UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

Igor Lamberger

MODEL ZAŠČITE ELEKTRONSKIH PLAČILNIH SISTEMOV PRED ZLORABAMI

Doktorska disertacija

LJUBLJANA, 2011

Izjava o avtorstvu in objavi elektronske verzije doktorske disertacije in osebnih podatkov, vezanih na zaključek študija

Doktorand Igor Lamberger izjavljam, da sem avtor te doktorske disertacije in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovoljujem objavo doktorske disertacije na spletišču CEK-a.

Tiskana verzija doktorske disertacije je istovetna elektronski verziji, ki sem jo oddal v zbirko polnih besedil zaključnih del Ekonomske fakultete Univerze v Ljubljani.

Podpisani hkrati izjavljam, da dovolim objavo osebnih podatkov, vezanih na zaključek študija na spletnih straneh in v publikacijah Univerze v Ljubljani.

Ime in priimek doktoranda:	Igor Lamberger
Leto in kraj rojstva:	1967, Ptuj
Datum zagovora:	9. 12. 2011
Predsednik:	prof. dr. Tomaž Turk
Mentor:	prof. dr. Miro Gradišar
Somentor:	prof. dr. Samo Bobek
Član:	prof. dr. Andrej Kovačič

Ljubljana, 24. 11. 2011 Podpis doktoranda:

MODEL ZAŠČITE ELEKTRONSKIH PLAČILNIH SISTEMOV PRED ZLORABAMI

Povzetek

Elektronsko bančništvo je v zadnjih nekaj letih doseglo velik razmah in brez dvoma pomeni prihodnost plačilnega prometa na finančnih trgih. Zaradi velike količine finančnih sredstev, ki se preko sistemov elektronskega bančništva prelivajo med finančnimi institucijami in komitenti, so ti sistemi pod udarom storilcev različnih zlorab, goljufij in drugih kriminalnih dejanj. Kriminalna dejanja povzročajo škodo in zmanjšujejo tudi zaupanje komitentov v finančne institucije in storitve.

Za zaščito pred zlorabami elektronskega bančništva je potrebno celovito gledati na njegovo varnost in z naborom različnih varnostnih modelov preprečevati ali vsaj zmanjšati zlorabe na še zadovoljivo raven.

V nalogi smo preučili bančno poslovanje na področju izvajanja plačilnega prometa, njegovo informatizacijo in načine za doseganje zaščite in varnosti poslovanja na tem področju. Analizirali smo nepravilnosti in zlorabe, ki se na tem področju dogajajo in jih razvrstili po modusih izvedbe in skupnih značilnostih, da bi na osnovi teh ugotovitev lahko opredelili dejavnike, ki vplivajo na varnost elektronskega bančništva. Na osnovi proučevanja razmer na področju elektronskega bančništva in zlorab v bankah smo zasnovali smo celovit varnostni model za preprečevanje zlorab, v katerega smo vključili tako preventivne, kot tudi represivne dejavnike. Model smo testirali in ugotovili, da je za zagotavljanje varnosti potrebno pridobiti oceno tveganja informacijske varnosti. Proučili smo metode, ki so namenjene ocenjevanju informacijskega tveganja in na podlagi dobljenih rezultatov, in specifičnosti bančnega poslovanja, zasnovali novo metodo za ocenjevanje informacijskega tveganja v finančnih institucijah. Metodo smo testirali pri tistih, ki v bankah skrbijo za varnost informacijskih sistemov in z rezultati potrdili potrebo po novi metodi, ki je prilagojena specifičnostim bančnega poslovanja.

KLJUČNE BESEDE: elektronski plačilni sistemi, elektronsko bančništvo, finančna kriminaliteta, zlorabe, goljufije, banke

A MODEL OF ELECTRONIC SYSTEM PROTECTION AGAINST MISUSE

Summary

Electronic banking has recently expanded substantially; as such it is undoubtedly a future issue of payments transfers on financial markets. Due to high amounts of financial means that are being transferred through electronic banking systems between financial institutions and clients, these systems are subject to different forms of misuse, fraud and other criminal acts. Criminal acts cause damage and decrease trust of clients in financial institutions and services.

In order to ensure protection against electronic banking misuse, a holistic overview of its security is required, along with a set of various security models that prevent or at least decrease the occurrences of misuse on the level that is still satisfactory.

Banking operations in the area of implementing payment transfers, its informatization and ways of achieving security and protection of operations in the area referred to were examined. We analyzed irregularities and misuse occurring in this area, classifying them by modus operandi and common characteristics in order we could – based on these findings – classify factors influencing upon the banking system security. Based on examining the conditions in the area of electronic banking and misuses in banks we created a holistic security model for preventing misuse, including preventive as well as repressive factors. The model was tested; according to our findings the risk assessment of information security is required. We examined the methods intended to assess the information risk and based on the obtained results and specific features of banking operations drafted a new method of assessing information risk in financial institutions. The method was tested at those in charge of security of information systems in banks, and with the results confirmed the need for a new method adapted to specificity of banking operations.

KEY WORDS: electronic payment systems, electronic banking, financial crime, misuse, fraud, banks

KAZALO VSEBINE

KAZALO TABEL

KAZALO SLIK

UVOD

Bančne institucije opravljajo funkcijo posredovanja oziroma transformacije sredstev med posameznimi skupinami gospodarskih subjektov in posamezniki. Delovanje banke se pričenja s sprejemanjem vlog komitentov in pridobivanjem ostalih financ. Tako pridobljena sredstva omogočajo financiranje povpraševalcev po finančnih sredstvih v obliki posojil. V odvisnosti od dejavnosti banke, njene velikosti, organiziranosti, finančne aktivnosti, kot tudi ugleda, se preko dolžniško-upniških razmerij do poslovnih partnerjev oblikuje struktura virov financiranja banke. Pridobljena sredstva banke se s preudarnim usklajevanjem aktivne in pasivne strani bilance, glede na obseg, strukturo, realnost in ročnost, pretvori v naložbe. S tem banka z neprestanim dinamičnim procesom spremljanja tveganja neposredno upravlja s svojo izpostavljenostjo na finančnem trgu. Za kakovostno spremljanje in obvladovanje tveganja so pomembne kakovostne informacije iz okolja, nadzor in kvalitetno notranje komuniciranje.

Elektronski načini plačilnega prometa so kljub mnogim zaščitam še vedno premalo varovani. Vključujejo mnogo slabosti, tako na področju delovanja, kakor tudi nadzora. Praksa kaže, da je največja slabost magnetni zapis na plačilnih in kreditnih karticah, ki so največkrat predmet zlorab. Potrebno je posodobiti tehnično tehnološke in organizacijske rešitve glede varnosti. Z naborom različnih varnostnih modelov je treba onemogočiti ali vsaj omejiti možnost zlorab. Glede varnosti se zorni kot posrednikov na denarnem trgu v nekaterih točkah razlikuje od zornega kota policije. Zaradi tega je nujno, da se ti vidiki čim bolj zbližajo in uskladijo, saj je edino na ta način možno kakovostno obvladovati varnost na področju elektronskega plačilnega prometa tako s preventivno kakor tudi z nadzorstveno oz. kurativno dejavnostjo. Pri tem so pomembne vloge posameznikov in organizacij, ki so prisotne na tem področju. Potrebno je izdelati večdimenzionalni model preprečevanja zlorab elektronskih plačilnih sistemov, ki bo omogočal nemoteno odvijanje procesov in zmanjšal možnosti zlorab na minimum.

Plačilni promet spada med posredniške posle. Banka ali druga finančna organizacija posreduje med plačnikom in prejemnikom denarnih sredstev. Tako je neposredni način plačevanja, ki bi se opravljal med plačnikom in prejemnikom neposredno, spremenjen v posredni način. Banka se pojavi kot tretja oseba, preko katere se opravljajo plačila. Tako so v procesu plačevanja udeležene tri pravne ali fizične osebe. Plačnik pri banki spremeni svojo vlogo in postane dajalec naloga, banka kot pravna oseba je posrednica, tretja oseba pa je prejemnica.

Na področju plačilnega prometa, kjer banka posreduje med plačnikom in prejemnikom denarnih sredstev, obstaja več plačilnih instrumentov, katere imetniki, uporabniki in ponarejevalci spretno izrabljajo in banki povzročajo škodo.

Brezgotovinsko poslovanje, ki ga omogočajo kreditne in plačilne kartice, se je v sodobnem plačilnem prometu zelo razvilo in ponekod že presega gotovinsko plačevanje. Kreditne in plačilne kartice imenujemo tudi "plastični denar", saj se pojavljajo v obliki standardiziranih plastičnih kartic z nanešenim magnetnim zapisom. Magnetni zapis vsebuje vse podatke o imetniku kartice, izdajatelju, banki in možnosti plačevanja in dvigovanja gotovine na bančnih avtomatih. Prav magnetni zapis predstavlja eno od slabosti "plastičnega denarja", saj zaradi nezadostne zaščite prihaja do raznovrstnih zlorab tega plačilnega instrumenta.

Za uspešno preprečevanje zlorab plačilnih in kreditnih kartic ni dovolj samo tehnična zaščita in delovanje policije, ampak je potrebno vzpostaviti učinkovit varnostni model, ki je sestavljen iz različnih sklopov, ki ravno z medsebojnim delovanjem dosegajo optimalne rezultate. Ne gre samo za informacijsko varnost (tehnično gledano), ampak za model varnostnega sistema, ki zajema tako preventivne kot represivne dejavnike in ukrepe.

Predmet raziskovanja

Bančne institucije opravljajo funkcijo posredovanja oziroma transformacije sredstev med posameznimi skupinami gospodarskih subjektov in posamezniki. Delovanje banke se pričenja s sprejemanjem vlog komitentov in pridobivanjem ostalih oblik financiranja. Tako pridobljena sredstva omogočajo financiranje povpraševalcev po finančnih sredstvih v obliki posojil. V odvisnosti od dejavnosti banke, njene velikosti, organiziranosti, finančne aktivnosti kot tudi ugleda, se preko dolžniško-upniških razmerij do poslovnih partnerjev oblikuje struktura virov financiranja banke. Pridobljena sredstva banke se s preudarnim usklajevanjem aktivne in pasivne strani bilance, glede na obseg, strukturo, realnost in ročnost, pretvorijo v naložbe. S tem banka z neprestanim dinamičnim procesom spremljanja tveganja neposredno upravlja s svojo izpostavljenostjo na finančnem trgu. Za kakovostno spremljanje in obvladovanje tveganja so pomembne kakovostne informacije iz okolja, nadzor in kvalitetno notranje komuniciranje.

Elektronski načini plačilnega prometa so kljub mnogim zaščitam še vedno premalo varovani. Vključujejo mnogo slabosti, tako na področju delovanja kakor tudi nadzora. Praksa kaže, da je največja slabost magnetni zapis na plačilnih in kreditnih karticah, ki so največkrat predmet

zlorab. Potrebno je posodobiti tehnično-tehnološke in organizacijske rešitve glede varnosti. Z naborom različnih varnostnih modelov je treba onemogočiti ali vsaj omejiti možnost zlorab. Glede varnosti se zorni kot posrednikov na denarnem trgu v nekaterih točkah razlikuje od zornega kota policije. Zaradi tega je nujno, da se ti vidiki čim bolj zbližajo in uskladijo, saj je edino na ta način možno kakovostno obvladovati varnost na področju elektronskega plačilnega prometa tako s preventivno kakor tudi z nadzorstveno oz. kurativno dejavnostjo. Pri tem so pomembne vloge posameznikov in organizacij, ki so prisotne na tem področju. Potrebno je izdelati večdimenzionalni model preprečevanja zlorab elektronskih plačilnih sistemov, ki bo omogočal nemoteno odvijanje procesov in zmanjšal možnosti zlorab na minimum.

Plačilne kartice omogočajo odloženo plačilo ali pa so vezane na takojšnjo poravnavo s tekočega ali transakcijskega računa. Prve imenujemo kartice z odloženim plačilom, druge pa debetne, katerih uporaba je pri nas mogoča tudi za plačevanje in uporabo na bančnih avtomatih od leta 1999 naprej. Pri plačilu s kreditno kartico se bremeni kredit, ki se avtomatično razporedi na manjše bremenitve v roku nekaj mesecev.

Obstaja mnogo oblik zlorab plačilnih in kreditnih kartic, v grobem pa jih lahko razdelimo na zlorabe, ki jih povzročijo imetniki oz. uporabniki kartic, zlorabe, ki se zgodijo z izgubljenimi oz. ukradenimi karticami in zlorabe, ki se dogajajo s ponarejenimi karticami.

Za uspešno preprečevanje zlorab plačilnih in kreditnih kartic ni dovolj samo tehnična zaščita in delovanje policije, ampak je potrebno vzpostaviti učinkovit varnostni model, ki je sestavljen iz različnih sklopov, ki ravno z medsebojnim delovanjem dosegajo optimalne rezultate. Ne gre samo za informacijsko varnost (tehnično gledano), ampak za model varnostnega sistema, ki zajema tako preventivne kot represivne dejavnike in ukrepe.

Preventivni dejavniki otežkočajo uspešno izvedbo in možnost zlorab. Med preventivne dejavnike spadajo:

- ravnanje uporabnikov
- ravnanje zaposlenih
- nove tehnične zaščite - prepoznavalci tujih elementov, vgrajenih na bančne avtomate ali POS terminale
- zaščita kartic pred ponarejanjem

- pametne kartice
- informacijski sistemi za odkrivanje zlorab.

Če kljub zaščiti pride do zlorab in jih varnostni sistem zazna, se vključijo mehanizmi, ki na osnovi medsebojnega sodelovanja in obveščanja sprožijo določene ukrepe, ki preprečijo nadaljnje zlorabe (preklic kartice, zaprtje računa, obveščanje lastnika), na osnovi podatkov iz varnostnega sistema odkrijejo mesto zlorabe (bančni avtomat, plačilno mesto, POS terminal), sprožijo ustrezne mehanizme, ki privedejo do storilca zlorabe in njegovega sankcioniranja, vključno s povrnitvijo škode.

Represivne dejavnike razdelimo na:

- ukrepe, ki vodijo do preprečitve možnosti novih zlorab z že zlorabljeno kartico (preklic kartice, zaprtje računa)
- ukrepe, ki vodijo k odkritju mesta (točke) zlorabe kartice
- ukrepe, ki vodijo k odkritju načina in lokacije pridobitve podatkov o pravi kartici s pomočjo kopiranja - CPC (Common point of compromise**)**
- ukrepe, ki ob sodelovanju bank in izdajateljev kartic in policije vodijo k izsleditvi storilcev zlorab
- mednarodno sodelovanje in povezovanje policije in bank pri odkrivanju storilcev zlorab
- funkcijo Europola in Interpola
- primerno zakonodajo za sankcioniranje storilcev in odvzem pridobljene premoženjske koristi
- povrnitev škode oškodovancem zlorab.

Zastavljen model daje pozitivne rezultate, ki so vidni pri žal redko uspešno odkritih, preiskanih in tudi zaključenih primerih. Žal se pri tej vrsti gospodarske kriminalitete dogaja, da je zaradi velike mobilnosti storilcev, kratkega časa za ukrepanje in relativno slabih sledi s kraja kaznivega dejanja, velikokrat zelo težko odkriti in prijeti storilce zlorab. Ta težava pa se ne pojavlja samo pri nas, ampak pomeni težavo tudi za druge države, ki se z zlorabami kartic soočajo.

Kvaliteten varnostni model mora učinkovito preprečevati, zaznavati, odkrivati in sankcionirati zlorabe na področju plačilnega prometa s karticami. Ker gre na tem področju za mednarodni kriminal, je zelo pomembno dobro sodelovanje med domačimi in tujimi izdajatelji kartic, upravljalci bankomatnih mrež in seveda policijo. Sodelovanje in obveščanje mora potekati v realnem času, saj je zelo pomembno, da se storilec dobi pri izvrševanju kaznivega dejanja oz. takoj po tem. Izsleditev storilca kasneje je namreč zaradi njihove velike mobilnosti (pogosto gre za tujce, ki so v državi samo nekaj dni), zelo težavna. Pomembna je tudi dobra zakonodaja, ki mora omogočati ustrezno sankcioniranje zlorab, povrnitev povzročene škode uporabnikom finančnih storitev oz. bankam, kakor tudi odvzem premoženjske koristi.

Namen in cilji disertacije

Temeljni namen doktorske disertacije je ovrednotiti, kateri dejavniki in v kolikšni meri vplivajo na varnost elektronskih plačilnih sistemov, kako jih uporabljati in kombinirati, da bi dosegli največjo možno zaščito pred zlorabami. Na osnovi ugotovitev analiz zlorab in storilcev, tehnično-tehnoloških in organizacijskih možnostih zaščit informacijskih sistemov bomo izdelali celovit varnostni model za preprečevanje zlorab na področju elektronskih plačilnih sistemov. Model bomo testirali z izvedbo ankete na osnovi vprašalnikov in intervjuji pri zaposlenih, ki v bankah in drugih finančnih institucijah skrbijo za varnost elektronskega bančništva. Ker je varnost na tem področju povezana s tveganji, bomo na osnovi ugotovitev in zdaj znanih metod za ocenjevanje tveganj izdelali metodo, ki bo prilagojena ocenjevanju tveganj bančnih informacijskih sistemov. Metodo bomo testirali v bankah z intervjuji z zaposlenimi, ki skrbijo za varnost informacijskih sistemov. Nameravam torej:

1. Opredeliti in analizirati bančne plačilne sisteme in trenutne razmere na področju elektronskih plačilnih sistemov, ki potekajo preko informacijskih sistemov oziroma uporabljajo informacijsko tehnologijo.
2. Opredeliti, analizirati in pregledati zlorabe, ki se vršijo na področju elektronskega plačilnega prometa in šibke točke sistemov, ki zlorabe omogočajo, s poudarkom na ugotavljanju dejavnikov, ki preprečujejo učinkovitejšo zaščito.
3. Na podlagi analiz predlagati varnostno politiko preprečevanja zlorab v elektronskih plačilnih sistemih, vključno z vlogami posameznih organizacij in ključnimi dejavniki učinkovitega preprečevanja zlorab s posebno pozornostjo na mednarodni dimenziji sodelovanja pri preprečevanju zlorab.
4. Koncipirati in preizkusiti varnostni model preprečevanja zlorab elektronskih plačilnih sistemov, ki bo omogočal varnejšo uporabo sodobnih plačilnih sistemov za

uporabnike, zmanjšal možnosti zlorab in s tem znižal škodo, ki jo utrpijo finančne institucije, olajšal odkrivanje in sankcioniranje zlorab in s tem dvignil zaupanje uporabnikov v sodobne finančne produkte.

5. Izdelati varnostni model, ki bo omogočal spremljanje sprememb dejavnikov, ki vplivajo na varnost poslovanja finančnih institucij in obvladovanje nenehnih sprememb na tem področju v smeri obvladovanja varnosti in zmanjšanja zlorab.
6. Na osnovi problematike zlorab področja plačilnih sistemov pri nas in v tujini pokazati stanje na tem področju in možnosti za izboljšave.
7. Varnostni model v praksi preveriti v finančnih institucijah, ki se ukvarjajo z elektronskimi plačilnimi sistemi in se soočajo z zlorabami na tem področju.
8. Pregledati znane (organizacijske in tehnološke) rešitve na področju varnosti elektronskih plačilnih sistemov, oceniti njihove primernosti in zmožnosti za povezovanje v celovit model varnosti elektronskih plačilnih sistemov, ki bo upošteval dimenzije preventivne in nadzorstvene dejavnosti, povezane z odpravo groženj in dejanj, ki vplivajo na varnost.
9. Na osnovi obstoječih metod za ocenjevanje tveganja informacijskih sistemov izdelati metodo za ocenjevanje tveganj, ki bo prilagojena specifičnostim bančnega poslovanja.
10. Novo metodo testirati v bankah z izvedbo intervjujev in na osnovi ugotovitev potrditi ali ovreči primernost in potrebnost prilagojena metode za ocenjevanje tveganj v bankah in drugih finančnih institucijah.

Cilj doktorske disertacije bo izvedena analiza dejavnikov, ki vplivajo na varnost plačilnih sistemov in na obnašanje končnih uporabnikov in drugih za preprečevanje zlorab na tem področju, izdelava celovitega modela za zagotavljanje varnosti in koncipiranje nove metode za ocenjevanje tveganj bančnih informacijskih sistemov, potrditev postavljenih hipotez in s tem potrditev celovitega varnostnega modela.

Hipoteze disertacije

V doktorski nalogi smo postavili naslednje hipoteze:

1. Gospodarska kriminaliteta, kamor spada področje elektronskih plačilnih sistemov, se neprestano spreminja in posodablja.
2. Za preprečevanje zlorab je potrebno izdelati učinkovit varnostni model, ki bo zmanjšal možnost zlorab.

3. Za zmanjšanje zlorab je potrebno sprejeti učinkovite varnostne ukrepe na samih informacijskih sistemih, urediti in definirati nadzor sistemov, sporočanje, obveščanje in povezovanje različnih institucij, ki skrbijo za varnost plačilnih sistemov.
4. Varnostni model mora biti zasnovan tako, da bo omogočal takojšnje odzive na spremembe problematike področja in se bo lahko fleksibilno prilagajal novim, kompleksnejšim oblikam zlorab.
5. Uspešno in učinkovito preprečevanje zlorab v elektronskih plačilnih sistemih je mogoče le ob celovitem modelu zagotavljanja varnosti.
6. Varnostni model mora zajemati tudi preventivne dejavnike varnosti, saj lahko tudi na ta način zmanjšamo možnosti zlorab.
7. Na uresničevanje modela celovite varnosti vpliva nekaj ključnih dejavnikov, ki zagotavljajo uspešno in učinkovito preprečevanje zlorab.
8. Celovito varnost je potrebno uravnoteženo prenesti na organizacijske in tehnološke rešitve.
9. Celovit varnostni model mora upoštevati mednarodno dimenzijo.
10. Sprememba tehnologije zaščite posameznih delov sistemov in celote se mora prilagajati in nadgrajevati z razvojem tehnično - tehnoloških novosti na področju zaščit sistemov.
11. Samo kompleksna obravnava vseh vidikov in institucij, ki delujejo na področju elektronskih plačilnih sistemov, lahko prinese učinkovit varnostni model, ki bo lahko zmanjšal možnosti zlorab. Zavedati pa se moramo, da popolne varnosti na tem področju ni možno doseči, predvsem ne dolgoročno, brez ažurnega prilagajanja varnostnega modela novim razmeram.

Omejitveni dejavniki

Pristopi bank in drugih finančnih institucij k upravljanju in obvladovanju tveganj so različni, brez dvoma pa pomeni velikost finančne institucije tudi možnost kvalitetnejšega obvladovanja tveganj. Izkušnje tujih bank in finančnih institucij na tem področju so pomembne tudi za naše finančne institucije. S sprejetjem novega Zakona o bančništvu (Uradni list RS, št. 99/2010-UPB5) in postopnim prilagajanjem poslovanja evropskim bančnim direktivam se tudi v naših bankah začenja način vodenja bank po posameznih tveganjih, pomembna pa postaja tudi učinkovitost bančnega nadzora.

Omejitve lahko predstavlja tudi dostop do podatkov, ki jih obdelujejo in hranijo bančne institucije, saj le-ti pomenijo bančno tajnost, ki je v poslovnem svetu ena izmed najbolj varovanih.

Finančne institucije prav tako pogosto nimajo veliko interesa za prijavljanje zlorab organom odkrivanja in pregona, saj se lahko zgodi, da podatki o zlorabah, ki pridejo v javnost, negativno vplivajo na ugled banke, kar ima lahko zanjo usodne posledice.

Znanstvena raziskava gospodarske kriminalitete je tako v svetu kakor tudi pri nas šele na začetku. Predvsem raziskava gospodarske kriminalitete z ekonomskega vidika je slabo obravnavana, saj se s to problematiko lahko srečujemo le ekonomisti, zaposleni v kriminalistični policiji. Gospodarska kazniva dejanja so s pravnega vidika bolje obdelana, v raziskavah pa niso zajeti ekonomski vidiki. Literature, ki bi eksplicitno obravnavala omenjeno področje, je zelo malo.

Struktura disertacije

Pri izdelavi doktorske disertacije bomo v prvem delu z analitičnim pristopom – zbiranjem podatkov o zlorabah in dejavnikih zlorab, opredelili stanje na področju elektronskih plačilnih sistemov pri nas in v tujini s poudarkom na dejavnikih, ki omogočajo zlorabe. Pri tem si bomo pomagali z zbiranjem in analizo različnih virov podatkov pri nas in v tujini.

V nadaljevanju bomo s kvantitativno obravnavo oz. metodo deduktivne deskripcije opravili analizo podatkov o številu zlorab plačilnih kartic in informacijskih sistemov. S kvalitativno obravnavo podatkov oz. metodo induktivne deskripcije bomo opravili analizo praktičnih primerov gospodarske kriminalitete in zlorab elektronskih plačilnih sistemov, s čimer bomo opredelil največje probleme varnosti informacijskih sistemov.

Na osnovi sinteze tako pridobljenih spoznanj, bomo z metodo modeliranja organizirali varnostni model elektronskih plačilnih sistemov, ki bo zasnovan kot celovit model zagotavljanja varnosti. Na osnovi spoznanj iz kvantitativne analize bomo modelirali in raziskovali vloge organizacij v varnostnem modelu.

Za izdelavo varnostnega modela in njegovo verifikacijo bomo uporabili metodo tipa design. Ta metoda se uporablja za znanstveno obravnavo in preverjanje ustreznosti predlaganih novosti, kot so modeli (npr. abstrakcije, predstavitve), konstrukti (npr. geslovniki, simboli), metode (npr. postopki, algoritmi, prakse) ali primerki (npr. prototipi) (Hevner, A. R., 2004).

Primerna je za uporabo na področju informatike, pri procesnih modelih in v inženirstvu (Vaishnavi, V., Kuechler, W., 2004).

Osnovne smernice tega raziskovalnega pristopa so:

- predlaga se novost,
- izpostaviti je potrebno pomen, relevantnost in koristnost novosti,
- novost je potrebno preveriti v smislu koristnosti, učinkovitosti in kakovosti
- izpostaviti je potrebno pomembnost novosti kot prispevka k razvoju znanosti in področja, na katerem se predlaga,
- pri zasnovi, obravnavi in preverjanju novosti je potrebno uporabljati rigorozne znanstvene metode (Hevner, A. R., 2004).

V skladu s tem bomo izdelan varnostni model s pomočjo ankete in intervjuja verificirali v praksi, s pomočjo deduktivne deskripcije pa analizirali odzive organizacij na varnostni model. Model bo testiran v več izbranih organizacijah. Ker bo prilagojen model preverjan v posameznih organizacijah, bo imela raziskava tudi elemente aplikativne raziskave in sicer raziskave primerov. Na osnovi podatkov, pridobljenih z anketo, (kvantitativni pristop) bomo dobili podrobnejši odgovor na vprašanje, do kolikšne mere organizacije v resnici uporabljajo model in katerim zunanjim dejavnikom namenjajo premalo pozornosti. Ker pa želimo podrobneje analizirati dobljene rezultate, bomo izvedli tudi intervjuje z odgovornimi osebami (kvalitativni pristop).

Ker je varnost elektronskega bančništva povezana z ocenjevanjem tveganj informacijskih sistemov, bomo izdelali metodo za ocenjevanje tveganj, ki bo prilagojena bančnemu poslovanju. Z intervjuji bomo ustreznost in primernost metode testirali v bankah. S pomočjo SWOT analize bomo ocenili prednosti in slabosti metode za ocenjevanje tveganj informacijskih sistemov v bankah.

1 BANKE IN PLAČILNI SISTEM

Pod vplivom gibanj in sprememb na gospodarskem, političnem, družbenem in pravnem področju so se s časom oblikovale različne vrste kreditnih institucij (bank). Poslovne banke razdelimo po kriterijih: poslovna struktura (na univerzalne in specializirane banke), geografsko področje delovanja (na lokalne, regionalne, nadregionalne in mednarodne), gospodarska usmeritev (pridobitno gospodarske, neprofitne in banke s posebnimi nalogami oz. pospeševalne banke) in po kriteriju pravna oblika (na institucije zasebnega prava, javnopravne in zadružne). (Glogovšek, 2008).

Na področju univerzalnih bank (Glogovšek, 2008) ločimo:

- kreditne banke
- hranilnice in žirocentrale (centri z žiralnim denarjem)
- zadružne kreditne banke zadruge in zadružne centralne banke.

Na področju specializiranih bank poznamo:

- hipotekarne banke
- banke za stanovanjska posojila in varčevanje
- kreditne banke s posebnimi nalogami – pospeševalne banke.

1.1 Cilji poslovanja banke

Cilji poslovanja banke so danes lahko različni. Obstajajo različna stališča o tem, ali je med cilje poslovanja banke potrebno šteti tudi likvidnost in varnost poslovanja, kategoriji iz "magičnega trikotnika", v okviru katerega morajo banke voditi svojo poslovno politiko. Vse bolj prevladuje mnenje, da sta likvidnost in varnost stranska pogoja poslovanja banke in ne cilj, kajti likvidnost in varnost lahko le pospešujeta ali zavirata doseganje temeljnih ciljev poslovanja banke. (Bobek, D., 1998)

Ko govorimo o ciljih poslovanja banke, jih lahko ločimo na tiste, ki jih je možno izraziti vrednostno in tiste, katerih konkretizacija nima svojega vrednostnega izraza. Prve imenujemo ekonomske cilje, ki se izkazujejo kot finančni rezultati, drugi so neekonomski, ker jih praviloma ni mogoče izkazati v finančni obliki. Med ekonomske cilje štejemo rentabilnost in

gospodarsko rast banke. Neekonomski cilji so cilji, ki jih bankam postavljajo njihove članice, pa tudi "image" banke. (Bobek, D., 1992)

Ekonomski cilji

Ekonomski cilji imajo svojo konkretizacijo v finančnem rezultatu, ki se izkaže kot dobiček banke ali kot porast bilančne vsote. To je posledica povečanega poslovanja banke. S tem dosega banka hitrejšo rast, svoj razvoj in razvoj svojega gospodarskega okolja.

Rentabilnost štejemo za temeljni ekonomski cilj poslovanja banke. Prihodki, ki jih v svojem poslovanju ustvarja banka, se oblikujejo iz obresti od danih kreditov (aktivne obresti), iz zaračunanih provizij, plačil za bančne storitve in raznih drugih prihodkov. Banka pa s svojim poslovanjem ustvarja tudi stroške oziroma odhodke. Najvažnejši med njimi so predvsem obresti na depozite, hranilne vloge in prejete kredite (pasivne obresti), kakor tudi plačane provizije, obračunana amortizacija in stroški za poslovne kredite in opremo.

Presežek prihodkov nad odhodki predstavlja poleg kazalnika rentabilnosti še kazalnik ekonomičnosti. Medtem, ko se ekonomičnost lahko izkazuje količinsko in vrednostno, pa se rentabilnost lahko izkazuje samo vrednostno. Zaradi tega kazalnik ekonomičnosti v banki ni tako uporabljiv kot rentabilnost. Nastopa kot pomožni kazalnik, ki analizira predvsem organizacijsko-tehnično področje. Za poslovno politiko pa je bolj pomemben kazalnik rentabilnosti, ki je tudi temeljni cilj poslovanja banke.

Neekonomski cilji

Neekonomskih ciljev ni mogoče vrednostno izraziti ali jih zajeti v rentabilnosti. Navadno povzročajo izpad prihodka banke in ne povečujejo rentabilnosti. Dajanje kreditov po nižji (priviligirani) obrestni meri ali dajanje kreditov izven pravil, ki veljajo za ostale komitente, spada med neekonomske cilje. Podobnih neekonomskih ciljev je v bankah seveda še več.

Posebna vrsta cilja je "image" banke, ki ga vrednostno ni mogoče izmeriti, ima pa pomemben vpliv na rentabilnost in gospodarsko rast banke. Banka si mora pridobiti zaupanje prebivalstva in gospodarstva, saj z zbiranjem njihovih prostih finančnih sredstev, ki jih kasneje transformira, dosega namen svojega poslovanja. Še posebej je "image" pomemben v primeru večje konkurence na bančnem trgu. Vsak komitent se bo namreč odločil pri izbiri banke na

osnovi varnosti naložb, hitrosti opravljanja finančnih transakcij, zagotavljanju likvidnosti in solidnega poslovnega odnosa. Zato je "image" banke eden od glavnih pogojev za uspešno poslovanje banke z vidika poslovnosti.

1.2 Plačilni promet

Plačilni promet spada med posredniške posle. Banka ali druga finančna organizacija posreduje med plačnikom in prejemnikom denarnih sredstev. Tako je neposredni način plačevanja, ki bi se opravljal med plačnikom in prejemnikom neposredno, spremenjen v posredni način. Banka se pojavi kot tretja oseba, preko katere se opravljajo plačila. Tako so v procesu plačevanja udeležene tri pravne ali fizične osebe. Plačnik pri banki spremeni svojo vlogo in postane dajalec naloga, banka kot pravna oseba je posrednica, tretja oseba pa je prejemnica.

Plačilni promet, organiziran na tak način, je lahko gotovinski ali brezgotovinski. Tako je gotovinski denar poleg tega, da je denarna oblika, hkrati tudi instrument plačilnega prometa. Glede na sedež oseb, udeleženih v plačilnem prometu, ločimo notranji in mednarodni plačilni promet. Notranji plačilni promet poteka znotraj meja države, če pa ima ena izmed oseb, ki so bile udeležene v plačilnem prometu, sedež v drugi državi, govorimo o mednarodnem plačilnem prometu oziroma plačilnem prometu s tujino.

Pri nas smo področje plačilnih storitev delno uredili v Zakonu o plačilnem prometu (ZPlaP), ki je veljal do 11. 8. 2009, ko ga je nadomestil Zakon o plačilnih storitvah in sistemih (Ur. l. RS, št. 58/09). V novem zakonu so tako določene plačilne storitve in plačilni sistemi in upoštevana priporočila in direktive Evropske komisije[1]. Področje plačil, opravljenih z

[1] Direktiva 2007/64/ES Evropskega parlamenta in Sveta z dne 13. novembra 2007 o plačilnih storitvah na notranjem trgu in o spremembah direktiv 97/7/ES, 2002/65/ES, 2005/60/ES in 2006/48/ES ter o razveljavitvi Direktive 97/5/ES (UL L št. 319, z dne 5. 12. 2007, v nadaljnjem besedilu: Direktiva 2007/64/ES);

Direktiva 98/26/ES Evropskega parlamenta in Sveta z dne 19. maja 1998 o dokončnosti poravnave pri plačilih in sistemih poravnave vrednostnih papirjev (UL L št. 166, z dne 11. 6. 1998, v nadaljnjem besedilu: Direktiva 98/26/ES);

Direktiva 2000/46/ES Evropskega parlamenta in Sveta z dne 18. septembra 2000 o začetku opravljanja in opravljanju dejavnosti ter nadzoru skrbnega in varnega poslovanja institucij za izdajo elektronskega denarja (UL L št. 275, z dne 27. 10. 2000, v nadaljnjem besedilu: Direktiva 2000/46/ES).

elektronskimi plačilnimi instrumenti, je predmet urejanja v Priporočilu Komisije 97/489/EC glede plačil z elektronskimi plačilnimi instrumenti, predvsem glede razmerja med izdajateljem in imetnikom (Trstenjak, 2006).

Komisija je v svojih dokumentih zadostila zahtevam po jasni razmejitvi plačilnih storitev od drugih storitev, ki so povezane z opravljanjem plačil. Tako je izključila iz plačilnih storitev tehnične storitve, povezane z izvajanjem plačil in plačila digitalnih komunikacijskih storitev z uporabo mobilnega telefona in drugih telekomunikacijskih storitev, pri katerih je operater tesno povezan z razvojem teh storitev. Izključena so vsa tista plačila, ki jih ponujajo ponudniki telekomunikacijskih storitev in so povezana z izvajanjem PRS[2] (Premium Rate Services). S tem je Komisija potrdila stališče, da so plačilne storitve le tiste, ki omogočajo posredovanje plačila med plačnikom in prejemnikom plačila (Trstenjak, 2006).

