za dostop do forumov, spletnih strani idr., kot tudi za e-bančništvo. V primeru uporabe istega gesla nepridipravu olajšamo delo, saj z dostopom do gesla na forumu pridobi dostop do drugih internetnih virov, ki jih uporabnik uporablja in mu s tem povzroči škodo.

Poznamo dve obliki oblikovanja gesel (Hölbl, 2007):

- oblikovanje gesel s frazami;
- oblikovanje s polnopomenskimi besedami.

Oblikovanje gesel na podlagi fraz poteka tako, da vzamemo prve črke besed poljubno izbrane fraze ali povedi in dodamo nekaj posebnih znakov. Na primer iz povedi »Informacijski sistemi v upravi so Različni«, lahko oblikujemo geslo IsvusR#2. Pazljivi moramo biti v primeru, da je pri nekaterih virih, kjer so potrebna gesla, prepovedana uporaba posebnih znakov.

Drug način oblikovanja iz dveh polnopomenskih besed je, da si izberemo dve besedi in mednju dodamo še posebne znake in številke. Kot primer vzemimo besedi visok in nizek. Geslo lahko oblikujemo kot visok4>3nizek. Zopet pa je njegova uporaba kot pri prejšnjem oblikovanju odvisna od tega, če je uporaba vseh posebnih znakov dovoljena.

Pri oblikovanju gesel moramo biti pozorni na več stvari, saj si s tem zavarujemo podatke. Geslo naj bo dolgo vsaj 8 znakov, uporabljene morajo biti tako črke, številke, ločila kot tudi posebni znaki. Uporabiti moramo velike in male črke ter se izogniti uporabi enostavnih zaporedij na tipkovnici (Hölbl, 2007).

4.4 TEHNIKE RAZBIJANJA GESEL

Razbijanje gesel oziroma hekanje v začetnih dejavnostih ni bilo škodljivo. Bistvene dejavnosti hekerjev, ki so jih izvajali, so bile razna raziskovanja in izboljševanje programov (Taylor v: Dimic in Dobovšek, 2012, str. 142). Danes pa ima izraz heker negativni prizvok, saj velja, da so vsi hekerji negativni. Pojem heker vključuje tako pozitivno naravnane hekerje, ki se ukvarjajo z informacijsko varnostjo, kot tudi negativne hekerje, ki izvajajo kazniva dejanja (Dimic in Dobovšek, 2012). Poznamo več tehnik razbijanja gesel. To so ugibanje, napad z grobo silo, napad s slovarjem in mavrične tabele. Pomembna je razlika med ugibanjem in napadom z grobo silo. Pri napadu z grobo silo iščemo vse možne kombinacije gesel, pri ugibanju pa se napadalec osredotoči na osebne podatke uporabnika, sezname najpogostejših gesel, razna privzeta gesla in podobno. Večkrat se zgodi tudi, da si pri napadu z grobo silo pomagajo tudi z ugibanjem.

4.4.1 UGIBANJE

Kot prvo tehniko hekanja oziroma razbijanja gesel bom opisal ugibanje. Znano je, da veliko uporabnikov izbira šibka gesla ali pa privzetih gesel večinoma ne zamenja. S tem olajšamo delo potencialnemu napadalcu, saj je na spletu veliko seznamov in zbirk gesel,

ki so najpogosteje uporabljeni. Tako lahko napadalec razbije zaščito brez posebnih tehnik. Nekateri napadalci uporabljajo programe, ki s pomočjo podatkov o uporabniku pridobijo potencialna gesla (Hölbl, 2007).

4.4.2 NAPAD Z GROBO SILO

Napad z grobo silo velja za najpreprostejšo obliko napada na gesla, kjer napadalec poskuša z vsemi kombinacijami znakov. Čas ugotovitve gesla je odvisen tudi od zmogljivosti računalnika, saj se njegova zmogljivost razlikuje glede na potrebe in zahteve uporabnika. Tehnika napada z grobo silo je namenjena za ugotavljanje kratkih gesel. Zahtevnost napada pa je odvisna tudi od sestave gesla. Geslo, ki je sestavljeno iz enakega števila znakov in vsebuje samo črke, je lažje ugotoviti kot geslo, ki vsebuje tako črke, številke in posebne znake (Hölbl, 2007).

Kot primer lahko navedemo geslo, dolžine 6 znakov. Če geslo vsebuje vse možne znake, torej 96 možnih znakov, ki so lahko uporabljeni geslu, mora potencialni napadalec preizkusiti $782*10^9$ kombinacij. Če pa geslo vsebuje samo črke, velike in male, brez šumnikov, torej ima 52 možnih znakov, se število kombinacij zmanjša na $19*10^9$. S pomočjo Gibson's Research Corporation kalkulatorja smo izračunali hitrost napada in razbitja gesla, dolžine 6, z grobo silo. Kalkulator nam je na podlagi ugibanj na sekundo podal okvirni čas razbitja gesla. Ugotavljali smo čas razbitja gesla 1000 ugibanj/sekundo, $100*10^9$ ugibanj/sekundo in $100*10^{12}$ ugibanj/sekundo. Izbrali smo si gesli dolžine 6: Medved (vsebuje male in velike črke) in Med4_d (vsebuje vse možne znake). Za razbitje gesla Medved bi potencialni napadalec pri 1000 ugibanj/sekundo potreboval 7,69 meseca. Za razbitje gesla z $100*10^9$ ugibanj/sekundo bi potrebovali 0,2 sekunde in 0,0002 sekunde pri hitrosti ugibanja $100*10^{12}$. V primeru izbire nekoliko zahtevnejšega gesla kot je Med4_d podaljšamo čas. Pri 1000 ugibanj/sekundo se čas razbijta gesla poveča na približno 2250 let. Pri napadu z $100*10^9$ ugibanj/sekundo bi porabili približno 11,76 minute ter pri napadu z $100*10^{12}$ 0,7 sekunde (Gibson, 2012). Za lažjo predstavo smo navedli primer navadnega namiznega računalnika v raziskavi, ki je bila opravljena leta 2009 (Lucas, 2009). Takratni računalniki z dvojedrnim procesorjem bi lahko odkrili gesli Medved in Med4_d zelo hitro. Ob predpostavki, da bi uporabili geslo Medved, bi potencialni napadalec za ugotovitev gesla potreboval približno 33 minut. Pri uporabi gesla Med4_d pa nekoliko več, in sicer 22 ur. Vendar pa zaradi razvoja tehnologije in Moorovega zakona, ki pravi, da se moč procesorjev vsakih 18 mesecev podvoji, sklepamo, da se je ugibanje gesel na sekundo povečalo za več kot $100*10^6$ gesel na sekundo z uporabo procesorja računalnika (Lucas, 2009) (McGrath, 2009).

Napadi z grobo silo se poskušajo pospešiti z različnimi tehnikami, kot so že prej omenjeno ugibanje in tudi napad s slovarjem. Število kombinacij, ki jih mora odkriti spletni napadalec, je odvisno od dolžine gesla in tudi vrste uporabljenih znakov. Od tega je odvisen tudi čas ugotovitve gesla. Daljše kot je geslo, več kombinacij s tem dobimo, več časa je potrebnega za razbitje gesla. V spodnjih tabelah smo prikazali različne dolžine gesel, ki vsebujejo samo številke ali pa vse možne znake in število možnih kombinacij. Če

geslo vsebuje samo številke, lahko izbiramo med desetimi znaki: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Z vsako dodatno številko v geslu se število možnih kombinacij poveča (Lucas, 2009).

Tabela 2: Dolžina številčnih gesel in njegove kombinacije

GESLO (0,1,2,3,4,5,6,7,8,9)	
DOLŽINA	KOMBINACIJE
2	100
3	1000
4	10.000
5	100.000
6	1.000.000
7	10.000.000
8	100.000.000
9	1.000.000.000

Vir: (Lucas, 2009)

Podobno situacijo imamo tudi pri geslih, ki vsebujejo črke, posebne znake in različne druge kombinacije povezane med seboj. Za primer vzemimo število možnih kombinacij ob uporabi velikih in malih črk, števil ter posebnih znakov – vseh možnih znakov je 96 (Lucas, 2009).

Tabela 3: Dolžina gesel pri uporabi vseh možnih znakov in njegove kombinacije

GESLO (vse črke, številke, posebni znaki)	
DOLŽINA	KOMBINACIJE
2	9216
3	884.736
4	$85*10^6$

5	$8*10^9$
6	$782*10^9$
7	$75*10^{12}$
8	$7,2*10^{15}$
9	$0,69*10^{18}$

Vir: (Lucas, 2009)

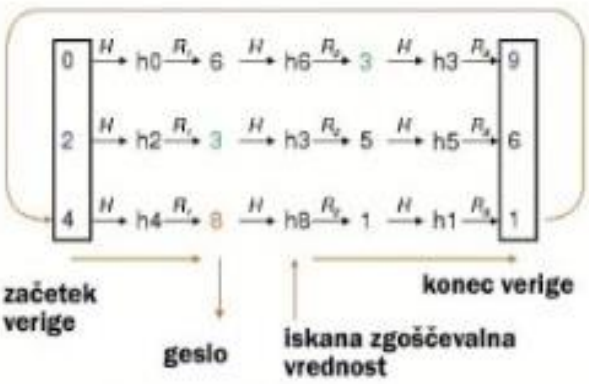
4.4.3 NAPAD S SLOVARJEM

Tako kot napad z grobo silo je tudi slovarski napad usmerjen na tiste uporabnike, ki uporabljajo krajša gesla, besede iz slovarjev in druga nevarne oblike gesel. Slovar uporabljajo tudi pri pošiljanju vsiljene pošte, saj z njim preverjajo obstoj poštnih naslovov. Glede napada z grobo silo pri slovarju izhajajo gesla iz besed, katere lahko najdemo v slovarju. Pri iskanju poštnih naslovov pa napadalci uporabijo slovar, ki vsebuje spisek najbolj pogostih uporabniških imen. Slovar vsebuje besede iz slovarjev različnih jezikov, osebna imena, krajevna imena, pogosta gesla ter pogoste kombinacije gesel. Napadalčeva aplikacija za vsako besedo izdela različne možnosti glede na vsebnost malih, velikih črk in podobno. Trajanje izvajanja napada je odvisno od več dejavnikov, in sicer od zmogljivosti računalnika in internetne povezave, dolžine slovarja ter same kakovosti uporabljenega slovarja (Kodermac, 2011).

4.4.4 NAPAD S POPREJŠNJIM RAČUNANJEM

Izumitelj mavričnih tabel je kripograf Martin Helmann. V sodobnih sistemih, kjer se gesla ne shranjujejo neposredno na disk, se gesla najprej obdelajo oziroma uporabijo postopki za shranjevanje gesel. Uporablja se zgoščevalna funkcija, s katero se geslo spremeni v ne berljivo obliko – povzetek (ang. Hash), ki ga shranimo. Gesla se shranjujejo po tem principu, ker v primeru uspešnega napada napadalec ne more pridobiti gesel preostalih uporabnikov, saj so v geslih shranjene samo zgoščevalne vrednosti. Tudi če napadalec pozna zgoščevalno vrednost, ne more ugotoviti gesla, razen če poizkusi vse možne kombinacije gesel in nad njimi izvede zgoščevalno funkcijo ter vrednost, ki jo dobi, primerja s tisto v shranjeni datoteki. Tukaj pa lahko uporabimo napad z mavričnimi tabelami. Geslo lahko razbijemo v nekaj sekundah. Mavrične tabele temeljijo na vnaprejšnjem računanju vseh možnih gesel in njihovih zgoščevalnih vrednosti. Dobimo veliko tabelo gesel in njegovih pripadajočih zgoščevalnih vrednosti. Mavrične tabele so oblikovane vnaprej oziroma izračunane, zato napadalcu prihranijo veliko časa, saj poišče le tisto vrednost v tabeli, ki jo potrebuje. Napadalcu torej ni potrebno poizkušati vsa gesla in čakati na odziv, ali je geslo pravilno (Hölbl, 2007).

Slika 5: shema mavrične tabele



Vir: (Hölbl, 2007)

4.5 NAJPOGOSTEJŠA GESLA V LETU 2013

Najpogostejša gesla so gesla, ki spletnim kriminalcem olajšajo delo, saj so splošno znana. Gesla objavijo nepridipravi, ki v določen sistem vdrejo, nato sledijo številne analize gesel različnih organizacij. Nekateri vdori so se zgodili velikim portalom, kot so MySpace, phpbb.com, hotmail, RockYou in drugi. V raziskavi (Žagar, 2010), ki je bila objavljena leta 2010, je avtor pripravil analizo slovenskih gesel, pridobljenih v letih 2001–2006 iz različnih virov. Analiziral je 55.096 gesel, najpogostejša gesla so prikazana v tabeli 4.

Tabela 4: Najpogostejša slovenska gesla

geslo	pojavitev
123456	0.45%
12345678	0.22%
abc123	0.15%
12345	0.14%
mateja	0.13%
sonce	0.13%
mojca	0.12%
1234	0.11%
geslo	0.11%
123456789	0.10%
matej	0.09%
marko	0.09%
alenka	0.09%
ljubezen	0.09%
123	0.09%
krneki	0.08%
klemen	0.08%
password	0.08%
andrej	0.08%
soncek	0.08%

Vir: (Žagar, 2010)

Iz tabele je razvidno, da sta najpogostejši gesli 123456 in njegova daljša različica 12345678. Kot vidimo, večinoma uporabljamo slovenščino, zato tisti napadalci, ki uporabljajo napade s slovarji večinoma v angleškem jeziku, niso pretirano uspešni. Uporabljamo tudi veliko lastnih imen. V naših geslih uporabljamo tudi gesli, kot sta password in geslo. Najpogostejša so 6 znakovna gesla, sledijo 7 znakovna in 8 znakovna gesla. Zelo malo je gesel, ki so daljša od 13 mest, in sicer 0,83 % (Žagar, 2010).

Glede svetovnih gesel je SplashData objavil svoj seznam najslabših oziroma najpogostejših gesel. Seznam je bil objavljen iz dokumentov, ki so bili ukradeni in na spletu objavljeni v letu 2013. V spodnji sliki so po pogostosti objavljena gesla, ki so jih ljudje uporabljali v letu 2013, in sicer od prvega gesla, ki je najpogosteje uporabljeno, pa vse do konca, s katerim pogostost vpada.

Slika 6: Seznam 25 najpogostejših gesel v letu 2013

1) 123456	6) 123456789	11) 123123	16) 1234	21) password1
2) password	7) 111111	12) admin	17) monkey	22) princess
3) 12345678	8) 1234567	13) 1234567890	18) shadow	23) azerty
4) qwerty	9) iloveyou	14) letmein	19) sunshine	24) trustno1
5) abc123	10) adobe123	15) photoshop	20) 12345	25) 000000

Vir: (SplashData Inc, 2014)

5 EMPIRIČNA RAZISKAVA

5.1 ANALIZA GESEL

V diplomskem delu smo opravili analizo gesel študentov na Fakulteti za upravo. Analizirali smo 6204 gesel študentov, ki so obiskovali in še vedno obiskujejo Fakulteto za upravo. Pri raziskavi ni bilo vzpostavljeno nikakršno povezovanje gesel z osebnimi podatki študentov, tako da je bila zaščita osebnih in tajnih podatkov zagotovljena. S pomočjo analize gesel sem skušal ugotoviti številne lastnosti gesel naših študentov, kot so:

- število malih črk v geslu;
- število velikih črk v geslu;
- število številk v geslu;
- število posebnih znakov v geslu;
- število oseb, ki uporabljajo samo velike črke;
- število oseb, ki uporabljajo samo male črke;
- število oseb, ki uporabljajo samo številke;
- število oseb, ki uporabljajo samo posebne znake;
- število oseb, ki uporabljajo tako črke, številke kot tudi posebne znake;
- število oseb, ki uporabljajo črke in številke;
- število oseb, ki uporabljajo črke in posebne znake;
- število oseb, ki uporabljajo številke in posebne znake;
- uporaba črk, številk in posebnih znakov v geslu ter njihovo povprečje, minimumi, maksimumi ter standardni odkloni v geslu;
- število oseb, ki uporabljajo svoje ime ali njegov del v svojem geslu;
- število oseb, ki uporabljajo svoj priimek ali njegov del v svojem geslu;
- število oseb, ki uporabljajo ime ulice različnih dolžin v svojem geslu;
- število oseb, ki uporabljajo kraj rojstva različnih dolžin v svojem geslu;
- število oseb, ki uporabljajo dan rojstva v svojem geslu;
- število oseb, ki uporabljajo mesec rojstva v svojem geslu;
- število oseb, ki uporabljajo letnico rojstva (xx) v svojem geslu;
- število oseb, ki uporabljajo letnico rojstva (xxxx) v svojem geslu;
- število oseb, ki uporabljajo izbrana najpogostejša gesla v Sloveniji in
- število oseb, ki uporabljajo izbrana najpogostejša gesla na svetu.

Analizo gesel smo opravili z orodjem Microsoft Excel. Uporabili smo nekatere funkcije in sicer: COUNTIF, COUNTIFS, AVERAGE, MIN, MAX, STDEV idr. Analiza gesel je vsebovala različne parametre, kot so ime, priimek, spol, kraj rojstva, ulica stalnega prebivališča, GSM, telefon ter geslo. Na podlagi omenjenih parametrov smo opravili analizo gesel študentov Fakultete za upravo. Skušali smo ugotoviti lastnosti, ki so naštete v prvem poglavju analize gesel. Omeniti velja, da zaradi varovanja osebnih podatkov študentov ni bil omogočen vpogled v parametre.

V spodnjih slikah je prikazan način dela, s katerim smo analizirali gesla. Zaradi velikega števila podatkov smo analize razdelili po posameznih delih zaradi boljše preglednosti.

Slika 7: Parametri za analizo gesel

IME	PRIIMEK	SPOL	DATUM_ ROJSTVA	KRAJ_ROJSTVA	ULICA_STALNO	GSM	TELEFON	GESLO2

Vir: Lasten

Kot je razvidno iz zgornje slike, so vsi osebni parametri zbrisani zaradi varovanja osebnih podatkov. Tudi med samo analizo gesel teh podatkov nismo imeli, saj bi s tem kršili pravice študentov do varovanja osebnih podatkov.

Slika 8: Analiza sestave gesel

Geslo-številka	Geslo-mala črka	Geslo-velika črka					
1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8	dolžina	število številk	število malih črk	število velikih	število posebnih znakov

Vir: Lasten

Pri analizi sestave gesel smo ugotovili, da so vsa gesla na Fakulteti za upravo 8-mestna. To je posledica takratne politike gesel, ki pa se je v letu 2012 že spremenila in omogoča tako daljša kot krajša gesla. Geslo smo torej lahko razdelil od 1–8, torej ima vsak znak svoj prostor. Uporabili smo funkcijo =MID($I4;J$3;1), ki vrne določeno število znakov iz besedilnega niza z začetkom pri navedenem položaju in na osnovi navedenega števila znakov.

Pri ugotavljanju številk v geslu smo uporabili pogojno funkcijo =IF(ISNUMBER(VALUE(J4));1;0), ki nam na podlagi pogoja ISNUMBER vrne vrednost 1 ali vrednost 0. Če gre za vrednost 1 potem naše geslo vsebuje številko in obratno, če funkcija vrne vrednost 0, potem naše geslo številk ne vsebuje. Za ugotovitev malih črk v geslu smo uporabili zopet pogojno formulo IF(OR(EXACT(J4;"a");EXACT(J4;"b"),...)1;0), ki nam je v primeru malih črk vrnila vrednost 1 oziroma v primeru, da znak ni bil majhna črka, vrednost 0. Podobno formulo smo uporabili tudi za velike črke s tem, da smo

majhne črke v formuli zamenjali z velikimi IF(OR(EXACT(J4;"A");EXACT(J4;"B"),...)1;0). Tako kot za majhne črke velja enako tudi za velike črke glede vrednosti 0 in 1.

Dolžino gesel smo ugotavljali s funkcijo =LEN(I4), ki nam vrne število znakov v besedilnem nizu. Pri ugotavljanju števila številk v geslu smo uporabili funkcijo =SUM(R4:Y4), ki je v stolpcu Geslo-številka seštela vrednosti od 1–8. Prav tako smo uporabili funkcijo =SUM za ugotavljanje števila malih črk in velikih črk. Za ugotavljanje posebnih znakov pa smo od dolžine gesla odšteli število številk, malih črk in velikih črk. Dobljen rezultat je predstavljal število posebnih znakov v geslu.

Slika 9: Analiza gesel z začetnimi parametri (ime, priimek, datum roj., idr.)

ujemanje z deli imena dolžine 3	ujemanje z deli imena dolžine 4	ujemanje z deli imena dolžine 5	ujemanje z deli priimka dolžine 3	ujemanje z deli priimka dolžine 4	ujemanje z deli ulice dolžine 1	ujemanje z deli ulice dolžine 2	ujemanje z deli ulice dolžine 3	ujemanje z deli kraj_roj dolžine 2	ujemanje z deli kraj_roj dolžine 3	ujemanje z deli kraj_roj dolžine 4

Vir: Lasten

Pri analizi z začetnimi parametri, kot so ime, priimek, datum rojstva in ulica stalnega prebivališča smo ugotavljali ujemanje z njihovimi deli. Vse formule so bile enake, le stolpci in številke dolžin ujemanja so bile drugačne, in sicer =IFERROR(FIND(LEFT($A4;3);$I4);0). IFERROR vrne navedeno vrednost, če se formula vrednoti kot napaka, v nasprotnem primeru vrne rezultat formule. Zgornja formula je primer ugotavljanja ujemanja gesla z deli imena dolžine 3. Torej za formulo potrebujemo ime osebe, dolžino, ki jo iščemo ter geslo. V primeru ujemanja gesla z imenom nam formula vrne vrednost, na kateri je to ujemanje. Funkcijo LEFT smo uporabili, ker vsebuje navedeno število znakov na levi strani. Torej vedno začne iskati vrednosti iz leve strani niza. To formulo smo uporabili pri vseh ugotovitvah, ki so razvidne iz zgornje slike.

Za ugotavljanje števila oseb, ki v svojem geslu uporabljajo dele imena, smo uporabili funkcijo =COUNTIF(AU4:AU6207;">0"), katera prešteje celice v obsegu, ki ustrezajo pogoju. Tokrat je bil naš pogoj, da funkcija prešteje vse vrednosti, ki so večje od 0. V tem primeru bi lahko uporabili tudi pogoj, pri katerem bi lahko v formulo vstavil tudi pogoj, kjer so vrednosti enake 1. Torej je funkcija preštela vse vrednosti, ki so ustrezale pogoju >0 ali =1. Formulo =COUNTIF smo uporabili za ugotavljanje vseh parametrov tudi pri ugotavljanju parametrov, kot so priimek, datum rojstva, ulica stalnega prebivališča, kraj rojstva in najpogostejših gesel, le da je bil vsakič pogoj in pa obseg podatkov drugačen. Za ugotavljanje oseb, ki ne uporabljajo delov imen za svoje geslo, pa smo prav tako uporabili funkcijo =COUNTIF(AU4:AU6207;"=0"), vendar je bil v nasprotju s prejšnjo pri tem pogoj, da funkcija prešteje vse vrednosti, ki so enake 0. Za lažjo predstavo smo izračunali tudi odstotke tistih, ki dele imen v geslih uporabljajo. Uporabili smo

matematično formulo X/Y * 100, pri čemer je X spremenljivka za število oseb, ki uporabljajo dele imena, Y spremenljivka pa število oseb, ki v svojem geslu ne uporabljajo delov imena.

Slika 10: Analiza gesel parametra datum in letnica rojstva

dan rojstva	mesec rojstva	letnica rojstva yyyy	letnica rojstva yy	je v geslu dan rojstva	je v geslu mesec rojstva	letnica rojstva je v geslu yyyy	je v geslu letnica rojstva yy

Vir: Lasten

Za ugotovitev in analizo datuma in letnice rojstva v geslu smo uporabili =TEXT. Če smo hoteli ugotoviti, ali geslo vsebuje datum in letnico rojstva, smo najprej morali iz začetnega parametra DATUM_ROJSTVA razdeliti datum na dan, mesec in letnico rojstva. Za dan rojstva smo uporabili funkcijo =TEXT($D4;"dd"), ki nam vrne dan rojstva v dveh nizih, saj imamo največ 31 dni v mesecu. Za mesec rojstva smo uporabili funkcijo =TEXT($D4;"m"). Črka »m« se uporablja kot koda za določitev meseca v letu. Raziskovali smo tudi ujemanje s celotno letnico rojstva s funkcijo =TEXT($D4;"yyyy") in ujemanje s krajšo obliko zapisa letnice rojstva =TEXT($D4;"yy"). Sledilo je ugotavljanje, ali so dan, mesec ter letnica rojstva v geslu. Uporabili smo že znano formulo iz prejšnjega odstavka =IFERROR(FIND(BF4;$I4);0), ki nam je v primeru najdenega parametra vrnila vrednost, na kateri se rezultat nahaja.

Slika 11: Analiza gesel na podlagi najpogostejših gesel v Sloveniji in svetu

Najpogostejša gesla v Sloveniji (natanko				svetovna gesla (natanko 8 znak		
password	12345678	qwertzui	ljubezen	trustno1	xxxxxxxx	11111111

Vir: Lasten

Glede analize gesel na podlagi najpogostejših gesel v Sloveniji in svetu smo uporabili formulo =COUNTIF(I4;BA3), katera prešteje celice v obsegu, ki ustrezajo danemu pogoju. V našem primeru je obseg stolpec I4, ki vsebuje različna gesla, dan pogoj pa je točno določeno geslo. Gesla, ki sem jih iskal, so prikazana na sliki 11. V primeru, če je oseba uporabila geslo iz zgornje slike, je funkcija izpisala vrednost 1, v nasprotnem primeru pa vrednost 0.