Cilj plačilnih storitev in sistemov je olajšati in pospešiti transakcije v državi. Pri tem je potrebno spoštovati pravne predpise iz Zakona o bančništvu (Zban-1D), Zakona o Banki Slovenije (ZBS1-UPB1), Obligacijski zakonik (OZ-UPB1) in Zakona o deviznem poslovanju (ZDP-2A).

Brezgotovinski način plačevanja se je najbolj uveljavil v poslovnem svetu. Podjetja v celoti uporabljajo brezgotovinsko plačevanje. Zato pa morajo imeti svoja denarna sredstva na banki in sicer v takšni obliki, da jih je možno vsak trenutek dvigniti. Neprimerna za brezgotovinsko plačevanje so vezana sredstva, ki jih je poprej potrebno spremeniti v depozite na vpogled. Gotovinski plačilni promet, ki je tudi instrument plačilnega prometa, se vedno opravlja v gotovini. Vmesna stopnja med gotovinskim in brezgotovinskim plačilnim prometom je polgotovinski plačilni promet. Pri tem se ena faza plačila (n.pr. vplačilo) opravi z gotovino, druga (n.pr. izplačilo) pa brezgotovinsko.

[2] PRS so storitve, ki jih ponujajo telekomunikacijske družbe (posebne informacije, zabavne storitve, glasovanja…), kjer operater nastopa kot ponudnik storitve, hkrati pa tudi kot končni prejemnik plačila.

Izvajalci plačilnega prometa

Plačilne storitve izvajajo kreditne institucije, kot so banke, hranilnice, hranilno-kreditne službe in Pošta Slovenije. Naloge v plačilnem sistemu v osnovi delimo na tiste, ki jih opravlja centralna banka in tiste, ki jih opravljajo poslovne banke.

Centralna banka (Glogovšek, 2008) gospodarstva deluje v kompleksnem prepletu odnosov z drugimi sektorji:

- z državo
- s tujino
- z gospodarstvom in zasebniki (v matični državi)
- z nacionalnim sistemom poslovnih bank.

Če izhajamo iz ugotovitve, da sta struktura denarnega obsega (plačilne navade strank) in struktura sistema (stopnja koncentracije) z vidika centralne banke podatka, je s tem že vnaprej dana »naravna« stopnja odvisnosti sistema poslovnih bank (SPB) od centralno bančnega sistema (CBS). Vendar se CBS s tem ne more zadovoljiti, saj je njegova naloga v okviru monetarne konjukturne politike prav vpliv na SPB, torej oblikovanje te odvisnosti. To oblikovanje poteka z instrumenti politike Centralne banke, ki tako predstavljajo nadaljnjo determinanto odnosa med CBS in SPB (Glogovšek, 2008).

Poslovne banke sprejemajo depozite in dajejo posojila za svoje stranke.

Med institucije, ki izvajajo plačilni promet, sodijo:

- Poravnalne banke: banke ali finančne institucije, ki delujejo na osnovi Zakona o bančništvu. Te institucije imajo odprt poravnalni račun pri Banki Slovenije, preko katerega se vsa plačila izvršijo takoj. Sprožijo lahko tudi prenos za sebe in za svoje komitente, ki imajo sredstva na računih.
- Neporavnalne banke : posredni udeleženci nimajo poravnalnih računov, imajo pa korespondenčne nostro račune. Plačila se izvedejo preko poravnalnih računov, ki jih imajo njihove poravnalne banke pri centralni banki. Neporavnalne banke lahko izvedejo plačila v imenu svojih komitentov.
- Posredni udeleženci: druge organizacije in subjekti, ki so komitenti poravnalnih ali neporavnalnih bank (Pukmajster, 2001: 8).

Storitve plačilnega prometa

Glede na sedež oseb, udeleženih v plačilnem prometu, ločimo notranji in mednarodni plačilni promet. Plačilni promet v državi poteka znotraj meja države, če pa ima ena izmed oseb, ki so bile udeležene v plačilnem prometu, sedež v drugi državi, govorimo o mednarodnem plačilnem prometu oziroma plačilnem prometu s tujino.

Odkar je Slovenija postala polnopravna članica Evropske unije in kot plačilno sredstvo prevzela evro, se v našem bančništvu ukvarjajo z vzpostavitvijo Enotnega območja plačil v evrih – SEPA[3]. Tako bo enotno območje plačil v evrih tisto območje, kjer bomo lahko državljani, gospodarstvo in drugi ekonomski subjekti znotraj Evrope prejemali in plačevali v evrih, ne glede na to, v kateri evropski državi smo. Poleg 15 držav evroobmočja[4] in 12 preostalih držav EU[5], vključuje območje SEPA še Islandijo, Norveško, Lichtenstein in Švico in devet območij pod upravo EU[6] (Širaj, 2008). Območje SEPA zajema več kot 504 milijone prebivalcev, okoli 9.000 bank, 25 milijonov gospodarskih družb ter 73 milijard elektronskih kreditnih transakcij (www.europeanpaymentscouncil.eu).

Pomembna plačilna storitev SEPA bo tudi kartično plačilo SEPA. Večja varnost in učinkovitost sta tukaj na prvem mestu. Zato SEPA predvideva za zagotavljanje večje varnosti uvedbo čipne tehnologije kartic (standard EMV[7]) do konca leta 2010, ko naj bi uporabniki kartičnih storitev uporabljali pri plačilih le še PIN številko namesto podpisa. Večjo učinkovitost kartičnih plačil bi naj omogočila možnost uporabe ene same kartice na vsem območju SEPA pod enakimi pogoji (Širaj, 2008).

---

[3] Single Euro Payments Area

[4] Belgija, Nemčija, Irska, Grčija, Španija, Francija, Italija, Ciper, Luksemburg, Malta, Nizozemska, Avstrija, Portugalska, Finska in Slovenija

[5] Bolgarija, Češka, Danska, Estonija, Litva, Latvija, Madžarska, Poljska, Romunija, Slovaška, Švedska in Velika Britanija

[6] Francoska Gvajana, Guadeloupe, Martinique, reunion, Azori, Madeira, Kanarski otoki, Ceuto in Melillo ter Gibraltar

[7] Europay-Mastercard-Visa

Vsa plačila, kjer sta nalogodajalec in prejemnik sredstev komitenta iste banke (ne glede na to ali gre za podjetja ali fizične osebe), se obdelajo le znotraj te banke in tako dobijo značaj internega plačilnega prometa. To pomeni, da je tisti trenutek, ko je obremenjen račun plačnika, odobren tudi račun upnika. (Pukmajster, 2001: 18)

Dejansko je odnos gotovina/žiralni denar funkcija plačilnih navad. Spremembe, ki jih je opaziti po vsem svetu, kažejo tendenco sproščanja med CBS in SPB. Ta trend je posebno izražen povsod, kjer je prehod z izplačevanjem dohodkov v gotovini na brezgotovinsko poslovanje že končan. (Glogovšek, 2008)

1.3 Plačilni sistemi

Plačilni sistemi imajo ključno vlogo pri opravljanju plačilnega prometa, saj uporabnikom zagotavljajo hitro in zanesljivo izvrševanje transakcij. Transakcije morajo biti opravljene s čim nižjimi stroški in kakovostnim zapisom.

Med uporabnike plačilnih sistemov štejemo centralne banke, poslovne banke in njihove komitente, klirinške hiše in druge finančne institucije, ki delujejo v posameznih državah. (Pukmajster, 2001: 25)

Plačilne storitve v Sloveniji opravljajo banke, hranilnice, hranilno-kreditne službe, Banka Slovenije in Pošta Slovenije. Kot je razvidno iz tabel 1 in 2 , v Sloveniji deluje 18 bank in 5 hranilnic, poleg njih pa tudi 61 hranilno-kreditnih služb. Te iste institucije opravljajo tudi transakcije s tujino. Delovanje vseh institucij plačilnega sistema nadzira Banka Slovenije.

Tabela 1: Slovenske poslovne banke

ABANKA VIPA d.d. LJUBLJANA	Slovenska 58	Ljubljana
BANKA CELJE d.d.	Vodnikova 2	Celje
BANKA KOPER d.d.	Pristaniška 14	Koper
BANKA SPARKASSE d.d.	Cesta v Kleče 15	Ljubljana
BANKA VOLKSBANK d.d.	Dunajska c. 128 a	Ljubljana
BAWAG BANKA d.d.	Tivolska cesta 30	Ljubljana
DEŽELNA BANKA SLOVENIJE d.d.	Kolodvorska 9	Ljubljana
FACTOR BANKA d.d.	Tivolska cesta 48	Ljubljana
GORENJSKA BANKA d.d.	Bleiweisova c. 1	Kranj
HYPO ALPE ADRIA BANKA d.d.	Dunajska 117	Ljubljana

KD BANKA, d.d.	Neubergerjeva 30	Ljubljana
NOVA KBM d.d.	Ul. Vita Kraigherja 4	Maribor
NOVA LJUBLJANSKA BANKA d.d.	Trg republike 2	Ljubljana
POŠTNA BANKA SLOVENIJE d.d.	Ul. Vita Kraigherja 5	Celje
PROBANKA d.d. MARIBOR	Trg Leona Štuklja 12	Maribor
RAIFFEISEN BANKA d.d.	Zagrebška cesta 76	Maribor
SKB d.d.	Ajdovščina 4	Ljubljana
SLOVENSKA INVESTICIJSKA BANKA[8]	Čopova 38	Ljubljana
SLOVENSKA IZVOZNA IN RAZVOJNA BANKA d.d	Ul. J. Turnograjske 6	Ljubljana
UNICREDIT BANKA SLOVENIJA d.d.	Šmartinska 140	Ljubljana

Vir: *Bilten BS, marec 2011*

Tabela 2: Slovenske hranilnice

DELAVSKA HRANILNICA LJUBLJANA	Dalmatinova 4	Ljubljana
HRANILNICA LON d.d.	Bleiweisova 2	Kranj
HRANILNICA IN POSOJILNICA VIPAVA d.d.	Glavni trg 15	Vipava

Vir: *Bilten BS, marec 2011*

Glede poravnavanja obveznosti in terjatev velja v tržnem gospodarstvu popolna svoboda, zato se plačilni sistemi v teh gospodarstvih med seboj močno razlikujejo. Razlike so odvisne od tradicije in zakonodaje, ki ureja plačilne sisteme. Prav tako velja, da ne obstaja en sam zakonski predpis, ki bi urejal plačilni sistem. V Sloveniji plačilni sistem urejajo naslednji zakoni: Zakon o bančništvu (ZBAN – 1), Zakon o Banki Slovenije (ZBS1 – UPB1), Zakon o deviznem poslovanju (ZDP – 2) ter Obligacijski zakonik (OZ - UPB1).

1.4 Instrumenti plačilnega prometa

Plačilni instrumenti so dokumenti, s katerimi se sproži izvršitev plačila in so lahko v papirni obliki, na magnetnem traku, disketi ali v drugačni obliki. Ločimo jih glede na to, ali gre za gotovinsko ali negotovinsko poslovanje.

[8] V likvidaciji

Gotovinski instrumenti plačevanja

Najbolj razširjen instrument te vrste je že omenjena gotovina. Uporablja se, ko gre za direktno plačilo (iz rok v roke) ali pa v primerih, ko plačnik nima računa pri banki, vendar mora izvesti vplačilo na določen transakcijski račun. To lahko stori na različne načine.

- Splošne položnice: preko položnice lahko v banki ali na pošti podjetje ali fizična oseba vplača gotovino na določen transakcijski račun. Lahko gre tudi za vplačilo gotovine v dobro plačnikovega računa. Splošna položnica ima tri dele, in sicer: potrdilo (ostane vplačniku), sporočilo o vplačilu (dobi lastnik računa) in sporočilo za arhiv (ostane banki).
- Posebne položnice: ta vrsta položnice, ki je dokaj nova in predstavlja posodobljeno splošno položnico, je namenjena plačevanju obveznosti do upnika. Omogočeno je optično branje obrazca. Posebna položnica ima štiri dele: dve potrdili za vplačnika, sporočilo o vplačilu in sporočilo za arhiv.
- Vplačilni nalog in posebna nakaznica: oba instrumenta uporablja pravna oseba: prvega pri polaganju gotovine na svoj transakcijski račun, drugega za nakazilo denarnih sredstev na račun prejemnika.

Za dvig gotovine oziroma izplačilo pravne (za plače, potne stroške, dnevnice, izplačilo vrednostnega papirja ipd) in fizične osebe uporabljajo nalog za gotovinsko izplačilo.

Negotovinski instrumenti plačevanja

Pri negotovinskem plačevanju ne moremo upravljati z gotovino, temveč s sredstvi, ki jih imamo na računih v banki. Ta sredstva imenujemo tudi knjižni denar. Z denarnimi sredstvi na naših računih plačujemo blago in storitve preko spodaj navedenih instrumentov.

- Ček: je vrednostni papir, s katerim dajemo nalog banki (pri kateri imamo razpoložljiva denarna sredstva), da izplača imetniku čeka, na čeku označenemu uporabniku ali pa osebi, ki jo ta določi, določen znesek denarja. V postopku plačevanja s čekom sodelujejo trasant (imetnik računa), trasat (banka, pri kateri je odprt račun) in remitent (upravičenec do denarnih sredstev). Pri tem mora imeti tisti, ki izda ček, na računu denarno kritje vsaj v višini zneska, ki je na čeku. Izdajanje čeka, ki nima kritja, je

kaznivo dejanje po 253. členu[9] Kazenskega zakonika Republike Slovenije in se kaznuje z zaporom do petih let. Banka se mora pri uporabi tega plačilnega instrumenta ravnati po veljavnih predpisih oziroma dogovorih, ki določajo pogoje in način unovčenja čekov. (Pukmajster, 2001: 21)

- Plačilni nalogi (nalog za prenos, nalog za unovčenje, akceptni nalog, nalog za obračun): v času, ko je še obstajala Agencija Republike Slovenije za plačilni promet, so imele banke omenjene štiri vrste nalogov. Danes se vse te transakcije opravljajo preko plačilnega naloga. S plačilnim nalogom, ki je lahko v elektronski ali papirni obliki, lastnik računa zadolži banko, pri kateri ima odprt račun, da prenese denarna sredstva z njegovega računa na račun drugega imetnika.
- Trajni nalog: je precej podoben plačilnemu nalogu, saj gre za isto vrsto plačila. Vendar se ta plačila konstantno ponavljajo (npr. mesečno, polletno, letno), zato jih lahko imetnik računa poenostavi. Imetnik računa pooblasti banko, da na določen dan v mesecu ali letu izvede plačilo fiksnega (npr. pri varčevanjih) ali spremenljivega zneska (npr. pri plačevanju elektrike) na račun upnika. Ob tem je potrebno poudariti, da sta tako dan kot tudi račun upnika vnaprej določena.
- Menica: Imetnik računa lahko pooblasti banko, da v breme njegovega računa opravi plačilo zneska upravičencu (upniku) na podlagi izdane menice, ki jo menični upnik predloži v plačilo pri banki, ki je na menici označena kot oseba, pri kateri je menica plačljiva (domiciliat). Ko upnik banki predloži menico, banka pozove glavnega meničnega dolžnika, ki ima pri njej račun, in od njega zahteva pooblastilo za izplačilo menice. Če dolžnik banki ne da pooblastila, banka ni upravičena izplačati meničnega zneska, čeprav so sredstva na računu. Pri menicah v bančnem okolju ni avtomatskega izplačila iz računa. Upniki zato ob predložitvi domiciliarne menice banke ne izpolnjujejo še naloga za vnovčenje, kot je bila to praksa pri Agenciji RS za plačilni promet. (Pukmajster, 2001: 13) Poznamo lastne, tuje in bianco menice.
- Akreditiv: je pooblastilo banki, da na dan roka, ki je določen na njem, črpa denarna sredstva z računa komitenta banke. Uporabnik družbenih sredstev na ta način da na voljo denarna sredstva banki.. Pri izplačilu navadnega ali osebnega akreditiva ni nikakršnih pogojev, ob izplačilu dokumentarnega pa mora uporabnik predložiti ustrezne dokumente, s katerimi je plačilo pogojeno. Poznamo še permanentne in domače akreditive. Na vsakem akreditivu mora biti zaznamovan rok veljavnosti,

[9] S 1.11.2008 smo dobili nov Kazenski zakon (KZ-1), kjer je prišlo do spremembe 253. člena v nov 246. člen

vendar ta rok ne sme biti daljši od enega leta (razen pri permanentnem, ki velja do preklica).

- Direktna obremenitev in odobritev: direktna obremenitev je posebna oblika negotovinske poravnave obveznosti, ki se lahko izvrši na plačnikovem računu. Plačnik sklene pogodbo z upnikom in banko. S pogodbo pooblasti upnika, da pod določenimi pogoji in na določen dan banki predloži nalog za obremenitev računa plačnika v višini zneska za opravljeno storitev. Direktna odobritev pa se izvrši v dobro računa prejemnika plačila. Pooblastilo imetnika transakcijskega računa (nalogodajalca) je vsebovano v pogodbi z banko, v kateri je opredeljena tudi vrsta direktne odobritve (plače, pokojnine, dividende…). Za izplačilo pripravi nalogodajalec podatke za vse prejemnike plačila z direktno odobritvijo in jih posreduje bankam. (Pukmajster, 2001: 13)

Banka lahko izvede plačilo brez soglasja imetnika transakcijskega računa na podlagi sodnega sklepa o izvržbi na denarna sredstva imetnika transakcijskega računa kot dolžnika ali na podlagi izvršljivega sklepa o prisilni izterjavi davčnega oziroma carinskega organa ali drugega organa, kadar so za izvržbo po posebnih predpisih dolžni uporabljati Zakon o davčnem postopku. (Pukmajster, 2001: 14)

Instrumenti plačevanja majhnih plačil

Čeprav število takšnih transakcij bistveno presega število transakcij velikih plačil, pa je njihova vrednost v okviru celotnega plačilnega prometa zelo majhna.

To so v bistvu plačila, ki jih imetniki računa opravljajo v vsakdanjem življenju. Med najbolj razširjene instrumente takšnega plačevanja poleg že omenjenih čekov, ki se danes postopno opuščajo, sodijo tudi:

- bankomati: na njih komitenti banke dvigujejo gotovino s pomočjo debetne kartice tekočega računa, kartice z odlogom plačila ali kreditne kartice. Z debetno kartico pa lahko tudi vplačajo denar na svoj bančni račun, plačajo položnice ali kupijo vrednostno kartico za enega izmed treh mobilnih operaterjev.

- V Sloveniji trenutno deluje okoli 1.814 bankomatov[10].
- Kreditne kartice, kartice z odlogom plačila in debetne kartice: bistvo kartice z odlogom plačila je zamik plačila. Imetnik kartice lahko preko celega meseca s takšno kartico plačuje, ne da bi imel za to razpoložljiva stanja na svojem bančnem računu. Ta stanja pa mora imeti na dan, ko ga banka bremeni za vsa opravljena plačila. Ta datum je določen ob sklenitvi pogodbe med komitentom banke in banko.
- Tudi kreditna kartica ima zamik plačila. Za opravljeno transakcijo se račun bremeni postopno. Gre za nekakšno obročno odplačevanje. Višina in število obrokov je odvisno od zneska plačila, ostale pogoje pa določa banka izdajateljica.
- Debetna kartica je identifikacijska kartica računa imetnika. Z njo lahko imetniki plačujejo ali dvigujejo gotovino, njihov račun pa je obremenjen takoj.
- S kartico z odloženim plačilom, kreditno ali debetno kartico lahko komitenti banke plačujejo na POS terminalih ali preko plačilnega dokumenta - slipa. Bistvena razlika je v tem, da imajo POS terminali kontrolo stanja na računu oziroma kontrolo dovoljenega dnevnega in mesečnega limita in kontrolo morebitnih zapor računa ali kartice. Tako npr. komitenti ob pomanjkanju stanja na računu na POS terminalih ne morejo plačevati z debetno kartico, pri papirnih dokumentih pa je kontrola slabša. Trgovci in ostali, ki sprejemajo kartico, si lahko pomagajo s papirno ali elektronsko STOP listo, ki pa se v praksi redko kontrolira.
- Ostali plačilni nalogi: nalogi majhnih plačil se lahko izvedejo tudi preko Interneta ali na kak drug način preko komunikacijskega omrežja.
- Trgovinske kartice: izdaja kartic trgovskih podjetij bistveno zaostaja za izdajo bančnih kartic. V bistvu gre le za boljše pogoje kreditiranja ali druge oblike bonitet (npr. popusti).

1.5 Žiro kliring

Z omenjenimi instrumenti plačujemo manjše zneske, zato se le-ti zaradi prevelike količine in velikih stroškov banke ne izvršijo posamezno, temveč se zbirajo in nato izvršijo v skupnem znesku. Vsako plačilo gre tako skozi tri faze plačilnega sistema.

[10] Bilten Banke Slovenije marec 2011

- Prenos: v prvi fazi se v klirinškem centru zbirajo plačilni nalogi, ki jih predložijo ali pošljejo plačniki. V ta center lahko nalogi pridejo v papirni obliki, v obliki magnetnega zapisa ali po elektronski poti. Ko se nalogi preverijo, se prenesejo v centralno enoto banke.
- Kliring: zbrani in preverjeni plačilni nalogi se razvrstijo po računih bank. Vse odobritve in bremenitve, ki jih nalogi predstavljajo, se seštejejo oziroma odštejejo. Ta seštevek, imenujemo ga neto pozicija, se nato pošlje ustrezno banki oziroma drugemu prejemniku.
- Poravnava obveznosti preko poravnalnega sistema

Poznamo dve vrsti žiro kliringa. Pri bilateralnem udeleženka sama poravna svoje obveznosti, pri multilateralnem pa pri tem sodeluje poravnalni agent.

1.6 Sistem BPRČ

V Sloveniji je od leta 1998 za velika plačila vzpostavljen sistem BPRČ, ki deluje na multilateralni osnovi. Gre za sistem, v katerem se plačila poravnavajo na individualni osnovi, neposredno po sprejemu, če so na poravnalnem računu zadostna sredstva. Pri tem velja, da so vsa plačila, ki so bila izdana v višini kritja na račun, tudi dokončna s simultanim knjiženjem plačila v breme in v dobro poravnalnih računov. Dokončnost plačila ima svoje posledice pri obeh neposrednih udeleženkah prenosa sredstev.

Pošiljateljica naloga, ki je dokončen, ne more več preklicati, prejemnica pa lahko takoj odobri račun komitenta za znesek plačilnega naloga, saj ve, da tovrstna transakcija ne more biti razveljavljena. (Pukmajster, 2001: 18)

Seveda mora biti za vsako transakcijo na računu plačnika denarno kritje. V nasprotnem primeru banka počaka z obremenitvijo, dokler denarna sredstva ne pridejo. S tem lahko seveda pride do neželenih zamudnih obresti.

Sestavljen je iz dveh komponent (Pukmajster, 2001: 19):

- Central Accounting Sistem (CAS), ki omogoča izvršitev poravnave ter knjigovodsko obdelavo posredovanih plačilnih nalogov,
- S.W.I.F.T., ki zagotavlja komunikacijo med neposrednimi udeleženkami.

Elektronsko poslovanje med bankami poteka že nekaj časa. Izoblikovalo se je mednarodno omrežje bančnih organizacij, ki omogoča hitro in nemoteno opravljanje transakcij med bankami v različnih državah po svetu. Kreditne banke so za opravljanje plačilnega prometa s tujino leta 1973 ustanovile Society of Worldwide Interbank Financial Telecommunication (S.W.I.F.T.)[11], v katero je danes včlanjenih okoli 4000 v 95 državah. Preko mreže za prenos podatkov, ki jo vzdržuje ta družba, se odvija brezpapirna izmenjava podatkov po vsem svetu. S clearingom opravljenih borznih poslov je racionalizacija v kreditnih poslih, poleg plačilnega prometa, zajela tudi področje vrednostnih papirjev.

Stroške, ki jih ima banka z opravljanjem plačilnega prometa, zaračuna komitentom po posebni tarifi. O nastalih stroških obvešča lastnike računov praviloma mesečno. Pošlje jim obvestilo o obremenitvi računa zaradi stroškov plačilnega prometa.

1.7 Informatizacija bančnega poslovanja

Elektronsko poslovanje v podjetjih je obstajalo že pred nastankom interneta. Že v 60. letih prejšnjega tisočletja so v podjetjih preko informacijske tehnologije menjavali naročila, dobavnice,fakture in druge dokumente. Sodelovanje med različnimi podjetji je pripomoglo k temu, da se je razvila računalniška izmenjava podatkov (RIP) (Gradišar, 2003, str. 21).

Elektronsko poslovanje je takšno poslovanje, kjer stranke poslujejo med seboj elektronsko, ne pa fizično in tudi niso v fizičnem stiku. Elektronsko poslovanje (Gradišar, 2003, str. 20, 21) je pomembno predvsem na štirih področjih:

- povezovanje med potrošniki in organizacijami
- notranjem poslovanju v organizacijah
- poslovanju med večimi organizacijami
- poslovanju državne administracije med seboj in z občani.

Razvoj elektronskega poslovanja v bančništvu je sledil razvoju na ostalih področjih, pri čemer so bile prednosti v tem, da je zaradi velikega obsega poslovanja bank, kot velikih institucij,

[11] S.W.I.F.T. – omrežje bančnih organizacij

strošek uvajanja informacijskih sistemov pomenil manjšo obremenitev, saj je uvajanje elektronskega poslovanja do uvedbe interneta pomenilo visok strošek in so si ga lahko privoščile samo velike organizacije (Gradišar, 2003, str. 22-23).

Tehnizacija in avtomatizacija bančnega poslovanja sta bili v začetku pomembni z ekonomskega vidika, omogočili sta racionalnejšo organizacijo delovnih postopkov; sledilo je izboljšanje servisa in marketinga. Sočasno so povečanje zmogljivosti pomnilnikov in boljša komunikacija med bankami podatkov, večje možnosti nabave in obdelave podatkov in razvoj ustreznih programskih orodij prispevali h kakovostnejši dokumentaciji, na kateri je temeljilo odločanje managementa (Enders, 1994, str. 4-9).

Za pretekla štiri desetletja beležimo naslednje štiri razvojne stopnje:

1. uporabo elektronske obdelave podatkov (EOP) pri opravljanju množičnih poslov
2. izboljšanje komunikacije znotraj banke in podpora stikom s strankami s pomočjo sistemov EOP
3. samopostrežne bankomate za stranke
4. komunikacijo s strankami in sodelavci preko elektronskih medijev.

Pogoj za začetek delovanja Evropske monetarne unije 1. januarja 1999 je bil enoten plačilni sistem. V ta namen so pod oznako TARGET (Transeuropaeisches Automatisiertes Echtzeit Brutto Ueberweisungssystem) povezali in razvijali nacionalne sisteme. TARGET je v začetku ponujal storitve plačilnega prometa, ki glede hitrosti ustrezajo najmanj tistim, ki so bile običajne na ravni posameznih držav. (Glogovšek J., 2008, str. 262).

Zaradi nekaterih slabosti, kot je bila nestandardizirana oblika podatkov in kompleksnosti, pride do nadaljnjega razvoja, ki se usmeri na (Škrlec I. 2002, str. 18):

1. natančno določeno obliko podatkov in dokumentov, ki se izmenjujejo med različnimi aplikacijami na podlagi natančno določenih standardov
2. lažja dostopnost in razumnost za širši krog uporabnikov, preprostost uporabe.

Internet je prav tako tudi znižal stroške komunikacije, odprl pot do novih oblik poslovanja, novih storitev, omogočil osvojitev novih trgov, povečal učinkovitost, omogočil hitrejšo poslovanje in globalno povezanost sveta na področju ekonomskega poslovanja. V zgodovini človeštva je elektronsko poslovanje inovacija, ki je prinesla največ koristi za človeštvo, tako za organizacije, posameznike in družbo kot celoto (Gradišar M., 2005, str. 148).

Uvajanje bančnih avtomatov je bil prvi korak k samopostrežnemu bančništvu. Ta pojem razumeva opravljanje bančnih storitev brez prisotnosti bančnega uslužbenca. Uvajanje bančnih avtomatov se je v Evropi začelo v sedemdesetih letih prejšnjega stoletja, v Sloveniji pa je prvi bančni avtomat dvajset let kasneje postavila Nova Ljubljanska Banka. Zaradi njihove uporabnosti in priljubljenosti pri komitentih je do danes njihovo število naraslo na skoraj dva tisoč (Kos G., 2007, str. 40).

Kljub številnim drugim storitvam, ki jih lahko opravimo na bankomatu, je dvigovanje denarja še vedno najpogostejša storitev, ki jo uporabljajo komitenti na bančnem avtomatu. Sledita poizvedba o stanju in nakup dobroimetja za predplačniške telefone. Raziskava World Paymants Report iz leta 2007 je pokazala, da smo v Sloveniji po številu dvigov gotovine na bančnih avtomatih v zgornji polovici med državami EU, po višini dvignjenih sredstev pa na zadnjem mestu (Cerar G., 2004, str. 37).

Razmah je doživel tudi postopek elektronskega plačevanja blaga in storitev na Point of Sale (POS) terminalih. Na mestih, kjer je velika koncentracija ljudi in trgovin (nakupovalna središča), so instalirane naprave, ki omogočajo plačevanje računov na osnovi kreditne ali bančne kartice, s podpisom imetnika ali z vnosom identifikacijske številke (Berndt H., 1995 str. 369 – 372).

V Sloveniji je bila prva POS transakcija opravljena 24.05.1994 na Banki Koper. Do konca leta 1994 je bilo nameščenih že okoli sto POS terminalov[12]. Po podatkih Banke Slovenije je bilo na začetku leta 2008 pri nas že 33.815 POS terminalov[13]. Ti so v lasti domačih in tujih

[12] Povzeto po: (http://www.activa-card.com/pametnaKartica/zgodovina.asp?content=05).

[13] Bilten Banke Slovenije, junij 2009: Letnik XVIII št. 6

bank, pod določenimi pogoji, zapisanimi v pogodbah s prodajnimi mesti, pa jih oddajo trgovcem v uporabo. Določila pogodb med bankami in prodajnimi mesti so poslovna skrivnost (Šalamun A.,2007, str. 18).

V prvi polovici 90-tih let se je pričela era komunikacije med banko in stranko prek elektronskih medijev. Kreditne banke so najprej dajale poudarek možnostim plačilnega prometa in pozneje tudi prodaje močno standardiziranih storitev preko telefona in telefaxa, od leta 1995 dalje pa je vsa pozornost namenjena v »homebanking« s pomočjo osebnih računalnikov (Lunt P. 1995, str. 36 – 45).

V ZDA so ta razvoj najprej prepoznali kot možnost za prodajo bančnih storitev predvsem zato, ker je imel tipičen lastnik internetnega priključka (star praviloma med 20 in 40 let) praviloma visoko izobrazbo in nadpovprečne dohodke. (Lunt P. 1995, str. 36 – 45).

Prva banka, ki je bila prisotna izključno na internetu, je bila Security First Network Bank, ki je pričela delovati v oktobru 1995. Uporabnik PC »vstopi« v to ustanovo skozi grafično bogato opremljen »virtualni« vhod v banko, ki v resnici sploh ne obstaja. Z vnosom tajne številke gre mimo varnostnikov in pri okencu pusti sporočilo, prikliče informacije, naroči čeke ali da nalog za nakazilo. Če ima pritožbo, ga sprejme – simulirani – direktor banke v svoji pisarni. (Lunt P. 1996, str. 29).

Danes ima večina bank v svetu in tudi pri nas možnost komunikacije med banko in uporabnikom preko interneta. Poleg spletnih strani, ki jih imajo banke na internetu, ima velika večina bank tudi možnost priklica informacij, izmenjave informacij in sprožitve obdelave podatkov na daljavo s strani komitenta. (Duclaux D. 1996, str. 20 – 22). Med prvimi bankami, ki so uvedle »online banking« po internetu, je bila Stadsparkasse Dortmund. Tudi v tem primeru so bili računi koncipirani samo za transakcije po telefonih in preko bančnih avtomatov, a so delovanje že v letu 1996 razširili na internet.

Prvi problem uvajanja »online bankinga« po internetu so veliki začetni stroški, saj naj bi samo koncepcija, implementacija in zagon informacijskega sistema na svetovnem spletu stala približno 100.000 US$, poleg tega pa so visoki tudi mesečni obratovalni stroški. Za oblikovanje internetne banke z možnostjo transakcij so ocenjeni stroški približno 1,5 mio. US$, tekoči mesečni stroški pa znašajo približno 100 – 300.000 US$, kar pa predstavlja le delček fiksnih stroškov razvejanega sistema podružnic. Drug problem za bančno organizacijo je zagotavljanje varnosti v elektronskem poslovanju, saj je teoretično možno z vsakega računalnika, priključenega na internet, prebrati vse občutljive podatke o računu. Zaradi tega se podatki na začetku komunikacije najprej kodirajo in v tej obliki pošljejo prejemniku, kjer se najprej dekodirajo in nato obdelajo. (Birkelbach J. 1996, str. 40).

Ponudniki elektronskih storitev na področju bančništva morajo upoštevati predvsem želje in zahteve strank in razvitost tehnologije v posamezni regiji, državi. Zato je potrebno upoštevati naslednja dejstva (Bračun F. 1997, str. 150):

- uporabniki želijo storitve opravljati kjerkoli, kadarkoli, na kakršenkoli način
- uporaba tehnologije, ki jo stranke že imajo (brez vsiljevanja lastne)
- stanje telekomunikacijske infrastrukture v Sloveniji
- kakšno povezavo želi banka vzpostaviti s komitentom
- kakšni so dolgoročni in kratkoročni učinki
- zaupanje uporabnikov v storitev
- najvišja mogoča stopnja varnosti
- ciljna skupina uporabnikov.

Nove možnosti komunikacije ne nudijo samo tehnične osnove za stik med banko in stranko. Prav tako si je mogoče predstavljati, da bančni uslužbenci v svojem stanovanju opravljajo določene naloge in so z delodajalcem povezani preko svojega računalnika. Takšno delo na daljavo obeta večje možnosti za prosto časovno razporeditev in samostojnost zaposlenih, iz česar sledita večja motivacija in produktivnost. Tako so v Evropi sredi 90. let sprožili obsežne znanstvene iniciative za podporo ustreznim modelom projektov, vendar je bilo doslej v bankah odprtih zelo malo takšnih delovnih mest. (Brueckner M. 1997, str. 26).

1.8 Elektronsko bančništvo

Elektronsko bančništvo oz. elektronsko bančno poslovanje je področje, ki se je v zadnjih letih izjemno razvilo tako v svetu, še večji razvoj pa je v izjemno kratkem obdobju doživelo v Sloveniji. Elektronsko bančništvo za fizične in za pravne osebe se je pri nas od začetka reforme plačilnega prometa zelo razmahnilo. Pri nas v povprečju dve tretjini pravnih oseb že uporablja elektronsko bančništvo, pri nekaterih bankah pa elektronske transakcije že pokrivajo 90% vseh transakcij. Marsikdo ne razmišlja, da gotovina ni zastonj. Stroške, ki jih ima država z gotovino, plačamo davkoplačevalci preko dajatev državi. Po nekaterih podatkih naj bi stroški gotovine znašali okoli 0,5% BDP države. Slovenija je v zadnjih letih dosegala vrednost BDP nekaj na 30 mrd. evrov, kar pomeni, da bi cena gotovine znašala letno nad 150 milijonov evrov.