Drugi del analize gesel smo prav tako opravili v Excelu. Zanimalo nas je povprečje različnih parametrov ter število oseb, ki uporabljajo določene parametre. V spodnjih slikah smo prikazali način ugotavljanja parametrov.

Slika 12: Analiza parametrov dolžina, število številk, malih in velikih črk ter posebnih znakov

	število številk	število malih črk	število velikih	število posebnih znakov
max	8	0	8	4
min	0	0	0	0
average	2,02	0,00	5,96	0,02
st.dev	2,90	0,00	2,90	0,17

Vir: Lasten

Tabela 5: Števila oseb, ki uporabljajo različne znake v geslu

	Samo črke	Samo številke	Samo posebne znake	Številke	Črke	Vse znake	Številke in črke	Številke in znake	Črke in znake
Število oseb	3381	957	0	2759	5247	20	1802	20	83
Delež (%)	54,5	15,4	0	44,5	84,6	0,3	29	0,3	1,3

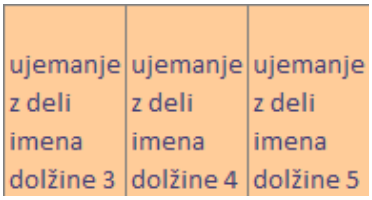
Vir: Lasten

Kot vidimo iz zgornje slike, smo v tem delu ugotavljali maksimum, minimum, povprečje ter standardni odklon določenih parametrov. Uporabili smo funkcije =MAX, =MIN, =AVERAGE in =STDEV.

Analiza je pokazala, da gesla naših študentov vsebujejo 8 znakov. Nekateri študentje uporabljajo samo številke za svoje geslo, nekateri pa samo črke. Nobeno od analiziranih gesel ni v celoti vsebovalo samo posebnih znakov. Povprečje pri uporabi številk v geslu znaša 2.02. Torej v povprečju 25 % dolžine gesla študentov Fakultete za upravo predstavljajo številke. Kot je bilo rečeno, je najbolje, da geslo vsebuje vse znake, tako črke, številke, kot tudi ostale posebne znake. Analiza je pokazala, da je takšnih gesel le 0,3 % (20). Imamo tudi študente, ki za svoje geslo uporabljajo samo črke, brez ostalih znakov. Povprečje uporabe črk je bilo 5,96, kar pomeni, da približno 75 % dolžine gesla

naših študentov predstavljajo črke. Glede posebnih znakov sem ugotovil, da jih nekateri sploh ne uporabljajo oziroma njihovo geslo vsebuje največ 4 posebne znake. Povprečje študentov, ki uporabljajo posebne znake, je tako zelo majhno in znaša 0,02. Iz tega lahko vidimo, da študentje, razen nekaterih izjem, ne uporabljajo posebnih znakov. Delež študentov, ki uporabljajo samo črke, je 54,5 % (3381), delež študentov, ki za geslo uporabljajo samo številke, 15,4 % (957) in delež študentov, ki uporabljajo posebne znake, je 0 % (0). Ugotovili smo tudi, koliko je študentov, ki imajo v geslu vsaj eno črko, in sicer je takšnih 84,6 % (5247). Delež študentov, ki imajo v geslu vsaj eno številko, je 44,5 % (2759). Delež števila študentov, ki uporabljajo samo številke in črke, je 29,5 % (1802), samo številke in znake 0,3 % (20) ter 1,3 % (83) je takšnih, ki uporabljajo v geslu črke in znake. Ugotovili smo tudi, da je delež študentov, ki uporabljajo tako črke, številke kot tudi posebne znake le 0,3 % (20).

Slika 13: Analiza gesel na podlagi parametra ujemanje z deli imen različnih dolžin



Vir: Lasten

Tabela 6: Število oseb, ki v geslih uporabljajo ujemanje z imeni različnih dolžin

	Ujemanje z deli imena dolžine 3	Ujemanje z deli imena dolžine 4	Ujemanje z deli imena dolžine 5
Število oseb	1515	1277	1140
Delež (%)	24,42	20,58	18,38

Vir: Lasten

Analiza je pokazala, da 24,42% (1515) študentov v svojem geslu uporablja zaporedje znakov dolžine 3, ki se pojavlja tudi v imenu. Delež študentov, ki v svojem geslu uporablja zaporedje znakov dolžine 4 je 20,58 % (1277), znakov

dolžine 5 pa 18,38 % (1140). Torej iz analize gesel vidimo, da 75,58 % (4689) študentov za svoje geslo ne uporablja imen.

Slika 14: Analiza gesel na podlagi u parametra ujemanje z deli priimka različnih dolžin

ujemanje z deli priimka dolžine 3	ujemanje z deli priimka dolžine 4	ujemanje z deli priimka dolžine 5

Vir: Lasten

Tabela 7: Število oseb, ki v geslih uporabljajo ujemanje s priimki različnih dolžin

	Ujemanje z deli priimka dolžine 3	Ujemanje z deli priimka dolžine 4	Ujemanje z deli priimka dolžine 5
Število oseb	651	433	336
Delež (%)	10,17	7,14	5,42

Vir: Lasten

Iz tabele vidimo, da 10,17% (631) študentov v svojem geslu uporablja zaporedje znakov dolžine 3, ki se pojavljajo tudi v priimku, 7,14 % (433) dolžine 4 in 5,42 % (336) dolžine 5.

Slika 15: Analiza gesel na podlagi parametra ujemanje z deli ulice različnih dolžin

ujemanje z deli ulice dolžine 3	ujemanje z deli ulice dolžine 4	ujemanje z deli ulice dolžine 5

Vir: Lasten

Tabela 8: Število oseb, ki v geslih uporabljajo ujemanje z deli ulice različnih dolžin

	Ujemanje z deli ulice dolžine 3	Ujemanje z deli ulice dolžine 4	Ujemanje z deli ulice dolžine 5
Število oseb	70	56	47
Delež (%)	1,3	0,90	0,76

Vir: Lasten

Ugotavljali smo tudi ujemanje z deli ulice dolžine 3, 4 in 5. Pri 1,3 % (70) študentih se geslo ujema z zaporedjem znakov dolžine 3, ki se pojavijo tudi v imenu ulice. Ujemanje dolžine 4 se pojavi pri 0,9 % (56) študentih in dolžine 5 pri 0,76 % (47) študentih.

Slika 16: Analiza gesel na podlagi parametra ujemanje z deli kraja rojstva različnih dolžin

ujemanje z deli kraj_roj dolžine 3	ujemanje z deli kraj_roj dolžine 4	ujemanje z deli kraj_roj dolžine 5

Vir: Lasten

Tabela 9: Število oseb, ki v geslih uporabljajo ujemanje z deli kraja rojstva različnih dolžin

	Ujemanje z deli kraj_roj dolžine 3	Ujemanje z deli kraj_roj dolžine 4	Ujemanje z deli kraj_roj dolžine 5
Število oseb	66	50	19
Delež (%)	1,06	0,81	0,31

Vir: Lasten

Delež študentov, ki v svojem geslu uporablja zaporedje znakov dolžine 3, ki se pojavi tudi v imenu kraja rojstva, je malo, 1,06 % (66), dolžine 4 znakov 0,81 % (50) študentov in dolžine 5 znakov 0,31 % (19) študentov.

Slika 17: Analiza gesel na podlagi parametra ujemanja z datumom rojstva

dan rojstva	mesec rojstva	letnica rojstva yyyy	letnica rojstva yy	je v geslu dan rojstva	je v geslu mesec rojstva	letnica rojstva je v geslu yyyy	je v geslu letnica rojstva yy

Vir: Lasten

Tabela 10: Število oseb, ki v geslih uporabljajo ujemanja z datumom rojstva

	Dan rojstva	Mesec rojstva	Letnica rojstva yyyy	Letnica rojstva yy
Število oseb	454	965	175	441
Delež (%)	7,32	15,55	2,82	7,11

Vir: Lasten

Dan rojstva v svojem geslu uporablja 7,32 % (454) študentov. Mesec rojstva uporablja 15,55 % (1965) študentov. Ugotavljali smo tudi ali študentje uporabljajo v svojem geslu celo letnico rojstva ali samo njeni zadnji dve številki. Zadnji dve številki letnice rojstva je torej uporabilo 7,11 % (441) študentov, 2,82 % (175) študentov pa je uporabilo v geslu celotno letnico rojstva.

Slika 18: Analiza gesel na podlagi parametra ujemanja z najpogostejšimi gesli

Najpogostejša gesla v Sloveniji (natanko				svetovna gesla (natanko 8 znak		
password	12345678	qwertzui	ljubezen	trustno1	xxxxxxxx	11111111

Vir: Lasten

Tabela 11: Število oseb, ki za geslo uporabljajo eno izmed najpogostejših gesel v Sloveniji in tujini

	Najpogostejša gesla v Sloveniji				**Najpogostejša gesla v tujini**		
	password	*12345678*	*qwertzui*	*ljubezen*	*trustno1*	*xxxxxxxx*	*11111111*
Število oseb	3	78	1	65	11	1	18
Delež (%)	0,05	1,26	0,02	1,05	0,18	0,02	0,29

Vir: Lasten

Najpogostejša izbrana gesla uporablja kar 2,85 % (177) vseh študentov. Iz zgornje tabele vidimo, da 1,26 % (78) študentov uporablja za svoje geslo 12345678, 1,05 % (65) študentov uporablja za svoje geslo besedo ljubezen in 0,29 % (18) študentov ima geslo 11111111.

5.2 ANKETA

Poleg analize gesel študentov na Fakulteti za upravo smo v diplomskem delu opravil tudi anketo, ki je metoda zbiranja in pridobivanja podatkov. Z anketo smo želeli ugotoviti ozaveščenost študentov glede varnosti gesel in njihovi uporabi. Anketo smo izvedli na spletu. Ciljna populacija anketirancev so bili študentje različnih fakultet Univerze v Ljubljani, različnega spola in starosti. Kratko anketo, ki je bila anonimna, je rešilo 100 študentov, in sicer 37 moških in 63 žensk. Anketa je vsebovala 13 vprašanj, ki so bila tako zaprtega, kombiniranega, kot tudi odprtega tipa.

Rezultati ankete:

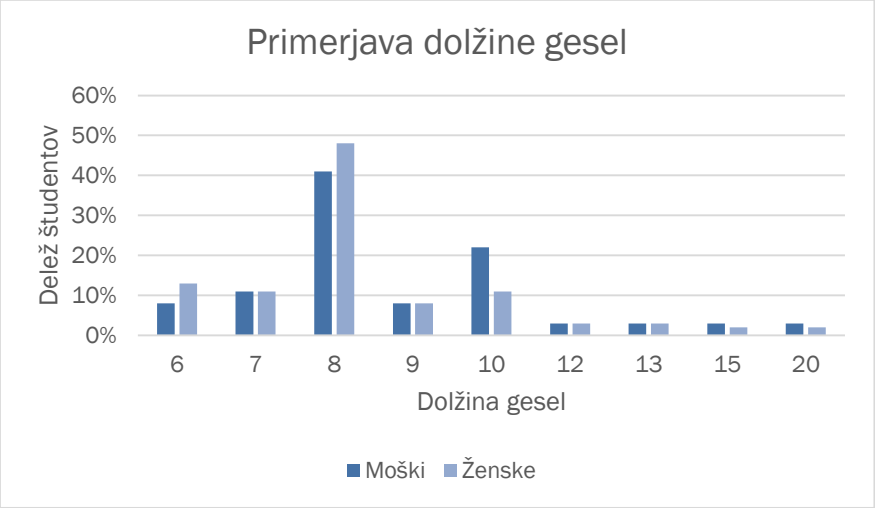
V1: Koliko znakov so v povprečju dolga vaša gesla?

Kot vidimo iz rezultatov ankete, je najpogostejša dolžina gesla naših anketirancev 8, kar je bolje kot ugotavlja raziskava o geslih uporabnikov po svetu, kjer je povprečna dolžina gesla dolga 6 znakov (Žagar, 2010). Menimo, da je do tega prišlo predvsem zaradi vse večjega ozaveščanja in oglaševanja na raznih spletnih straneh, socialnih omrežjih in drugih virih.

Grafikon 1: Grafični prikaz odgovorov na prvo vprašanje

Vir: Lasten

Grafikon 2: Grafični prikaz odgovorov na prvo vprašanje moški/ženske



Vir: Lasten

S prvim vprašanjem smo želeli izvedeti povprečno dolžino gesel, ki jih študentje uporabljajo. Na vprašanje je odgovorilo 100 študentov. Izkazalo se je, da je povprečna dolžina gesel 8,7 znakov, minimalno število znakov je 1, maksimalno pa 20 znakov. Standardni odklon je 2,40. Ker naj bi varno geslo vsebovalo vsaj 8 znakov, takšno geslo pa ima 45 % (45) anketirancev, sklepamo, da nekateri študentje v svojem geslu uporabljajo ustrezno število znakov. Zanimiva se nam je zdela primerjava dolžine gesel

med moškimi in ženskami. Ugotovili smo, da v povprečju oba spola uporabljata približno enako dolžino gesel. Gesla dolžine 8 uporablja več žensk, gesla dolžine 10 pa več moških.

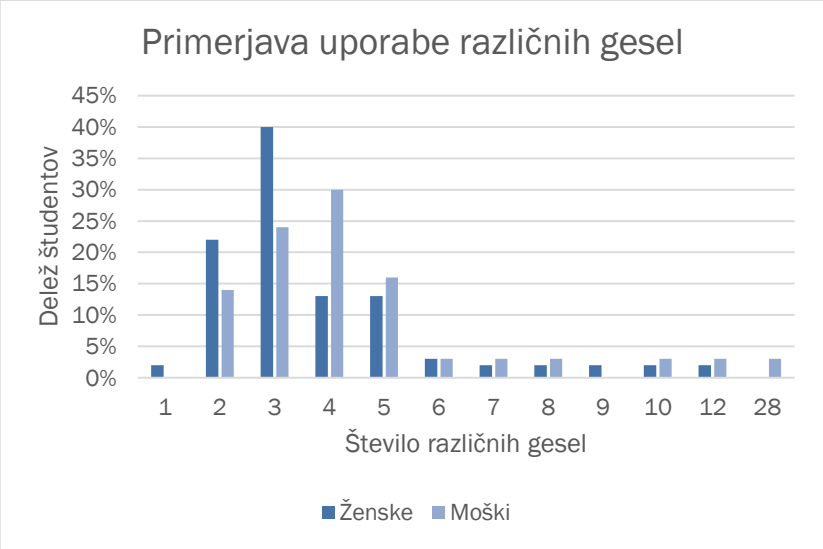
V2: Približno koliko različnih gesel uporabljate za različne storitve na spletu? (npr. e-pošta, soc. omrežja, internetne strani, e-bančništvo)

Več različnih gesel naj bi omogočilo večjo varnost. Vendar pa je vse odvisno od gesla samega in njegove dolžine ter uporabe različnih znakov. Menimo, da so uporabniki, ki imajo na primer 10 gesel dolžine 6 in ta vsebujejo samo eno vrsto znakov, manj varni pred morebitnim napadom kot uporabniki, ki uporabljajo gesla z vsemi znaki dolžine 8 ali več. Večje kot je število različnih znakov, več kombinacij morajo potencialni napadalci ugotavljati, dalj časa je potrebnega za dostop do podatkov.

Grafikon 3: Grafični prikaz odgovorov na drugo vprašanje

Vir: Lasten

Grafikon 4: Grafični prikaz odgovorov na drugo vprašanje moški/ženske



Vir: Lasten

Pri drugem vprašanju smo želeli izvedeti, ali študentje uporabljajo za različne storitve tudi različna gesla in koliko. Na vprašanje je odgovorilo 100 študentov, ki v povprečju uporabljajo 4,2 različnih gesel. Minimalno število različnih gesel je 1, maksimalno pa 28. Pri tem znaša standardni odklon od povprečja 3,17. Tudi v tem primeru se nam je zdela zanimiva primerjava odgovorov med moškimi in ženskami o uporabi različnih gesel. Ugotovili smo, da 3 različna gesla v povprečju uporablja več žensk kot moških, 4 različna gesla pa več moških kot žensk. Ostala različna gesla so v povprečju uporabljena približno enako.

V3: Ali je vaše geslo za Facebook, e-pošto, e-bančništvo, spletne strani, socialno omrežje:

a) **po navadi krajše**
b) **enako dolgo kot vedno**
c) **po navadi daljše**
d) **ne uporabljam**

Z razvojem tehnologije in interneta se je drastično povečala uporaba interneta in s tem tudi spletnih storitev, kot so socialna omrežja, e-pošta, e-bančništvo razne spletne strani

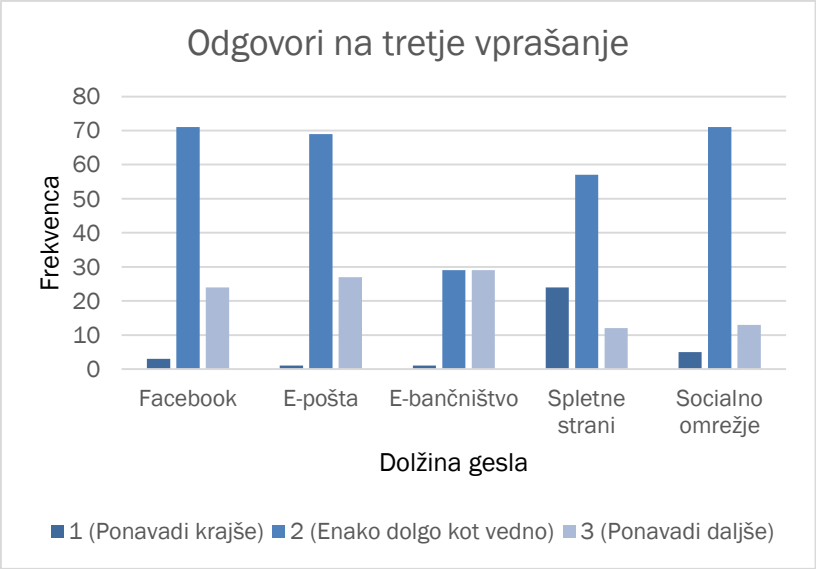
ipd. Še vedno menimo, da nekateri uporabniki niso ozaveščeni o varnosti svojih gesel, ker izbirajo krajša in enaka gesla za vse storitve, saj si je eno geslo najlažje zapomniti.

Tabela 12: Prikaz odgovorov na tretje vprašanje

V3	**Ali je vaše geslo za:**		
	Odgovori	Frekvenca	Odstotek
V3a	Facebook		
	1 (Po navadi krajše)	3	3,1 %
	2 (Enako dolgo kot vedno)	71	72,4 %
	3 (Po navadi daljše)	24	24,5 %
Veljavni	Skupaj	98	100 %
V3b	e-pošto		
	1 (Po navadi krajše)	1	1 %
	2 (Enako dolgo kot vedno)	69	71,2 %
	3 (Po navadi daljše)	27	27,8 %
Veljavni	Skupaj	97	100 %
V3c	e-bančništvo		
	1 (Po navadi krajše)	1	1,7 %
	2 (Enako dolgo kot vedno)	29	49,15 %
	3 (Po navadi daljše)	29	49,15 %
Veljavni	Skupaj	59	100 %
V3d	spletne strani		
	1 (Po navadi krajše)	24	25,8 %
	2 (Enako dolgo kot vedno)	57	61,3 %
	3 (Po navadi daljše)	12	12,9 %
Veljavni	Skupaj	93	100 %
V3e	socialno omrežje		
	1 (Po navadi krajše)	5	5,6 %
	2 (Enako dolgo kot vedno)	71	79,8 %
	3 (Po navadi daljše)	13	14,6 %
Veljavni	Skupaj	89	100 %

Vir: Lasten

Grafikon 5: Grafični prikaz odgovorov na tretje vprašanje



Vir: Lasten, tabela 12

Tretje vprašanje nam poda vpogled v dolžino gesel za Facebook, e-pošto, e-bančništvo, spletne strani in socialna omrežja. Facebook sicer spada med socialna omrežja, vendar pa smo ga zaradi, po mojem mnenju, pogostejše uporabe med študenti, obravnavali posebej. Na vprašanje je odgovorilo 98 študentov. V večini primerov imajo študentje za Facebook enako dolgo geslo kot po navadi. Tako je namreč odgovorilo kar 72,4 % (71) anketirancev. Daljše geslo kot po navadi pri Facebook-u uporablja 24,5 % (24) anketirancev. Zanimiv se nam zdi podatek, da le 2 % (2) anketirancev ne uporabljata Facebook-a. Podobno lahko vidimo pri e-pošti, kjer 71,2 % (69) anketirancev uporablja enako dolgo geslo kot vedno, ne uporablja pa je 3 % (3) anketirancev. Daljše geslo kot po navadi ima 27,8 % (27) anketirancev. Pri e-bančništvu smo ugotovili, da kar 41 % (41) študentov te storitve ne uporablja, 49,15 % (29) jih ima geslo navadno daljše geslo kot običajno, 49,15 % (29) enako dolgo kot običajno in 1,7 % (1) študentov ima krajše geslo. Pri naslednjem vprašanju nas je zanimala dolžina gesel, ki jih uporabljajo študentje za dostop do spletnih strani, torej do različnih spletnih forumov, spletnih trgovin, spletnih iger, aplikacij in podobno. Največ študentov, 61,3 % (57), ima geslo enako dolgo kot po navadi, 25,8 % (24) krajše in 12,9 % (12) daljše geslo kot po navadi. Pri ostalih socialnih omrežjih, kot so Twitter, Myspace, Instagram in drugi, uporablja 79,8 % (71) študentov enako dolgo geslo, 5,6 % (5) krajše in 14,6 % (13) daljše geslo kot po navadi. Ostalih socialnih omrežij ne uporablja 11 % (11) študentov.

V4: Kako pogosto v geslu ali za dele gesla uporabite:

a. **različne datume**
b. **imena ljudi (prijatelji, sorodniki, partner …)**
c. **vam znana druga imena (hišni ljubljenčki, priljubljeni pevci, igralci, kraji …)**
d. **druge besede, ki so del jezika (iz slovarja)**

Šibka gesla so gesla, ki napadalcem dajejo možnost za hiter dostop do vaših podatkov. Z uporabo različnih datumov, imen ljudi itd. pa napadalcu to omogočimo. Menimo, da prav uporaba osebnih podatkov v geslu omogoči lažji vdor potencialnemu napadalcu.

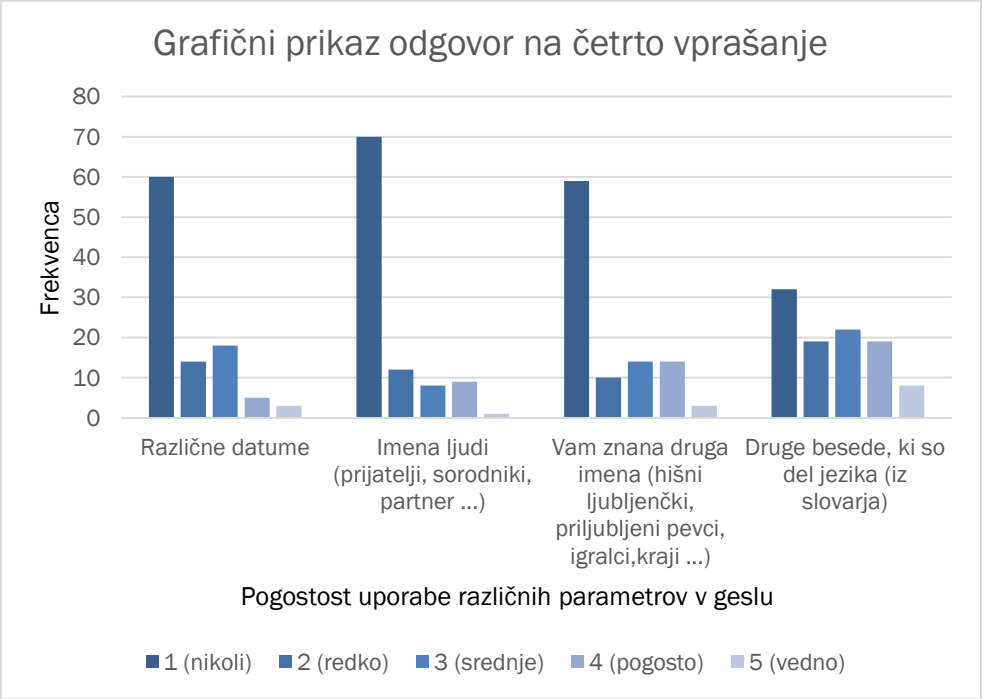
Tabela 13: Prikaz odgovorov na četrto vprašanje

V4			
	Odgovori	Frekvenca	Odstotek
V4a	Različne datume		
	1 (nikoli)	60	60 %
	2 (redko)	14	14 %
	3 (srednje)	18	18 %
	4 (pogosto)	5	5 %
	5 (vedno)	3	3 %
Veljavni	Skupaj	100	100 %
V4b	Imena ljudi (prijatelji, sorodniki, partner ...)		
	1 (nikoli)	70	70 %
	2 (redko)	12	12 %
	3 (srednje)	8	8 %
	4 (pogosto)	9	9 %
	5 (vedno)	1	1 %
Veljavni	Skupaj	100	100 %
Q4c	Vam znana druga imena (hišni ljubljenčki, priljubljeni pevci, igralci,kraji ...)		
	1 (nikoli)	59	59 %
	2 (redko)	10	10 %
	3 (srednje)	14	14 %
	4 (pogosto)	14	14 %
	5 (vedno)	3	3 %
Veljavni	Skupaj	100	100 %