Razmah in razvoj tega področja v Sloveniji in tujini je prinesla izredno močna konkurenca na področju bančnih storitev, ob razvoju sodobne tehnologije, ki omogoča relativno varno poslovanje preko elektronskih bančnih poti. Na intenzivnost uvajanja elektronskega poslovanja vplivajo konkurenca, vrsta dejavnosti, stopnja razvitosti organizacije, stopnja razvitosti okolja, države, potrošnikov in znanje ter osveščenost o elektronskem poslovanju (Pucihar A., Gričar J. 2000, str. 209).

Tudi vlada ima pomembno funkcijo pri razvoju elektronskega bančništva. Pri nas žal z njeno vlogo, predvsem na področju uporabe, ne moremo biti zadovoljni[14]. Storitve e-uprave naj bi bile dostopne vsem državljanom enostavno in učinkovito tudi z vidika uporabe plačilnih instrumentov. V pripravljenosti in razvoju e-uprave se Slovenija uvršča v svetu na 26. mesto in v Evropi na 17. mesto, kar je relativno dober rezultat. Žal pa smo na področju možnosti plačil online storitev na 43. mestu na svetu (www.unpan.org). Uporabniki nekaterih storitev državne uprave pri nas so celo diskriminirani s provizijo, ki jo morajo plačati, če uporabijo plačilno kartico (Nabergoj, 2007).

Elektronsko poslovanje pomeni prehod iz klasičnega načina poslovanja preko izmenjave informacij na papirju ali preko telefona v elektronsko obliko sporazumevanja in poslovanja.

[14] F.T. Hartman iz ECB na konferenci SEPA sistema Activa v Portorožu, 14.06.2007

Zajema celoto procesov, ki podpirajo trgovsko in poslovno dejavnost in vključujejo proizvajalce, prodajalce, ponudnike storitev, posrednike in potrošnike (Pavliha M. 2002, str. 24).

Glede na velik obseg pojma »elektronsko poslovanje« lahko njegova razlaga pomeni proučevanje iz različnih pogledov (Kalakota R. 1997, str. 3):

- Komunikacijski pogled: je prenos informacij, proizvodov in storitev preko telefonskih linij, računalniških omrežij ali drugih povezav.
- Poslovno – procesni pogled: v poslovni proces s pomočjo programskih orodij vnaša avtomatizacijo procesov in transakcij.
- Storitveni pogled: omogoča večjo učinkovitost poslovanja z nižjimi stroški, večjo ravnijo kvalitete in hitrejšo dobavo blaga ali izvedbo storitve.
- Povezovalni pogled: deluje v med seboj povezanih omrežjih.

Med ključne tehnološke elemente elektronskega poslovanja štejemo računalnik, programsko aplikacijo (rešitev) in komunikacije. Dodati je potrebno še organizacijo poslovanja, saj šele skupaj z njo osnovne tehnološke sestavine podpirajo cilje poslovnega sistema (Toplišek J. 1998, str. 5)

Elektronsko bančništvo lahko opredelimo kot kakršenkoli način poslovanja stranke z banko, ki poteka neodvisno od poslovanja poslovalnic bank ter temelji na informacijski tehnologiji in elektronskih medijih. V širšo razlago (Miš Svoljšak I. 1997, str. 12) vključujemo vse bančne storitve, ki se opravljajo po elektronski poti:

- bančne avtomate
- elektronsko bančništvo preko interneta
- telefonsko bančništvo
- mobilno bančništvo
- kartično poslovanje.

S pojmom elektronska banka lahko opredelimo način opravljanja bančnih storitev, ki jih lahko komitent banke opravi neposredno od doma, s svojega delovnega mesta, brez neposredne pomoči bančnega uslužbenca, kadarkoli, 24 ur na dan, 365 dni v letu. Elektronska banka nam med drugim omogoča, da pripravimo naloge za plačilo v naprej. Omogoča tudi prenos (izvoz in uvoz) podatkov iz računovodsko-knjigovodskih programov. Povezljivost tako pomeni prihranek časa in zmanjšuje možnost napak. (Pavlič G., 2004).

Bančno poslovanje vsebuje specifične dejavnosti, zaradi katerih so na tem področju zelo dobre možnosti za uvajanje elektronskega poslovanja (Cetinski A. 1999, str. 149):

- bančne storitve temeljijo na informacijah
- večina občanov mora uporabljati bančne storitve, kar pomeni razmeroma veliko komitentov za naše banke, ki so po svetovnih merilih sicer majhne
- banke omogočajo komitentom široko ponudbo storitev, od katerih so nekatere takšne, da jih mnogo strank koristi skoraj vsak dan ali dokaj pogosto.

Elektronsko poslovanje med stranko in poslovnim sistemom omogoča večji vpliv pri oblikovanju produktov, kako so produkti narejeni in način dostopa do njih. Govorimo o poslovanju med stranko in poslovnim sistemom, ki ga v primeru bančnega sistema imenujemo elektronsko bančništvo (Bračun F., Cetinski A. 1998, str. 144).

Da lahko ločimo storitve elektronskega bančništva od drugih, nestandardnih sistemov, jih določimo po naslednjih kriterijih (Kovačič M. 1997):

- neprekinjena dosegljivost 24 ur na dan
- dosegljivost 7 dni v tednu
- dosegljivost kjerkoli
- varnost
- popolna avtomatizacija.

Banke se morajo zavedati dejstva, da so zahteve strank različne. Poleg čim cenejših storitev želijo stranke predvsem preprost in hiter dostop do svojega denarja ter hitro in kakovostno

storitev, drugi spet še vedno dajo veliko na prijazno besedo bančnega uslužbenca, zato je želje strank potrebno spoznati. Elektronsko bančništvo ni bančna storitev, ampak samo distribucijski kanal, navdušenje nad njim pa bančnikom ne sme zamegliti pogleda, da ne bi pozabili na osnovno nalogo bank (Miš Svoljšak, 1998, str. 7). Obstaja več vrst elektronskega bančništva, vsaka pa je namenjena določenemu segmentu komitentov. Bistveni element je zagotavljanje varnosti elektronskega poslovanja.

Tudi projekt SEPA[15] daje pomembno mesto tako elektronskemu bančništvu, kakor še posebej kartičnemu poslovanju. Problemi namreč nastopajo pri čezmejnih plačilih zaradi različnih tarif in nacionalnih standardov, pravil, praks in procesorjev, ki nastopajo kot posledica razdrobljenosti. Za imetnika kartice pa so cilji SEPA jasni: možnost, da bo lahko lastno kartico kjerkoli v Evropi uporabil enako kot doma. Zaradi tega bo velika pozornost preobrazbi plačilnih sistemov namenjena prav vsem oblikam kartičnega poslovanja in povečevanju njegovega deleža na račun zmanjševanja gotovine[16] v obtoku. Pomembno vlogo pri tem ima seveda elektronsko poslovanje (Nabergoj, 2007).

V teoriji različni avtorji različno opredeljujejo pojem »elektronskega bančništva«. Tako ta pojem zajema ožje opredelitve, kamor spadajo osnovne storitve bančnega poslovanja, izvedene po elektronski poti ali pa avtorji govorijo o širši opredelitvi »elektronskega bančništva«, kamor štejejo zelo širok spekter bančnih storitev in poslov. Seveda so temo primerne tudi zelo stroge zahteve, ki opredeljujejo kvaliteto »elektronskega bančništva«.

1.9 Varnost v elektronskem poslovanju

Z razvojem informacijske tehnologije je izvrševanje kriminalnih dejanj postalo enostavnejše in bolj prikrito. Razvoj svetovnega spleta je omogočil, da vsakodnevno na različne elektronske naslove po vsem svetu roma ogromno različnih sporočil in ponudb, od katerih jih je veliko tudi takšnih, ki imajo namen pridobiti premoženjsko korist od naslovnika in ga oškodovati (Lamberger I., 2005).

[15] Single Euro Payments Area

[16] Spletna transakcija je stokrat cenejša od tiste na bančnem okencu

Po nekaterih ocenah bi naj internet vseboval 800 bilijonov dokumentov, od tega je 11.5 bilijonov vidnih dokumentov (surface web), ostalo pa so uporabniku nevidni dokumenti (deep web). Deep web (deep net, invisible/hiden web) vsebuje internetno vsebino, ki ni del vidne vsebine in predstavlja sam sistem interneta, zagotavlja obstoj interneta in njegovo delovanje ter delovanje iskalnih sistemov. Deep web vsebuje za okoli 95.000 terabytov podatkov, surface web pa samo okoli 7.500 terabytov. Vidimo, da je večina procesov in vsebin, ki se nahajajo na internetu, običajnemu uporabniku nevidna in nedosegljiva ter da ta nima dejanske možnosti vplivanja na delovanje nevidne vsebine ob uporabi vidne (Europol, 2006).

Skoraj vsak uporabnik interneta se skoraj dnevno sooča z različnimi oblikami ponudb, od katerih so nekatere tudi takšne, ki lahko pomenijo kriminalno dejanje, katerega žrtev postane uporabnik, če se na takšno ponudbo odzove. Število žrtev goljufij in drugih oblik kriminalitete, za katere se kot sredstvo storitve uporablja svetovni splet, je vedno večje (Power R. 1998). Zaradi širjenja kroga uporabnikov medmrežja in vključevanja novih uporabnikov se veča tako obseg kakor tudi raznovrstnost in nove oblike izvajanja računalniške in druge kriminalitete.

Pogoj za varnost sistemov je izdelava varnostne politike. Ko pride do motenj, je potrebno hitro in pravilno ukrepati in oblikovati skupino, ki bo pripravila in izvedla načrt okrevanja. Tako določimo in definiramo naloge, pooblastila in odgovornosti vsakega posameznika iz skupine, ki je odgovoren za varnost (Borak, 1997, str. 156).

Značilnosti učinkovite in pravilne varnostne politike morajo biti:

- omogočanje realizacije preko procesov sistemske administracije
- realizacija s sistemom varnostnih orodij ali s sistemom sankcij, če varnostna orodja niso možna
- definiranje odgovornosti uporabnikov in administratorjev (Cowichan, 2000, str. 16-19).

Razvite države poskušajo z dopolnjevanjem in prilagajanjem zakonodaje opredeliti nove vrste zlorab in jih tako sankcionirati in omogočiti kazenski pregon storilcev kaznivih dejanj.

Vzpostavitev enotnega območja plačil SEPA je obsežen projekt, ki ga lahko primerjamo s prevzemom skupne evropske valute. Na področju varnosti elektronskega bančništva želi SEPA s poenotenjem tehnične infrastrukture in standardov za izmenjavo podatkov olajšati in poceniti medsebojno varnostno povezovanje med bankami, procesorji in podjetji. V Sloveniji imamo od leta 2006 dogovor o podatkovnem standardu za elektronski plačilni promet, ki smo ga s projektom SEPA razširili z zahtevami SEPA CT 2.3 in ga imenujemo ZBSxml 2.0[17] in omogoča paketno izmenjavo podatkov med imetnikom računa in izvajalcem plačilnega prometa. Omogoča nespremenjen prenos podatkov o nalogu, kot ga je vpisal komitent. Pri kartičnem poslovanju je pretežni del kartic pri nas že v skladu z okvirjem SEPA, ki predpisuje varnejše čip kartice (Košir A., 2008)

Ponudnik elektronskega bančništva mora ponuditi primerno programsko in strojno opremo, ki zaščiti komitente pred nepooblaščenimi dostopi do podatkov in izvajanjem nedovoljenih transakcij (Vrešak S. 1997, str. 61).

Za zaščito uporabnika pred zlorabami so sistemi podatkovnih komunikacij zaščiteni z vrsto oblik zaščit med njimi so:

- gesla
- kriptografija
- elektronski podpis
- digitalni certifikati
- javni ključi
- varni protokoli in sistemi na internetu
- požarni zid.

Gesla

V današnjem času in z današnjo stopnjo razvoja tehnologije se povprečen občan z uporabo različnih gesel srečuje dokaj pogosto. Varovanje s sistemom gesel ne predstavlja zelo visoke stopnje varnosti, je pa najenostavnejši način identifikacije uporabnika in se pogosto uporablja kot zaščita dostopa do varovanih podatkov. Problematična je izbira gesel, ki jih lahko uporabnik sam določi, ker zaradi obilice gesel, ki jih ponavadi uporablja na različnih sistemih

[17] Standard je javno objavljen in je za rabo na voljo brezplačno

dostopanja, izbira gesla, ki si jih lažje zapomni, oz. so v določeni povezavi z njegovim imenom ali imeni sorodnikov. Zaradi tega je tudi odkrivanje teh gesel lažje oz. je možnost zlorab večja. Razkrivanje uporabnikovih gesel navadno poteka na podlagi poznavanja njegovih podatkov, že uporabljenih gesel in elektronskih slovarjev. Ob identifikaciji z geslom se uporabnik razkrije ter na ta način omogoči naslovniku izdajanje z njegovim geslom, prav tako pa so gesla navadno nešifrirana, uporabnik pa izbira enaka gesla tudi pri identifikaciji na drugih sistemih (Bobek, S., 1993).

Kriptografija

Po internetu se prenaša množica podatkov, ki pa niso namenjeni vsakemu uporabniku. Zaradi tega je potrebno podatke tako zaščititi, da jih bo lahko prebral le tisti, kateremu so namenjeni. To se doseže s šifriranjem podatkov (enkriptiranjem podatkov) na strani pošiljatelja, na strani prejemnika pa moramo podatke dešifrirati (dekriptiranje) (Bedjanič B., Lorenz K. 1997, str. 58). Za šifriranje in dešifriranje imajo pri elektronskem bančništvu svoj ključ tako banka kot tudi vsak posamezen komitent. Poznamo javne in zasebne ključe. Javni ključ se uporablja za šifriranje podatkov, zasebni ključ pa za dešifriranje.

V grobem kriptografijo delimo na:

- simetrično
- in asimetrično.

Klasične kriptografske metode so primerne in uporabne samo za razumevanje osnovnih pojmov in njihovega delovanja, vendar pa jih je z uporabo računalnika lahko razbiti. Zato poznamo zelo učinkovite kriptografske metode, ki so prilagojene za uporabo v računalniških komunikacijah (Vidmar, T., 2002, str. 550-554).

Sprva se je uporabljala samo **simetrična kriptografija**, ki uporablja en sam skrivni ključ za šifriranje in dešifriranje, kjer pa prihaja do težave pri varni razdelitvi šifrirnega ključa med uporabnike oz. upravičence. Pošiljatelj mora vedno za vsakega upravičenca vedeti, kje se nahaja skrivni ključ, kar pa iz vidika varnosti predstavlja nevarnost prestrezanja in dešifriranja sporočila. Prednost simetričnega šifriranja proti nesimetričnem je v njegovi hitrosti šifriranja. Zaradi tega se navadno uporablja v kombinaciji z drugimi algoritmi. Na področju bančništva je tako najbolj poznan in razširjen sistem oziroma algoritem SET (Secure Electronic Transaction).

Simetričen sistem uporablja en sam zasebni ključ, ki ga poznata pošiljatelj in prejemnik. S tem ključem pošiljatelj sporočilo šifrira, z enakim ključem pa ga prejemnik dešifrira. Pomanjkljivost simetrične kriptografije je ta, da lahko nekdo ključ ukrade med pošiljanjem (Gradišar M., 2003, str. 268).

Asimetrična kriptografija ali kriptografija javnih ključev pa temelji na konceptu dveh ključev oz. paru ključev, pri čemur je en ključ namenjen šifriranju, drugi pa dešifriranju sporočila. Taka ključa imenujemo par asimetričnih ključev. Za izvedbo komunikacije mora vsak uporabnik posedovati dva ključa: zasebni ključ in javni ključ. Medtem, ko je zasebni ključ shranjen varno pri uporabniku, se javni ključ navadno nahaja na strežniku in je tako dostopen vsakomur. Ključa sta sicer matematično sorodna, a se razlikujeta v tolikšni meri, da je na podlagi poznavanja enega nemogoče odkriti drugega. Pošiljatelj zaupno sporočilo šifrira z naslovnikovim javnim ključem, ta pa ga dešifrira s svojim zasebnim ključem. Prednost pred simetrično kriptografijo je predvsem v tem, da se lahko javni ključ brez strahu pred zlorabo pošilja osebam ali sistemom, s katerimi želimo komunicirati. Strah pred prestrezanjem in zlorabo je odveč, saj tudi v primeru prestrezanja javni ključ brez zasebnega ključa nima posebne uporabne vrednosti. Slabost asimetričnih sistemov šifriranja pa je v hitrosti šifriranja, ker je nekajkrat počasnejše od simetričnega šifriranja, zato se v praksi uporablja hibridni pristop. Pri elektronski pošti se podatki šifrirajo z naključnim simetričnim ključem, sam ključ pa se šifrira še z javnim ključem prejemnika. Zagotavlja nam celovitost, zaupnost, nezatajivost sporočila in preverjanje identitete pošiljatelja (SET Business Description, 1997).

Asimetrično šifriranje je bolj varno od simetričnega, saj uporablja dva šifrirana ključa, javnega in zasebnega, ki nista enaka. Zasebni ključ je poznan samo lastniku, javni ključ pa je na voljo vsem dopisnikom. Sporočilo, ki je šifrirano z zasebnim ključem, dešifriramo z javnim in obratno. Sistem javnih ključev omogoča tudi elektronski podpis (Gradišar M., 2003, str. 268).

Elektronski podpis

Poznanih je mnogo oblik elektronskega podpisovanja. Enostavni elektronski podpis, ki temelji na metodologiji simetričnih ključev, ne zagotavlja visoke stopnje varnosti. Takšni podpisi, ki so ustvarjeni z elektronsko tehnologijo, ne omogočajo neokrnjenosti podpisanega

dokumenta in identifikacije podpisnike, kar omogočajo digitalni podpisi (Toplišek J., 1998, str. 30).

Istovetnost elektronskega in lastnoročnega podpisa zagotavljamo z naslednjimi zahtevami:

- avtentičnost
- ni možnosti ponarejanja
- ni možnosti kopiranja
- ni možno spreminjanje vsebine podpisanega dokumenta
- ni možno zanikanje podpisnika dokumenta.

Bistvo elektronskega podpisa je v tem, da dokument podpisujemo s svojim zasebnim ključem, podpis pa se preverja z javnim ključem podpisnika.

Proces digitalnega podpisovanja se začne z izdelavo matematičnega seštevka prvotnega sporočila. Ta zagotavlja, da ob spremembi besedila seštevek ni več enak in da iz njega ne moremo več kreirati besedila (Osojnik M., 2002, str. 125-126).

Elektronski podpis je funkcionalno enak pravemu podpisu in se ga zakonsko enako obravnava. Temelji na sistemu javnih ključev (Gradišar M., 2003, str. 268-270).

Digitalni certifikati

Kriptografija javnih ključev temelji na uporabi dveh ključev, javnega in zasebnega, katere lahko ustvarimo sami, z uporabo programov za elektronsko pošto ali internetnim brskalnikom. Ko ustvarimo ključa, poskrbimo za zaščito zasebnega ključa, javni ključ pa pošljemo osebam, s katerimi želimo komunicirati. Tak način izdelave in pošiljanja ključev pa ni najboljši, saj postopek ne zagotavlja verodostojnosti pošiljatelja. Par ključev lahko izdela druga oseba, ki se naslovniku lažno izdaja za znanega pošiljatelja.

Za zagotavljanje varnosti in preprečevanje zlorab verodostojnosti je zastavljen postopek overjanja javnih ključev pri uporabi asimetrične kriptografije. Overjanje opravijo agencije za certificiranje javnih ključev, katere izdajo lastniku javnega ključa digitalno podpisano potrdilo – certifikat. S tem se drugim uporabnikom v zadostni meri zagotavlja verodostojnost ključa. Če certifikat od izdaje ni bil spremenjen ali preklican, ga lahko uporabimo. Digitalno potrdilo

je kopija javnega ključa in predstavlja digitalni identifikacijski dokument (Makarovič B., 2001, str. 48-49). Digitalni certifikat vsebuje podatke o:

- verziji formata certifikata
- serijski številki certifikata
- identifikatorju algoritmov
- izdajatelju certifikata
- veljavnosti certifikata
- lastniku javnega ključa
- javnem ključu in lastniku
- enolični oznaki uporabnika
- razširitvah
- namenu uporabe in
- digitalnem podpisu podatkov, narejenim z zasebnim ključem.

Agencije za certificiranje javnih ključev so lahko ustanovljene s strani komercialne organizacije ali pa s strani vladne ustanove. Agencija mora imeti zasnovano tudi bazo preklicanih in neveljavnih certifikatov, kjer se uporabljeni certifikati preverjajo . V Sloveniji za potrebe javne uprave in projekt e – poslovanja izdaja digitalna potrdila in skrbi za certificiranje javnih ključev Center Vlade RS za informiranje (CVI), ki izdaja dve različici digitalnih potrdil (Jerman Blažič B., 2001):

- SIGEOV – CA (Slowenian Governmental Certification Authority), ki je namenjena uporabi v javni upravi in
- SIGEN – CA (Slowenian General Certification Authority), ki je namenjena pravnim in fizičnim osebam za poslovanje z organi javne uprave.

Infrastruktura javnih ključev

Infrastruktura javnih ključev (PKI – Public Kay Infrastructure) pomeni sistem za upravljanje s ključi in digitalnimi potrdili. Sestavlja ga kombinacija strojne in programske opreme ter politika in pravila certificiranja. Osnovna naloga je omogočanje varnega elektronskega poslovanja uporabnikov, ki si medsebojno niso poznani, želijo pa medsebojno komunicirati. Gre za sistem programske in strojne opreme in jasno postavljenih pravil certificiranja. Osnovni namen je zagotavljanje varnega elektronskega poslovanja med uporabniki, ki se med seboj ne poznajo. Temelji na uporabi digitalnih certifikatov, s katerimi se potrdi uporabnikov

elektronski podpis in njegov javni ključ. Sistem z uporabo asimetrične kriptografije lahko združuje sisteme za certificiranje, agencijo za registracijo in sistem distribucije certifikatov. Agencija za registracijo opravlja vlogo posrednika med uporabnikom in agencijo za certificiranje in preverja pristnost podatkov prosilca za izdajo certifikata. Če ugotovi, da ni nobenih zadržkov, posreduje podatke agenciji za certificiranje, ki na podlagi obstoječega zaupanja izda certifikat.

Obstajajo tudi protokoli za zaščito transakcij v javnem omrežju. Najpogostejši so:

- SSL (Secure Sockets Layer)
- TLS (Transport Layer Security)
- WTSL (Wireless Transport Layer Security).

Vsem je skupna vzpostavitev varnih kanalov med strežnikom in brskalnikom. V uporabi pri elektronskem bančništvu in pri elektronskih bančnih sistemih je najpogosteje uporabljen protokol SSL, kateri je sestavni del brskalnikov Internet Explorer ali Netscape. Uporabo SSL in TLS uporabnik lahko prepozna po predponi odprte internetne vsebine, ko standardno predpono http nadomesti predpona https, določeni sistemi prikažejo uporabo varnega kanala z rumeno ključavnico v okencu. To se ponavadi zgodi pri odpiranju bančnih dostopnih sistemov (Europol, 2006).

Varni protokoli in sistemi na internetu

Zagotavljanje varnosti na internetu poteka na različnih ravneh, navadno na aplikacijski, transportni ali omrežni ravni. Aplikacijski način zagotavljanja varnosti je način zagotavljanja varnosti, ko že sama aplikacija vsebuje varnostne mehanizme, pri transportnem in omrežnem načinu pa je varnost zagotovljena z vzpostavitvijo varnih komunikacijskih kanalov, ki zagotavljajo zaupnost podatkov in preverjanje identitete.

Najbolj pogosto uporabljena metoda je vzpostavljanje navideznega zasebnega omrežja znotraj javnega omrežja, kot je internet. Uporaba javnega omrežja je z vidika vloženega denarja veliko bolj ekonomična, saj ni potrebna izgradnja zasebnega omrežja. Izmenjava podatkov med oddaljenimi računalniki poteka v šifrirani in digitalno podpisani obliki. Na ta način je zagotovljena neokrnjenost, overjanje podatkov in zaupnost.

Opisan protokol SSL zagotavlja varen prenos podatkov, ne zagotavlja pa varnosti strežnikov ali brskalnikov oziroma ne preprečuje vdorov. Tako npr. pri spletnem nakupovanju uporabnik lahko varno pošlje svoje podatke o številki kartice, številki računa in datumu poteka kartice, ni pa zagotovila o varnosti njegovega brskalnika kakor tudi ne o varnosti strežnika in lahko le upa v poštenost trgovca in v njegov sistem varovanja podatkov pred zlorabami (SET Business Description, 1997).

Požarni zid

Požarni zid si lahko predstavljamo kot vratarja ali varnostna vrata, ki nepooblaščenim osebam preprečujejo vstop. Delujejo na različnih principih omejevanja dostopanj. Lahko preprečujejo dostopanje v uporabnikov sistem od zunaj, omogočajo pa komuniciranje iz smeri uporabnikovega sistema navzven, lahko pa dovoljujejo samo določene operacije, npr. dovoljujejo samo promet elektronske pošte ipd.

Požarni zid je eden izmed ukrepov za zagotavljanje varnosti elektronskega poslovanja. Nameščen je med organizacijo, ki zaposlenim omogoča elektronsko poslovanje in internetom. Prepušča le promet, za katerim se ne skrivajo zlonamernosti (Tulloch M., 2005, str. 183).

Ponavadi pa požarni zidovi ne preverjajo prisotnosti virusov v podatkih in tudi ne omejujejo zlorab pooblaščenih uporabnikov omrežja. Tako lahko pooblaščeni uporabniki za dostopanje operirajo s podatki in jih tudi zlorabijo. Delujejo lahko na omrežni ravni, pri čemer ugotavljajo IP naslov in številko protokola in na podlagi tega dovoljujejo komunikacijo ali pa delujejo na aplikacijski ravni. V tem primeru so postavljeni v posebej za to namenjene proxy strežnike, kateri se nahajajo med zasebnim zaščitenim omrežjem in internetom in preprečujejo direktni pretok informacij. Strežnik prestreže IP naslov in spusti informacijo samo pooblaščenim uporabnikom (Šavnik J., 2007).

Požarna pregrada je namenjena preverjanju podatkov, ki se prenašajo med internetom in lokalnim omrežjem. S filtrom se nad podatki izvedejo opravila v skladu z varnostno politiko in navodili administratorja. Podatki se filtrirajo glede na uporabniška imena, IP naslove pošiljateljev, prejemnika, imenih domen in številkah komunikacijskih vrat (Kalakota R., 1997, str. 125).

1.10 Nepravilnosti v plačilnem prometu

Pri tako velikem številu opravljenih transakcij v plačilnem prometu se pojavljajo napake in neredko tudi kriminalna dejanja. Kriminaliteto lahko delimo na tisto, ki jo storijo uslužbenci finančnih institucij in tisto s strani komitentov banke oziroma drugih finančnih institucij. Obe pa je prav zaradi množičnih transakcij težko odkriti.

Za preprečevanje kriminalitete komitentov, fizičnih oseb, pri sklepanju različnih kreditnih pogodb, so banke in hranilnice v R Sloveniji s 1.1.2008 uvedle elektronski informacijski sistem SISBON. Ta omogoča medsebojno izmenjavo in obdelavo osebnih podatkov o komitentih - fizičnih osebah med bankami in hranilnicami, podpisnicami Dogovora o postavitvi in uporabi informacijskega sistema SISBON. V informacijskem sistemu se zbirajo in obdelujejo podatki, ki se nanašajo na zadolženost in korektnost izpolnjevanja pogodbenih obveznosti fizičnih oseb posameznikov in so dodatna informacija za določitev njihove kreditne sposobnosti, od katere je odvisna odobritev posla in določitev pogojev za posamezno storitev, s tem pa se seveda zmanjša tudi izpostavljenost kreditodajalca pri sklepanju poslov s prebivalstvom (Lamberger I., 2008). Za preprečevanje kriminalitete pravnih oseb se uporabljajo drugi načini preverjanja bonitet.

Računalniški kriminal je splošen izraz za uporabo računalniških sistemov pri nezakonitih dejanjih. Takšen kriminal spada med gospodarsko kriminaliteto in gospodarstvu zadaja vedno večjo škodo (Gradišar M., 2003, str. 254).

Storilci kriminalnih dejanj na področju računalniške kriminalitete so različnih profilov in jih lahko razvrstimo v tri skupine: zaposleni v organizaciji, zaposleni izven organizacije in računalniški zagnanci, imenovani tudi hekerji. V računalniško razvitih okoljih je računalniški kriminal vedno večji problem in z leti narašča. Posredna in neposredna škoda, ki jo računalniški kriminal povzroča v svetu, pa znaša milijarde dolarjev (Gradišar M., Jaklič J., Turk T., 2007, str. 278).

Prav zaposleni so tisti, ki najbolj poznajo sitem plačevanja v bankah. Tako npr. vedo, katere transakcije in v kakšni količini se zgodijo v določenem času na določenem računu pravne osebe. Če gre za velike zneske, se majhni odtegljaji, ki jih uslužbenec lahko naredi dnevno,

pravni osebi prav gotovo ne bodo poznali, dokler ne bo prišlo do kontrole računa – do letnega poračuna. Namen zaposlenih pri tej vrsti kriminala je vsekakor pridobitev premoženjskih koristi. Zaradi tega poskušajo na različne načine poneveriti finančna sredstva drugih pravnih oseb in jih z navidezno transakcijo nakazati na svoje račune ali račune sorodnikov, zakoncev ali prijateljev (Lamberger I. 2001: 136).

Za preprečitev zlorab je nujen postopek avtentifikacije, ki potrjuje izvor plačilnega naloga. V ta namen je bil uveden elektronski podpis, zaradi katerega pošiljatelj ne more zanikati sporočil. Zaščita se nanaša tudi na uporabo sodobnih načinov za preverjanje identifikacije uporabnikov (avtorizacija) ter kodiranje podatkov pri prenosu (enkripcijo), ki preprečuje možnost spreminjanja elektronskih omrežij. (Pukmajster, 2001: 21)

2 PLAČILNE KARTICE

Brezgotovinsko poslovanje, ki ga omogočajo plačilne kartice, se je v sodobnem plačilnem prometu zelo razvilo in ponekod že presega gotovinsko plačevanje. Kreditne in plačilne kartice imenujemo tudi "plastični denar", saj se pojavljajo v obliki standardiziranih plastičnih kartic, z magnetnim zapisom. Magnetni zapis vsebuje vse podatke o imetniku kartice, banki izdajateljici in možnosti plačevanja in dvigovanja gotovine na bančnih avtomatih. Prav magnetni zapis predstavlja eno od slabosti "plastičnega denarja", saj zaradi nezadostne zaščite prihaja do raznovrstnih zlorab tega plačilnega instrumenta. (Lamberger, 2001: 57)

Banke izdajo večino plačilnih kartic v slovenskem prostoru (bančne kartice), in sicer samostojno ali na podlagi sklenjene licenčne pogodbe s tujim partnerjem. Podjetniške kartice izdajajo podjetja, prav tako samostojno ali na podlagi sklenjenih licenčnih pogodb. Nekatere kartice, izdane v Sloveniji, so uporabne samo v slovenskem prostoru (domače kartice), nekatere, izdane na podlagi licenčnih pogodb, pa je moč uporabljati tako v Sloveniji kot v tujini (licenčne kartice). (Šteblaj, 1999: 43)

Pri nas je stanje zelo podobno kot v tujini. Tudi v Sloveniji nekatere banke ponujajo gotovinsko uporabo plačilnih kartic, poleg tega pa imamo v Sloveniji trenutno 1814 bančnih avtomatov, razporejenih po celi Sloveniji[18].

Zaradi ugodnosti, ki jih nudijo plačilne kartice, so le-te že precej izrinile ček iz poslovanja. Po svoji naravi plačilna kartica ni vrednostna listina, je pa izkazni dokument. Z njeno predložitvijo se lastnik izkaže pri prevzemu blaga in z njo plača kupljeno blago. Dejansko v trenutku nakupa oziroma prevzema blaga do plačila še ne pride, kajti lastnik z njeno predložitvijo in podpisom potrdi prevzem blaga, prodajalec pa mora račun izstaviti izdajatelju kartice. Izdajatelj kartice plača račun prodajalcu in ga nato zaračuna lastniku kreditne kartice. Končno plača račun seveda lastnik te kartice, to je kupec (Odar, 1993).

2.1 Vrste plačilnih kartic

Plačilne kartice se delijo predvsem na debetne kartice (debit cards), kreditne kartice (credit cards) in kartice z odloženim plačilom. Zlasti kartice z odloženim plačilom so zelo uveljavljene kot pomemben način plačevanja (Logar, 1998, str. 108).

Kartice lahko razdelimo na skupine:

- Kartice kot plačilno sredstvo: v to skupino spadajo debetne kartice, ki ob izvedeni transakciji takoj obremenijo račun imetnika. Sredstva na računu so zmanjšana takoj ali v zelo kratkem času[19].
- Kartice kot vir financiranja: sem spadajo kartice, pri katerih lastnik obveznosti plačuje v določenih časovnih obdobjih, največkrat mesečno. Obstaja možnost, da pri poravnavi ne poravna vseh obveznosti naenkrat, ampak v več obrokih.
- Kartice za ugotavljanje istovetnosti: identifikacijske kartice, ki se uporabljajo za identifikacijo lastnika.

Glede na izvor in način izdaje kartic ločimo:

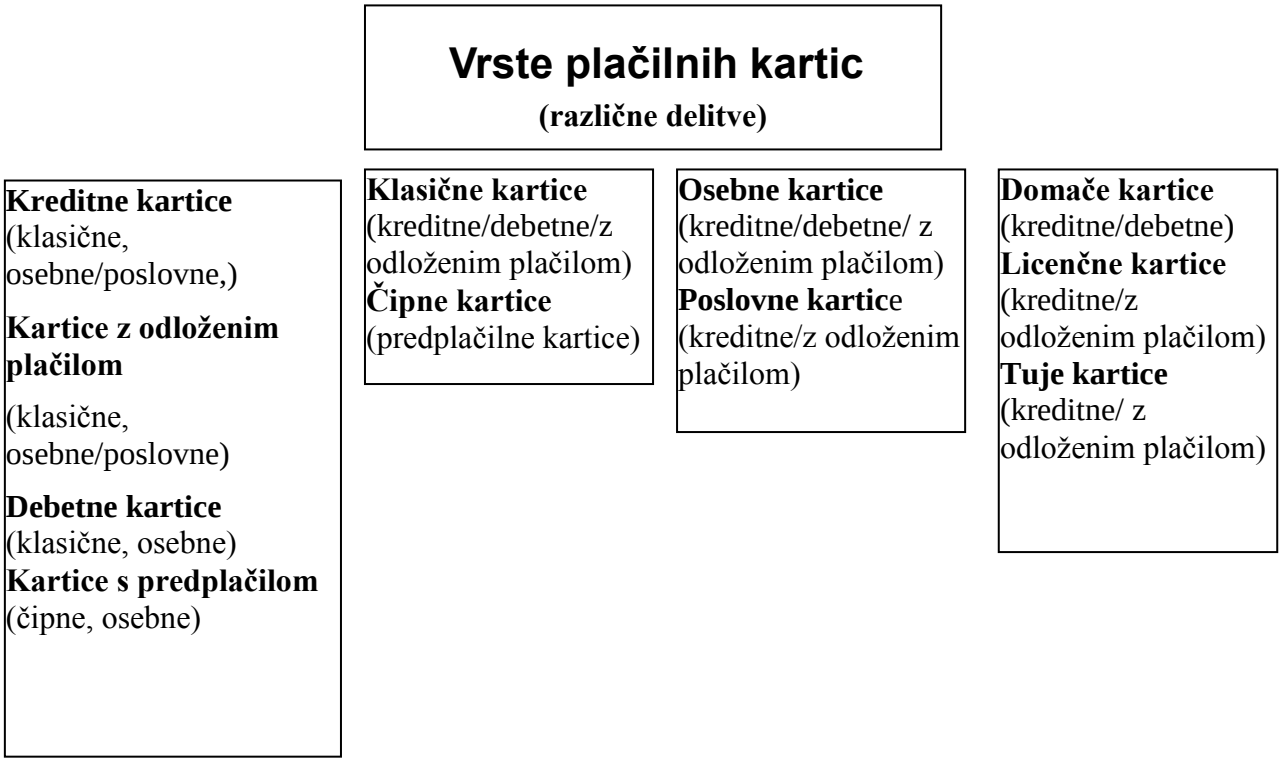
[18] Bilten Banke Slovenije, marec 2011

[19] Predolg čas od transakcije do obremenitve povečuje možnost zlorab

- domače kartice (Karanta, Activa, Magna…)
- tuje kartice (American Expres, Visa, Master Card, Diners)
- licenčne kartice, ki so lahko domače in tuje; pravico do izdaje takšne kartice dobi samo določena banka.