V4d	Druge besede, ki so del jezika (iz slovarja)		
	1 (nikoli)	32	32 %
	2 (redko)	19	19 %
	3 (srednje)	22	22 %
	4 (pogosto)	19	19 %
	5 (vedno)	8	8 %
Veljavni	Skupaj	100	100 %

Vir: Lasten

Grafikon 6: Grafični prikaz odgovorov na četrto vprašanje



Vir: Lasten, tabela 13

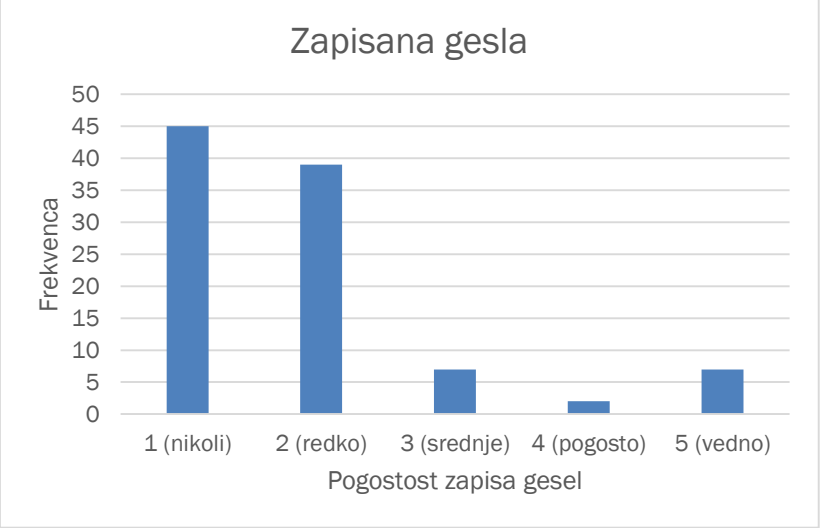
Ker veliko ljudi v svojih geslih uporablja različna znana imena prijateljev, hišnih ljubljenčkov in tudi datume, smo se na to tematiko osredotočili pri četrtem vprašanju. Izvedeli smo, da zelo malo študentov uporablja različne datume v svojih geslih, in sicer 60 % (60) študentov nikoli ne uporabi datumov, 14 % (14) redko in 5 % (5) pogosto. Datume vedno uporabljajo le trije študenti. Prav tako 70 % (70) študentov nikoli ne uporabi imen prijateljev, sorodnikov, partnerjev v svojem geslu ter 12 % (12) redko. Pogosto jih uporablja 9 % (9) študentov in vedno 1 % (1). Enako lahko vidimo tudi pri

uporabi drugih znanih imen v geslu, kot so imena domačih živali, pevcev, igralcev in podobno. 59 % (59) anketirancev teh podatkov nikoli ne uporabi v svojih geslih, 10 % (10) jih uporabi le redko, 14 % (14) pogosto in 3 % (3) vedno. Druge besede, ki so del jezika iz slovarja nikoli ne uporabi 32 % (32) anketirancev, redko 19 % (19), pogosto 19 % (19) in vedno 8 % (8). Gesla, ki so sestavljena iz besed iz slovarja so nevarna, saj potencialni hekerji napadejo tudi s pomočjo slovarja.

V5: Kako pogosto si zapišete geslo?

Timothy B. Lee (Vox, 2014) meni, da je zapisovanje gesel na list bolj varno kot uporabljanje različnih programov za shranjevanje gesel, saj v list ne more vdreti noben, po drugi strani pa omenja slabosti, kot so izguba ali kraja. Menimo, da gesla v nobenem primeru ni dobro zapisati zaradi razlogov, omenjenih zgoraj. Če geslo pozabimo, lahko enostavno zahtevamo novo geslo in si ga poljubno izberemo, pri tem pa upoštevamo vse varnostne smernice za močno geslo. Lahko si pomagamo tudi s »password strenght« metri in tako oblikujemo geslo, ki bo hkrati zapomnljivo in močno.

Grafikon 7: Grafični prikaz odgovorov na peto vprašanje



Vir: Lasten

Grafikon 8: Grafični prikaz odgovorov na peto vprašanje moški/ženske

Vir: Lasten

Pri petem vprašanju smo ugotovili, da si gesla nikoli ne zapiše 45 % (45) anketirancev, redko si ga zapiše 39 % (39), vedno pa 7 % (7) anketirancev. Vidimo tudi primerjavo med moškimi in ženskami. Moški si v povprečju manjkrat zapišejo gesla kot ženske. Nikoli si gesla ne zapiše 68 % (25) moških in 32 % (20) žensk.

V6: Če si geslo zapišete, kam in kje ga hranite?

To je bilo vprašanje odprtega tipa. Nanj so lahko študentje odgovorili poljubno. Nekateri najpogostejši odgovori so omenjeni v diskusiji.

V7: Kako pogosto svoje geslo poveste še komu? (sošolcu/ki, prijatelju, sorodniku ipd.)

Več ko je ljudi, ki poznajo naša gesla, manj varni smo pri uporabi spleta. Gesla so namenjena temu, da zagotavljajo varnost in zasebnost pri različnih storitvah. Menimo, da gesla ne smemo deliti z nikomer, saj s tem zmanjšamo varnost podatkov in verodostojnost uporabnika.

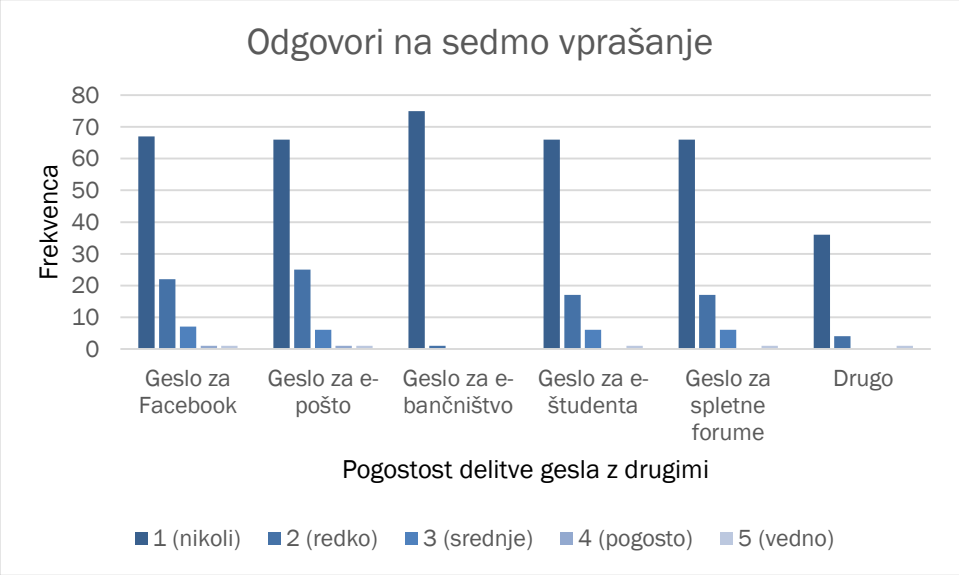
Tabela 14: Prikaz odgovorov na sedmo vprašanje

V7			
	Odgovori	Frekvenca	Odstotek
V7a	Geslo za Facebook		
	1 (nikoli)	67	68,5 %
	2 (redko)	22	22,4 %
	3 (srednje)	7	7,1 %
	4 (pogosto)	1	1 %
	5 (vedno)	1	1 %
Veljavni	Skupaj	98	100 %
V7b	Geslo za e-pošto		
	1 (nikoli)	66	66,7 %
	2 (redko)	25	25,3 %
	3 (srednje)	6	6 %
	4 (pogosto)	1	1 %
	5 (vedno)	1	1 %
Veljavni	Skupaj	99	100 %
V7c	Geslo za e-bančništvo		
	1 (nikoli)	75	98,7 %
	2 (redko)	1	1,3 %
	3 (srednje)	0	0 %
	4 (pogosto)	0	0 %
	5 (vedno)	0	0 %
Veljavni	Skupaj	76	100 %
V7d	Geslo za e-študenta		
	1 (nikoli)	70	73, %
	2 (redko)	19	19,8 %
	3 (srednje)	5	5,2 %
	4 (pogosto)	1	1 %
	5 (vedno)	1	1 %
Veljavni	Skupaj	96	100 %
V7e	Geslo za spletne forume		
	1 (nikoli)	66	73,3 %
	2 (redko)	17	18,9 %
	3 (srednje)	6	6,7 %
	4 (pogosto)	0	0 %
	5 (vedno)	1	1,1 %
Veljavni	Skupaj	90	100 %
V7f	Drugo (dopiši):		
	1 (nikoli)	36	87,8 %
	2 (redko)	4	9,8 %
	3 (srednje)	0	0 %

	4 (pogosto)	0	0 %
	5 (vedno)	1	2,4 %
Veljavni	Skupaj	41	100 %

Vir: Lasten

Grafikon 9: Grafični prikaz odgovorov na sedmo vprašanje



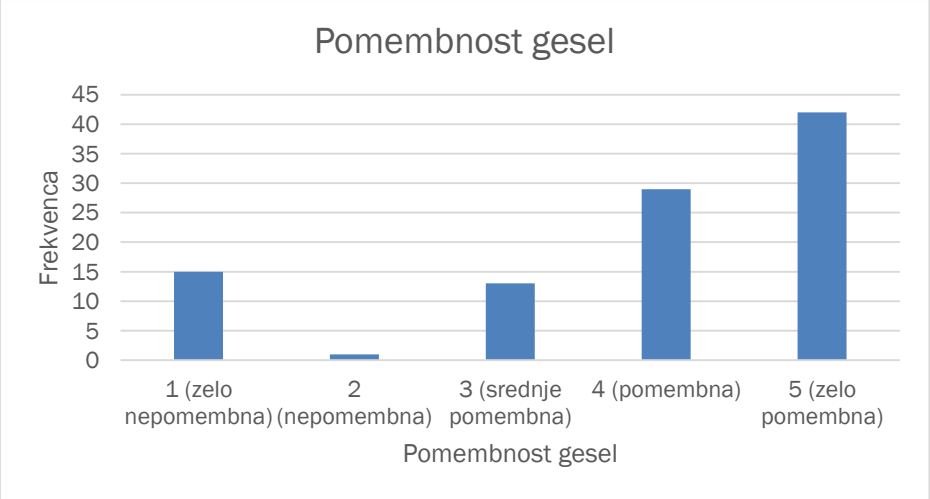
Vir: Lasten, tabela 14

Pri sedmem vprašanju smo želeli izvedeti, kako pogosto študentje svoje geslo delijo z drugimi, npr. sošolci, prijatelji, sorodniki, partnerji in drugimi. Več kot je ljudi, ki poznajo naša gesla, manj varni smo pri uporabi spleta. Na prvo podvprašanje je odgovorilo 98 študentov. Geslo za dostop do Facebooka nikoli ne deli z drugimi 68,5 % (67) anketirancev, redko jih deli 22,4 % (22), pogosto 1 % (1) in vedno tudi 1 % (1). Podobno situacijo imamo pri e-pošti, kjer jih izmed 99 anketiranih, 66,7 % (66), nikoli ne deli svojega gesla z drugimi, redko 25,3 % (25), pogosto 1 % (1) in vedno tudi 1 % (1). Zanimiv se nam zdi podatek za e-bančništvo, kjer izmed 76 anketiranih, ki ga uporablja, gesla nikoli ne delijo z drugimi. Teh je kar 98,7 % (75), z drugimi pa geslo za e-bančništvo redko deli 1,3 % (1) študentov, pogosto in vedno pa nihče. Četrto podvprašanje je izpolnilo 96 študentov. Gesla za dostop do e-študenta nikoli ne deli z drugimi 73 % (70) anketiranih, redko ga deli 19,8 % (19) anketiranih, pogosto 1 % (1) in vedno 1 % (1). Peto podvprašanje, ki se nanaša na spletne forume, je rešilo 90 študentov. Gesla za spletne forume nikoli ne deli z drugimi 73,3 % (66) anketirancev, redko 18,9 % (17), pogosto 0 % (0) in vedno 1,1 % (1) anketiranih. Pri tem vprašanju

smo postavili tudi podvprašanje, ki je bilo odprtega tipa. Anketirani so lahko dopisali še druge možnosti, pri katerih uporabljajo geslo in ga morebiti delijo z drugimi. Dobili smo različne odgovore, in sicer 87,8 % (36) anketiranih, ki uporabljajo gesla za dostop do računalniških iger, vstop v računalnik ipd., nikoli ne deli svojega gesla z drugimi. Nekateri na to podvprašanje niso odgovorili ali pa so napisali, da ne uporabljajo ostalih storitev.