Iz sheme 1 je razvidna različna delitev kartic, in sicer glede na način plačila obveznosti, obliko kartice, lastnika in izdajatelja kartice.

Shema 1: Različna delitev plačilnih kartic



Debetne kartice

Debetne kartice omogočajo imetnikom, da z njimi plačujejo blago in storitve. Pri nas so se pojavile v letu 1997, ko so banke klasični identifikacijski funkciji plastične kartice dodale možnost izvajanja plačil na elektronskih terminalih. Plačila za nakupe takoj po izvršeni transakciji ali neposredno po njej bremenijo imetnikov račun pri banki, ki je kartico izdala. Debetna kartica je kartica, ki jo dobimo v banki ob otvoritvi računa. Združuje dve funkciji. Gre za nadomestilo čekovne kartice, ki je služila potrjevanju čekov - identifikacijska funkcija in dvigovanju gotovine na bančnih avtomatih - bankomatska funkcija. Debetna kartica nadomešča čeke, bankomatska funkcija pa ostaja enaka kot pri čekovni kartici. Novost debetne kartice v primerjavi s čekovno pa je predvsem v možnosti plačevanja na elektronsko opremljenih prodajnih mestih - POS terminali.

Za obročna plačila so se banke interesu komitentov prilagodile z drugimi načini plačil s karticami (posojilne kartice). Uporaba debetnih kartic v Sloveniji postopno narašča, vse več je prodajnih mest, ki debetne kartice sprejemajo (prodajna mesta morajo biti opremljena s POS terminali), prav tako pa uporabniki vse bolj spoznavajo prednosti brezgotovinskega načina plačevanja in uporabe kartice za dostop do gotovine na bančnih avtomatih (Šteblaj, 1999, str. 50).

Debetna kartica izvira iz bankomatne kartice, s katero se najlažje opravi dvig gotovine. Ker so banke želele omogočiti tudi enostavno plačevanja blaga in storitev, je prišlo do uvedbe debetne kartice, ki jih izdajajo vse banke v Sloveniji in jih je po številu tudi največ (Krivec V., 2008).

Tabela 3: S strani bank izdane debetne kartice v Sloveniji

Leto	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Št. (v1000)	1.496	1.708	2.469	2.310	2.330	2.412	2.498	2.627	2.611	2.742

Vir: Bilten BS, marec 2011

V tabeli št. 3 so prikazani podatki o gibanju števila izdanih debetnih kartic v Sloveniji. Iz podatkov vidimo, da število in s tem tudi uporaba debetnih kartic v Sloveniji zaradi razširitve ponudbe in funkcionalnosti še vedno narašča, minimalni padec števila kartic je razviden samo v letu 2009.

Skupaj s kartico prosilec pridobi tudi osebno geslo oziroma PIN kodo. Z debetno kartico in osebnim geslom uporabnik plačuje na prodajnih mestih, opremljenih s POS terminali. Na bankomatih obstaja možnost dvigovanja gotovine, opravljanja depozitov (polog gotovine in plačevanje položnic), preverjanja stanja na računu ali nakupa GSM kartice (kodirana števila). Vrednost izvedenih nakupov in transakcij bremeni imetnikov račun. Uporaba kartice je možna tudi pri elektronskem bančništvu, saj je transakcijski račun podlaga za uporabo storitev, ki jih elektronsko bančništvo omogoča z uporabo interneta in osebnega računalnika. Elektronsko bančništvo uporabljajo tako fizične kot pravne osebe.

Tabela 4: Število uporabnikov elektronskega bančništva in obseg poslovanja

	Število uporabnikov		Število transakcij v 1000			
	Fizične osebe in s.p.	Pravne osebe	Fizične osebe in s.p.		Pravne osebe	
Leto			Doma	V tujino	Doma	V tujino
2000	15.028	1.206	984	0	159	24
2001	63.440	14.091	3.403	0	6.900	93
2002	98.669	34.094	7.014	7	23.879	285
2003	142.334	41.592	9.520	12	31.002	410
2004	192.560	45.008	12.616	28	32.751	552
2005	261.928	48.543	15.957	73	33.642	709
2006	351.111	70.287	20.982	70	35.657	808
2007	407.210	61.995	24.735	108	47.205	974
2008	463.337	81.816	27.499	169	42.096	1.176
2009	509.572	96.401	29.867	173	40.585	1.116
2010	566.759	100.998	31.376	235	40.213	1.226

Vir: Bilten BS, marec 2011

Kot je razvidno iz tabele št. 4, se število uporabnikov elektronskega bančništva z leti povečuje tako pri fizičnih kakor tudi pri pravnih osebah. Podoben trend ima tudi število transakcij, kjer se je le pri pravnih osebah v letih 2008, 2009 in 2010 število transakcij doma zmanjšalo glede na predhodna leta. Razlog verjetno tiči v gospodarski in finančni krizi. Iz podatkov Banke Slovenije je razviden tudi porast vrednosti transakcij, izvedenih preko elektronskega bančništva. Tako je znašala vsota vseh transakcij, opravljena preko elektronskega bančništva, v letu 2009 skupaj kar 9.037 mio. evrov fizičnih oseb in s.p. in 141.275 mio. evrov pravnih oseb. V letu 2010 se je obseg transakcij fizičnih oseb in s.p. povečal na že 9.156 mio. evrov, pri pravnih pa padel na 140.187 mio. evrov.

Tabela 5: Število bančnih avtomatov, število in vrednost transakcij

Leto	Št. bančnih avtomatov	Št. dvigov (v 1000)	Vrednost dvigov (v mio. EUR)
2000	865	41.048	1.773
2001	1.027	46.734	2.362
2002	1.095	52.160	2.682
2003	1.240	58.736	3.216
2004	1.389	63.700	3.723
2005	1.490	66.485	4.102
2006	1.522	64.160	4.214
2007	1.643	61.146	4.731
2008	1.731	61.567	5.218
2009	1.786	61.370	5.356
2010	1.814	60.990	5.484

Vir: Bilten BS, marec 2011

Iz tabele št. 5 je razvidno, da z leti narašča tako število bančnih avtomatov, kakor tudi število dvigov in vrednost dvigov. Padec števila dvigov na bankomatih je opazen le v letih 2006 – 2010, kar je posledica uvedbe nove valute. Vrednost dvigov z leti konstantno narašča, kar je posledica tako višjega standarda, kakor tudi vedno večje uporabe elektronskih tržnih poti, ki jih ponujajo banke.

Poslovanje z debetno kartico se vrši v okviru sredstev na transakcijskem računu stranke. Uporabnik ima na običajnem računu možnost pridobitve rednega mesečnega limita, ki je običajno določen glede na mesečni priliv na računu (znaša približno polovico mesečnega priliva). Prav tako ima vsak uporabnik možnost pridobitve izrednega mesečnega limita, ki je lahko mnogo večji in je odvisen od bonitete stranke in seveda od njegovih prihodkov oz. finančnega stanja.

Večina debetnih kartic v Sloveniji je licenčnih (MasterCard) in nosi oznako Maestro ali Cirius. Kartica Maestro omogoča uporabo tudi v tujini.

Kreditne kartice in kartice z odlogom plačila

Razlika med kreditnimi karticami in karticami z odlogom plačila je v tem, da lahko imetniki pri kreditnih karticah koristijo posojilo banke izdajateljice (posojilne kartice izdajajo le

banke). Pri slednjih je običajno imetnikom odobreno okvirno posojilo v določeni višini, ki je odvisna od višine mesečnih prilivov. Posojilne kartice so nastale zaradi spremenjenega načina plačevanja s čeki in njihove težje uporabnosti za izvajanje obročnih plačil. Imetnik mesečno odplačuje odstotek zneska porabljenega posojila in pripadajočih obresti.

Pri karticah na odloženo plačilo gre za zamik v poravnavi plačila, opravljenega s tako kartico. Poravnava se opravi na določen dan enkrat mesečno, ki si ga lahko imetnik izbere izmed predlaganih s strani banke. Še vedno je izdanih več kartic z odlogom plačila kot kreditnih kartic. (Šteblaj, 1999: 44)

Po pravilih kartica ni last prosilca, ki izpolnjuje splošne pogoje, temveč je ta samo njen posestnik in uporabnik. Kartica načeloma ni prenosljiva, uporablja jo lahko le upravičeni zastopnik in ponavadi velja leto dni. Imetnik z njo lahko plačuje blago in storitve na vseh prodajnih mestih doma in v tujini, ki so vključena v sistem, po cenah in pogojih, ki veljajo za stranke. Pri plačilu s kartico imetnik kartice podpiše slip in zadrži drugi izvod slipa za svojo evidenco (Pavlin, 1996, str. 4). Ob uvajanju pametnih kartic se za identifikacijo imetnika uporablja tudi osebna številka.

S kreditno kartico oziroma kartico z odloženim plačilom imetnik plačuje in dviguje gotovino na enak način, kot z debetno kartico in posluje v okviru svojega osebnega mesečnega limita, ki je določen s strani poslovne enote in v dogovoru s stranko. V primeru, da želi uporabnik plačati znesek višje vrednosti od dovoljenega limita, mora to predhodno najaviti. Višina limita se odobri, vendar samo v primeru, da uporabnik korektno posluje, ima sredstva na katerem od računov, s katerih bo mogoče poravnati obveznosti (tekoči, transakcijski ali devizni račun). (Abanka Vipa, 2003: 12)

Tabela 6: S strani bank izdane plačilne kartice v Sloveniji

Leto	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Število (v1000)	788	847	828	1.011	1.094	1.207	1.244	1.379	1.461	1.531

Vir: Bilten BS, marec 2011

Tako kot se povečuje uporaba debetnih kartic, v Sloveniji narašča tudi število in uporaba kreditnih kartic, kar je razvidno iz tabele št. 6. Od leta 2001 se število plačilnih kartic konstantno povečuje.

Tabela 7: Število POS terminalov, opravljenih transakcij in njihova vrednost

Leto	Št. POS terminalov	Št. transakcij (v 1000)	Vrednost transakcij (v mio. EUR)
2000	21.723	49.376	1.309
2001	26.186	73.445	1.947
2002	29.452	91.750	2.442
2003	32.035	111.788	3.003
2004	34.770	110.771	3.392
2005	28.817	109.508	3.625
2006	29.234	115.367	3.944
2007	31.529	129.895	4.724
2008	33.490	134.581	5.457
2009	32.883	132.991	5.253
2010	32.021	138.853	5.616

Vir: Bilten BS, marec 2011

Iz tabele št. 7 je razvidno, da se promet preko POS terminalov, kakor tudi njihovo število, z leti povečuje. Opazno zmanjšanje števila POS terminalov v letih 2005 in 2006 naj bi bilo po pojasnilih Bankarta in sistema Activa posledica netočnih podatkov, saj sami beležijo konstantno naraščanje števila POS terminalov. Prav takšna je razlaga tudi za znižanje števila POS terminalov v letu 2009 in 2010, lahko pa je znižanje tudi posledica finančne in gospodarske krize.

Izdajatelji kreditnih kartic praktično živijo od članarine in/ali drugih zneskov, ki jih zaračunavajo imetnikom kreditnih kartic, pa tudi od provizije, ki jo zaračunavajo prodajalcem, ki sprejemajo take kartice. Z izdajanjem in uveljavljanjem kreditnih kartic izdajatelji uveljavljajo svoje ime ("blagovno znamko"), kar jim pomaga tudi pri drugih finančnih poslih, predvsem v povezavi z bankami ter pri dajanju in najemanju kreditov (Odar, 1993: 112).

Izdajatelj mora od lastnika kreditne kartice čim prej izterjati plačilo in tako skrajšati čas od plačila računa prodajalcu do prejetja plačila lastnika kartice. Ker je lastnikov veliko, mora

izdajatelj računati na njihovo nelikvidnost, bankrot ali druge težave, zaradi katerih plačila niso pravočasna. Tudi stroški tožb in izterjave zapadlih plačil so lahko precejšnji, zato izdajatelji kartic pred izdajo temeljito preverjajo boniteto morebitnih lastnikov. (Odar, 1993, str. 113)

Kartice s predplačilom

Zaradi nevarnosti ponarejanja kreditnih kartic so bile uvedene čipne ali elektronske kartice (imenovane tudi "pametne kartice"). Strošek elektronske plačilne kartice z vgrajenim čipom pa je bil do nedavnega previsok, da bi jo uporabljali kot plačilno kartico. Začeli so jo uporabljati kot predplačilno kartico (prepaid card) ali kot nekakšno denarnico gotovine. S pametno kartico se lahko taka denarnica ponovno napolni in je imetnik ne zavrže. Polni se lahko tudi preko telefona. To pomeni, da imetnikom ni več potrebno hoditi do banke ali bankomata. Ta kartica bi lahko tako postala "banka v žepu". To so večnamenske predplačilne kartice (Logar, 1998, str. 109).

Pri uporabi enonamenskih predplačilnih kartic, ki so večinoma podjetniške, gre za predplačilo storitev, ki jih nudi izdajatelj. Kartice so enkratno uporabne – ko je vsebovani znesek porabljen, jih ni mogoče ponovno napolniti z novim zneskom. (Šteblaj, 1999: 52)

Uporaba predplačniških kartic za plačila velikih zneskov pa je v primeru nezadostne identifikacije problematična tudi zaradi možnosti prikrivanja denarja, pridobljenega iz nezakonitih dejavnosti oz. pranja denarja.

2.2 Klasične in pametne kartice

Glede na tehnologijo izdelave ločimo klasične-magnetne kartice in kartice s čipom. Podatki klasičnih kartic so shranjeni v magnetnem zapisu kartice, ki jih je mogoče samo brati, ne pa tudi spreminjati. Zaradi potrebe po avtomatizaciji v bančništvu so plastični kartici dodali magnetni trak. Magnetni trak omogoča avtomatsko zajemanje bistvenih podatkov o imetniku (stanje na računu, limiti, blokade…).

Kasneje so magnetnim trakovom zaradi varnosti dodali funkcijo "read only", ki omogoča, da podatke s take magnetne kartice lahko beremo, ni pa jih možno spreminjati. Zaradi preprostega posnemanja magnetnega traku lahko kartico ponaredimo, zato niso dovolj varne.

Kartice s čipom se ne uporabljajo samo v bančnih sistemih. Namenjene so splošni rabi, zato jih najdemo tudi v telekomunikacijah, zdravstvu, šolstvu, vojski. Tu se uporabljajo pomnilne čipne kartice, ki izvajajo manjše logične operacije s pomočjo integriranih vezij.

V finančnih ustanovah pa se uporabljajo tako imenovane "pametne kartice". To so kartice z vgrajenim tipom obsežnega pomnilnika. Osnovne funkcije pametnih kartic so prenašanje, prepoznavanje lastnika kartice in nadomestilo za denar in varno plačilno poslovanje. Pametna kartica preprečuje lastniku prekoračitev dnevnega limita in s procesorjem nadzira vse interakcije, ki potekajo med zunanjimi napravami, ki berejo in pišejo na kartico, in med pomnilnikom pametne kartice. V prihodnje naj bi bila namenjena vsem vrstam transakcij. Omogočila naj bi preprostejše in za posameznika cenejše poslovanje, večjo varnost in združitev različnih tehnologij v eno. Pametna kartica uporabniku omrežja služi tudi kot nekakšen ključ za uporabo omrežnega računalnika, ki omogoča priključitev na delo v omrežju od koderkoli. Zagotavlja varnost, ki je potrebna za komunikacije v računalniških mrežah (združuje telekomunikacije in računalnike). Na ta način uporabljajo pametno kartico v elektronskem poslovanju. (Zupančič, 1998: 12, Jurišić idr., 1997)

2.3 Osebne in poslovne kartice

Izdajatelji izdajajo kartice fizičnim osebam (občanom)

- osebne kartice in podjetjem
- poslovne kartice.

Osebne kartice so vse tiste, ki so omenjene pod točko 3.1., in sicer debetne, kreditne ter predplačilne kartice. Za te kartice mora imetnik imeti odprt račun pri finančni instituciji.

Poslovne kartice so namenjene vodilnim in drugim delavcem v podjetjih ali samostojnim podjetnikom za plačilo potovalnih, reprezentančnih in drugi stroškov ali nakupov. Podjetje za uporabo poslovne kartice pooblasti eno ali več oseb, zaposlenih v podjetju in jim določi višino dovoljene porabe na mesec. Na kartici, ki je poslovna, sta odtisnjeni tako ime podjetja, ki je lastnik kartice, kot ime in priimek uporabnika kartice. (Šteblaj, 1998: 48)

Poslovne kartice so večinoma kreditne kartice in kartice z odlogom plačila, razen pri samostojnih podjetnikih, ki lahko imajo tudi debetne kartice. Z njimi je možno plačevati blago

in storitve na prodajnih mestih, skupaj z osebnim geslom dvigovati gotovino na bančnih avtomatih in enotah poslovnih bank.

Za pridobitev poslovne kartice je potrebna kreditna sposobnost imetnika kartice (podjetja, samostojnega podjetnika), kratka predstavitev podjetja, predložitev finančnih izkazov za pretekli dve leti ter tekočega poslovanja, predložitev osnovne dokumentacije (registracija, obvestilo zavoda za statistiko…) in zavarovanje odobrenega kredita (z menicami in menično izjavo). Ponavadi podobno kot ostale kartice vključujejo tudi različne vrste zavarovanj (nezgodno, zdravstveno, zavarovanje odgovornosti, kritje gmotne škode ob izgubi ali kraji s strani izdajatelja kartice…). (Abanka Vipa, 2003: 20)

2.4 Domače, licenčne in tuje kartice

Vse te kartice so kreditne kartice in kartice z odlogom plačila, domače pa tudi debetne.
Domače kartice izdajajo banke ali podjetja rezidenti. Lahko so kreditne kartice ali debetne kartice bančnih računov (npr. Karanta, LB plačilna kartica).

Licenčne na podlagi pravic iz pridobljene licence (iz tujine) izdajajo banke in podjetja rezidenti. Te kreditne kartice veljajo tudi v tujini (npr. Visa, Mastercard, Maestro)
Tuje pa so izdane v tujini in jih za plačila v Sloveniji uporabljajo pretežno nerezidenti. Te kartice so izdale tuje banke in tudi uporabljajo jih tujci (posamezniki) v Sloveniji. Podobne so licenčnim (isti izdajatelji), le da so licenčne izdelane pri nas, tuje pa v tujini (npr. Eurocard, Visa, American Express, Diners Club). Gre samo za razliko v izdajatelju kartic.

2.5 Plačilne kartice v Sloveniji

Na slovenskem trgu je že nekaj časa precej plačilnih kartic. Pri nas so plačilne kartice predvsem kreditne kartice, mednje pa uvrščamo kartice z odloženim plačilom in kartice, ki imetnikom omogočajo obnavljajoče se posojilo v višini odobrenega negativnega stanja na računu. (Logar, 1998: 326)

V Sloveniji so razširjene tudi tuje licenčne kartice, ki jih prav tako izdajajo domače banke, vendar njihova uporaba ni omejena zgolj na področje Slovenije. Čeprav je delež domačih kartic večji kot delež licenčnih, pa relativni delež izdanih licenčnih kartic narašča hitreje kot

delež domačih kartic. Razvoj mreže prodajnih mest za licenčne kartice v Sloveniji je v letu 1996 omogočil hitro povečevanje uporabe plačilnih kartic tudi za tujce. Slovenski državljani veliko uporabljajo plačilne kartice tudi v tujini. (Logar, 1998, prav tam)

2.6 Trgovinske kartice

Trgovska podjetja tudi pri nas izdajajo svoje kartice – za plačilo v svojih prodajalnah, na bencinskih črpalkah in drugod. Te kartice (zanje se plača članarina) imajo značaj plačilne ali kreditne kartice, običajno pa jih je mogoče uveljavljati tudi pri različnih popustih. Za banke je poslovanje s temi karticami praktično brez tveganja, saj gre v tem primeru pravzaprav za predhodno plačilo. (Jurak, 1996: 183)

Nekatere najbolj znane trgovinske kartice v Sloveniji so Magna, kartica Kluba Mercator - Pika (različni popusti pri plačevanju z gotovino, ni članarine, nakup samo v Sloveniji, plačevanje mesečno z zamikom), Namina kartica (možnost odloženega plačila, ni članarine, popust pri plačilu z gotovino, tudi poslovna), City card.

2.7 Fizične karakteristike

Kartica je sestavljena iz jedra iz PVCA umetne mase, ki je barvno in natisnjeno. To je s sprednje in z zadnje strani zaščiteno s prozorno folijo – prevleko. Mere, vsebina, zaščitni varnostni elementi, mesto in vrsta zapisa podatkov ter podatkovni del – magnetni trak ali spominski čip so točno predpisani in standardizirani z ISO standardi 7810, 7811, 7812, 7813 in 4909. Standardizacija fizičnih lastnosti celotne kartice omogoča kompatibilnost kartic in njeno uporabnost kjer koli na svetu.

Kartica je debeline 0,76 mm, dolžina kartice je 8,576 cm, širina 5,389 cm. Prečna stranica v vogalu med stranico dolžine in stranico širine meri 3,18 mm. Kartica na sprednji strani vsebuje logotip izdajatelja, številko kartice, veljavnost, podatke o imetniku in označbo vrste kartice. Na zadnji strani se nahaja magnetni trak, ki se začne na razdalji 0,592 mm od prečnice vogala kartice, in mesto za podpis imetnika.

Embosiran tekst kartice in vsebina kartice sta na sprednji strani kartice vodoravno razdeljena na deset nivojev glede na namembnost uporabe kartice, navpično pa na tri nivoje. Prvi nivo je

namenjen za podatke izdajatelja, drugi za podatke identifikatorja, tretji pa določa dolžino številke kartice, vezano na deset vodoravnih nivojev (Europol, 2006).

Tabela 8: Razdelitev sprednje strani kartice glede na izdajatelje

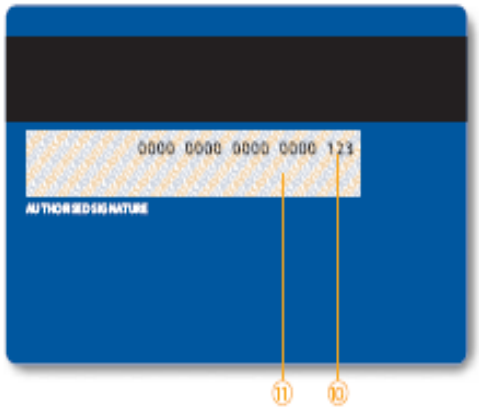
0	Rezervirano za nove dejavnosti in za ISO
1	Letalski promet
2	Letalski promet in druge nove dejavnosti na tem področju
3	Potovanje in zabava
4	Bančništvo in finance
5	Bančništvo in finance
6	Trgovina in bančništvo
7	Dejavnosti, povezane s proizvodnjo in prodajo naftnih derivatov
8	Telekomunikacije in druge nove dejavnosti na tem področju
9	Rezervirano za nacionalne urade za standardizacijo

Vir: Europol 2006

Standard določa tudi vodoravno razdelitev sprednje strani kartice glede na izdajatelje (Dyners Club, American Express, VISA in Master Card), na ta način določa mesto zapisa številke izdajatelja, za vsakega izdajatelja posebej prvi dve številki števila identifikatorja, dolžino števila identifikatorja ter dolžino številke kartice (npr. VISA številka identifikatorja 36xxxx ali 38xxxx, dolžina številke kartice 13 ali 16 znakov). Z vidika varnosti in pa razločevanja med bankami izdajateljicami je določeno število BIN – Bank Identification Number, ki določa, da prvih šest številk v številu kartice določa vrsto kartice in pa banko izdajateljico. V strokovni literaturi se za isti izraz in kratico uporablja IIN – Issuer Identification Number (Europol, 2006).

Sprednja stran kartice je strogo predpisana in omejena z namenom standardizacije uporabe kartic in zagotavljanja enkratnosti sleherne izdane kartice, kakor tudi ločevanja glede namembnosti kartice, njene uporabe, izdajatelja. V primeru novih čipnih ali ti. pametnih kartic je na sprednji strani v levem delu nameščen čip oziroma spominsko-procesorski del kartice. Velikost čipa je s standardom omejena na 25 mm^2, velikost čipa pa je omejena tudi iz fizikalnega razloga, saj bi se ta lahko na sicer mehki kartici ob upogibanju prelomil.

Zadnja stran kartice je opremljena z magnetnim trakom in prostorom za podpis imetnika.



Podatki na plačilni kartici:

1. magnetni zapis ali čip (ali oboje skupaj)
2. identifikacijska številka izdajatelja,
3. številka kartice
4. hologram
5. ime izdajatelja/logotip
6. zaščitni znak
7. datum veljavnosti
8. ime in priimek imetnika/fotografija
9. kontrolna številka
10. CVC številka
11. podpisno polje.

Slika 1: Izgled kartice s sprednje in zadnje strani

Varnostne karakteristike in elementi zaščite (Šavnik, 2007):

- embosiran tekst
- CSC številke (kontrolne, dodeljene, zakrite, natisnjena na zadnji strani kartice pri VOID nalepki, ujema se s številko na sprednji strani)
- hologramski napisi in podobe
- skriti zapisi, vidni pod UV svetlobo
- mikro zapisi, vidni pod povečavo
- nalepka za podpis, občutljiva na poškodbe (VOID), napis VOID se pokaže ob kakršnem koli posegu na podpis kartice
- veljavnost kartice
- poševna pisava (indent printing)
- varnostne karakteristike na nosilcu, tj. magnetnem traku ali čipu.

3 ANALIZA ZLORAB PLAČILNIH KARTIC

Obstaja vrsta oblik zlorab plačilnih kartic, med najbolj nevarnimi pa je ponarejanje kreditnih kartic in kartic z odloženim plačilom, ki prerašča v novo področje mednarodnega organiziranega kriminala. Kriminalne združbe pri tem ponarejajo potne listine, vozniška dovoljenja in druge osebne dokumente, s katerimi "dokazujejo" upravičenost in veljavnost ponarejenih kartic. (Pavlin, 1996: 16)

Do zlorab plačilnih kartic lahko prihaja zaradi (Lasbaher, 1997):

- načina uporabe kartice; zaradi zamika plačil pri kreditnih karticah in karticah z odloženim plačilom ima imetnik kartice možnost reklamacije šele po prejemu izpisa prometa; medtem pa je lahko kartica zlorabljena brez vednosti imetnika
- lažne ("navidezne") storitve; zaradi navideznih loterij, iger na srečo, casinojev, porno strani, oglaševalnih storitev je poizvedovanje o zlorabi plačila nemogoče
- lažnih strani interneta; lažno predstavljanje različnih podjetij, ki npr. sprejemajo prednaročila za storitve in blago
- na internetu dostopnih programov o generiranju številk kartic in navodila o načinu izvedbe zlorabe kartic (programi, ki naključno generirajo številke, ponujajo izbiro številk obstoječih plačilnih kartic)
- problematičnega preverjanja tujih imetnikov plačilnih kartic
- nedorečene zakonodaje; med zakonodajalci, izdajatelji kartic in ponudniki elektronskih storitev še ni celovitega sodelovanja.

Pri zlorabah plačilnih kartic gre pogosto za organizirane oblike kriminala (posebne skupine so specializirane za določena področja, npr. ponarejanje, distribuiranje). Za tovrstni kriminal so značilne povezave med podzemljem in finančnimi ustanovami, dobro poznavanje tehnoloških novosti in varnostnih mehanizmov. Kriminalci uporabljajo raznovrstno tehnologijo, ki jim je lahko na voljo, in izkoriščajo slabosti razvijajočega se svetovnega komunikacijskega omrežja. Preiskovalni organi ugotavljajo, da se s tovrstnimi goljufijami ukvarjajo predvsem pripadniki specifičnih etničnih manjšin, še posebej azijskih in nigerijskih. (Zupančič, 1998: 19)

Vse oblike zlorab delimo na tiste, ki nastanejo na strani izdajatelja kartic (tako imenovane issuer fraud) in tiste, ki nastanejo pri lastnikih prodajnih mest (tako imenovane acquirer fraud).

Osnovne značilnosti zlorab (ZBS, 2002: 30):

- dobro organiziran kartični kriminal, specializiran za določena področja
- povezave med podzemljem in viri v finančnih institucijah
- povezave med podzemljem in goljufivimi trgovci
- poznavanje tehnoloških značilnosti in varnostnih mehanizmov
- lahko dostopna tehnologija (magnetni čitalci, tehnične specifikacije na internetu, fantomski POS terminali)
- slabosti kartic
- neomejene možnosti preizkušanja
- različni viri informacij o karticah
- izpisek prometa po kreditnih karticah in karticah z odloženim odlogom plačila le enkrat mesečno.

V zvezi z osnovnimi značilnostmi je ugotovljeno, da se zlorabe selijo iz ene oblike v drugo (ZBS, 2002: 31):

- iz kreditnih v debetne
- iz domačega v mednarodni promet
- iz klasičnih v POS transakcije in internet
- iz ene banke v drugo
- iz ene države v drugo – v obeh primerih so zlorabe odvisne od sprejetih ukrepov in hitrosti odkrivanja.

3.1 Zlorabe kartic s strani imetnika

Za pridobitev plačilne kartice mora imetnik v banki odpreti tekoči ali transakcijski račun. Ob tem z banko sklene pogodbo, v kateri so zapisani pogoji in pravila poslovanja s kartico ter obveznosti imetnika. V pogodbi je lahko določen tudi znesek limita – dovoljenega negativnega stanja (Gradišar, M., Lamberger, I., 2011).

Prav v povezavi z limitom se zgodi največ zlorab s strani imetnikov. Ti namreč zavestno presegajo dovoljeno negativno stanje. Tako kljub doseženemu limitu še naprej dvigujejo gotovino in plačujejo blago ali storitve. Največ takšnih zlorab je možnih s kreditno kartico in kartico z odloženim plačilom.

Včasih, ko na prodajnih mestih še ni bilo POS terminalov, so bile zlorabe še lažje. Uporabljali so se (ponekod se še danes) imprinterji, ki so odtis kartice samo kopirali, niso pa preverjali stanja na računih. Danes so zlorabe z debetnimi karticami težje. POS terminali namreč preberejo magnetni zapis kartice. Takšen terminal je povezan s centralnim sistemom v banki, ki je kartico izdala. V primeru, da je kartica na "stop listi" ali je blokirana, centralni sistem ne dovoljuje plačila s takšno kartico. Hkrati trgovcu oziroma prodajnemu mestu sporoči, da takšno kartico odvzame in zato dobi nagrado. Kartica se na "stop listi" znajde na zahtevo enote banke, kjer je račun odprt. Ta predlaga blokado iz različnih razlogov (nekorektno poslovanje, izguba, nedovoljeno negativno stanje).

Stanje na računu se pri debetni kartici preverja na podlagi številke kartice preko linije, ki povezuje bankomat ali prodajno mesto z banko. Pri karticah z odlogom plačila pa se na tak način preverja stanje prostega limita in ne stanje računa. Seveda je z uporabo POS terminalov kontrola prekoračitev dovoljenih negativnih stanj mnogo boljša (od uporabe imprinterjev), zato so takšne terminale, kljub velikim stroškom, ki so povezani z njihovo uvedbo, na večini prodajnih mest uvedli tudi pri nas.

Glede na njihov socialni položaj lahko storilce zlorab uvrstimo v eno izmed naslednjih skupin:

- imetniki, ki trenutno niso plačilno sposobni, se zadolžijo s karticami ali nakupom na obroke, ker mislijo, da bodo z nakupljenim čez čas finančno pridobili in s tem poravnali dolg; seveda morajo ob tem poznati sistem poslovanja
- plačilno sposobni imetniki, ki so trenutno zaradi različnih vzrokov v finančni stiski
- skrajni primer pa so tisti, ki brezglavo "zapravljajo" in tako zabredejo v velike dolgove (psihološki problem), iz katerih se ne morejo rešiti; zaradi teh dolgov pogosto zaidejo na področje kriminala.

V primerih, ko dolgovi banki niso poravnani, banka račun blokira, kasneje tudi zapre, kartico pa bi moral imetnik vrniti. Vendar izdajatelj kartice nima pooblastila, da bi imetnika prisilil,

da bi mu vrnil kartico. Pa tudi dolgovi s tem niso povrnjeni. Tako izdajatelju kartice ostajajo dolgotrajni postopki pred sodiščem.

Kazenski zakonik v 253. členu[20] (Izdaja nekritega čeka in zloraba bančne ali kreditne kartice) navaja: "Kdor z namenom, da bi sebi ali komu drugemu pridobil protipravno premoženjsko korist, uporabi bančno kartico na bančnem avtomatu za dvig gotovine, čeprav ve, da nima kritja na tekočem računu, ali uporabi kreditno kartico, čeprav ve, da ob plačilu ne bo imel kritja, in si tako pridobi premoženjsko korist, se kaznuje z zaporom do petih let. Če je bila s tem dejanjem pridobljena velika premoženjska korist, pa z zaporom od enega do osmih let."

To kaznivo dejanje se vedno zgodi z naklepom. Storilec je lahko vsakdo, tudi pravna oseba, vendar pa mora biti lastnik veljavne bančne kartice, ki jo uporabi na bančnem avtomatu za dvig gotovine. Ob tem ve, da nima kritja na tekočem ali transakcijskem računu ter da zneska ne bo povrnil in si bo tako pridobil premoženjsko korist. Pri kreditni kartici ni potrebno, da bi imel storilec denarno kritje ob uporabi kartice. Vendar že ob uporabi ve, da v času plačila ne bo imel kritja in da si na tak način pridobi premoženjsko korist.

Pregon za to kaznivo dejanje zastara v petih letih. Izreče se lahko zaporna kazen zapora od petnajstih dni do petih let, z omilitvijo denarna kazen. (Deisinger, 2002: 561-563)

Druga oblika zlorabe s strani imetnika pa je lažna prijava ukradene ali izgubljene kartice. Imetnik kartico v predpisanem roku od "izgube" ali "kraje" prekliče, vendar jo še vedno uporablja. Lahko jo uporablja sam in promet zanika, lahko pa jo da v uporabo drugi osebi (sorodnikom, prijateljem), ki nato z njegovim dovoljenjem plačuje blago in storitve.

Takšne zlorabe je zelo težko dokazovati, ker dokazov (ki bi govorili imetniku v korist ali breme) praktično ni. Na srečo pa pri elektronski uporabi kartice te zlorabe niso možne, ker blokada velja takoj.

[20] Od 1.11.2008 velja nov Kazenski zakonik KZ-1. kaznivo dejanje Izdaja nekritega čeka in zloraba bančne in kreditne kartice je opisana v členu 246, vendar je opis isti, prav tako pa velja tudi komentar iz navedenega vira

3.2 Zloraba izgubljene ali ukradene kartice

Pri klasični kriminaliteti kot so tatvine, vlomi in ropi, pridejo kriminalci tudi do plačilnih in kreditnih kartic. Imetniki pa lahko kartice tudi izgubijo. Vse kartice, ki na takšen ali drugačen način pridejo v roke kriminalcem, so predmet zlorabe, saj se z njimi dviguje denar ali plačuje blago in storitve. Čeravno je potrebno pri plačilih s karticami preveriti istovetnost imetnika tudi z osebnim dokumentom, le malo prodajalcev to v praksi tudi počne. Zadovoljijo se s kolikor toliko podobnim podpisom na slipu, ki ga primerjajo s tistim na kartici, osebnih dokumentov pa praviloma ne zahtevajo. Izgubljene in ukradene kartice morajo imetniki kar najhitreje prijaviti izdajatelju, ki jih uvrsti na "stop listo". Problem prepovedanih kartic pa je v tem primeru podoben kot pri prekoračitvi limita. Na elektronskih POS terminalih je možno uporabo takšne kartice preprečiti v 24 urah od prijave, na klasičnih terminalih pa je kontrola težja. Storilci tovrstne kriminalitete so seznanjeni za 24 urni rok, ki jim je na voljo, preden se kartica pojavi na "stop listi", zato je 90 % zlorab ukradenih in izgubljenih kartic v prvih 24 urah od kraje ali izgube.

Zlorabe ukradenih kartic ne sodijo v organiziran kriminal. Gre bolj za priložnostne tatove, ki kartice pridobijo s klasičnimi kaznivimi dejanji, kot so vlomi, ropi. Dejansko gre pri plačilih z ukradeno kartico za plačilo majhnih zneskov, saj tisti, ki zlorabljajo, vedo, da trgovci majhnim zneskom ne namenjajo velike pozornosti. Čeprav bi morali vedno poleg podpisa istovetnost preveriti tudi z ustreznim osebnim dokumentom, se ponavadi zadovoljijo s kolikor toliko podobnim podpisom na slipu, kot je na kartici.

Seveda pa lahko lastnik kartico tudi preprosto izgubi – pozabi na bančnem avtomatu ali prodajnem mestu, izgubi skupaj z denarnico ali torbico itn.

V obeh primerih mora lastnik kartice izgubo ali krajo debetne kartice sporočiti klicnemu centru, ki kartico v roku ene ure uvrsti na tako imenovano stop listo. Takoj po blokadi debetne kartice vse stroške zlorabe krije banka izdajateljica. Za stroške zlorab z karticami z odlogom plačila in kreditnimi karticami pa je imetnik odgovoren še 24 ur po preklicu, čeprav danes riziko odgovornosti zavarujejo že tudi zavarovalnice ob plačilu zavarovalne premije.

Po blokadi oziroma po preteku 24 ur je možno kartico uporabljati samo še na prodajnih mestih brez POS terminalov, takih pa je v Sloveniji že zelo malo.

Zlorabe ukradenih in izgubljenih kartic delimo na dva tipa (Abanka Vipa d.d., 1999: 2):

- Zlorabe z avtorizacijo, za katere je značilna uporaba neposredno po kraji, in sicer gre za nakupe visokih zneskov (zlorabe pred blokacijo). Navadno pri tovrstnih zlorabah sodelujejo tudi trgovci, ki zahtevajo avtorizacijo na podlagi telefonskega obvestila o podatkih s kartice, ne da bi kartico sploh imeli v rokah.
- Zlorabe brez avtorizacije, pri katerih je značilno, da gre za nakupe manjših zneskov (pod tako imenovanimi floor limiti trgovcev), največkrat pa se tovrstni nakupi opravljajo v supermarketih in na bencinskih črpalkah.

Oglejmo si primer tatvine kartice Eurocard in dva primera kraje kartice.

Imetnici je sodelavka v službi iz denarnice ukradla kreditno kartico Eurocard. Ker imetnica ni takoj ugotovila, da kartice nima, je storilka uspela kartico uporabiti na 16-ih prodajnih mestih, od tega dvakrat v Italiji. Po pogovoru imetnice s storilko pa so se nakupi končali. Na nobenem od prodajnih mest niso zahtevali avtorizacije (šlo je za ročne nakupe z imprinterji) in so šele po pogovoru s trgovci ugotovili, da gre za isto osebo, ki je ustrezala opisu sodelavke. Ta je nato priznala vseh 16 goljufij.

V Sloveniji so obravnaval skupino tatov (skupaj z Avstrijci in Hrvati), ki je z iz avtomobilov ukradenimi karticami kupovala razne tehnične predmete in oblačila v Avstriji. Tako so realizirali nakupe za 90.000 dolarjev. Ob uveljavitvi davka na dodano vrednost so bili prijeti v Avstriji in obsojeni na zaporne kazni.

Članu Eurocarda je bila kartica ukradena v gostinskem lokalu v Ljubljani. Eurocard je kartico takoj razveljavil in po telefonu obvestil vse večje trgovine v Ljubljani, naj bodo pozorni na osebo z ukradeno kartico. Pri tem so izvedeli, da je malo pred njihovim klicem v veleblagovnici Supermarket v Ljubljani nekdo kupoval blago in kreditno kartico pozabil v trgovini. O tem so takoj obvestili policijo in osumljenca so prijeli v trgovini, kamor je prišel iskat pozabljeno kartico.

Nigerijske kriminalne združbe si pri vnovčevanju ukradenih (preko žepnih tatvin ali tatvin poštnih pošiljk) plačilnih kartic pomagajo s ponarejenimi identifikacijskimi dokumenti. Pred tem se po različnih kreditnih in bančnih sistemih pozanimajo o stanju na računu oziroma plačilni kartici.

3.3 »Pogled čez ramo«ali »Libanonska zanka«

Pri teh vrstah zlorab gre za način pridobivanja PIN številke kartice uporabnika, ki se lahko dogaja z dovoljenjem imetnika ali brez njega. Storilec se postavi v bližino bančnega avtomata in opazuje uporabnika, ko odtipka PIN številko, ki jo bančni avtomat zahteva pred opravljeno transakcijo. Storilci uporabljajo različne pripomočke in pretveze, ki jim olajšajo pridobitev PIN številke. Tako je poznana uporaba ogledal, fotografskih in video kamer, s katerimi »preko rame« bodočega oškodovanca pridobijo PIN številko, veliko revolucijo in uporaben pripomoček pa je z razmahom tehnologije postala kamera na mobilnih telefonih, ki jo storilci pod pretvezo telefoniranja v vrsti pred bančnim avtomatom uporabljajo za snemanje uporabnikovih prstov pri odtipkanju PIN številke. Storilci uporabljajo pri starejših in tehnološko neukih komitentih tudi različne pretveze, s katerimi v bistvu z vednostjo komitenta pridobijo PIN številko. Tako poznamo primere, da je storilec na bančni avtomat sam napisal obvestilo, da se pojavljajo težave pri delovanju avtomata in naj uporabnik večkrat odtipka PIN številko, če bi avtomat to zahteval. Nekateri storilci celo prepričajo komitenta, da jim zaupa PIN številko in potem seveda navidezno poskušajo pomagati, da bi bila storitev opravljena. V režo bankomata za vstavitev kartice se pred tem namestijo preprosti plastični trakovi, ki jih imenujemo Libanonske zanke. Libanonska zanka - "Lebanese loops" je naprava, nameščena v mehanizem za branje kartic, ki ob poskusu dviga gotovine kartico zadrži. Ker bančni avtomat zazna napako pri branju kartice, se storitev ne opravi. Komitent je zmotno prepričan, da je kartico bančni avtomat zaradi napake zadržal in se napoti v bančno poslovalnico, k temu pa ga največkrat napoti tudi storilec, ki se nahaja v bližini ali mu je pri poskusu dviga na avtomatu tudi »navidezno« pomagal. Kriminalci kartico kasneje vzamejo, poznajo tudi PIN številko in na bližnjem bančnem avtomatu takoj dvignejo razpoložljiva sredstva s komitentovega računa.

Pri identifikaciji storilcev in preiskovanju tovrstnih zlorab so v pomoč kamere, nameščene v samih bančnih avtomatih ali v okolici. Problem predstavljajo dobro organizirani in mobilni kriminalci iz tujine, ki se v naši državi zadržujejo samo nekaj dni in so po odkritju zlorab že nedosegljivi in tudi bistveno težje izsledljivi po fotografijah. Mnogo storilcev k nam prihaja tudi samo v času turistične sezone oz. takrat nastopajo kot »tranzitni« storilci, ki samo potujejo preko naše države in hkrati izvršujejo kazniva dejanja.

3.4 Družinske goljufije ali zlorabe

Tovrstne zlorabe potekajo v družinskih krogih ali krogih znancev. Storilec pozna osebo, imetnika kartice, prav tako pa tudi PIN številko, ki mu jo je znanec ali sorodnik zaupal, ali jo ima spravljeno oz. zapisano na vidnem mestu. Kartico in PIN številko v času, ko je imetnik ne nadzira, uporabi na bančnem avtomatu za dvig gotovine, potem pa kartico neopaženo vrne v listnico ali torbico lastnika. Lastnik zlorabo navadno opazi šele po obisku bančnega avtomata, ko je stanje na računu spremenjeno oz. šele pri pregledu mesečnega poslovanja s kartico. Storilci se poslužujejo pri teh zlorabah največkrat tehnike dvigovanja manjših zneskov, ker računajo, da lastnik kartice manjših zneskov ne bo opazil. Indic za družinske goljufije je gotovo ta, da kartica ni bila odtujena in se nahaja pri imetniku, zlorabe oz. sumljivi dvigi pa se vseeno pojavljajo. Ponavadi se tovrstne zlorabe preiskujejo s prepoznavo fotografij, ki jih je posnel bančni avtomat oz. s pastmi za »domače tatove«, kjer se z uporabo kemičnih ali tehničnih sredstev ugotavlja, kdo v krogu družine vstopa v listnice ali torbice članov družine.

3.5 Zamenjava plastike

Pri tej vrsti zlorab storilci pogosto delujejo v skupini. Tarča takšnih dejanj so podobno kot pri »pogledu preko rame« tudi starejši ljudje. Ob postopku dviga gotovine na bančnem avtomatu jih storilci poskušajo zamotiti in preprečiti spremljanje dogajanja na bančnem avtomatu. Z nagovarjanjem, pogosto v tujem jeziku, vpraševanjem o uporabi bančnega avtomata ali lokaciji kašne turistične znamenitosti odvrnejo uporabnikovo pozornost, kar izkoristi eden od storilcev in prekine postopek na bančnem avtomatu in vzame kartico. Nato imetniku kartice dopustijo, da nadaljuje s transakcijo. Ker transakcija ni več možna, ker ni v bančnem avtomatu kartice, je komitent presenečen in ne ve, kaj se je zgodilo. Prepričujejo ga, da se je to zgodilo tudi že njim in naj še enkrat odtipka PIN številko. Če to dejansko stori v prisotnosti storilcev, ki mu navidez pomagajo, so le ti prišli do kartice in PIN številke, kar jim omogoča, da na sosednjem bančnem avtomatu pridejo do sredstev, ki jih je imel komitent na računu.

Preiskovanje tovrstnih zlorab poteka podobno kot pri »Libanonskih zankah«. Storilci so prav tako večinoma iz tujine.

3.6 Trojanski konj ali lažni bankomati

Pri iskanju podatkov, ki omogočajo zlorabe kartic, si storilci pomagajo tudi z namestitvijo lažnih bankomatov. Imetnik kartico vstavi v tak bankomat, odtipka svojo osebno identifikacijsko kodo, ki se zapiše v lažni bankomat, ta pa nato javi obvestilo, da bančni avtomat trenutno ne deluje. (Zupančič, 1998: 17)

Takšni bankomati se pojavljajo predvsem v večjih mestih oz. na lokacijah, kjer je veliko ljudi, ki ne opazijo, da se je bančni avtomat pojavil, kjer ga pred tem ni bilo, pozneje pa spet izginil.

Poleg tega pa kriminalci nameščajo tudi lažne terminale na prodajnih mestih. Tu gre lahko za sodelovanje s trgovci ali pa izgovor, da terminal trenutno ne dela. V obeh primerih pa se podatki pridobivajo za izdelavo bele plastike.

Znanih je tudi nekaj primerov lažnih bankomatov v tujini. Storilec je pred eno od nemških veleblagovnic postavil lažen bankomat. Ko so ljudje hoteli dvigniti gotovino s karticami, jim je avtomat ni izplačal. Na videz se ni zgodilo nič, v resnici pa so kriminalci na ta način pridobili magnetne zapise kartice in PIN številke, ki so jih kasneje uporabili in prenesli na belo plastiko in na bančnih avtomatih pobrali sredstva z računov imetnikov pravih kartic.

3.7 Zlorabe bankomatov zaradi fizičnih in tehničnih karakteristik

Zlorabe bančnih avtomatov storilci izvajajo na ta način, da izkoriščajo tehnične in fizične karakteristike posameznih tipov bančnih avtomatov. Podajalci denarja v bančnih avtomatih so izvedeni v obliki predala, žleba in reže. Zlorabe so prilagojene vsaki vrsti izvedbe.

3.7.1 Napad na bančni avtomat s predalom

Storilec na bančnem avtomatu najprej prične s transakcijo in dvigom manjšega zneska gotovine. Ko se predal odpre, pusti v njem en bankovec ali kos papirja ustrezne velikosti. Nadaljuje z drugo transakcijo in dvigom najvišjega možnega zneska gotovine. Bančni avtomat prenese gotovino v predal in zazna, da je v njem ostala gotovina še od prejšnje transakcije. Zaradi tega zadnjo transakcijo stornira, storilec pa odpre predal in iz njega pobere gotovino. Takšen postopek lahko ponavlja, saj se transakcije stornirajo ena za drugo.

3.7.2 Napad na bančni avtomat z žlebom

Storilec pri tej vrsti zlorab najprej prične s transakcijo in dvigom najvišjega možnega zneska. Ko je storitev odobrena, bančni avtomat prenese gotovino iz sefa v žleb. Loputa, ki pokriva žleb za gotovino, se odpre, storilec pa prekrije senzor, ki zaznava izstavitev gotovine iz bančnega avtomata. Zaradi tega bančni avtomat pošlje na bančni strežnik informacijo o napaki, ki sproži storno transakcije. Storilec odvzame gotovino in ponavlja postopek na bančnem avtomatu.

3.7.3 Napad na bančni avtomat z režo

Tudi pri tej vrsti zlorab storilec prične z najvišjim možnim zneskom transakcije. Ko bančni avtomat prenese gotovino iz sefa v režo, storilec odvzame samo sredinske bankovce iz svežnja, pusti pa prvega in zadnjega. Bančni avtomat zazna, da gotovina ni bila vzeta, v režo potegne preostala bankovca in pošlje kodo o napaki na bančni strežnik. Ta na osnovi podatka o napaki stornira transakcijo, storilec pa lahko s početjem nadaljuje.

Storilci lahko vse tri vrste zlorab izvajajo s karticami, ki pripadajo njihovim računom, pri čemer tvegajo, da bodo na podlagi podatkov iz informacijskega sistema identificirani in dobljeni, lahko pa zlorabe izvršujejo s tujimi karticami, ki so jih pridobili z druge vrste zlorabami. S takšnim načinom zlorab se lahko izognejo limitom na računih.

3.7.4 Onemogočanje dvigov in dostave denarja na bančnem avtomatu

Storilci pri tem načinu zlorab mehansko preprečijo odpiranje lopute podajalca denarja tako, da jo zalepijo ali drugače fizično onemogočijo. Ko komitent opravi dvig na bančnem avtomatu, se loputa ne odpre in ne more do denarja. Predvideva, da je sistem v okvari in transakcija ni uspela. Ko se oddalji od bančnega avtomata, storilec odstrani blokado lopute podajalca in si prisvoji denar.

3.8 Ponarejanje kartic

Hekerji, ki sodelujejo pri ponarejanju in kopiranju plačilnih kartic, so sposobni pretvoriti "surove" bančne podatke v varnostne kode. Osnovni vir podatkov jim predstavljajo podatki, shranjeni na zapuščenih obrazcih zakonitih kartic (pozabljena potrdila ali pridobljena potrdila s podkupovanjem osebja v restavraciji, bencinski črpalki itd.). Podatke pridobivajo še z

vdorom v računalniške sisteme bank in družb, ki izdajajo kreditne kartice. Računalniški strokovnjaki, ki sodelujejo pri tovrstnem kriminalu, lahko iz nekaterih, za imetnika kartice nepomembnih podrobnosti, izdelajo popolne ponaredke. Med imetniki ponarejenih kartic se pojavljajo imena otrok, imena umrlih oseb in imena (bivših) zapornikov (naslov zapora, kjer (je) prestaja(l) zaporno kazen). Pri distribuiranju in iskanju imen, primernih za kasnejše uporabnike belih kartic, si ponarejevalci pomagajo z zbiranjem imen, ki se nahajajo na poštnih nabiralnikih. (Clough, 1997)

Osnovne bančne podatke ponarejevalci pretvorijo v varnostne kode, jih prenesejo na ponarejene kreditne kartice, narejene v ilegalnih tiskarnah, ali pa jih uporabijo pri različnih prenosih v omrežju Internet. (Zupančič, 1998: 17)

Proces reševanja problemov pri ponarejanju kartic je nekoliko težji kot pri ukradenih karticah. Lastnik kartice dokaj hitro ugotovi, da mu je kartica "izginila" in jo lahko takoj razveljavi. Podatki na ponarejeni kartici pa so pravi in je le od pravega lastnika odvisno, kako hitro bo ugotovil, da se je nekdo okoristil z njegovim denarjem. Tu je problem obveščanja o prometu na računu le enkrat mesečno, zato je spornih plačil lahko veliko. Neprijetno je tudi dokazovanje, da določena plačila ni opravil lastnik sam.

Raziskovalci ugotavljajo, da je med ponarejenimi največ zlatih in platinastih kartic (kreditni limit pri teh karticah je zelo visok). Poleg tega pa "elektronsko ponarejanje" omogoča tudi izdelavo tako imenovanih kloniranih kartic, ki so nepopisane, popolnoma ponarejene plastične kartice (v ponaredku je tudi že "hologram"). (Zupančič, 1998, str.18)

Ponarejanje kartic poteka skozi več faz. Najprej je potrebno pridobiti osnovne materiale za izdelavo kartice, kot so plastika, magnetni trak in hologram. V svetu obstajata dve podjetji za izdelavo hologramov, več pa je ilegalnih, pri katerih je za hologram potrebno odšteti od 5 do 15 dolarjev. Prvi problem pri izdelavi kartice je vstavljanje hologramа. Hologram ne sme biti na površini kartice, ne sme se ga čutiti s prsti, zato je slabo ponarejene kartice lahko prepoznati. Lažja je izdelava magnetnega traku, v katerega vtisnejo izmišljene podatke (ime in priimek, številko računa, višino limita idr.).

Ponarejanje kartic se lahko vrši na dva načina; s pravo kartico, na katero dodamo oziroma ji spremenimo podatke (spreminjanje in reembosiranje pravih kartic), lahko pa izdelamo drugo kartico, tako da obstajata dve s popolnoma enakimi podatki.

3.8.1 Spreminjanje in reembosiranje kartic

Ko ponarejevalec na nek način dobi kartico imetnika, jo skuša prenarediti. S tem skuša spremeniti fizični zapis na kartici – zapis imena in priimka ali številko kartice.

Pri imenu in priimku se lahko črka enostavno doda in dobimo novo ime ali priimek. Moškemu imenu Bojan lahko npr. dodamo črko a in dobimo žensko ime Bojana, seveda gre tudi v obratno smer.

Eden od primerov takšnega spreminjanja kartic je bil, ko je storilec k imenu uporabnika na kartici dodal črko N. Tako je iz imena Marija dobil ime Marijan. Čeprav je bil ponaredek zelo slab, prodajalka tega ni opazila in mu je prodala kakovosten fotoaparat. Ponarejevalca niso nikoli našli.

Številk pa ne moremo enostavno dodajati, ker je število cifer omejeno in vedno enako. Zato ponarejevalci na izgubljenih ali ukradenih karticah s pomočjo toplote uničijo zadnje številke in jih nato reembosirajo z novimi številkami. Tako kartica pridobi drugo identifikacijsko številko kartice, ki ima več možnosti, da ni na stop listi, kajti ukradene in izgubljene kartice se ponavadi znajdejo tam.

Ta metodologija (toplotno spreminjanje) je bila pogosta v ZDA v poznih 70-tih letih, ko je postalo ponarejanje resen problem kartične industrije. To je vodilo v vpeljavo hologramov v letu 1983, katere sta sprejela tako MasterCard kot Visa. Hologrami so bili na začetku zelo uspešni, saj so bili narejeni tako, da se deformirajo, če so izpostavljeni vročini. S tem so za nekaj časa odvrnili kriminalce od spreminjanja in reembosiranja plačilnih kartic.

Danes so kriminalci sposobni uporabljati različne kemikalije, s katerimi zaščitijo holograme in jih s tem obvarujejo pred poškodbami zaradi vročine. Posledica je, da je ukradeno ali izgubljeno kartico mogoče spremeniti z majhnimi napori, trgovci na prodajnih mestih pa imajo težave pri ugotavljanju, ali je kartica prava. (Abanka Vipa d.d., 1999: 4)

Ta metodologija privlači organiziran kriminal zato, ker so zanjo potrebni manjši stroški kot pri izdelavi popolnoma ponarejenih plačilnih kartic. Čeprav so spremenjene in reembosirane kartice pogosto uporabljene v povezavi s korumpiranimi trgovci, se ne razlikujejo od navadnih kartic in se lahko uporabljajo na vseh trgovskih lokacijah.

Vseeno pa spreminjanje embosirnih znakov originalnih kartic kriminalcem ne omogoča dostopa do bančnih avtomatov, ki delujejo na osnovi magnetnih zapisov in PIN-ov. (Newton, 1996: 27)

Če trgovec ne more ugotoviti, da je kartica ponarejena – če je ponaredek res dober, mu tudi ne moremo očitati nobene krivde. V tem primeru krivdo pripišemo izdajatelju kartice, ki je ni primerno zavaroval.

3.8.2 Spreminjanje zapisa na magnetnem traku kartice

Tudi tu gre za originalno kartico, ki je bila bodisi izgubljena ali ukradena. Prav tako se tu originalna kartica "zamenja" z neko drugo originalno kartico, ki po možnosti ni na stop listi.

Tovrstne kartice se lahko zlorabijo le na POS terminalih, ki delujejo na principu SBT (Signature Based Transactions) in ne zahtevajo vnosa osebne identifikacijske številke. Vsekakor pri tem načinu poneverb, razen če kartice niso tudi reembosirane, obstoji relativno enostavna možnost izsledite kriminalcev že zgolj na podlagi preverjanj podatkov na kartici z izpisanimi podatki na potrdilu o nakupu. (Abanka Vipa d.d., 1999: 4)

Če je šlo v 70-tih letih za toplotno spreminjanje kartic, je "tehnika ponarejanja" v 80-tih napredovala, saj so začeli spreminjati magnetni zapis na karticah. To jim je omogočil razvoj tehnologije. V boju proti tovrstnemu ponarejanju so zato izdajatelji razvili tako imenovane "kartične kode".

Kartične kode so po posebnem algoritmu izračunane številke, pri izračunu katerih se uporabljajo: podatki o številki izdajatelja, številki kartice, datum veljavnosti in drugi podatki na posamezni kartici. Kartične kode so zakodirane na drugi stezi magnetnega traku. V kolikor kriminalci nimajo dostopa do omenjenega algoritma ali kode, le-te ne morejo prenesti iz originalne kartice, ki jo morajo imeti fizično pri sebi, in tako ne morejo ponarediti kompletnega magnetnega zapisa na kartici. Prej je bilo to mogoče le na podlagi poznavanja vseh podatkov, odtisnjenih na kartici in poznavanja ustrezne sekvence zapisa podatkov na magnetnem traku, za kar ni bilo potrebno, da bi imeli kartico dejansko v posesti. (Abanka Vipa d.d., 1999: 4)

3.8.3 Popolno ponarejanje plačilnih kartic

Tu pa je situacija drugačna, saj imamo dve kartici – originalno, ki jo uporablja imetnik kartice in ponarejeno, ki jo brez vednosti imetnika uporablja ponarejevalec. Kartici sta si popolnoma identični, razlikujeta se lahko le v obliki podpisa. Tako prihaja do bremenitev računa z obeh kartic hkrati. Lastnik tega ponavadi ne opazi vse dokler ne dobi izpisa o poslovanju preko tekočega ali transakcijskega računa. Vendar je takrat že prepozno, saj do tistega trenutka nastale stroške krije sam. Imetniku so pripisani vsi stroški, saj se mu očitata kar dve vrsti malomarnosti. Prva je ta, da prometa po računu ne spremlja sproti in čaka na bančni izpis. Druga pa je nepozornost pri plačevanju na prodajnih mestih. Ponarejevalci si potrebne podatke namreč (ponavadi) priskrbijo med običajnim nakupom, ko kopirajo tako fizični kot tudi magnetni zapis na kartici.

Takemu načinu kopiranja, kjer s posebno napravo magnetni zapis kartice prekopiramo na drugo, pravimo skimming.

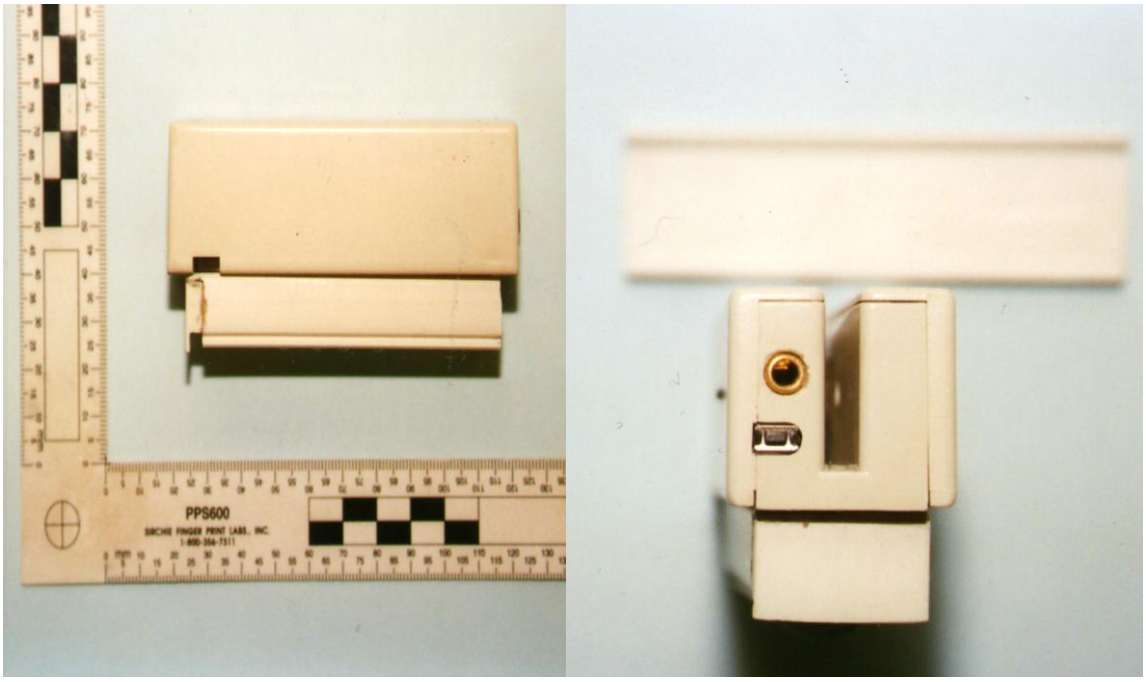
Najučinkovitejši način kopiranja magnetnih zapisov plačilnih kartic lahko izvrši zaposleni na prodajnem mestu. V tem primeru lahko storilec na svojem delovnem mestu sam in neopazno namesti ustrezno napravo v POS terminal, prek nje pa sebi ali komu drugemu omogoča pridobivanje podatkov s plačilnih kartic.

Druga možnost kopiranja magnetnih zapisov plačilnih kartic s strani zaposlenega na prodajnem mestu je z uporabo prenosne samostojne naprave (slika št. 2), ki jo prinese s seboj na delo. Napravo ima lahko skrito v določenem prostoru na delovnem mestu. V tem primeru mora od stranke pridobiti plačilno kartico in dovoljenje, da jo lahko odnese z njenega vidnega polja (na primer do blagajne za točilnim pultom) in poleg plačila storitev s kartico na POS terminalu izvede tudi skimming na svoji napravi. Storilec za tem vrne plačilno kartico lastniku in mu izroči potrdilo o plačilu, na katerega se podpiše, v kolikor ni treba vnesti PIN številke. Ker lastnik kartice nima pod nadzorom, ne more zaznati, da so bili podatki prekopirani z magnetnega zapisa njegove kartice.

Storilec ima lahko napravo za kopiranje magnetnih zapisov plačilnih kartic med opravljanjem dela kar pri sebi. Ta način je uporaben predvsem v restavracijah, gostinskih lokalih oziroma na ostalih prodajnih mestih, kjer se plačila s karticami opravljajo prek prenosnih POS terminalov. Dobro izurjen storilec opravi kopiranje magnetnega zapisa plačilne kartice kar

pred lastnikom kartice, ko mu jo ta izroči za plačilo. Storilec si ob začetku dela na prikrit način namesti napravo, prek katere lahko v vsakem trenutku neopazno izvede kopiranje. Napravo si lahko namesti na hlačni pas, na predpasnik ali celo nad gleženj in ob tem uporablja običajne in nesumljive kretnje, kot so pogled čez ramo in rahel zasuk telesa, pobiranje kartice s tal in podobno. Po opravljenem kopiranju magnetnega zapisa kartico vrne lastniku in mu izroči prenosni POS terminal, po možnosti tako, da lahko vidi in si zapomni vnešeno PIN številko.

Slika 2: Prenosna naprava za kopiranje magnetnih zapisov



Vir: Europol 2006

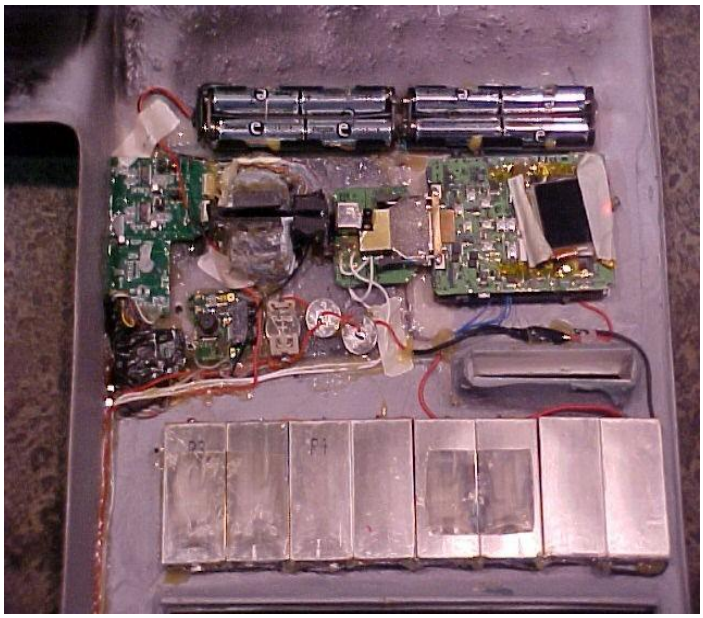
Pri tem načinu zlorab storilci ne potrebujejo pomočnika iz banke, saj do podatkov pridejo s kopiranjem magnetnega zapisa. Po kopiranju magnetnega zapisa in izdelavi ponarejene kartice se z le-to plačuje enako kot s pravo kartico. Kopiranje magnetnega zapisa se zgodi ponavadi pri plačevanju s kartico, ko lastnik ni fizično prisoten pri POS terminalu, kar se najpogosteje dogaja v restavracijah in drugih gostinskih objektih. Uporabniki kartic se morajo tega zavedati in ne smejo kartice nikoli izgubiti iz vidnega polja. (Lamberger, 2001: 59)

Skimming se prav tako pojavlja na bankomatih, ko se preko čitalnika (slika št. 4) presname magnetni zapis in s kamero posname PIN, ki ga lastnik vtipka ob dvigu gotovine (slika št. 3), ne vedoč, da ga pri tem snemajo. Tako prirejen bančni avtomat je prikazan na sliki št. 5.

Slika 3: Bančni avtomat z označenimi mesti, kamor se nameščajo naprave za: 1 - kamere, 2 - čitalnika magnetnega zapisa

Vir: Europol 2006

Slika 4: Notranjost naprave za kopiranje magnetnega zapisa kartice, nastavljena na bankomatu



Vir: Europol 2006

Slika 5: Prirejen bančni avtomat s kamero in čitalnikom magnetnega zapisa

Vir: Europol 2006

Storilci podatke s kamere spremljajo preko naprave, nameščene v neposredni bližini bančnega avtomata, kot lahko vidimo na slikah št. 6 in 7. Na bančnem avtomatu nameščen oddajnik prenaša podatke do sprejemnika, ki je nameščen v neposredni bližini bančnega avtomata. Ta je lahko nameščen v osebnem vozilu, poznani pa so tudi primeri, ko so bile telekomunikacijske naprave postavljene na drugih prevoznih sredstvih.

Slika 6: Parkirano kolo s sprejemnikom in spominsko enoto

Vir: Europol 2006

Slika 7: Sprejemnik in spominska enota, nameščena v osebnem avtomobilu

Vir: Europol 2006

Zlorabe s popolnoma ponarejenimi karticami so slabo raziskane in nevarne, ker jih trgovci na prodajnih mestih niso sposobni prepoznati. Še težje jih je odkriti na bankomatih.

Do podatka o osebni številki kartice lahko storilci brez nameščanja kamer pridejo tako, da preko prave tipkovnice namestijo še »lažno tipkovnico«. Ta si v posebnem spominskem vezju zapomni osebne številke, ki pripadajo posameznim karticam, ki jih komitenti vstavijo v bančni avtomat. Takšna tipkovnica je prikazana na sliki št. 8.

Slika 8: Pridobivanje osebne številke z lažno tipkovnico ali videokamero

Vir: Europol 2006

V nadaljevanju si oglejmo nekaj primerov popolnega ponarejanja kartic:

V Belgiji so ponarejevalci kreditnih kartic v celoti uspeli ponarediti kreditno kartico s pravimi podatki v magnetnem zapisu. Belgijski policisti in kriminalisti so ugotovili, da obstaja vsaj tisoč tako ponarejenih kreditnih kartic Visa, Mastercard in Eurocard. Ugotovili so, da s takšnim ponarejanjem ni več moč ločiti prave kartice od ponaredka. Samo od pravega imetnika kartice je odvisno, kdaj bo ugotovil, da se je nekdo okoristil z njegovim denarjem in mu povzročil neprijetno dokazovanje, da ni kupoval določenih artiklov na določenih mestih.

Sredi leta 1992 je policija v Hong Kongu zaprla tiskarno in odkrila tisoč ponarejenih kreditnih kartic.

Slovenska kriminalistična policija je od izdajatelja plačilnih kartic dobila prijavo o zlorabah plačilnih kartic. Šlo je za zelo visoke zneske, plačane doma in v tujini, z zlatimi in srebrnimi poslovnimi karticami, ki imajo visok dnevni limit. Magnetni zapisi na ponarejenih karticah so bili popolnoma pravilni. Tuji organi so sporočili, da so prijeli osebo, pri kateri so v računalniku našli magnetne kode in številke skoraj 300 plačilnih kartic. Te podatke je storilcu izročila oseba, ki je opravljala personalizacijo kartic. Sodelovale so še tri osebe, ki so opravljale dejanske nakupe. Vsi storilci so bili ovadeni suma storitve kaznivega dejanja

ponareditve listin in goljufije. Skupna škoda, ki jo je pri tem utrpela banka, je znašala približno 100.000 DEM[21].