V8: Kako pomembna se vam zdijo varna gesla?

Grafikon 10: Grafični prikaz odgovorov za pomembnost varnih gesel



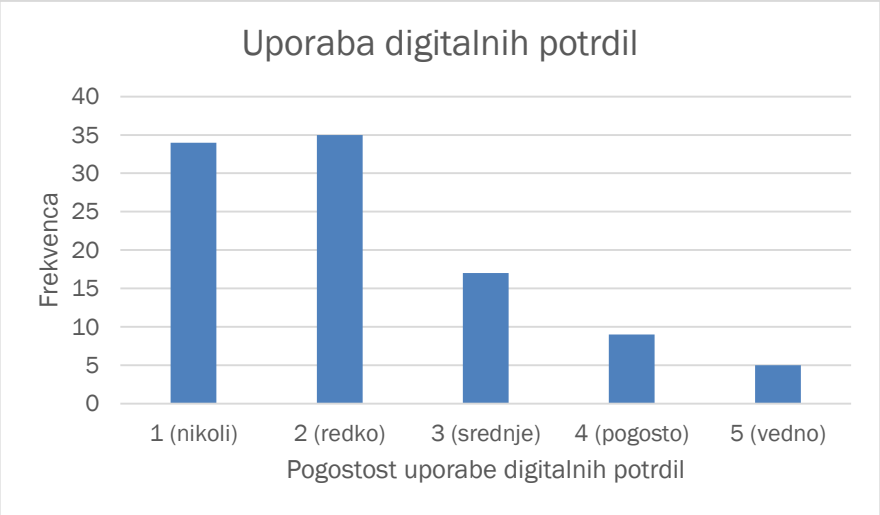
Vir: Lasten

Pri tem vprašanju smo želeli izvedeti, kako pomembna se študentom Univerze v Ljubljani zdijo varna gesla. Izmed 100 anketiranih študentov jih 15 % (15) meni, da so varna gesla zelo nepomembna, 1 % (1) meni, da so nepomembna. Srednje pomembna se zdijo varna gesla 13 % (13) anketiranim, pomembna 29 % (29) in zelo pomembna 42 % (42) anketiranim.

V9: Ali uporabljate digitalna potrdila?

Sodobna družba teži k uporabi digitalnih potrdil, s pomočjo katerih lahko dostopamo do različnih storitev (e-uprava, e-davki, e-dohodnina, e-VŠ idr.). Menimo, da si s tem olajšamo delo, prihranimo čas in vse storimo prek računalnika.

Grafikon 11: Prikaz odgovorov glede uporabe digitalnih potrdil



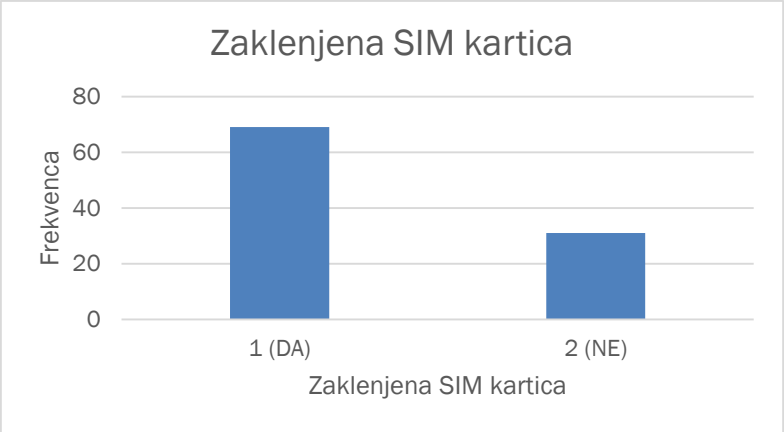
Vir: Lasten

Izvedeti smo želeli, kako pogosto študentje uporabljajo digitalna potrdila. Na vprašanje je odgovorilo 100 anketiranih študentov. Nikoli jih ne uporablja 34 % (34) študentov, redko 35 % (35), srednje 17 % (17), pogosto 9 % (9) in vedno le 5 % (5) anketiranih.

V10: Ali ima vaš telefon zaklenjeno SIM kartico?

Tako zaklenjena SIM kartica kot tudi zaklenjen telefon predstavljata oviro potencialnemu tatu. S tem preprečimo dostop do osebnih podatkov.

Grafikon 12: Grafični prikaz odgovorov za zaklepanje SIM kartice



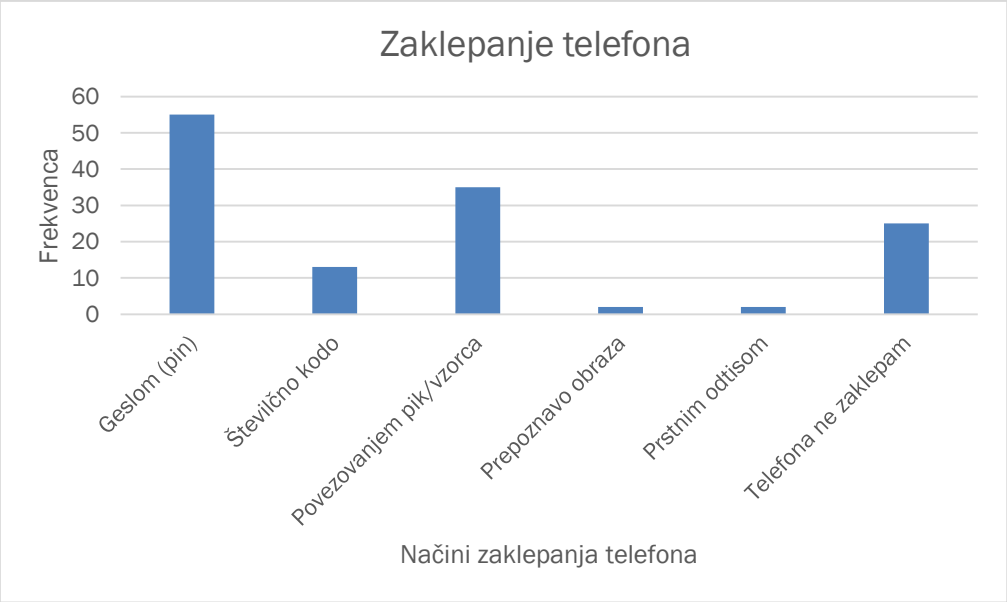
Vir: Lasten

Ugotavljali smo tudi varnost pri uporabi mobilnih telefonov, kjer je pomembno, da imamo zaklenjeno tako samo SIM kartico kot tudi telefon. Rezultati ankete so nam pokazali, da nimajo vsi študenti zaklenjene SIM kartice, saj jo ima izmed 100 anketiranih zaklenjeno 69 % (69) anketiranih.

V11: Ali je vaš telefon zaklenjen s/z:

a. **geslom (PIN)**
b. **številčno kodo**
c. **povezovanjem pik/vzorca**
d. **prepoznavo obraza**
e. **prstnim odtisom**
f. **telefona ne zaklepam**

Grafikon 13: Grafični prikaz odgovorov za zaklepanje telefona

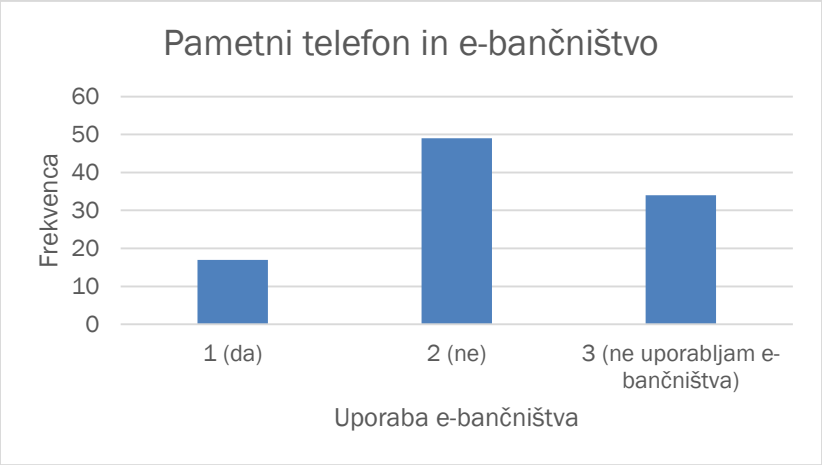


Vir: Lasten

Na enajsto vprašanje je prav tako odgovorilo 100 anketiranih. Anketa je pokazala, da samega telefona ne zaklepa 25 % (25) anketiranih. Ostali pa telefon zaklepajo najpogosteje z geslom PIN, sledi povezovanje pik ali vzorca, številčna koda, prepoznava obraza in tudi prstni odtis.

V12: Ali bi imeli na svojem pametnem telefonu preko gesla dostop do e-banke?

Grafikon 14: Grafični prikaz odgovorov za dostop prek pametnih telefonov

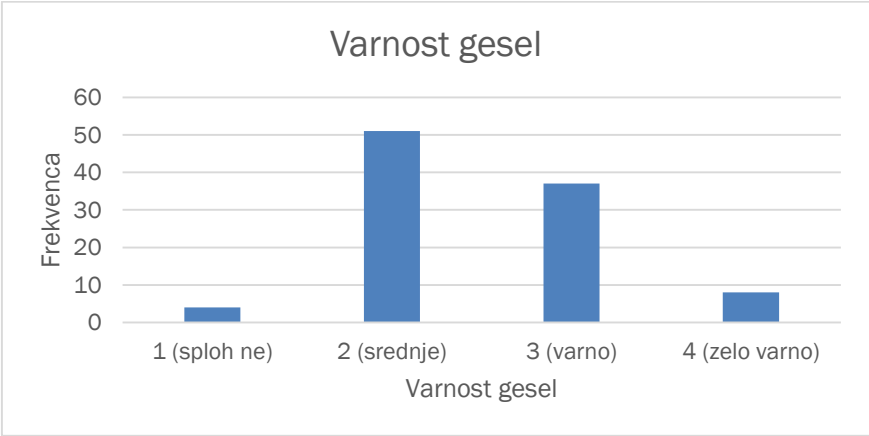


Vir: Lasten

V tem sklopu nas je zanimalo tudi, ali bi na svojem pametnem telefonu uporabljali dostop do e-banke. Uporabljalo bi ga le 17 % (17) anketiranih, 34 % (34) anketiranih pa je odgovorilo, da sploh ne uporablja e-bančništva.

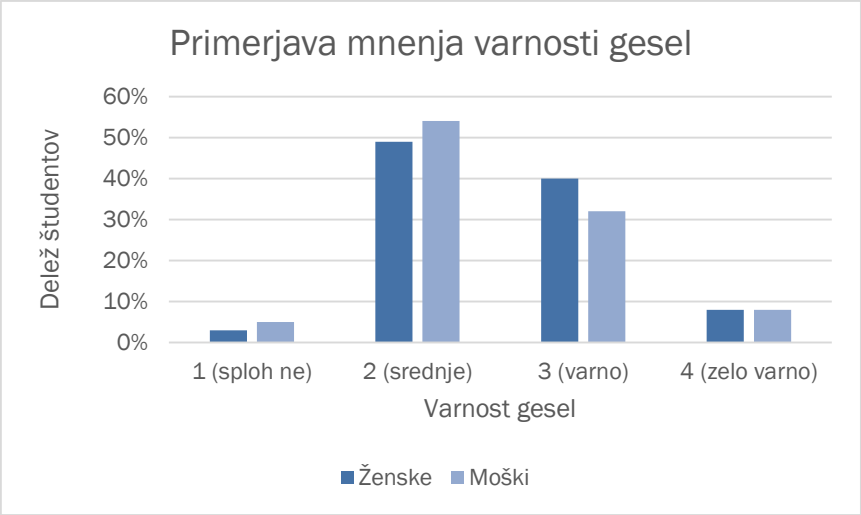
V13: Ali menite, da so vaša gesla varna?

Grafikon 15: Grafični prikaz odgovorov glede mnenja o varnosti gesel



Vir: Lasten

Grafikon 16: Grafični prikaz odgovorov glede mnenja o varnosti gesel – moški/ženske



Vir: Lasten

V tem vprašanju smo želeli zopet izvedeti osebno mnenje glede varnosti njihovih gesel. Izvedeli smo, da se 4 % (4) anketiranim študentom gesla ne zdijo varna, 51 % (51) srednje varna, 37 % (37) varna in le 8 % (8) jih meni, da imajo zelo varna gesla. Iz grafa vidimo, da se mnenja o varnosti gesel med moškimi in ženskami ne razlikujejo.