Etnično kitajski kriminalci so sprva spreminjali magnetne zapise na karticah, danes pa obvladujejo tudi tiste s kartičnimi kodami. Gre za storilce s področja Tajske, Malezije, Hong Konga.

Afriški kriminalci izdelujejo ponarejene kartice, ki pa so slabe kvalitete. Vseeno dokaj uspešno uporabljajo program Credit Master. Vpleteni so tudi v poštne in telefonske zlorabe naročil. Povezali so industrijo zlorab kartic in preprodajo drog. Pri svojem delovanju so na trgovskih lokacijah sposobni uporabljati tudi silo, da bi s tem prestrašili trgovce. (Ivanovič, 1995: 42)

3.8.4 Bele kartice

Bela plastika (White Plastic) je termin, ki se uporablja za bele PVC kartice z magnetnimi zapisi, ki opravljajo vse funkcije originalne plačilne kartice. Take kartice ne nosijo imena izdajatelja, logotipa plačilnega sistema ali kakšnega drugega razpoznavnega znaka. (Abanka Vipa d.d., 1999: 5)

Ker kartica nima razpoznavnih znakov prave kartice - je bela, brez logotipa, brez naziva, brez številke, jo je nemogoče uporabiti na običajen način, kot npr. popolnoma ponarejeno kartico. Uporablja se jo lahko le s pomočjo trgovcev, ki jih storilci prej podkupijo. Ker je magnetni zapis pravilen, se kartica uporabi na POS terminalu. Takšno kartico lahko storilci uporabijo tudi na bančnem avtomatu, vendar je to še težje, ker morajo za to imeti tudi osebno geslo lastnika prave kartice. Če so bele kartice tudi embosirane, jih lahko uporabijo tudi za ročne transakcije z imprinterji, vendar tudi tu potrebujejo pomoč trgovcev.

Čeprav obstajajo dokaj preprosti načini izsledite zlorab s pomočjo "bele plastike", ponavadi ni načina, ki bi preprečil selitve tovrstnih zlorab na novo lokacijo, z novim imenom trgovca in novim računom. (Abanka Vipa d.d., 1999:5)

[21] Približno 50.000 eur

3.9 Zlorabe nikoli prejetih kartic

Nikoli prejete kartice so kartice, ki jih imetniki zaradi kraje sploh niso prejeli. Pri tem gre lahko za kraje iz poštnih nabiralnikov, kraje s pomočjo korumpiranih bančnih uslužbencev ali kraje, ki so posledica lažne spremembe naslova imetnika. Tovrstne zlorabe se v svetu zmanjšujejo zaradi spremenjenih načinov distribucije kartic, aktiviranja kartic na podlagi potrditve imetnika o prejemu kartice in drugih zaščitnih ukrepov. (Abanka Vipa d.d., 1999: 3)

Pri karticah, ki jih izdajatelji pošiljajo na dom, gre predvsem za obnovljene kartice. Tako tisti, ki to pošiljko prestreže, ostane brez osebnega gesla, saj geslo ostaja enako kot pri prejšnji kartici. Pa tudi lastnik kartice kmalu ugotovi, da mu je kartica potekla in da nove ni dobil. Pri novih karticah pa se seveda lahko zgodi tudi, da poleg kartice nekdo prestreže tudi osebno geslo. Banka na podlagi te prijave ukradeno oziroma nikoli prejeto kartico blokira ter izdela kartico z novim osebnim geslom, ki ju imetnik prevzame na enoti banke.

Zaradi varnosti se kartice in PIN številke večinoma ne pošiljajo skupaj v isti pisemski pošiljki, ampak ločeno, PIN številka šele potem, ko izdajatelj kartice že dobi povratno informacijo, da je bila kartica prevzeta s strani naslovnika, pri čemer seveda nikoli ne obstaja gotovost, da jo je res dobil.

Obstaja primer iz Nemčije, kjer je pri tovrstnih zlorabah sodelovalo celotno osebje manjše pošte, ki so poznali sistem pošiljanja kartic in PIN številk. Vedeli so, da po pošiljki, v kateri je kartica, pride še pošiljka s PIN številko. Ko so pridobili obe, so zlorabili kartico imetnika, ki kartice nikoli ni prejel.

3.10 Zlorabe številk in računov

Med te vrste zlorab bi lahko šteli že omenjene zlorabe s strani trgovcev, ko kartico odnesejo z vidnega polja imetnika. Poleg tega pa se številke zlorabljajo tudi pri nakupih na daljavo.

Zlorabe iz naslova tako imenovanih MO/TO transakcij (Mail Order/Telephone Order Transactions) se navadno izvajajo na podlagi podatkov originalnih kartic, pridobljenih s pomočjo podkupljenih trgovcev, podatkov pod pretvezo izvabljenih od samih imetnikov ali podatkov, generiranih s pomočjo posebnih, ilegalnih računalniških programov. V obeh

primerih se podatki uporabijo z namenom opravljanja nakupov po pošti ali preko telefona. (Abanka Vipa d.d., 1999: 5)

Kriminalci uporabljajo računalniške programe, ki so zmožni generirati številke kreditnih kartic. Potem, ko temu programu povedo, katero kreditno kartico bi želeli, pri kateri banki naj bo izdana in kolikšno število številk bi želeli, da generira, program na ekranu prikaže številko izbrane kreditne kartice. Zraven tega je možno s pomočjo programa izbrati ime in priimek enega izmed komitentov izbrane banke, s katerim se bomo predstavljali ob navedeni številki računalniško generirane številke kreditne kartice. Storilci uporabljajo tako generirane številke kreditnih kartic pri različnih nakupih preko interneta in elektronskih oglasnih desk. (Markovič, 1997)

3.11 Zlorabe na podlagi pridobljenih potrdil o nakupu ali dvigu

Po izvedenih nakupih ali dvigih sredstev na POS terminalih ali bančnih avtomatih veliko komitentov pusti oz. zavrže potrdilo o nakupu ali dvigu. Ne zavedajo se, da lahko zaradi tega omogočijo storilcem izvedbo zlorab njihovih kartic. Na potrdilih se namreč nahaja veliko pomembnih podatkov o kartici, izdajatelju, lastniku, prodajnem mestu in drugih podatkov. Danes je teh podatkov bistveno manj, kot jih je bilo včasih, ravno zaradi zlorab, ki so se pojavljale, če so storilci pridobili potrdilo s podatki. Kljub temu še vedno obstaja nevarnost in možnost zlorab, kar je odvisno predvsem od samozaščitnega obnašanja uporabnikov.

Ko pridobijo storilci podatke o računu in podatke o naslovu imetnika kartice, poskušajo z njim navezati stik in pridobiti še druge podatke. Navadno preko telefona ali elektronske pošte navežejo stik in se predstavljajo za uslužbenca avtorizacijskega centra, ki preiskuje zlorabe in je odkril sumljivo transakcijo. Za pridobitev zaupanja posreduje imetniku podatke o tem, kje ja nazadnje kupoval, vrsti njegove kartice, številki kartice in rokom veljavnosti. Od imetnika v cilju preprečitve nadaljnjih zlorab zahteva celotno številko kartice oz. varnostno trimestno številko na zadnji strani kartice.

Pridobitev teh podatkov storilcem omogočajo plačevanja blaga in storitev preko svetovnega spleta, kjer za izvedbo plačila zadostujejo že ti podatki.

3.12 Phishing – ribarjenje

Ribarjenje v kartičnem poslovanju pomeni zavajanje uporabnika z namenom kraje identitete oz. osebnih podatkov. Storilci poskušajo na nedovoljen način pridobiti podatke uporabnika o številki računa kartice, številko kartice, CVV2 oz. CVC2 številko in seveda tudi PIN številko. Zlorabe se dogajajo s pošiljanjem ogromne količine elektronske pošte naslovnikom, kjer storilec poskuša ustvariti zaupanje s tem, da se navidezno predstavlja kot predstavnik organizacije, v katero ima naslovnik zaupanje. Ponavadi se predstavlja kot predstavnik bank ali avtorizacijskih centrov. Primer takšnega sporočila vidimo na sliki št. 9.

Slika 9: Primer ponarejenega elektronskega sporočila MasterCard

Vir: www.nlb.si

Za povečanje zaupanja so v sporočilu tudi povezave na spletne strani, ki so navidez povsem podobne spletnim stranem bank ali drugih izdajateljev kartic, ki jih uporabniki ponavadi uporabljajo za dostop do elektronskega bančništva. V sporočilu storilec zavaja naslovnika z reklamiranjem novih ugodnih storitev, banke, akcijah, popustih, brezplačnih ponudbah. Na ta način prepriča komitenta, da obišče lažno spletno stran »navidezne« banke in vnese v rubrike podatke o svoji kartici, ki storilcu omogočijo zlorabe. Stran je pogosto zelo podobna pravi spletni strani banke, s tem, da zahteva vnos dodatnih podatkov, ki jih prava stran ne zahteva. Na sliki št. 10 vidimo pravo spletno stran, na sliki št. 11 pa lažno spletno stran osebnega bančništva NLB d.d.

Slika 10: Prava vstopna stran spletnega bančništva

Vir: www.nlb.si

Slika 11: Lažna vstopna stran spletnega bančništva

Vir: www.nlb.si

Veliko vlogo pri preprečevanju zlorab na način ribarjenja imajo sami uporabniki. Zaščita pred ribarjenjem je uspešna, če:

- uporabniki spletnega bančništva dostopajo do spletnih mest z vnosom naslova internetne strani (URL) v naslovni vrstici in ne preko ponujenih povezav v elektronskem sporočilu, ki uporabnika preusmerijo na lažne strani, kakor tudi ne preko brskalnikov, ki lahko med ponujenim naslovom banke, ponudi tudi spletni naslov lažne strani
- zavrnejo sporočila, ki prihajajo z neznanih naslovov od nepoznanih pošiljateljev ali z naslovov, ki so samo navidez podobni naslovom bank
- ob komunikaciji s spletnim naslovom preverjajo ikono za šifriranje spletnega mesta in povezave z njim (ključavnica)
- sprotno kontrolirajo in nadzirajo transakcije na računu.

3.13 Pharming – zvabljanje

Zvabljanje pomeni podoben način izvajanja zlorab kot ribarjenje, vendar poteka na bolj modificiran način. Poznamo dve obliki zvabljanja:

- zvabljanje z napadi na DNS strežnike (zastrupljanje DNS strežnikov)
- zvabljanje z napadi na datoteko o gostiteljih (hosts file), ki se nahaja na računalniku uporabnika.

Preko DNS strežnikov (Domain Name System) poteka poosebljanje in spreminjanje IP naslovov spletnih mest v uporabniku bolj prijazne naslove oz. imena spletnih mest. Takšen naslov je uporabniku bolj prijazen in si ga lažje zapomni kot pa sama številka spletnega mesta.

3.13.1 Napadi na DNS strežnike (zastrupljanje strežnikov)

Pri teh načinih pridobivanja podatkov storilci usmerjajo napade na strežnike, preko katerih poteka promet več uporabnikov. S tem lahko v zelo kratkem času pridobijo veliko količino podatkov o komitentih, ki poslujejo preko tega strežnika. Z napadi na strežnike storilci dosežejo, da DNS strežnik ustvarja napačne oz. lažne povezave in uporabnika brez njegove

vednosti preusmeri iz pravega naslova na lažen naslov, ki je ponavadi identična kopija prave strani, ki bi jo uporabnik rad obiskal. Na tej strani je poleg običajnih podatkov največkrat potrebno vnesti še druge podatke o kartici, ki storilcu omogočajo izvajanje zlorab.

3.13.2 Napadi na host datoteke uporabnika

Host datoteka uporabnika je datoteka, v kateri so vpisani najbolj pogosto obiskani IP naslovi, s pripadajočimi URL naslovi. V računalniku se nahaja na mestu C:/WINDOWS/system/rivers/etc. Storilci z vdori v računalnike uporabnikov prepišejo prave datoteke z lažnimi naslovi in uporabnik tudi z uporabo pravilnega URL naslova dostopa na lažno spletno stran, ki je identična kopija prave spletne strani. Dostopi do host datotek se vršijo z vdori v sistem ali s pomočjo virusev ali trojanskih konjev. Za obrambo pred napadi na host datoteke je potreben ustrezen antivirusni program.

3.14 Zlorabe preko interneta

Internet zagotavlja neskončne razvojne možnosti za veliko število ponudnikov storitev, vključujoč trgovce, banke in druge nebančne izdajatelje kartic, ponudnike računalniških storitev, poštna in telekomunikacijska podjetja. Uporaba interneta, kot nizko stroškovnega omrežja, je že močno uveljavljena. Je cenejša kot uporaba najetih linij, vendar manj varna. To postavlja kartično industrijo v dilemo: po eni strani si ne moremo privoščiti zastoja v razvoju, po drugi strani pa uvedba interneta pomeni premik od varnega in zaprtega finančnega omrežja k odprtemu in nezaščitenemu komunikacijskemu omrežju. (Abanka Vipa d.d., 1999: 7)

Kljub temu, da se izdajatelji kartic zavedajo, da je poslovanje preko interneta lahko nevarno, morajo iti v koraku s časom. Zato še naprej razvijajo finančne storitve z vključenim internetom.

Pri zlorabah preko interneta se srečujemo s tremi skupinami zlorab (Newton, 1996: 41):

- z zlorabami kartic tistih imetnikov, ki preko interneta niso nikoli poslovali
- s ponavljajočimi transakcijami tistih imetnikov, ki so številko svoje kreditne kartice v sistem vnesli le enkrat, transakcije pa se nato bodisi s tega ali drugih prodajnih mest ponavljajo iz meseca v mesec

- z zlorabami na račun naivnosti imetnika, ki mora ob vpogledu na določeno internet stran vnesti številko kreditne kartice, kljub temu, da na strani piše, da je vpogled brezplačen.

Večina ponudnikov blaga in storitev na internetu posluje preko varnih strežnikov (SSL-protokol), kar pomeni, da je komunikacija med kupcem in prodajalcem varna. Koda SSL protokola je tako varna, da bi bili potrebni dobri računalniki in veliko časa za razbitje enega sporočila. Šibko točko v tej verigi predstavljata ponudnik in kupec. Kupci se tako najpogosteje ujamejo na zelo preproste "limanice" in sporočijo podatke svoje kreditne kartice neznanemu ponudniku, ki v resnici ničesar ne prodaja, temveč le zbira njihove podatke. (Tekavc, 1998: 68) Zaradi tovrstnih težav izdajatelji kartic poskušajo v internetno poslovanje v veliki količini uvesti elektronski podpis in kodiranje transakcij.

3.15 Lažne prošnje za izdajo kartic

Lažne prošnje se izdajajo za že obstoječe kartice - zlorabijo se osebni podatki osebe, ki že ima kartico. Ponavadi gre za lažno spremembo naslova. Tako storilci prestrežejo pošto.
Vendar je ta način že skorajda nemogoč, ker izdajatelji poleg strožjih ukrepov za ugotavljanje istovetnosti uvajajo tudi kontrolo sprememb stalnih prebivališč pri uradnih organih.

3.16 Zlorabe kartic s strani trgovcev (Merchant Fraud)

V trenutku, ko nam prodajalec vzame kartico, si z njo lahko pripravi osnovo za zlorabo kartice. To lahko kasneje zlorabi na več načinov:

- Telemarketing je pridobivanje podatkov o uporabnikih plačilnih kartic preko telefona ali e-pošte, sledijo mu zlorabe v obliki MO/TO transakcij, ko trgovec ponuja razne ugodnosti pri nakupu za pridobitev informacij.
- Pranje slipov je izmenjava odtisnjenih slipov med prodajnimi mesti.
- Multipliciranje slipov brez vednosti uporabnika kartice, pri reproduciranju slipov na "zip-zap" napravi ali izvedbi transakcije na POS terminalu.
- Elektronski zajem podatkov je zloraba shranjenih podatkov o karticah, ki jih imajo trgovci v svojih bazah, s strani uslužbencev ali tretje osebe (vdor v bazo podatkov).
- Prenaredba podatkov na slipu; po opravljeni transakciji in po podpisu uporabnika trgovec spremeni (poviša) znesek plačila.
- Sprejem bele plastike, to je kartice z embosiranimi ali skimiranimi podatki.

- Point of compromise: trgovec oskrbuje ponarejevalce s pravimi podatki o plačilnih karticah – scimming. Scimming se zgodi istočasno kot transakcija.
- Collusive merchant (prodajno mesto zarote): lastnik oziroma prodajalec sprejema v plačilo ukradene, izgubljene ali ponarejene kartice. (Abanka Vipa d.d., 2000)

Znan je slovenski primer zlorabe s strani trgovcev:

Po pojavu ponarejenih kartic je vse kazalo na scimming. Duplicirane kartice so se pojavile pri več slovenskih bankah in tudi uporabljene so bile po celi Sloveniji. Ob reševanju reklamacij je bilo ugotovljeno, da se vedno uporablja le en kos plastike, ki pa ima vedno drug zapis. Raziskovanje primera je pripeljalo do ugotovitve, da so vsi imetniki pred zlorabo obiskali omenjeno restavracijo. V povezavi s policijo je bilo ugotovljeno, da magnetne zapise "krade" natakar.

Iz tujine (ZDA) je poznan primer, ko je nekdanji obveščevalec tajne službe Albert Gonzales s pomočjo dveh sodelavcev ukradel podatke o 170 milijonih kreditnih kartic iz baz podatkov trgovskih hiš (T.J. Maxx, Barnes & Noble, Sports Authority, OfficeMax). Kot bivši obveščevalec je v službi lovil nepridiprave, ki so zlorabljali podatke o bančnih in kreditnih karticah, zdaj pa je proti njemu vložena obtožnica zaradi kraje informacij. Grozi mu celo kazen dosmrtnega zapora (www.mojevro.si, 18.08.2009).

3.17 Zlorabe kartic v Sloveniji

Največ zlorab kartic je do nedavnega prihajalo s strani imetnikov kartic. Veliko pa je bilo tudi zlorab ukradenih, izgubljenih in nikoli prejetih kartic.

Svetovni trend pa je tudi slovenske kriminalce pripeljal do organiziranih vdorov v računalniške sisteme izdajateljev kartic.
Od leta 1996 dalje prihaja tudi do organiziranih vdorov v sisteme slovenskih kartičnih izdajateljev. Osnovne značilnosti večjih vdorov so (Abanka Vipa d.d., 1999: 10):

- napadi se vedno pričnejo v četrtek ali petek (konec tedna)
- napadi se običajno pričnejo pred prazniki (1.maj, 15.avgust, Novo leto) ali čez poletje (julij, avgust)
- v večini primerov gre za računalniško generirane številke kartic in fizično ponarejanje kartic

- kartice pripadajo določenim intervalom posameznega kartičnega izdajatelja ali sistema,
- zadeti intervali in zadeti BIN-i sovpadajo z BIN-i in številkami kartic imetnikov, ki so resnično potovali v Hong Kong, Singapur, Indonezijo, Malezijo itd.
- napad traja 3 do 5 dni in se začne z množico transakcij istočasno
- transakcije se nanašajo na računalniško in audio-video tehniko, hotelske in gostinske storitve, letalske prevoze
- reakcija izdajatelja kartice je možna šele, ko pričnejo prihajati prvi slogi iz "clearinga" – poravnave.

Zlorabe se vršijo predvsem s ponarejanjem licenčnih kreditnih kartic.

3.18 Kdo so storilci?

Storilce, ki izvršujejo zlorabe na področju elektronskega bančništva, lahko razdelimo po oblikah zlorab, ki jih izvajajo. Kot smo ugotavljali v prejšnjih poglavjih, se zlorabe na tem področju med seboj razlikujejo tako po načinu izvedbe, kompleksnosti, kakor tudi po tipih storilcev, ki se specializirajo za določeno obliko zlorab.

Pri zlorabah, ki jih izvajajo lastniki kartic, ko zavedno, zaradi slabe evidence, finančne stiske ali drugega razloga, prekoračijo dovoljene limite na debetnih karticah oz. prekoračijo dovoljene limite nakupov s plačilnimi karticami in svojih obveznosti ne poravnavajo, so seveda v vlogi storilcev sami lastniki kartic oz. transakcijskih računov. Pri tej vrsti zlorab iskanje storilca seveda ni težavno, saj ima banka vse podatke o lastniku računa. Tudi preiskovanje kaznivega dejanja s strani policije ni težavno, saj je storilec znan že ob zaznavi kaznivega dejanja, največkrat ob prijavi banke.

Pri vseh drugih zlorabah kartic, ki so opisane, se nam pojavljajo domači in tuji storilci zlorab. V manjši meri gre pri nas tudi za domače storilce, ki se preizkušajo na tem področju. Zaradi majhnosti Slovenije in velike prepoznavnosti oseb pa se pogosto dogaja, da se z zlorabami ukvarjajo storilci, ki pridejo iz drugih držav, se pri nas zadržijo krajši čas, nato pa hitro zapustijo območje naše države skupaj s podatki, ki so jih pridobili o karticah ali pa z denarjem in predmeti, ki jim ga je uspelo dobiti s ponarejenimi ali kako drugače zlorabljenimi

karticami, podatki katerih so bili zlorabljeni in prekopirani v drugih državah. Govorimo o mednarodnem kriminalu in storilcih, ki so organizirani v strukture, podobne podjetniški organizaciji. Takšna združba ima šefa, vodje posameznih skupin in izvrševalce, ki imajo strogo razdeljene naloge, so specializirani za izvajanje določenega postopka, ki ima za cilj dosego premoženjske koristi. Kot vidimo, so takšni storilci dobro organizirani in imamo vse znake organizirane kriminalitete.

Pri nas se največkrat kot tuji storilci pojavljajo državljani Romunije, Bolgarije, Hrvaške in Madžarske, ki kot izvrševalci pridejo k nam z večjimi količinami ponarejenih kartic in v kar najkrajšem času poskušajo priti do denarja ali blaga, ki ga takoj zamenjajo za denar, našo državo pa po storjenih zlorabah zapustijo. Pri nas se ponavadi pojavljajo v skupinah po trije. Povprečen čas zadrževanja in izvajanja zlorab je dva do pet dni. Dvige izvršujejo v serijah in uporabljajo naenkrat več kartic na posameznem ali več bančnih avtomatih. Predvsem se zadržujejo v večjih mestih, saj so tam manj opazni. Zapisi kartic, ki jih zlorabljajo, največkrat izvirajo iz Velike Britanije, ZDA in drugih držav. Največkrat dvigajo denar na bančnih avtomatih in ga preko Western Uniona takoj nakazujejo svojim predpostavljenim, saj je v tem primeru težje izslediti pošiljatelja in prejemnika denarja. Obstajajo tudi že primeri, ko so storilci pri nas s pridobljenim denarjem kupili predplačniške vrednostne kartice za telefon in klicali na tuje plačljive številke. Na ta način so zakupnikom telefonskih številk dejansko nakazali protipravno premoženjsko korist in zmanjšali možnost izsledite in odvzema denarja s strani policije.

Storilci se največkrat nastanijo v hotelih in prenočiščih, ki so v neposredni bližini bančnih avtomatov, kjer izvajajo zlorabe. Do bančnih avtomatov ponavadi pridejo peš, pri sebi pa imajo samo manjše število kartic in denarja, saj se na ta način izognejo večji izgubi in obremenilnim dokazom ob prijetju. Pripomočke za ponarejanje, vse druge ponarejene kartice in večje vsote gotovine hranijo v sobah, kjer so s sostorilci nastanjeni ali v avtomobilih, ki so v neposredni bližini mest, kjer izvajajo zlorabe.

Poznani so tudi primeri, kjer tuji državljani pridejo k nam, da bi prekopirali oz. pridobili zapise kartic, ki se uporabljajo pri nas. Z nameščanjem naprav za presnemavanje magnetnih zapisov v bančne avtomate in POS terminale poskušajo priti do podatkov iz magnetnih zapisov kartice in PIN kode. V kolikor so uspešni, podatke takoj izročijo drugim, ki jih

obdelajo, prenesejo na ponarejene ali bele kartice in v drugih državah izvršujejo zlorabe. V primerih, ki so se zgodili v Sloveniji, so bile pri nas prekopirani magnetni zapisi kartic uporabljeni v Romuniji in Bolgariji.

Tuje storilce je veliko težje identificirati in prijeti, saj so v kratkem času po opravljeni zlorabi že na drugem koncu Evrope. Prav tako jim je zelo težko odvzeti premoženjsko korist, ki so jo dosegli, saj jo na različne načine takoj po pridobitvi prenesejo svojim nadrejenim, tako da tudi ob prijetju pri njih denarja ne najdemo.

4 STATISTIČNI PODATKI O ZLORABAH

Pridobitev statističnih podatkov o vseh zlorabah na tem področju v Sloveniji in Evropi predstavlja nerešljiv problem. Podatke o zlorabah seveda vodijo posamezne banke, lastniki licenc in policija, ki zlorabe obravnava. Zaradi različnih omejitev, kot so nepopolne evidence, poslovne in bančne tajnosti, prikrivanje zlorab pred konkurenco in zakonske omejitve, pa popolnih podatkov ni mogoče dobiti, predvsem pa ne podatkov, ki bi zajemali vse zlorabe na nekem območju z vsemi karticami, ki so v uporabi.

4.1 Podatki policije

Policija vodi podatke o kaznivih dejanjih, ki jih obravnava v okviru svojega dela. Prvi problem se pojavi, ker policija ne obravnava vseh zlorab na tem področju, saj do podatkov o sumih zlorab lahko pridejo samo na osnovi prijave oškodovanca, lastnika kartice, banke ali koga drugega. Za gospodarsko kriminaliteto, kamor spadajo tudi zlorabe na področju elektronskega bančništva tako velja, da so posledice te kriminalitete skrite in na zunaj niso vidne. Prav tako v evidenci kaznivih dejanj, ki jih je obravnavala policija, ni zlorab, ki so se dejansko zgodile, a policija zaradi različnih razlogov (težavnost preiskovanja, premalo podatkov, mednarodna razsežnost, nesodelovanje finančnih institucij, (ne)uspešnost preiskovalcev, usposobljenost preiskovalcev…) ni uspela zbrati dovolj dokazov za potrditev kaznivega dejanja oz. ni uspela kaznivega dejanja dokazati znanemu storilcu in je bilo na tožilstvo podano samo poročilo. Torej lahko iz policijskih evidenc dobimo samo tiste podatke o zlorabah, ki jih je policija obravnavala in za te zlorabe tudi podala kazenske ovadbe. Seveda je v tem številu zajetih samo en del zlorab, ki so se zgodile. Policija vodi statistiko kaznivih dejanj po členih, ki so opredeljeni v kazenskem zakoniku. Področje zlorab na področju elektronskega bančništva pa nima za vsako zlorabo posebnega (specialnega) kaznivega dejanja, ampak se za določene zlorabe uporabljena splošna kazniva dejanja. Tako smo npr. v preteklosti (do 1.11.2008) imeli posebno kaznivo dejanje samo za zlorabe kartic, ki so jih storili lastniki kartic (Izdaja nekritega čeka in zloraba bančne ali kreditne kartice po 253. členu KZ), za zlorabe kartic na bankomatih, kjer je storilec s ponarejeno (skimming) kartico in posneto PIN številko dvignil gotovino iz bančnega avtomata, pa smo uporabljali za kvalifikacijo kaznivo dejanje velike tatvine (212. člen KZ), ki niti ni sodilo med »gospodarska« kazniva dejanja, ampak je kaznivo dejanje, ki opredeljuje vse klasične tatvine (kdor nekomu nekaj vzame…, pa pri tem premaguje večjo oviro). Podatki o zlorabah bančnih kartic se tako »izgubijo« med vsemi kaznivimi dejanji tatvin in na osnovi teh podatkov ne moremo z gotovostjo razbrati število zlorab. Glede na obstoječi informacijski sistem

slovenske policije bi bilo to spremljanje zaradi načina evidentiranja podatkov težavno, saj se kaznivo dejanje evidentira takoj po zaznavi ali naznanitvi. Dejanje je pogosto naznanjeno na policijski postaji, kjer policist s premalo izkušnjami napačno okvalificira samo kaznivo dejanje. V nadaljnjem postopku preiskovanja se sicer dejanje prekvalificira ob podani kazenski ovadbi ali poročilu, vendar v osnovni maski evidence ostane prvotna kvalifikacija ob evidentiranju. Kaznivo dejanje »Tatvina« se prav tako ob evidentiranju veže na odtujene predmete in če so v primeru odtujitve kartice poleg nje odtujeni še ostali predmeti, se pogosto dogaja, da je vnos vezan na druge predmete in ne samo na kartico (npr. denar, osebni dokumenti). V osnovni maski vnosa kaznivega dejanja tudi ni razvidna morebitna nadaljnja zloraba, ki ob naznanitvi še ni znana. Od 1.11.2008 smo dobili v Sloveniji z novim kazenskim zakonikom tudi nova kazniva dejanja, ki posebej veljajo samo za zlorabe na področju elektronskega bančništva. Tako kaznivo dejanje uporaba ponarejene bančne, kreditne ali druge kartice po 247. členu KZ-1 zajema zlorabe ponarejenih kartic in samo preslikavanje zapisov kartic, kakor tudi uporabo takšnih kartic. S temi spremembami bo tudi statistika policije v bodoče bolj verodostojna, še vedno pa se moramo zavedati, da bodo v teh številkah samo tisti primeri zlorab, kjer je policija uspela pridobiti dokaze za podajo kazenske ovadbe. Policijska statistika tako za preteklo obdobje razpolaga z naslednjimi podatki s področja kartičnih zlorab. Za našo nalogo je pomemben trend izvrševanja kaznivih dejanj na področju elektronskega bančništva, ne pa toliko absolutne vrednosti. Iz trenda bomo namreč lahko zaznali ali gre za naraščanje ali upadanje problematike in s tem za večanje ali manjšanje zlorab na tem področju.

Tabela 9: Število preiskanih kaznivih dejanj

Člen	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
225	2	6	2	10	30	24	88	283	98	76
242	1	1	0	0	5	6	4	6	9	15
253	1.865	2.516	2.687	1.465	2.158	2.625	2.110	1.496	774	428
247[22]								3	424	1.075

Vir: letna poročila policije

Iz tabele št. 9 je razviden stalen porast kaznivih dejanj s področja zlorab informacijskih sistemov, ki se v zadnjih dveh letih sicer umirja. To področje pokrivata kaznivi dejanji po 225. členu Neupravičen vstop v zaščiteno računalniško bazo podatkov[23] in 242. členu Vdor v

[22] Z novim KZ-1 imamo od 01.11.2008 novo KD Uporaba ponarejene bančne, kreditne ali druge kartice

[23] Od 01.11.2008 se to KD imenuje Napad na informacijski sistem po 221. členu KZ

računalniški sistem[24]. Policija ne vodi podatka, ali gre za bančni informacijski sistem ali za informacijski sistem druge institucije, zato ne moremo reči, koliko napadov na informacijske sisteme bančnih institucij se je dejansko zgodilo oz. je bil storilec tudi odkrit. Dokaj visoko število skozi celotno obdobje, čeprav v zadnjih letih beležimo upadanje, pa predstavlja kaznivo dejanje po 253. členu KZ »Izdaja nekritega čeka in zloraba bančne ali kreditne kartice[25]«. Pričakovali bi, da se bo število teh kaznivih dejanj zmanjšalo z zmanjšanjem čekovnega prometa[26], vendar se je na račun zmanjšanja plačilnega prometa s čeki povečalo število plačilnih kartic bančnih in nebančnih institucij, promet z njimi in tudi število njihovih zlorab. Konec leta 2008 je prišlo do spremembe kazenske zakonodaje in novih kaznivih dejanj. To je vplivalo tudi na statistiko kaznivih dejanj. V letu 2009 je opazen visok padec števila obravnavanih kaznivih dejanj po 253. členu KZ iz 1.496 na 774. Policija v svojem letnem poročilu za leto 2009 ne podaja razlage za tako izrazit padec, sklepamo pa lahko, da je do tega prišlo zaradi uvedbe novega kaznivega dejanja »Uporaba ponarejene bančne, kreditne ali druge kartice«, katerih kaznivih dejanj je policija v letu 2009 obravnavala skupaj 424. Tudi v letu 2010 se je število obravnavanih kaznivih dejanj po 253. KZ členu zmanjšalo, na kar 1.075 pa povečalo število obravnavanih kaznivih dejanj »Uporaba ponarejene bančne, kreditne ali druge kartice«.

4.2 Podatki bank

Banke seveda zbirajo in obdelujejo podatke o zlorabah na področju elektronskega plačilnega prometa. Na osnovi teh podatkov se odločajo o dodatnih zaščitah in o pogojih poslovanja s prodajnimi mesti in tudi s komitenti. Vsi podatki o zlorabah, kakor tudi drugi podatki, pa predstavljajo bančno in poslovno tajnost. Tako teh podatkov nismo mogli dobiti za našo raziskavo, poleg tega pa bi spet bili to samo delni podatki o zlorabah v Sloveniji, saj imamo pri nas veliko bank. Čeprav banke na področju elektronskega plačilnega prometa dokaj dobro sodelujejo med seboj v okviru Združenja bank Slovenije, pa se tudi v okviru združenja ti podatki ne zbirajo in obdelujejo, ker jih banke ščitijo pred konkurenco, kakor tudi pred javnostjo zaradi ohranjanja ugleda institucije. Podatke o zlorabah pri licenčnih karticah

[24] Od 01.11.2008 se to KD imenuje Vdor v poslovni informacijski sistem po 237. členu KZ

[25] Od 01.11.2008 je spremenjen člen tega KD v 246. člen KZ

[26] Novembra 2000 so banke sprejel nov, spremenjen dogovor o načinu unovčevanja čekov, ki je bil prilagojen Zakonu o čeku. Bistvo novega dogovora je bilo, da so se čeki lahko unovčevali le pri banki izdajateljici in da jih je banka plačala pod pogojem, da je imel izdajatelj na računu kritje

morajo banke, v skladu s pogodbami, sporočati tudi lastniku licence. Če je zlorab veliko, mora banka lastniku licence plačati kazen, saj sama ne bi dovolj storila za varnost poslovanja.

4.3 Podatki lastnikov licenc

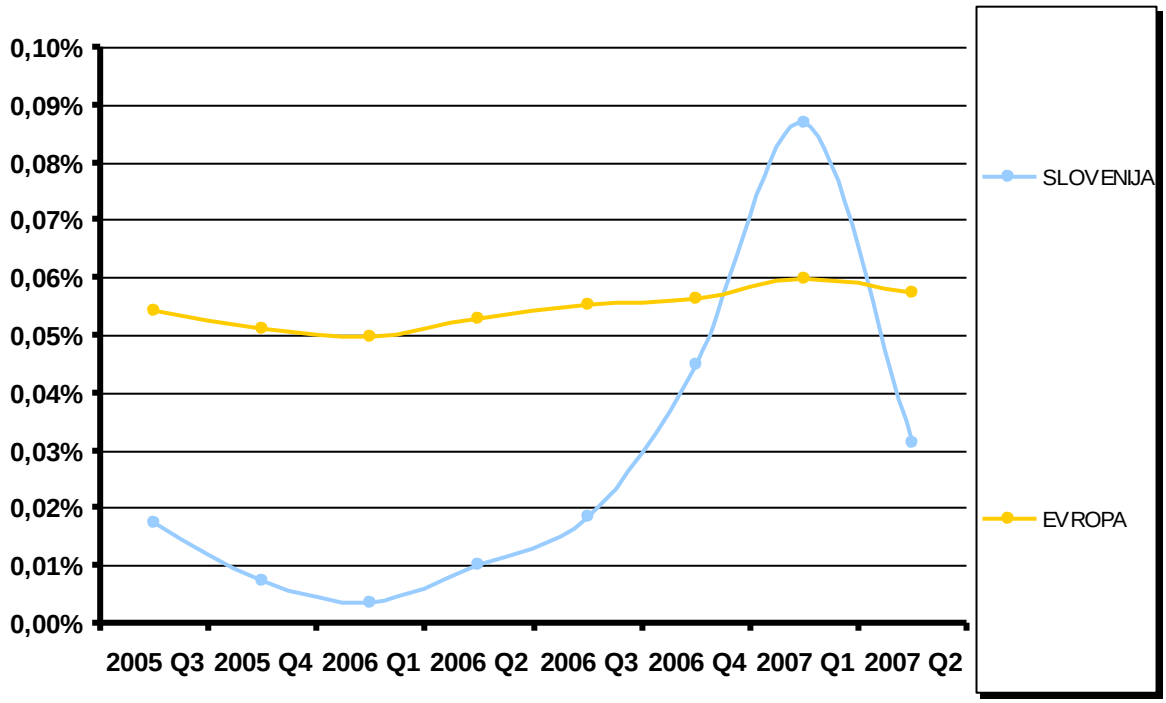
Lastniki licenc imajo vse podatke o uporabi njihovih kartic, saj se ti podatki obdelujejo v njihovih procesnih centrih. Od števila transakcij je seveda odvisna tudi licenčnina, ki jo banke plačujejo za uporabo licenčnih kartic. Število kartičnih transakcij posameznega lastnika licence je ogromno, s tem pa tudi zaslužek lastnika licence. Vsi lastniki licenc (Master Card, Visa, American Expres, Diners) prihajajo iz ZDA in zaradi tega se iz Evrope in ostalega sveta v ZDA steka ogromno denarja za plačilo licenčnih dajatev. Tudi zaradi tega se je v Evropski uniji pričela udejanjati pobuda, da bi v okviru EU ustanovili in izdali svojo licenčno kartico, s katero bi se lahko plačevalo blago in storitve po celem svetu.

V nadaljevanju bodo predstavljeni nekateri podatki o zlorabah enega izmed lastnikov licence. Na željo predstavnika lastnika licence, ki je posredoval podatke, ime lastnika licence ne bo objavljeno, gre pa za podatke enega izmed štirih največjih lastnikov licenc.

Število transakcij uporabe kartic po vsem svetu tega lastnika licence znaša okoli 9.000 v sekundi. Vse transakcije spremljajo na svojem informacijskem sistemu in jih analizirajo tudi z vidika varnosti poslovanja. Banke so jim dolžne sporočati vse zlorabe, ki se z njihovimi karticami dogajajo, da lahko prilagodijo zaščitne mehanizme. Več kot je zlorab, več se namenja za zaščito pred zlorabami. Ker pa dodatni zaščitni mehanizmi povečujejo stroške in zmanjšujejo dobiček, se za večjo varnost poslovanja odločajo na podlagi stroškov in koristi. V Ameriki kljub večjemu številu zlorab kot v Evropi še ne razmišljajo na prehod na pametne (čip) kartice, za kar se je Evropa že odločila, ker prehod na novo tehnologijo branja podatkov in njihovega obdelovanja pomeni velikanski strošek nadgraditve in zamenjave naprav.

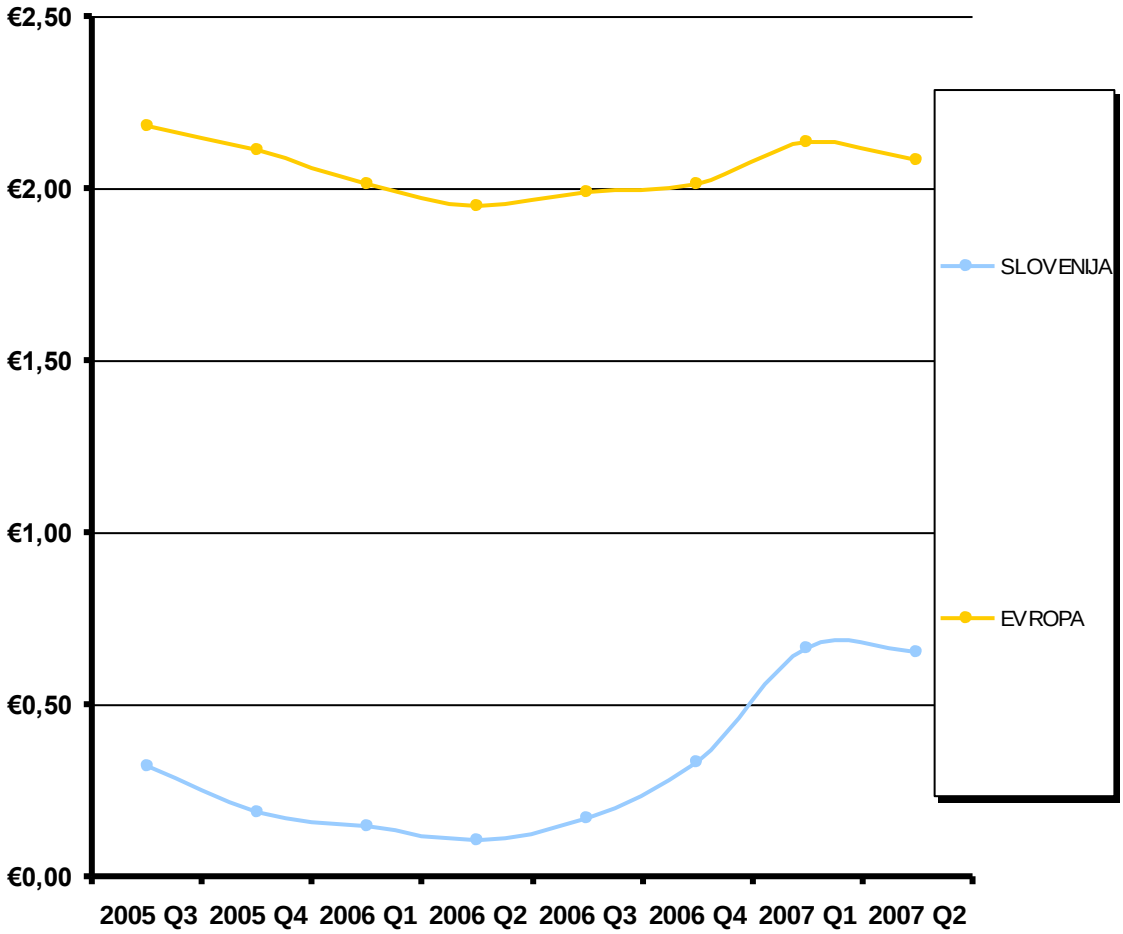
Zlorabe merijo v deležu, ki ga predstavlja razmerje med zneskom zlorab in zneskom transakcij. Delež 0,05 (na 100 EUR prometa 0,05 EUR zlorab) pomeni mejo med »normalnimi« zneski zlorab, ki niso pretirano zaskrbljujoči, vse, kar je nad to mejo, pa pomeni že impulz za ukrepanje.

Slika 12: Stopnje zlorab v Sloveniji in Evropi



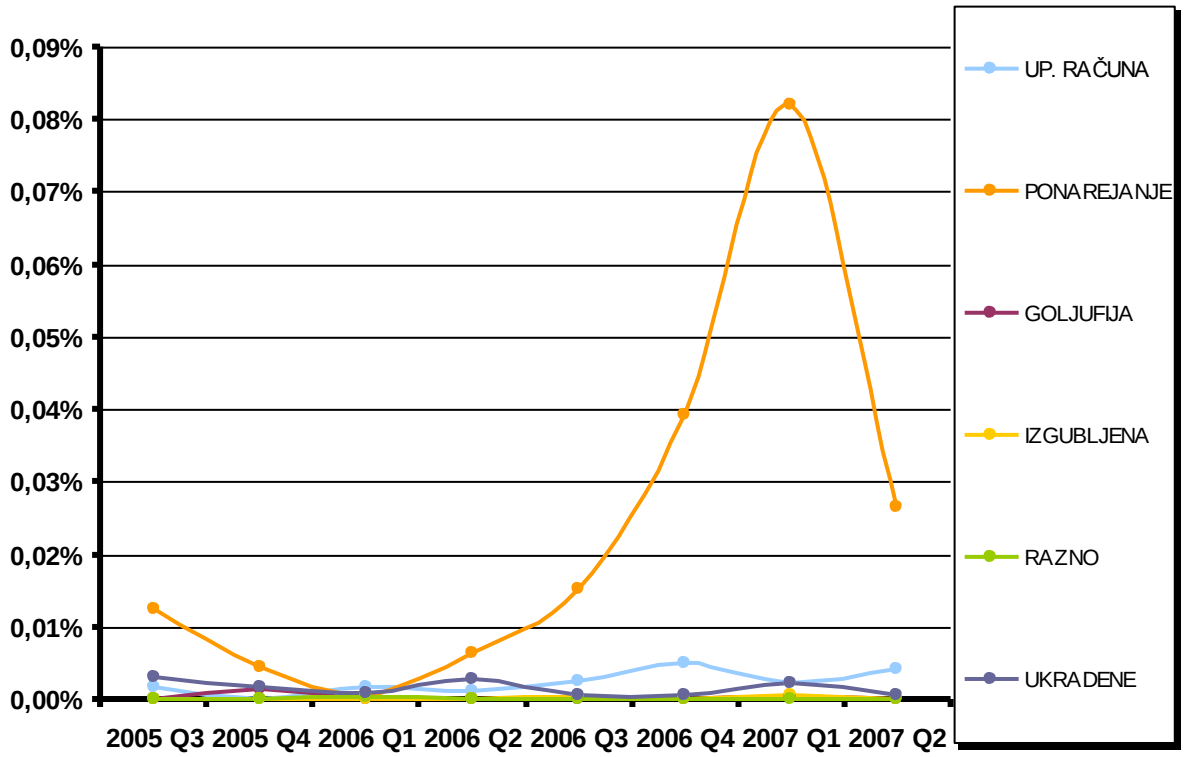
Iz podatkov o razmerju zlorab v Sloveniji in primerjave s povprečjem EU je razvidno, da smo pri nas imeli relativno malo zlorab, ki pa se je v obdobju ob prevzemu nove valute enormno povečalo. To povečanje ni nič običajnega, saj se je zgodilo tudi v drugih državah, ko so prevzemale evro. V Sloveniji smo ob prehodu na evro posvečali večjo pozornost nevarnosti ponarejanja denarja in tatvin pošiljk bankovcev in kovancev ob zamenjavi, ne pa zlorabam plačilnih kartic. Mogoče bi lahko s povečano dejavnostjo vseh udeležencev, ki skrbijo za varnost na tem področju, zmanjšali zlorabe oz. jih ohranili na prejšnjem, relativno ugodnem nivoju. Vidimo, da zlorabe v Evropi nihajo med vrednostjo 0,05 in 0,06 % glede na opravljen promet, kar ostaja v mejah, ki še veljajo za ne preveč rizične in jih je še mogoče obvladovati.

Slika 13: Povprečna vrednost zlorab na posamezno kartico



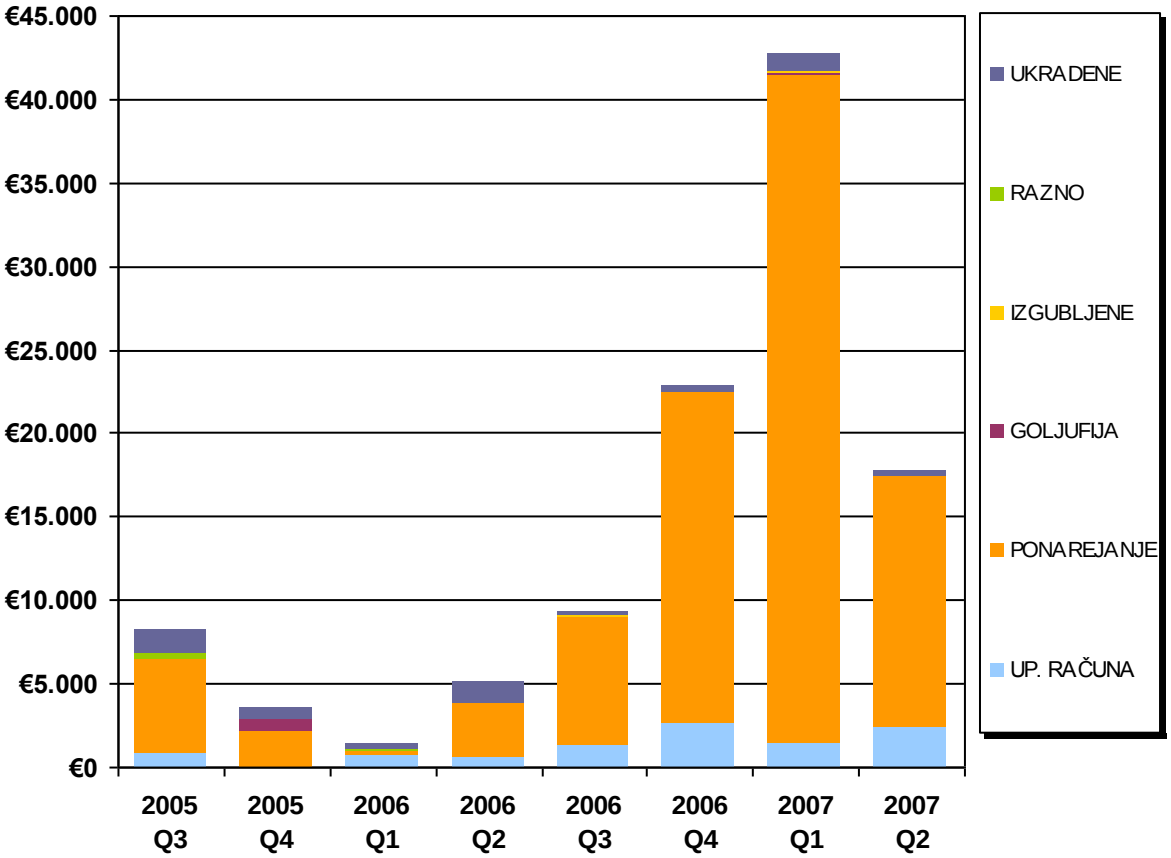
Slika prikazuje povprečno vrednost zlorab po posamezni kartici lastnika licence. Vidimo, da za celotno Evropo znaša ta vrednost okoli 2 EUR na kartico. Za Slovenijo do leta 2007 (prevzem Evra) velja relativno dokaj nizka vrednost zlorab, ki ne presega 0,5 EUR na kartico. Tudi po prevzemu evra, je vrednost malenkost višja od 0,5 EUR, kar v primerjavi z zlorabami po Evropi ostaja na zadovoljivi ravni.

Slika 14: Zlorabe kartic glede na način storitve



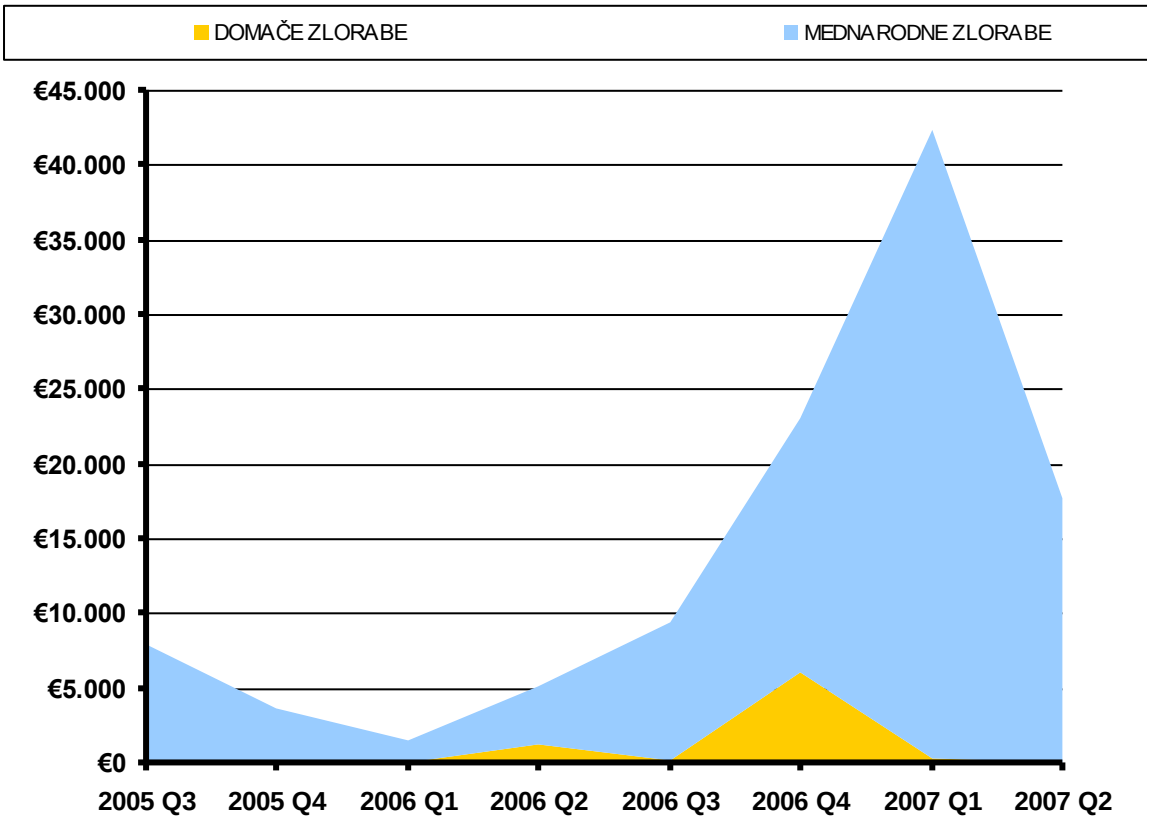
Iz slike vidimo, katere zlorabe in v kolikšnem razmerju se dogajajo s karticami nosilca licence, izdane pri nas. Največ zlorab oz. največja škoda je povzročena s ponarejanjem kartic, pri čemer je mišljeno ponarejanje magnetnega zapisa na kartici (SKIMMING). Ostali načini zlorab, od izgubljenih, ukradenih in kako drugače zlorabljenih kartic, niso tako pogosti in ne povzročajo velike škode. Iz grafa je razviden tudi razlog porasta zlorab ob prevzemu nove valute, ki je posledica zlorab kartic s ponarejanjem magnetnega zapisa. Število ostalih vrste zlorab se ni bistveno spremenilo.

Slika 15: Vrednost zlorab glede na način storitve



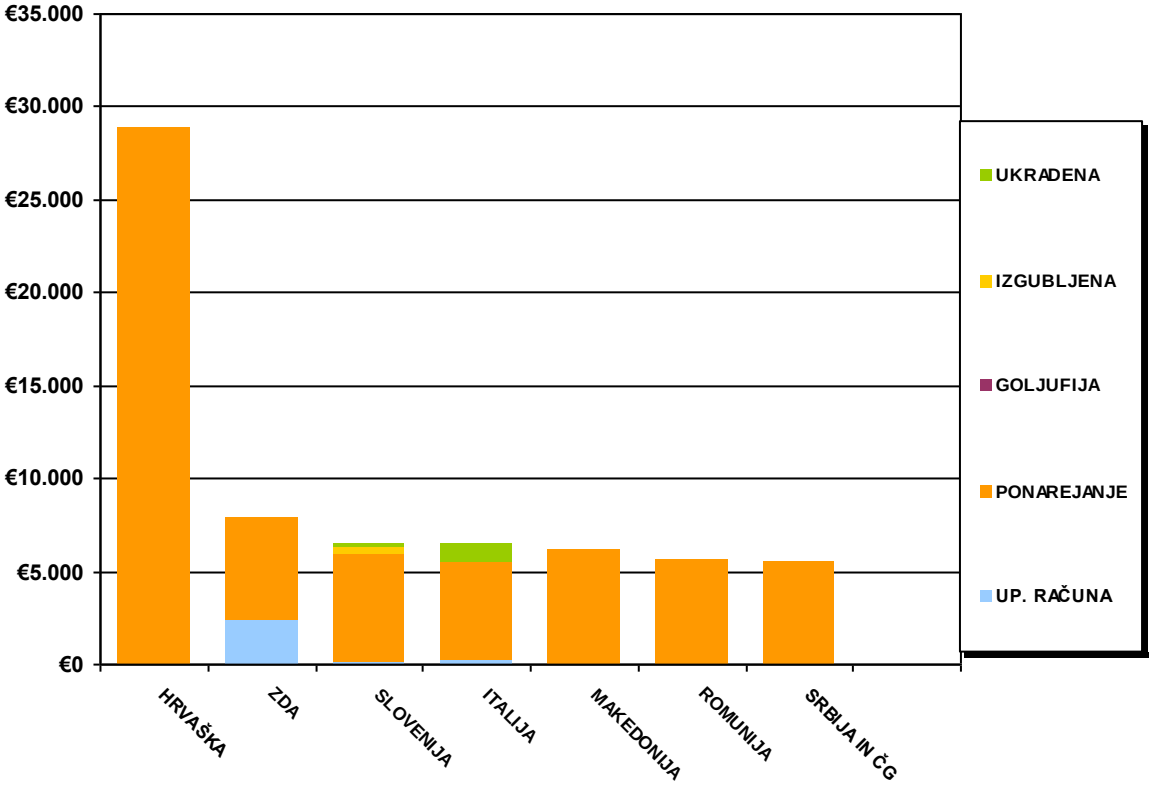
Iz slike vidimo vrednost zlorab glede na znane vrste zlorab. Večina zlorab naših kartic (samo enega lastnika licence) se zgodi s ponarejanjem magnetnega zapisa na kartici in tudi v absolutnem znesku povzroči največjo oškodovanje. Zlorabe na ta način so se najbolj povečale v prvem četrtletju leta 2007 in se nato znova zmanjšale.

Slika 16: Domače in mednarodne zlorabe



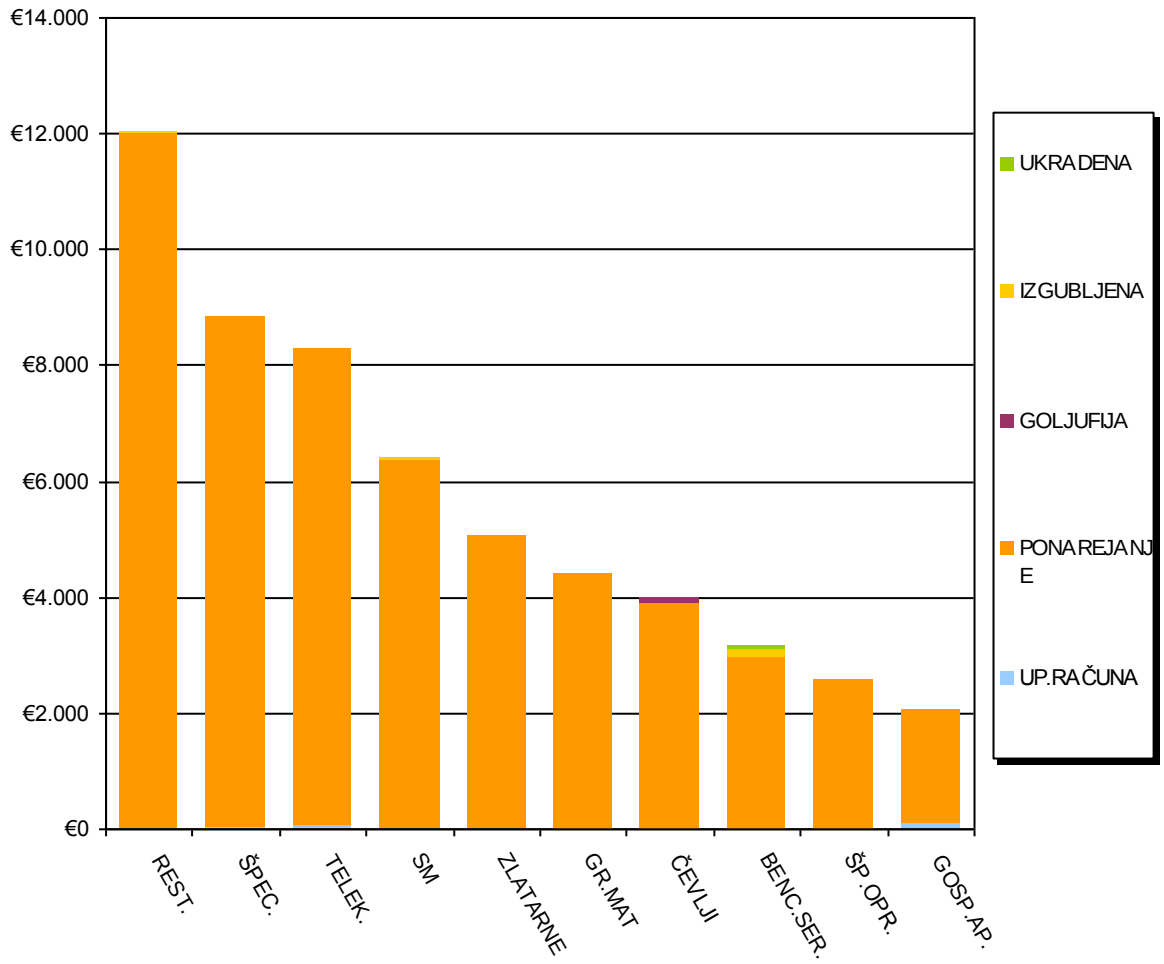
Slika prikazuje razmerje med domačimi in tujimi, mednarodnimi zlorabami. Razviden je znatno večji delež mednarodnih zlorab, kar pomeni, da so bile naše kartice zlorabljene v tujini. Zelo majhen delež zlorab naših kartic se je zgodil v Sloveniji, pa še ta zgolj v letu 2006. Razlogi za mednarodni aspekt so lahko tudi manjša možnost izsledite storilca in daljši čas do odkritja zlorabe, kar lahko omogoči večje število zlorab ene kartice oz. njenega zapisa in probleme pri zbiranju dokaznega gradiva, saj so sledovi storilca že izbrisani.

Slika 17: Zlorabe po državah (drugo četrtletje 2007)



Slika prikazuje, katere zlorabe naših kartic se najpogosteje zgodijo v drugih državah. Velika večina naših kartic (podatki so samo za eno licenčno kartico), je zlorabljena v sosednji državi Hrvaški na način, da je bil prekopiran magnetni zapis kartice. Ostale zlorabe na ta način, ki jih je tudi največ, se dogajajo v približno enakem obsegu (okoli 5.000 EUR) v ZDA, Italiji, Makedoniji, Romuniji, Srbiji in Črni gori. V ZDA je opazna tudi večja vrednost naših kartic z uporabo računa, kar je posledica obiskov različnih spletnih strani in zlorab na osnovi številk računov, ki so jih lastniki navajali pri plačilu različnih storitev ali blaga. Italija je tudi država, kjer je bilo večje število kartic tudi ukradenih in zlorabljenih.

Slika 18: Mesta zlorab naših kartic (drugo četrtletje 2007)



Slika prikazuje mesta, kjer so naše kartice največkrat zlorabljene. Vidimo, da so najpogostejše zlorabe spet s kopiranjem magnetnega zapisa kartice, ki se največkrat zgodi v restavracijah. Sledijo trgovine z živili, trgovine s telekomunikacijsko opremo, supermarketi, zlatarne, trgovine z gradbenim materialom, čevlji in bencinski servisi. Zlorabe se dogajajo še v trgovinah s športno opremo in pri plačevanju gospodinjskih aparatov.

5 METODE OCENJEVANJA INFORMACIJSKEGA TVEGANJA

V literaturi se pojavlja več vrst različnih metodologij za analizo in izračun tveganja. Zaradi naraščanja pomena in obsega elektronskega poslovanja, kakor tudi kompleksnosti in težavnosti ocenjevanja v institucijah, bo v prihodnosti potreba po učinkovitem ocenjevanju in upravljanju z informacijskimi tveganji naraščala in zahtevala prilagojene metodologije in orodja.

Pomemben del obvladovanja tveganja je poznavanje tveganj, ki izhajajo in so specifične za dejavnost organizacije (Moultor, R., Moultor, M., 1996), kajti izračun ocene tveganja lahko v dobršni meri pomaga pri prepoznavanju večine najpomembnejših tveganj. Ko so tveganja prepoznana, jim sledijo postopki za upravljanje s tveganji, katerih cilj je zmanjševanje tveganj.

Vsaka organizacija lahko za ocenjevanje tveganj in njihovo upravljanje sama uporabi katerikoli pristop glede na svoje specifične potrebe. Ocena tveganja pa mora poleg informacijske tehnologije zajeti tudi druge dejavnike, kot so človeški faktor, nepredvidene vremenske razmere, okvare in napake, zakonodajo, družbene in ekonomske razmere in drugo.

5.1 Splošne metode za izračun ocene tveganja

Metode za izračun ocene tveganja delimo na:

- kvalitativno metodo
- semi-kvalitativno metodo
- kvantitativno metodo
- kombinacijo metod.

Ko za izračun ocene tveganja nimamo na voljo zanesljivih podatkov o verjetnostih in stroških, je uporabna kvalitativna metoda za izračun ocene tveganj, kjer se skuša oceniti tveganje z bolj subjektivnimi in splošnimi ocenami (visoko, srednje, nizko). Rezultati takšnih ocen so tako bolj odvisni od znanja strokovnjaka, ki oceno izvaja. Za izračun je možno uporabljati tudi kombinacije kvalitativnih in kvantitativnih metod (GAO, 1999, str. 8).

5.1.1 Kvalitativna metoda

Ta metoda temelji na opisnem vrednotenju z uporabo različnih pridevnikov, številčnih vrednosti ali oznak za definiranje ocene tveganja, ranljivosti in groženj. V ta namen uporabljamo stopnje pomembnosti (nepomemben, manj pomemben, zmerno pomemben, zelo pomemben in izjemno pomemben) in stopnje tveganja (sprejemljivo, pogojno sprejemljivo in nesprejemljivo).

Prednosti kvalitativne metode so:

- enostavnost
- intuitivnost
- razširjenost.

Slabosti te vrste analize pa so:

- subjektivnost
- nenatančnost.

5.1.2 Kvantitativne metode

Kvantitativna metoda temelji na uporabi realnih številčnih podatkov in vrednosti. Na ta način lahko posledice možnih incidentov tudi stroškovno ovrednotimo. Poznamo več kvantitativnih metod za analizo tveganj:

- primerjalne analize (temeljijo na primerjavi)
- verjetnostni modeli, ki upoštevajo verjetnost dogodka
- neverjetnostni modeli, ki temeljijo na subjektivni oceni učinka dogodka, kot je npr. analiza scenarijev (Shon, 2006).

Prednosti kvantitativnih metod:

- objektivnost in
- natančnost

Slabosti kvantitativnih metod so:

- odvisnost od kakovosti podatkov in predpostavk
- zahtevna uporaba
- pomanjkanje statističnih podatkov za določanje frekvence posameznih sredstev

- potrebno je upoštevati celovit proces ocenjevanja
- težavnost denarnega vrednotenja sredstev (vseh dejavnikov ni mogoče kvantitativno ovrednotiti)
- težavnost vrednotenja kontrol
- potrebno je upoštevati tudi stroške sodnih postopkov in drugih posledic, ki jih je težko ovrednotiti.

5.2 Metode za ocenjevanje tveganja informacijske varnosti

Literatura navaja številne metode za oceno tveganja, ki se nanašajo na informacijske sisteme. Ocenjevanje tveganja vključuje tudi protiukrepe v smislu orodij za zmanjševanje verjetnosti uresničitve groženj pri varovanju informacij. Ta orodja so lahko različna, od organizacijske kontrole, kontrole logičnega dostopa, kontrole podatkov in informacij, kontrole škodljivih programov, kontrole aplikacij, do kontrole osebja. Razpoložljive metode za oceno tveganj so naslednje:

5.2.1 Metoda CRAMM

Kratica CRAMM pomeni CCTA Risk Analysis and Management Methodology (metodologija za analizo in obvladovanje tveganja). CCTA je osrednja agencija za računalništvo in telekomunikacije Velike Britanije. CRAMM metoda obravnava tveganje s tremi koraki in so nujni za pridobitev vseh potrebnih informacij za oceno tveganja. Metodo sestavljajo koraki: vrednotenje, grožnje in ranljivosti (CRAMM, 2001).

Tveganje je sestavljeno iz dveh sestavnih delov: stroškov posledic in posledic na sredstvih. Obe sestavini moramo ovrednotiti, če želimo tveganje izmeriti. Posledice na sredstvih sestavljajo grožnje in ranljivosti.

Proces CRAMM se prične z identificiranjem in vrednotenjem sredstev znotraj sistema in vključuje informacije, programsko opremo, strojno opremo in vse odnose med sestavnimi deli sistema. Grožnje in ranljivosti se ocenjujejo z vprašalniki po določeni lestvici. Mere tveganja se izračunajo z uporabo matrice tveganja, v zadnjem koraku pa se pripravi vodstveno poročilo (Braun G., 2002).

5.2.2 Metoda OCTAVE

Metoda OCTAVE daje širok pregled nad stanjem tveganj na področju informacijske varnosti in je temelj, ki ga uporabljamo pri osredotočanju na aktivnosti pri izboljšanju informacijske varnosti in zmanjševanju tveganj (Alberts C., 2003). Ta metoda se izvaja periodično, saj je vrednotenje tveganja le del upravljanja tveganja na področju informacijske varnosti in je potrebno ponavljati oceno za identificiranje novih nevarnosti, ranljivosti in drugih sprememb, ki bi lahko ogrožale informacijsko varnost organizacije. Poznamo OCTAVE metodo in OCTAVE kriterije.

OCTAVE kriteriji zajemajo vrsto načel, atributov in izhodov. Načela predstavljajo osnovni koncept vrednotenja in so razdeljena na tri kategorije:

- osnovna načela vrednotenja tveganja informacijske varnosti
- osnovna načela upravljanja tveganja
- organizacijska in kulturna načela organizacije.

Atributi predstavljajo karakteristike vrednotenja, izhodi pa izhodne informacije, ki jih moramo pridobiti v posamezni fazi metode. OCTAVE kriteriji zajemajo tri faze. Vsaka faza zajema vrsto aktivnosti, ob njenem zaključku pa dobimo potrebne izhodne informacije.

Tudi metoda OCTAVE je sestavljena iz treh faz, skozi katere analiziramo organizacijske in tehnološke probleme in oblikujemo sliko organizacijskih potreb varovanja. Sestavljena je iz procesov, ki predstavljajo skupek faz OCTAVE kriterijev, kot rezultat vseh procesov pa dobimo ustrezno strategijo varovanja in plan zmanjševanja tveganja za posamezna kritična sredstva.

5.2.3 Metoda ISRAM

Metoda ISRAM je metoda, namenjena analizi tveganja informacijskih sistemov na takšen način, da omogoča sodelovanje vodilnih in osebja v organizaciji (Karabacak B., Sogukpinar I., 2005). Temelji na sedmih korakih in jo opredeljuje formula:

Tveganje = možnost dogodka varnostne luknje X posledice dogodka varnostne luknje

Prvi štirje koraki metode ISRAM so namenjeni oblikovanju vprašalnika, v petem koraku se vprašalnik izvede, šesti in sedmi korak pa sta namenjena pridobivanju podatkov in rezultatov.

1. korak: zavedanje problema informacijske varnosti
2. korak: a.) seznam dejavnikov, ki vplivajo na možnost dogodka varnostne luknje in teža posameznega faktorja
   b.) seznam dejavnikov, ki vplivajo na posledice dogodka varnostne luknje in teža posameznega faktorja
3. korak: preoblikovanje dejavnikov v anketne vprašalnike, oblikovanje možnih odgovorov in določitev številčnih vrednosti za posamezen odgovor
4. korak: priprava tabele tveganja za možnost varnostne luknje in priprava tabele tveganja za posledice varnostne luknje
5. izvedba vprašalnika za možnost dogodka varnostne luknje in izvedba vprašalnika za posledice dogodka varnostne luknje
6. korak: uporaba formule in izračun
7. korak: ocena rezultatov izračunov in analiza izpolnjenih vprašalnikov s strani osebja.