5.3 DISKUSIJA IN KOMENTARJI

5.3.1 DISKUSIJA IN KOMENTARJI ANALIZE GESEL

Namen analize gesel študentov Fakultete za upravo je bil, da s pomočjo analize ugotovimo, kakšna gesla uporabljajo naši študenti. Analiza je bila opravljena na podlagi osebnih podatkov študentov, kot so ime, priimek, datum rojstva, ulica stalnega prebivališča ter geslo. Pri prvi analizi smo ugotavljali dolžino in samo sestavo gesel naših študentov. Vsa analizirana gesla so vsebovala 8 znakov, kar se nam zdi odlično, saj študentje uporabljajo ustrezno dolžino gesel, ki so po navadi tudi varnejša, saj ob morebitnem vdoru z različnimi tehnikami, kot so napad z grobo silo, napad s slovarjem, mavrične tabele in podobno, zahtevajo dalj časa za razbitje gesla. Analiza je pokazala, da so si gesla zelo različna, nekatera vsebujejo samo številke, samo črke, kombinacije črk in številk, kombinacije črk in posebnih znakov ter kombinacije številk in posebnih znakov. Zanimiv se nam zdi podatek, da nobeno izmed analiziranih gesel ne vsebuje samo posebnih znakov ter da je samo 20 takih gesel, ki hkrati vsebujejo črke, številke in posebne znake. Menimo, da je vzrok v tako majhnem številu takšnih gesel v tem, da si je takšno geslo težje zapomniti, kot če geslo vsebuje le črke in številke. S tem ko posebnih znakov (poznamo 24 posebnih znakov) ne uporabimo v našem geslu, potencialnim napadalcem omogočimo lažje delo pri vdoru, saj se zmanjša izbor vseh znakov in s tem

kombinacij. Prav tako je podobno pri številkah, saj so tisti, ki jih ne uporabljajo, manj varni pri zaščiti svojih podatkov, ker imajo potencialni napadalci manj možnih kombinacij za ugotovitev gesla. Ugotovili smo, da v povprečju 25 % dolžine gesla študentov Fakultete za upravo predstavljajo številke, kar je seveda dobro, saj s tem onemogočimo potencialnim napadalcem lahek vstop v e-študenta. Več kot je različnih številk, črk in posebnih znakov, težje in dlje traja postopek vdora. Pri analizi sestave gesla smo ugotovili, da na naši fakulteti ni bilo mogoče za svoje geslo uporabiti malih črk. Študentje tako lahko uporabijo samo velike črke, številke in posebne znake. Ugotovili smo, da so velike črke posledica pretvorbe malih črk, saj jih je sistem ob vpisu gesla avtomatsko pretvoril v velike črke in tako tudi shranil. Smo pa izvedeli, da tega ni več, saj je Fakulteta za upravo ugotovila neustrezno stopnjo varnosti, zato sistem sedaj omogoča študentom gesla daljših dolžin od 8, velike in male črke ter posebne znake. Prav tako Fakulteta za upravo ne shranjuje več gesel, temveč samo povzetke (HASHe) gesel, ki so izračunani s pomočjo matematičnega algoritma SHA1. Ko študent določi svoje geslo, računalnik generira naključno dolgo zaporedje znakov, ki ga shrani poleg študentovega gesla v bazo, oboje združi in s pomočjo omenjenega algoritma izračuna povzetek, ki se shrani. S tem niti študent niti napadalci ne morejo priti do gesla, ker ga Fakulteta za upravo nima. Menimo, da se je lahko varno geslo tvorilo tudi pred spremembo sistema, saj lahko tudi z velikimi črkami, številkami in posebnimi znaki oblikujemo varno geslo. Izbira gesla je odvisna od posameznika, kakšne znake bo izbral in ali se mu zdi varnost pri uporabi e-študenta pomembna. Menimo, da bi na naši fakulteti pri izbiri gesla morali uporabiti pogoje, ki bi zahtevali tako uporabo malih, velikih črk, številk, kot tudi posebnih znakov. Če pa to ni možno iz kakšnih tehničnih razlogov, bi ga ob izbiri gesla sistem samodejno preusmeril na katero izmed aplikacij za merjenje varnosti gesel, ki so na voljo na spletu. S tem bi omogočili varnost na najvišji ravni, saj je 8-znakovna gesla, ki vsebujejo različne znake, zelo težko ugotoviti.

Sledile so analize posameznih parametrov, kot so ujemanje gesla z deli imena, priimka, ulice stalnega prebivališča ter datumom rojstva. Ugotavljali smo ujemanje z različnimi dolžinami omenjenih parametrov. Menimo, da za svoje geslo ne izbiramo svojih osebnih podatkov, saj potencialni napadalci najprej preverijo ujemanje na podlagi le-teh. Največ študentov uporablja zaporedje znakov dolžine 3, ki se ujema z imenom. Menimo, da je razlog v tem, da imajo nekateri študenti kratko ime, uporabljajo krajše vzdevke svojih imen ali krajše oblike svojega imena. Pri tem velja opozoriti, da je ujemanje lahko tudi naključno. Določeno zaporedje treh črk se lahko pojavi v različnih imenih, besedah in ni povezano z geslom. Kot primer lahko navedemo ime osebe Vladimir, ki za svoje geslo uporablja ime premirje. Ujemanje je v tem primeru naključno. Zaskrbljujoč se nam zdi podatek, da kar 18,38 % (1140) študentov uporablja v svojem geslu zaporedje znakov dolžine 5, ki se pojavi v imenu. Večina slovenskih imen je namreč sestavljena iz 4 do 6 črk. Pri takšnih osebah je omogočen hitrejši vdor kot pri ostalih, saj kot sem omenil že prej, potencialni napadalci preverijo vse v povezavi z osebnimi podatki in na ta način poizkušajo vstopiti v sistem. Na podlagi podatka, da 75,58 % (4689) študentov v svojem geslu ne uporablja imen, so glede varnosti gesel naši študenti kar dobro ozaveščeni.

Z naslednjo analizo smo ugotavljali ujemanje gesel s priimki dolžine 3 in ugotovili, da študentje za svoja gesla bolj uporabljajo dele imena kot pa dele priimka.

V naslednji analizi smo ugotavljali ujemanje z deli ulice dolžine 3, 4 in 5.

Sledila je analiza gesel naslednjega parametra, in sicer ujemanje gesla dolžine 3, 4 in 5 z deli kraja rojstva študenta. S to analizo smo ugotovili, da študentje svoj kraj rojstva redko uporabljajo v svojem geslu.

Z analizo gesel na podlagi ujemanja z datumom rojstva smo ugotovili, koliko ljudi v svojem geslu uporablja dan, mesec, letnico ali zadnji dve številki letnice rojstva. Nekaj gesel je vsebovalo dan rojstva in mesec rojstva. Vendar pa menimo, da gre pri tem lahko tudi za naključje. Kot primer lahko navedem geslo, ki vsebuje številke 12345678, ki vsebuje sicer številko 12, vendar je študent ni uporabil kot dan ali mesec svojega rojstva. Pričakovano je zato več študentov uporabilo zadnji dve številki letnice rojstva v svojem geslu. Zanimivo se nam zdi, da je 2,82 % (175) študentov uporabilo v geslu celotno letnico svojega rojstva. Tukaj se nam zdi naključje malo verjetno, saj smo analizirali 4 mesta. Tudi tukaj lahko zaznamo dobro ozaveščenost naših študentov.

Za zadnjo analizo smo uporabili najpogostejša gesla v Sloveniji in svetu, ki smo jih našli v različnih raziskavah. Naključno smo izbrali nekatera izmed najpogostejših gesel. Gesla so morala biti obvezno 8-znakovna. Izbrali smo naslednja gesla in ugotovili, koliko študentov jih uporablja:

- password;
- 12345678;
- qwertzui;
- ljubezen;
- trustno1;
- xxxxxxxx;
- 11111111.

Izmed najpogostejših gesel, ki smo jih izbrali, je vsaj 1 študent, ki geslo uporablja. Največ študentov uporablja geslo 1234678, sledijo mu geslo ljubezen, 11111111, trustno1, password, qwertzui ter xxxxxxxx. Ugotovili smo, da je skupno 177 študentov, ki uporabljajo izbrana najpogostejša gesla. Menimo, da bi bila številka še višja, če bi izbral še več najpogostejših gesel dolžine 8. Študentje, ki uporabljajo ta gesla, so premalo ozaveščeni o varnosti gesel, saj uporabljajo gesla, s katerimi ogrožajo varnost svojih podatkov. Seznam najpogostejših gesel lahko dobi vsak, ki uporablja internet, zato ta gesla nikakor ne bi smeli uporabljati za nobeno storitev.

5.3.2 DISKUSIJA IN KOMENTARJI ANKETE

Ugotovili smo, da ima večina študentov primerno dolžino gesel, vendar pa pri tem velja opozoriti, da ustrezno število znakov še ne pomeni ustrezne varnosti gesla. Kot primer lahko navedemo dolžino gesla z 8 znaki, in sicer 12345678, kar je ustrezna dolžina,

vendar pa to geslo spada med najpogostejša gesla, zato geslo ni varno. Študentje za različne storitve uporabljajo v večini tudi različna gesla. Število različnih gesel je odvisno tudi od števila storitev, ki jih uporabljajo. Uporaba različnih gesel je priporočljiva, saj se s tem lahko zaščitijo pred morebitnimi krajami podatkov. Eden izmed anketiranih je navedel, da uporablja kar 28 različnih gesel. Tega bi lahko sicer pri analizi izločil, saj obstaja možnost, da se je nekdo zmotil pri pisanju odgovora, vendar smo ga pustili, saj lahko uporablja toliko gesel kot ima storitev. Je sicer malo verjetno, a možno, če uporablja program, ki shranjuje gesla, kot je npr. KeePass. Ugotovili smo tudi, da študentje uporabljajo za socialna omrežja, različne spletne strani in tudi e-pošto v večini enako dolga gesla kot običajno. Zanimiv se nam zdi podatek, da v svetu, ko večina storitev temelji na sodobni tehnologiji in elektronskem poslovanju, kar 41 anketiranih študentov ne uporablja e-bančništva. Uporaba različnih znanih imen prijateljev, hišnih ljubljenčkov in tudi datumov v geslih je pogosta in tudi neustrezna, saj s tem zmanjšamo varnost svojih gesel. Potencialni napadalec lahko na podlagi teh pridobljenih podatkov ugotovi geslo in vdre. Izvedeli smo, da zelo malo študentov uporablja različne datume in imena v svojih geslih. Iz tega lahko sklepamo, da se študenti zavedajo nevarnosti uporabe svojih podatkov v geslu. Prav tako uporaba besed iz slovarja v svojem geslu vpliva na varnost gesla. Nekaj študentov drugih besed, ki so del jezika iz slovarja, ne uporablja, zato menimo, da imajo v svojem geslu različne posebne znake s kombinacijo številk in podobno. Tako se zavedajo pomembnosti, da geslo vsebuje tako črke, številke kot tudi ostale posebne znake. Zapisovanje gesel je lahko nevarno, saj zapis lahko kaj hitro pride v napačne roke. Prav tako je pomembno, komu zaupamo in kje imamo te pomembne podatke zapisane. V anketi smo želeli izvedeti, ali so študentje pripravljeni deliti informacijo o tem, kam si zapišejo geslo. Na to vprašanje so lahko odgovorili ali pa ne. Sami odgovorov seveda nismo pričakovali, je pa na to vprašanje odgovorilo kar 37 % študentov. Večina odgovorov je bila, da gesla hranijo zapisana v svojih rokovnikih, listkih, zvezkih, hranijo pa jih v predalih, računalnikih in podobno. Pri tem vprašanju smo dobili tudi zanimiv odgovor: nekdo je namreč napisal, da te zaupne informacije ne bo delil z nami. Iz tega lahko sklepamo, da se zaveda, kako pomembno je, da informacij ne izdajamo neznancem. Svoja osebna gesla naj ne bi delili z drugimi, zato smo se dotaknili tudi te tematike. Zanimalo nas je, kako pogosto študentje delijo svoje geslo za različne storitve z drugimi. Večina anketiranih svojih gesel ne deli z drugimi, kar se nam zdi v redu. Pri tem vprašanju smo postavili tudi podvprašanje odprtega tipa. Anketirani so lahko dopisali še druge možnosti, pri katerih uporabljajo geslo in ga morebiti delijo z drugimi. Dobili smo različne odgovore. Večina anketiranih, ki so odgovorili na to vprašanje in uporabljajo gesla za dostop do računalniških iger, vstop v računalnik ipd., nikoli ne deli svojega gesla z drugimi. Nekateri na to podvprašanje niso odgovorili ali pa so napisali, da ne uporabljajo ostalih storitev. Pomembno je, da se ljudje zavedajo pomembnosti uporabe varnih gesel. Ugotovili smo, da se večini anketiranih študentov varna gesla zdijo pomembna. Ker sodobna družba vedno bolj teži k uporabi digitalnih potrdil, smo želeli izvedeti, kako pogosto jih študentje uporabljajo. Večina študentov jih uporablja nikoli ali pa redko. Iz tega lahko sklepamo, da so študenti premalo seznanjeni z uporabo digitalnih potrdil. Ugotavljali smo tudi varnost pri uporabi mobilnih telefonov. Večina anketiranih zaklepa tako svoje SIM kartice kot tudi telefone, kar je dobro, saj so kraje mobilnih

telefonov danes zelo pogoste. S krajo pa lahko izgubimo mnogo podatkov, ki se nahajajo shranjeni v telefonu.

V tem sklopu nas je tudi zanimalo, ali bi na svojem pametnem telefonu uporabljali dostop do e-banke. Ugotovili smo, da študentje ne želijo ali pa ne uporabljajo e-bančništva na svojih pametnih telefonih. Navsezadnje pa nas je zanimalo tudi njihovo osebno mnenje glede varnosti njihovih osebnih gesel. Izvedeli smo, da se večini študentov zdijo njihova gesla precej varna.

6 ZAKLJUČEK

V uvodu sem si zastavil dve hipotezi, in sicer:

- H1: Študentje na Fakulteti za upravo uporabljajo za svoj dostop do e-študenta, kjer so zabeleženi vsi njihovi pomembni in zaupni osebni podatki, varna gesla.
- H2: Študentje Univerze v Ljubljani so premalo ozaveščeni o sami uporabi, pomembnosti in varnosti gesel.

Tekom pisanja diplomskega dela sem prišel do zaključka, da študentje na Fakulteti za upravo v večini nimajo varnih gesel. V nekaterih primerih se v geslu pojavljajo osebni podatki, kot so deli imena, priimka, kraja rojstva, ulice stalnega prebivališča in datum rojstva, vendar pa v večini primerov gesla teh podatkov ne vključujejo v večjih dolžinah zaporedij znakov, kar je sicer varno. Prav tako sama dolžina gesel na Fakulteti za upravo obvezno obsega 8 znakov, kar je v skladu s priporočili o varnosti gesel. Priporočila pa nam velevajo tudi, da naj gesla vsebujejo različne znake; tako črke, številke kot tudi ostale posebne znake. Te zahteve pa naši študentje na Fakulteti za upravo ne izpolnjujejo. Kar 3381 študentov v svojem geslu uporablja samo črke in 957 študentov samo številke. Srednje varna gesla se mi zdijo tista, ki vsebujejo številke in črke, teh je 1802. Najbolj varna gesla so tista, ki vsebujejo vse znake, teh je na Fakulteti za upravo zgolj 20. S tem sem svojo prvo hipotezo zavrgel.

Varnost gesel študentov na Fakulteti za upravo bi lahko povečali z uvedbo pogojev, ki predpisujejo, da geslo vsebuje različne znake, tako male črke, velike črke, številke kot tudi posebne znake in simbole. Obvezna dolžina bi morala biti 8 znakov. Vsak študent pa bi si moral varnost svojega gesla preveriti na merilcu moči gesla, ki pa bi moral presegati vsaj 85 %.

Z analizo ankete, ki sem jo opravil s študenti različnih fakultet Univerze v Ljubljani, sem prišel do zaključka, da so študentje kar dobro ozaveščeni o pomembnosti in varnosti gesel. Študentje namreč svojih gesel v večini primerov ne delijo z drugimi, uporabljajo zaščito tako pri različnih medijih in storitvah, kot so e-bančništvo, e-pošta, socialna omrežja, kot tudi na telefonskih napravah in računalnikih. Zlasti so previdni pri uporabi e-bančništva, kjer večina anketiranih ne deli svojega gesla z nikomer. Prav tako je povprečna dolžina gesel, ki jih uporabljajo 8,7, kar je ustrezna dolžina gesla. Za različne storitve v večini primerov uporabljajo različna gesla, kar je v skladu z varnostjo. Za te storitve uporabljajo v povprečju 4,2 različnih gesel. S to anketo sem zavrgel svojo drugo hipotezo.

Ozaveščenost študentov bi lahko tudi še izboljšali. Menimo, da bi bilo smiselno v šolstvu uvesti izobraževanja o varnih geslih, varni uporabi interneta in varstvu svojih podatkov na internetu. Prav tako menimo, da bi bilo potrebno bolj ozaveščati študente o smiselni uporabi digitalnih potrdil in drugih e-storitev.

V sodobnem svetu, kjer storitve vedno bolj temeljijo na uporabi IKT, je zelo pomembna uporaba varnih gesel, programov za zagotavljanje varnosti in drugih varnostnih mehanizmov. Ravno zato se mi zdi zelo pomembno poudarjanje in ozaveščanje vseh uporabnikov IKT, saj smo vsi lahko tarče potencialnih napadalcev, ki lahko povzročijo veliko škodo – tako uporabnikom kot tudi organizacijam.

LITERATURA IN VIRI

LITERATURA

- Dečman, Mitja. (2013). *E-uprava: Informacijsko-storitveni servis za uporabnike.* [PowerPoint predstavitev]. Informacijski sistemi v upravi. Fakulteta za upravo, Ljubljana.
- Dimic, Maja, Dobovšek, Bojan. (2012). *Kriminaliteta v informacijski družbi.* Ljubljana: Fakulteta za varnostne vede.
- Golčman, Nataša. (2008). *Varnost e-poslovanja v slovenskih podjetjih.* Diplomsko delo, Maribor: Ekonomsko-poslovna fakulteta.
- Gradišar, Miro, Resinovič, Gortan. (1998). *Informatika v organizaciji*. Kranj: Moderna organizacija.
- Gradišar, Miro. (2003). *Uvod v informatiko.* Ljubljana: Ekonomska fakulteta.
- Kavčič, Karin. (2011). *Javna uprava in civilna družba.* Diplomsko delo, Ljubljana: Fakulteta za upravo.
- Kotnik, Katarina. (2003). *Geografski informacijski sistem in njegova uporabnost na področju varstva pred naravnimi in drugimi nesrečami.* Diplomsko delo, Ljubljana: Fakulteta za družbene vede.
- Kovačič, Andrej, Vintar, Mirko. (1994). *Načrtovanje in gradnja informacijskih sistemov.* Ljubljana: DZS.
- Kričej, Dušan. (2002). *E-uprava na dlani*. Ljubljana: Pasadena.
- Pintarič, Uroš, Svete, Uroš. (2007). *Elektronsko upravljanje in poslovanje v službi uporabnika=e-governance and e-bussines at the service of customer.* Ljubljana: Fakulteta za družbene vede.
- Sriča, Velimir, Treven, Sonja, Pavlič, Mile. (1995). *Informacijski sistemi.* Ljubljana: Gospodarski vestnik.
- Toplišek, Janez. *Elektronsko poslovanje.* Ljubljana: Atlantis.
- Turban, Efarim. et.al. (2007). *Introduction to informatics systems: supporting and transforming business.* NJ: Hoboken.
- Verdonik, Ivan, Bratuša, Tomaž. (2005). *Hekerski vdori in zaščita.* Ljubljana: Pasadena.
- Vintar, Mirko, Grad, Janez. (2004). *E-uprava: Izbrane razvojne perspektive*. Ljubljana: Fakulteta za upravo.

VIRI

- Gibson, Steve. (2012). *GRC's Interactive Brute Force Password "Search Space" Calculator.* Privzeto 26. 8. 2014 iz: https://www.grc.com/haystack.htm

- Hölbl, Marko. (2007). *Gesla in napadi nanje*. Privzeto 4. 4. 2014 iz http://www.monitor.si/clanek/gesla-in-napadi-nanje/122762/
- Križanovski, Žan. *Kriptografija.* Privzeto 21. 8. 2014 iz: http://www.nauk.si/materials/6414/out/#state=1
- Lee, B. Thimoty. (2014). *The best defense against hackers is...paper?.* Privzeto 26. 8. 2014 iz: http://www.vox.com/2014/4/16/5614258/the-best-defense-against-hackers-writer-your-passwords-down-on-paper
- Lucas, Ivan. (2009). *Password recovery speeds.* Privzeto 23. 8. 2014 iz http://www.lockdown.co.uk/?pg=combi#Classes
- Marinšek, Damijan. *Informacijska varnostna politika javne uprave.* Privzeto 21.8. 2014 iz: http://uploadi.www.ris.org/editor/1264334858MARINSEK_Informacijska_varnostna_politika.pdf
- Mcgrath, Dylan. *ISuppli: Gear costs to derail Moore's Law in 2014.* Privzeto 26. 8. 2014 iz: http://www.eetimes.com/document.asp?doc_id=1171175
- Ministrstvo za javno upravo. (2010). *Priporočila informacijske varnostne politike javne uprave.* Privzeto 14. 7. 2014 iz: http://www.mpju.gov.si/fileadmin/mpju.gov.si/pageuploads/DIES/IVPJU_01.pdf
- Možina, Stane. et al. (2002). *Managment – nova znanja za uspeh.* Privzeto 15. 7. 2014 iz http://www2.arnes.si/~ssmbtrgov1/e-poslovanje/e-Poslovanje.pdf
- Služba Vlade RS za zakonodajo. (2013). *Pravno-informacijski sistem.* Privzeto 20. 7. 2014 iz: http://www.pisrs.si/Pis.web/cm?idStrani=vecOPis
- SplashData Inc. (2014). *"Password" unseated by "123456" on SplashData's annual "Worst Passwords" list.* Privzeto 18. 7. 2014 iz: http://splashdata.com/press/worstpasswords2013.htm
- (2004). Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP). *Uradni list Republike Slovenije,* 98/04. Privzeto 11. 4. 2014 iz: http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1973
- Žagar, Gorazd. *Informacijska varnost.* Privzeto 13. 5. 2014 iz: http://infosec.si/?p=169

PRILOGE

ANKETA

Q1 - Koliko znakov so v povprečju dolga vaša gesla?

Q2 - Približno koliko različnih gesel uporabljate za različne storitve na spletu? (npr. e-pošta, soc. omrežja, internetne strani, e-bančništvo) 0=Uporabljam isto geslo za vse storitve

Q3 - Ali je vaše geslo za:

	Po navadi krajše	Enako dolgo kot vedno	Po navadi daljše	ne uporabljam
Facebook	○	○	○	○
e-pošto	○	○	○	○
e-bančništvo	○	○	○	○
spletne strani	○	○	○	○
socialno omrežje	○	○	○	○

Q4 - Kako pogosto v geslu ali za dele gesla uporabite:

	nikoli	redko	srednje	pogosto	vedno
Različne datume	○	○	○	○	○
Imena ljudi (prijatelji, sorodniki, partner ...)	○	○	○	○	○
Vam znana druga imena (hišni ljubljenčki, priljubljeni pevci, igralci,kraji ...)	○	○	○	○	○

	nikoli	redko	srednje	pogosto	vedno
Druge besede, ki so del jezika (iz slovarja)	◯	◯	◯	◯	◯

Q5 - Kako pogosto si zapišete geslo?

◯ nikoli
◯ redko
◯ srednje
◯ pogosto
◯ vedno

Q6 - Če si geslo zapišete, kam in kje ga hranite?
odgovorite če želite

Q7 - Kako pogosto svoje geslo poveste še komu? (sošolcu/ki, prijatelju, sorodniku, ipd.)
če odgovora na Drugo (dopiši) ni = ne uporabljam

	nikoli	redko	srednje	pogosto	vedno	ne uporabljam
Geslo za Facebook	◯	◯	◯	◯	◯	◯
Geslo za e-pošto	◯	◯	◯	◯	◯	◯
Geslo za e-bančništvo	◯	◯	◯	◯	◯	◯
Geslo za e-študenta	◯	◯	◯	◯	◯	◯
Geslo za spletne forume	◯	◯	◯	◯	◯	◯
Drugo (dopiši):	◯	◯	◯	◯	◯	◯

Q8 – Kako pomembna se vam zdijo varna gesla?

◯ zelo nepomembna
◯ nepomembna
◯ srednje pomembna

○ pomembna
○ zelo pomembna

Q9 - Ali uporabljate digitalna potrdila?

○ nikoli
○ redko
○ srednje
○ pogosto
○ vedno

Q10 - Ali ima vaš telefon zaklenjeno SIM kartico?

○ DA
○ NE

Q11 - Ali bi imeli na svojem pametnem telefonu preko gesla dostop do e-banke?

○ da
○ ne
○ ne uporabljam e-bančništva

Q12 - Ali je vaš telefon zaklenjen s/z:
Možnih je več odgovorov

☐ geslom (PIN)
☐ številčno kodo
☐ povezovanjem pik/vzorca
☐ prepoznavo obraza
☐ prstnim odtisom
☐ telefona ne zaklepam

Q13 - Ali menite, da so vaša gesla varna?

○ sploh ne
○ srednje
○ varno
○ zelo varno

XSPOL - Spol:

○ Moški
○ Ženski