Metoda ISRAM je kvantitativna metoda in uporablja vrednosti in števila, ki so povezana z vprašalnikom in tabelami tveganja. Ne vsebuje kompleksnih izračunov in matematičnih enačb, kar pomeni prednost te metode, kljub temu pa izpolni tako tehnološke kot poslovne zahteve.

5.2.4 Metoda BPIRM

Ta metoda je sestavljena iz dveh glavnih elementov (Coles R., Moulton R., 2003):

- zagotavlja odgovornost in lastništvo informacijskih tveganj, njihovo upravljanje, določitev prioritet in povratne informacije o vpeljavi kontrol in nadzoru
- model zagotavlja vključenost vseh ključnih oseb v proces sprejemanja odločitev in so upoštevana vsa ključna področja tveganj.

Proces ima šest komponent:

1. začetek oz. začetno točko, kjer se določi, kaj želi poslovni proces doseči, kaj je potrebno za to in kakšen bi lahko bil nasprotni udarec; določimo tudi namene in cilje procesa ob upoštevanju zunanjih dejavnikov okolja in sredstev, ki vplivajo na pristop, ki ga organizacija sprejme

2. določitev identifikacijskih zahtev, ki so lahko informacijske, pravne ali IT
3. ocena je osnova procesa in zajema analizo in kontrolo vseh področij izgube; kontrole naj bi zaznale luknje, izmerile izgube ali jih preprečile
4. izvedba pomeni proces nameščanja in testiranja kontrol v procesu
5. z upravljanjem razumemo dnevno delovanje kontrol
6. s potrditvijo se obravnava proces zagotovitve

Vsebina modela temelji na vrednostni verigi poslovanja in zajema vse ključne elemente poslovnega procesa. Znotraj okvirja lastništva je sedem slojev:

1. sloj: vodstvo organizacije in človeški viri
2. sloj: vodstvo procesa informacijske tehnologije
3. sloj: človeški viri procesa informacijske tehnologije
4. sloj: podatki – podprocesi/aplikacije – informacije
5. sloj: infrastruktura
6. sloj: tretje osebe
7. sloj: tehnologija

Cilj upravljanja s tveganji je, omogočiti lastniku tveganja, upravljati ta tveganja z izbiro primernih in cenovno učinkovitih kontrol. Kontrole morajo biti vpeljane na pravem mestu, kjer so potrebne in učinkovite. Za to je potrebno poznavanje in razumevanje pravih tveganj.

5.2.5 Metoda EBIOS

Ta metoda se uporablja za oceno in obravnavanje tveganja, ki je povezano z varnostjo informacijskih sistemov. Lahko se uporablja za različne namene, ki so povezani z varnostjo (priprava politik, različnih planov…). Metoda EBIOS formalizira občutljivosti in grožnje ter opredeljuje tveganja za organizacijo (EBIOS, 2004).

Sestavljena je iz različnih korakov. Prvi korak je seznanitev z organizacijo (organizacijska struktura, dejavnost, področje dela, zakonodaja), določitev predmeta obdelave (sistem in podatki, ki so z njim povezani, funkcionalni opis, varnostna pravila…) in pa opredeljevanje varnosti sistema (povezave med elementi in povezanimi elementi). V drugem koraku prepoznavamo varnostne potrebe in opredelimo varnostne zahteve, njihove kriterije in vplive. V tretjem koraku analiziramo grožnje in ranljivosti in kot rezultat dobimo seznam groženj. Četrti korak zajema primerjavo groženj in varnostnih potreb in kot rezultat dobimo tveganja,

povezana s sistemom. Določiti moramo dejavnosti, ki bodo odpravile tveganja in določiti varnostne nivoje. V zadnjem koraku definiramo, kako doseči varnostne cilje in kako upravljati s tveganji.

5.2.6 Metoda MEHARI

Metoda MEHARI je bila zasnovana kot pomoč varnostnim inženirjem pri izvajanju varovanja informacij. Metoda je opredeljena v več priročnikih:

- MEHARI: Koncepti in mehanizmi
- MEHARI: Analiza sredstev in klasifikacija
- MEHARI: Vodnik vrednotenja za varnostne inženirje
- MEHARI: Vodnik za analizo tveganja
- MEHARI: Baza znanja in referenčni priročniki (Jouas J., Roule J., 2007).

Metoda MEHARI se uporablja predvsem za analizo tveganja in upravljanje z njimi, glavni cilj metode pa je analiza tveganja in zmanjšanje tveganj sistema. Različna orodja in modeli metode se lahko uporabljajo tudi posamezno. Rezultat metode so priporočila, katerih upoštevanje nam zmanjša tveganja.

Pri oceni varnosti pri metodi MEHARI obstajata dve možni oceni:

- modul hitre ocene (glavne slabosti in analiza ranljivosti)
- podrobnejši modul ocene (podrobno ugotavljanje slabosti z ekspertno bazo za oceno tveganja).

Analiza sredstev je sestavljena iz lestvice vrednosti okvar (nepomembno, resno, zelo resno in nujno potrebno) in klasifikacije informacij in informacijskih sredstev glede na razpoložljivost, celovitost in dostopnost.

Ta metoda omogoča kvalitativno in kvantitativno vrednotenje faktorjev, ki so povezani z informacijsko varnostjo in se navezujejo na informacijsko varnost in zmanjšanje tveganja in faktorjev, ki se nanašajo na dejavnost organizacije. Pri tej metodi se najprej izberejo cilji, parametri in komponente in v kakšnem zaporedju si bodo sledili. Potem sledi analiza in klasifikacija sredstev in presoja ranljivosti. Tako odkrijemo in izberemo situacije tveganja, ki jih nato analiziramo. Pri situacijah tveganja se ocenjujejo različni scenariji glede na možnost

pojava tveganja (ni možno, zelo malo verjetno, malo verjetno, verjetno in zelo verjetno) in možnost pojava vpliva, ki ga bo tveganje imelo. Vsak scenarij vsebuje vrste posledice in sredstva ter vrste povodov, ki lahko pripeljejo do situacije tveganja. V bazi metode MEHARI je okoli sto sedemdeset različnih scenarijev, ki so povezani s karakterističnimi dogodki, kot so nesreče, napake, nenamerna in namerna dejanja.

6 CELOVIT VARNOSTNI MODEL PREPREČEVANJA ZLORAB

Na osnovi izvedene analize zlorab plačilnih in kreditnih kartic smo zasnovali celovit varnostni model za preprečevanje zlorab. Mehanizmi modela, ki zajema različne dejavnike, omogočajo zaščito informacijskih sistemov in preprečujejo zlorabe, ki so na tem področju možne. Nekateri dejavniki vplivajo na obnašanje komitentov oz. uporabnikov informacijskih storitev na področju elektronskega bančništva in jih vzpodbujajo k boljšemu preventivnemu delovanju, drugi spet vplivajo na obnašanje storilcev zlorab, saj bi jih naj preko zagroženih kazni v kazenskih postopkih in odvzema protipravno pridobljenega premoženja navajali na to, da ne izvršujejo zlorab. V modelu so zajeti tudi drugi vidiki zaščite, ki skozi tehnično-tehnološke in organizacijske vidike ukrepov izboljšujejo varnost poslovanja. Varnostni model preprečevanja zlorab je tako zasnovan iz vloge bank in drugih finančnih institucij, vloge uporabnikov in vloge represivnih organov ter vpliv generalne prevencije na bodoče storilce zlorab.

Varnost je kompleksen pojem in ga ne moremo zajeti samo z enim raziskovalnim pristopom (Ambrož, Traudi, Mihalič, 2000). Golob (1997) govori, da je pojem varnostni sistem opredeljen kot sistem za zagotavljanje notranje varnosti in da skrbi za ohranitev reda, spoštovanja zakonov, osebne varnosti, kakor tudi zaščite imetja in celotne infrastrukture.

Vzpostavitev varnostne politike pomeni načrtovanje računalniške varnosti in razvoj načrta zanjo v smislu naslednjega (Holbrook, 1993):

- kaj hočemo zavarovati (podatkovne baze, spletne strani, zaupne dokumente…)
- pred kom želimo zavarovati (vsiljivci po internetu, industrijski vohuni, radovednimi zaposlenimi)
- predvideti možne nevarnosti, ki grozijo (odvisno od vsebine in vrste vsiljivcev)
- določitev spodje stopnje ali ravni varnosti, ki jo želimo doseči (odvisno od vsebine)
- razviti in uveljaviti mehanizme, ki bodo na racionalen način zagotovili zaščito
- kontinuirano spremljati proces varovanja in ga izboljšati vsakič, ko naletimo na slabost.

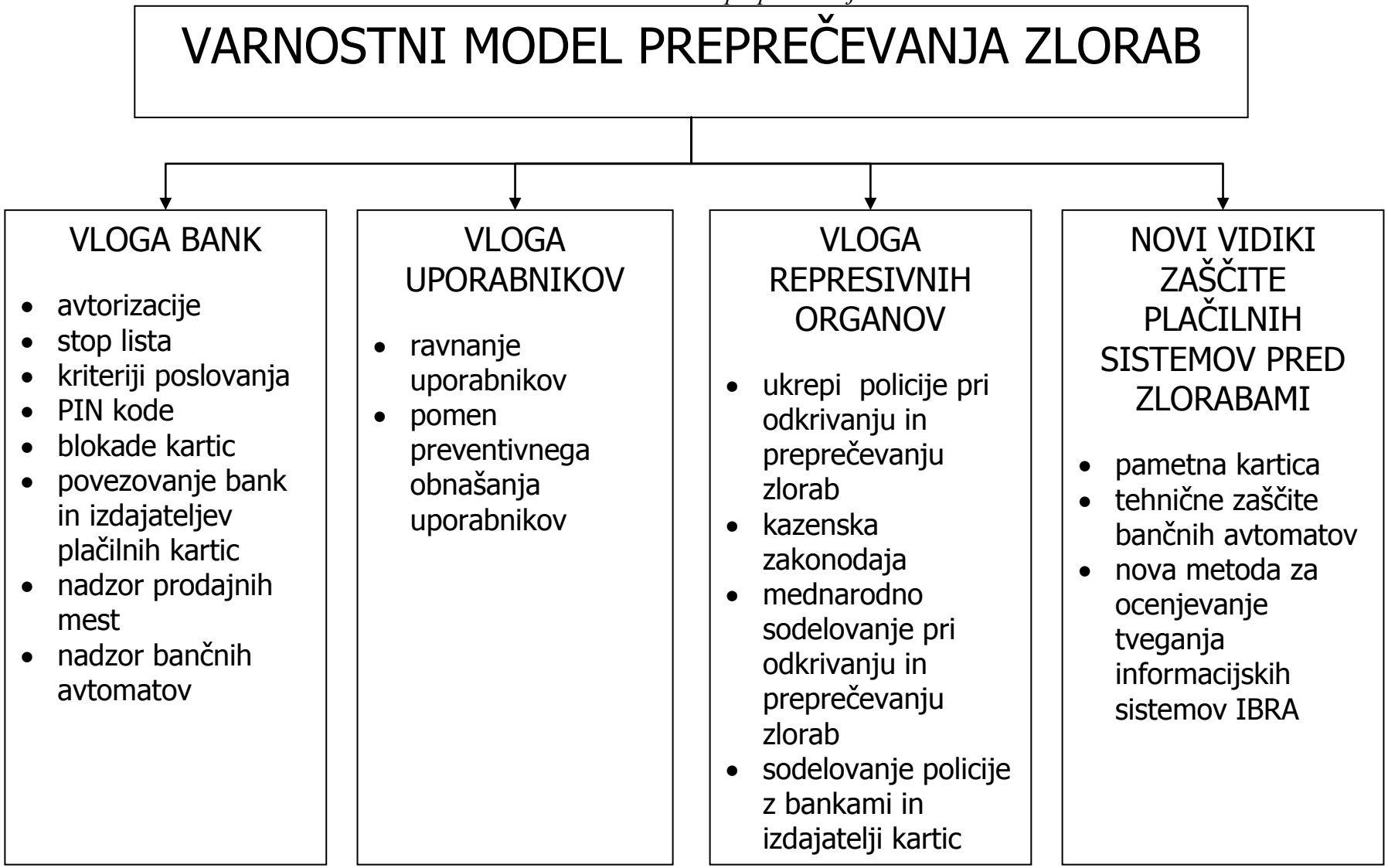
Pri hujših vdorih v podjetja ali bančne ustanove, katerih namen je največkrat finančna korist, samo tehnično znanje glede varnosti največkrat ni dovolj. Vdiralci pogosto potrebujejo tudi informacije o notranjih procesih ustanove. Zaradi tega se pogosto izkaže, da so pri vdorih v

bančne sisteme vpletene osebe, ki poleg tehničnega znanja poznajo tudi notranje procese in tokove informacij (Kajić, 1999).

Varnostna politika v obliki dokumenta je pripomoček vodilnim in tistim, ki so odgovorni za varnost. Z njo se izognemo nejasnostim in prelaganju odgovornosti. Smiselno je, da določimo možen cilj vdora in vitalne podatke, ki jih ščitimo. V skladu s tem določimo varnostno politiko in varnostne mehanizme, s katerimi jo dosegamo.

Glavna cilja računalniške varnosti sta zanesljivost in zaščita. Pri zanesljivosti sistema se ukvarjamo z zagotavljanjem razmer za delovanje storitev in normalno delo uporabnikov, v okviru zaščite pa govorimo o razmerju med dejanskim delovanjem sistema in njegovo predvideno namembnostjo (Trampuž in drugi, 2005).

Slika 19: Varnostni model preprečevanja zlorab



Slika 20: Dvodimenzionalni varnostni model

DEJAVNIKI	**PREVENTIVNI**	**REPRESIVNI**
ORGANIZACIJSKI	• kriteriji poslovanja • povezovanje bank in izdajateljev kartic • ravnanje uporabnikov kartic • preventivno obnašanje uporabnikov	• ukrepi policije pri odkrivanju in preprečevanju zlorab • kazenska zakonodaja in ukrepi • mednarodno sodelovanje pri odkrivanju in preprečevanju zlorab • sodelovanje policije z bankami in izdajatelji kartic
TEHNOLOŠKI	• avtorizacije • stop lista • PIN kode za zaščito • blokade kartic • nadzor prodajnih mest • nadzor bančnih avtomatov • pametna kartica • tehnične zaščite bančnih avtomatov • nova metoda za ocenjevanje tveganja informacijskih sistemov IBRA	• mednarodno policijsko sodelovanje – informacijsko podprte baze zlorabljenih kartic in storilcev

Varnostne politike in varnostni modeli ponavadi obravnavajo rešitve z vidika organizacijskih in tehnoloških rešitev. Naš varnostni model za odkrivanje in preprečevanje zlorab smo prikazali še v dvodimenzionalni matriki, ki smo jo razdelil na organizacijske in tehnološke vidike in na preventivne in represivne ukrepe, kar je tudi novost in prednost našega modela, saj upošteva vse dimenzije varnostne politike. Vse dejavnike, ki vplivajo na področje zlorab elektronskega bančništva, smo vnesli v matriko, glede na to, v katero področje spadajo.

Iz same matrike je razvidno, da dejavniki enakomerno pokrivajo tri polja matrike, v četrtem polju (represivni ukrepi – tehnološki vidik) pa najdemo samo en dejavnik, ki vpliva na področje zlorab kartic.

Zastavljen model daje pozitivne rezultate, ki so vidni pri žal redko uspešno odkritih, preiskanih in tudi zaključenih primerih. Žal se pri tej vrsti gospodarske kriminalitete dogaja, da je zaradi velike mobilnosti storilcev, kratkega časa za ukrepanje in relativno slabih sledi s kraja kaznivega dejanja, velikokrat zelo težko odkriti in prijeti storilce zlorab. Ta težava pa se ne pojavlja samo pri nas, ampak pomeni težavo tudi za druge države, ki se z zlorabami kartic soočajo (Lamberger I., 2007).

6.1 Vloga bank in drugih finančnih institucij

Vloga bank in drugih finančnih institucij, ki opravljajo storitve na področju elektronskega bančništva, je vsekakor zelo pomembna, saj same (seveda v sodelovanju in v skladu s pogoji, ki jih postavljajo tudi lastniki licenc) določajo pogoje uporabe elektronskega bančništva, sklepajo pogodbe o poslovanju tako z uporabniki plačilnih in kreditnih kartic in tudi s prodajnimi mesti. Pri nas je velika teža pri preprečevanju in sankcioniranju zlorab namenjena tudi sodelovanju bank s policijo, ki se nanaša predvsem na kakovostno in hitro medsebojno obveščanje o zlorabah, kajti ravno hitra izvedba ukrepov na eni in drugi strani je pomembna za preprečitev nadaljevanja zlorab in tudi za identifikacijo in prijetje storilca. Seveda pa si pravočasnega ukrepanja enih in drugih ne moremo predstavljati brez 24 urne dosegljivosti. Pri policiji to ni problem, saj ima moštvo (sicer v omejenem številu) vedno na razpolago, pri bankah pa je problem, ker deluje samo v okviru delovnega časa. Zaradi tega na področju kartičnega poslovanja Združenje bank Slovenije v svojih priporočilih bankam priporoča med drugim tudi 24 urno dosegljivost odgovorne osebe in njenega namestnika (security manager, risk manager), ki imata pooblastila in znanje za ukrepanje in sprejemanje odločitev v primerih zlorab na področju kartičnega poslovanja. Za pridobitev vedenja oz. znanja, kako ukrepati v

teh primerih, pa so pomembna usposabljanja in izobraževanja zaposlenih, ki delajo na tem področju, čemur v bankah namenjajo tudi velik poudarek.

Pri nas poteka sodelovanje bank in izdajateljev kartic s policijo na področju kartičnega poslovanja in preiskovanja zlorab na precej visokem nivoju. Dejavnosti za odkrivanje in preprečevanje zlorab ter odkrivanje storilcev so usklajene v okviru Odbora za kartično poslovanje, Delovne skupine za varnost kartičnega poslovanja pri Združenju bank Slovenije, katerega članica je tudi Policija, vendar brez možnosti glasovanja o odločitvah, so pa vse dejavnosti v skladu z zakonodajo in policijskimi postopki. Takšno sodelovanje se je pokazalo za izjemno dobro in je zelo redko glede na druge države.

Bržkone je zelo pomembna tudi vloga Evropske unije oz. Evropske komisije v okviru projekta SEPA[27]. Kartični okvir SEPA SCF (SEPA Cards Framework[28]) je dokument, ki uveljavlja načela in pravila za uporabo kartic znotraj območja SEPA, vendar ne daje konkretnih odgovorov na specifična vprašanja. Pravila se bodo do 01.01.2011 uveljavila z drugimi dokumenti, ki jih pripravlja delovna skupina SEPA CWG[29] in bodo obvezna za vse članice EPC, tudi za ZBS in Slovenijo. V okviru SEPA CWG deluje tudi delovna skupina za preprečevanje zlorab (Card Fraud Prevention Task Force). Dejavnosti skupine so naslednje (Nabergoj, 2007):

- ukinitev oz. zmanjšanje zlorab magnetnih zapisov kartic EMV z upoštevanjem komercialnih vidikov
- uvajanje in širjenje varnih rešitev v poslovanju na daljavo (CVX2 in 3D Secure)
- analiza zbirnih podatkov o zlorabah kartičnega poslovanja in tesno sodelovanje z Evropsko centralno banko
- preprečevanje zlorab na področjih, kjer se kartica ne pojavlja v fizični obliki (elektronska in mobilna plačila).

[27] Single Euro Payments Area

[28] Od maja 2007 obstaja tudi prevod v slovenskem jeziku, ki je na voljo na spletnih straneh ZBS

[29] Card Working Group, delovna skupina EPC za kartično poslovanje

6.1.1 Avtorizacija

Avtorizacija je postopek, ki pomeni privolitev izdajatelja plačilne kartice za izvedbo zahtevane finančne transakcije. (Abanka Vipa d.d., 1999: 13)

Ob avtorizaciji se preverja:

- ali je znesek, za katerega se zahteva avtorizacija, v skladu z limiti porabe, ki so določeni za komitenta in njegovo kartico (če so le-ti preseženi, se avtorizacija zavrne)
- ali se kartica nahaja na STOP listi ukradenih, izgubljenih ali kako drugače zlorabljenih in blokiranih kartic
- ali je kartica veljavna in aktivna s strani izdajatelja.

Avtorizacija se opravi ob vsakem nakupu na prodajnem mestu ali dvigu gotovine na bančnem avtomatu. Ob dvigu gotovine se avtorizacija izvede avtomatsko preko bančnega avtomata in omrežja bankomatov, na prodajnem mestu pa preko komunikacijske povezave v avtorizacijski center izdajatelja ali preko POS terminala. POS terminali omogočajo neposreden nadzor nad poslovanjem imetnikov.

6.1.2 Stop lista

STOP lista je seznam kartic, katerih imetnikom izdajatelj kartice več ne dovoljuje uporabe kartice. Posamezna kartica se na STOP listo uvrsti na podlagi zahteve stranke (izguba ali kraja kartice) ali banke (nedovoljeno negativno stanje, sumljive transakcije, nekorektno poslovanje), lahko pa tudi zaradi suma kopiranja magnetnega zapisa kartice na prodajnem mestu ali bančnem avtomatu. Načini, kako banke obveščajo svojo prodajno mrežo o blokiranih karticah, so različni glede na tehnično opremljenost prodajnega mesta. Glede na to se STOP lista deli na: papirnato STOP listo, ki se je poslužujejo prodajna mesta, ki niso opremljena s POS terminali (papirnato listo prejmejo prodajna mesta dvakrat mesečno – 5. in 20. v mesecu[30]) ter elektronsko STOP listo, ki se preverja avtomatsko ob izvršitvi transakcije na POS terminalu. (Iglič, 1998: 57)

[30] Zaradi uvedbe elektronskih POS terminalov, se papirnate STOP liste več ne pošiljajo prodajnim mestom

6.1.3 Kriteriji poslovanja s plačilnimi karticami za komitente

Banke se pred tveganji kartičnega poslovanja in problemom neplačevanja komitentov zavarujejo na najrazličnejše načine (Iglič, 1998: 56):

- vzpostavitev in upoštevanja ustreznih bonitetnih kriterijev za pridobitev kreditne kartice in kartice z odloženim plačilom; vsaka prejeta vloga za izdajo plačilne kartice se obravnava v odvisnosti od:
  - ekonomske sposobnosti prosilca
  - njegovega zaposlitvenega statusa
  - trajanja ter korektnosti preteklega poslovnega sodelovanja z banko
- določitev individualnih limitov mesečne porabe, saj banka vsakemu imetniku kreditne kartice in kartice z odloženim plačilom določi limit mesečne porabe v odvisnosti od njegove ekonomske sposobnosti.

Debetne kartice se izdajo avtomatsko ob otvoritvi računa. Pri njih mesečna poraba in limiti niso določeni, temveč se z njo posluje v okviru stanja na računu in dovoljenih limitov.

6.1.4 PIN kode za uporabo kartic

PIN koda ali osebna številka je številka, ki omogoča ugotavljanje avtentičnosti kartice in ugotavljanje identitete imetnika kartice (banka je dolžna izdajati kartice v skladu z mednarodnimi (ISO) standardi in standardi plačilnih sistemov, v katere se banka vključuje, varnostni elementi in zaščita pred ponarejanjem je določena v skladu s standardi in tehnološkimi rešitvami in jih posamezna kartica mora vsebovati (embosiranje, holografi, magnetni trakov, podpisni trakovi, čip, itd.). Identiteta imetnika se lahko preverja tudi s podpisom imetnika, vendar je takšno preverjanje zaradi slabe kontrole na prodajnih mestih izredno pomanjkljivo.

6.1.5 Blokade kartic

Blokade kartic so povezane s STOP listo. Banka oz. izdajatelj kartice zaradi različnih razlogov (kraja, izguba, zloraba) uporabi mehanizem blokade posamezne kartice in takšno kartico uvrsti na STOP listo, s čimer doseže, da opravljanje transakcij s takšno kartico ni več mogoče. S tem prepreči uporabo kartice in nove zlorabe. Blokada posamezne kartice ali serije

kartic se lahko izvede na zahtevo imetnika ali po lastni presoji izdajatelja zaradi sumljivih transakcij oz. drugih pokazateljev, ki kažejo na zlorabo ali možnosti zlorab.

6.1.6 Povezovanje bank in izdajateljev plačilnih kartic

V posamezni državi obstaja več bank in drugih družb, ki izdajajo kreditne in plačilne kartice in opravljajo plačilni promet z njimi. Izdajajo svoje oz. domače kakor tudi tuje, licenčne kartice. Banka se lahko z zlorabo sreča kot tista, ki upravlja z računom komitenta, katerega kartica je bila zlorabljena, ali kot upravljavec računa prodajnega mesta, ki ima z njo podpisano pogodbo. Zaradi tega morajo banke in izdajatelji kartic tudi medsebojno sodelovati in si sporočati podatke o zlorabah in zlorabljenih karticah, da lahko preprečijo nadaljnje zlorabe in prekličejo originalne kartice, katerih magnetni zapis je bil zlorabljen.

V Sloveniji obstaja Združenje bank Slovenije, ki je prostovoljno združenje bank in drugih finančnih institucij s področja bančništva. Članice so skoraj vse banke v Sloveniji. V okviru ZBS deluje tudi Odbor za varnost kartičnega poslovanja, katerega naloga je ravno delovanje na področju zlorab plačilnih in kreditnih kartic.

6.1.7 Postopki pri nadzoru prodajnih mest

Naslednje postopke izvajajo banke pri nadzoru poslovanja in delovanja prodajnih mest, s katerimi imajo sklenjena pogodbe o poslovanju s plačilnimi in kreditnimi karticami. Trgovci oz. druge organizacije so lahko opremljene s POS terminali, imprinterji, kot internetna trgovina ali kot trgovci s posebnimi rešitvami. Posebna pozornost je namenjena analizi prometa na prodajnem mestu in zaznavanju neobičajnega odstopanja od povprečnih vrednosti, kar je lahko eden izmed znakov, da se na prodajnem mestu izvršujejo zlorabe. Po temeljiti analizi in preverjanju banka obvešča o sumu zlorab policijo, ki na podlagi obvestila oz. prijave izvede svoje postopke v skladu z zakonom. Pri preverjanju podatkov se banke poslužujejo tudi mednarodnega sodelovanja in mednarodnih baz podatkov (mednarodni sistemi za definiranje spornih prodajnih mest - CPP).

Redno dnevno spremljanje avtorizacij in transakcij

Na podlagi informacijske rešitve se dnevno spremlja promet vsakega prodajnega mesta tako avtorizacije kakor tudi vsota transakcij. Opravlja se analiza prometa in javlja vsako večje

odstopanje od povprečnih vrednosti na podlagi individualno določenih parametrov za vsako prodajno mesto posebej.

Redno dnevno spremljanje prometa komitentov

Z individualno postavljenimi parametri, ki so prilagojeni glede na plačniško obnašanje vsakega posameznega komitenta, je z informacijskimi rešitvami omogočeno analiziranje uporabe njegove plačilne kartice. Odstopanja od običajnega »obnašanja« komitenta se javljajo kot možnosti zlorab, ki se preverijo na druge načine (telefonsko preverjanje pri imetniku, nadzor prodajnega mesta, kontaktiranje procesnega centra). V kolikor se neobičajnosti poslovanja komitenta potrdijo kot sumi zlorab, lahko izdajatelj kartico blokira in o tem obvesti komitenta, banko, ki ima s prodajnim mestom sklenjeno pogodbo in policijo. Informacijski sistemi so s svojimi rešitvami in nastavitvami parametrov pripomogli tudi k temu, da so izključene možnosti zaračunavanja dvojnih oz. večkratnih enakih zneskov transakcij na prodajnih mestih (večkratni poteg kartice) in uporaba ene kartice v istem času na različnih območjih sveta (v primeru uporabe klona kartice v drugi, oddaljeni državi).

Analiza imetniških reklamacij

Opravlja se analiza reklamacij, podanih s strani imetnikov kartic. Posebna pozornost mora veljati tistim reklamacijam, pri katerih imetniki navajajo, da ni bila kartica vedno v njihovem vidnem polju (plačevanje v restavracijah brez prenosnih POS terminalov). Reklamacije lahko kažejo na možne zlorabe, saj imetniki reklamirajo plačila, za katere domnevno niso sami dali privoljenja. Če se reklamacija izkaže za resnično, obstaja sum, da je bila kartica kopirana, klonirana in uporabljena za plačilo brez vednosti in privolitve imetnika.

Izobraževanje in usposabljanje trgovcev

Banke skrbijo za usposabljanje in izobraževanje zaposlenih v organizacijah, s katerimi sklenejo pogodbe o opravljanju kartičnega plačilnega prometa. Poznavanje pravilnega postopka opravljanja plačil, zaščitnih elementov kartic, konstrukcije in lastnosti POS terminalov in drugih naprav za opravljanje plačilnega prometa, identifikacije kupca in poznavanje možnosti zlorab, omogočajo prodajalcem boljše možnosti za prepoznavanje zlorab. Na ta način zmanjšamo tveganja možnosti izvrševanja zlorab na prodajnih mestih, kjer

prodajalci niso udeleženi v zlorabah, saj s povečano pazljivostjo pri izvajanju plačil odvračajo storilce zlorab.

Ustrezni pogodbeni odnosi s podizvajalci

Za zagotavljanje elektronskega plačilnega prometa ima banka sklenjene pogodbe z mnogimi podizvajalci. Od izdelave, personalizacije, do vročitve kartice, opravljajo za banko izdajateljico različne storitve tudi drugi podizvajalci. Ti prav tako lahko vzdržujejo informacijske sisteme banke, bančne in POS terminale na prodajnih mestih. Z ustreznimi pogodbami in načrti morajo biti pogodbeni odnosi ustrezno urejeni. Tako mora biti zagotovljena identifikacija serviserjev, ki popravljajo ali zamenjujejo bančne avtomate in POS terminale na prodajnih mestih, obiski in zamenjave morajo biti zabeležene, potrebno je zagotoviti tudi tajnost podatkov, še posebej tistih, ki jih storilci potrebujejo za izvrševanje zlorab.

Medsebojno obveščanje med bankami

Medsebojno obveščanje pri sumih zlorab je zelo pomembno, da se lahko zlorabe preprečijo ali vsaj omejijo. Tako mora tisti (banka izdajateljica, procesni center), ki ugotovi sum zlorabe na podlagi reklamacije imetnika ali na drug način, obvestiti banko, ki ima s prodajnim mestom sklenjeno pogodbo, procesni center in policijo.

Medsebojno obveščanje članic ZBS

V priporočilih ZBS je določeno tudi medsebojno obveščanje vseh članic ZBS o konkretni zlorabi na prodajnem mestu in tudi medsebojno obveščanje o primerih novih modusov zlorab. S tem so lahko članice bolj pozorne na poslovanje konkretnega prodajnega mesta oz. na možnost zlorab na nove načine. Zaradi hitrega in kakovostnega obveščanja so članice medsebojno izmenjale tudi seznam kontaktnih oseb, ki v članicah skrbijo za varnost poslovanja, na seznamu pa so tudi kontaktne osebe v policiji, ki se ukvarjajo s problematiko zlorab na področju kartičnega poslovanja.

Medsebojno obveščanje lastnikov licenc mednarodnih plačilnih kartic

V skladu s pogodbami med bankami izdajateljicami in lastniki licenc mednarodnih plačilnih kartic so banke dolžne obveščati lastnika licence o vseh zlorabah, da lahko ta na podlagi podatkov reagira na zlorabe in prilagodi zaščitne in organizacijske rešitve, ki zmanjšajo možnost zlorab.

6.1.8 Postopki pri nadzoru bančnih avtomatov (BA)

Prav tako kot pri postopkih s prodajnimi mesti se tudi na področju bančnih avtomatov priporoča 24-urno dosegljivost odgovornih oseb (security manager, risk manager…) v bankah, lastnicah bančnih avtomatov. Te osebe morajo imeti pooblastila in znanje, vedenje za ukrepanje in komuniciranje z upravljalcem bankomatne mreže oz. policijo.

Preprečevanje zlorab na bančnih avtomatih, predvsem pa odkrivanje dodatno nameščenih naprav za izvajanje zlorab temelji na:

Redno pregledovanje bančnih avtomatov

Bančni avtomati se morajo s strani oskrbnika natančno redno pregledovati. Pomemben je zunanji pregled bančnega avtomata in odkrivanje nameščenih naprav oz. sledi, ki kažejo na to, da so bile ali še bodo nameščene. Pomembni so sledovi pripomočkov za pritrjevanje naprav kot npr. ostanki lepilnega traku ali poškodbe na ohišju bančnega avtomata, ki kažejo na to, da je bila nameščena dodatna naprava. Tudi različne škatlice s propagandnim materialom v prostoru okna bankomata kažejo na možnost namestitve video kamere, saj pri nas na samem bančnem avtomatu ne sme biti nameščenega nobenega propagandnega gradiva. Nameščene letvice z video kamero so pogosto oblepljene z logotipi bank ali izdajateljev kartic, kar bi naj prikrilo nameščeno napravo pred komitenti. Oskrbnik bančnega avtomata pa takšne dodatke takoj opazi in so redni pregledi zelo pomembni. Obstaja že tudi tehnična zaščita, ki prepozna nekatere dodatno nameščene elemente na bančnih avtomatih, kar olajša odkrivanje dodatno nameščenih naprav, pregledi s strani oskrbnika pa so kljub temu še potrebni.

Redno spremljanje neobičajne uporabe kartic na bančnih avtomatih

Oskrbnik bančnega avtomata mora biti pozoren na kartice, ki jih bančni avtomat zadrži. Vrsta kartic in izgled (bela plastika) lahko takoj pove, da so storilci na bančnem avtomatu vsaj poskušali izvrševati zlorabe in obstaja možnost zlorab tudi na drugih prodajnih mestih in bančnih avtomatih, prav tako pa je potrebno ugotoviti, kje in kdaj so prišli storilci do podatkov o pravih karticah (CPP). Na odvzetih karticah se lahko nahajajo biološki sledovi, ki nas pripeljejo do storilcev, zato mora biti oskrbnik bančnega avtomata poučen o tem, na kakšen način bo zavaroval takšno kartico. Pomemben podatek pri pregledu uporabe bančnih avtomatov je lahko tudi pogosto preverjanje stanja računov brez opravljenih transakcij dviga, ali dvigovanje postopnih, nižjih zneskov, do izkoriščenega limita. Ti podatki kažejo, da uporabnik bančnega avtomata ni poznal vseh parametrov o kartici oz. bančnem računu in je s poskušanjem in preverjanjem stanja ugotavljal, koliko lahko največ oškoduje lastnika računa, preden bančni avtomat zadrži kartico.

Usposabljanje oskrbnikov bančnih avtomatov

Pri usposabljanju oskrbnikov bančnih avtomatov je pomembno, da so seznanjeni z možnostmi zlorab in predvsem znaki, ki kažejo na zlorabe. Zaradi tega so oskrbniki vključeni v različne oblike usposabljanj oz. seznanjanja z novimi modusi zlorab, ki se pojavljajo, prav tako pa morajo poznati postopke in ukrepe, ki sledijo zaznavi zlorabe in katere osebe in institucije morajo obveščati, kako ravnati z napravami in karticami, ki jih odkrijejo, da ne opozorijo storilca na odkritje ali ne uničijo sledov, ki bi nas pripeljali do storilca.

Izbira ustrezne lokacije bančnega avtomata in primernega varovanja

Izbira primerne lokacije bančnega avtomata je brez dvoma pomembna zaradi večjih ali manjših možnosti za izvajanje zlorab ravno na določenem avtomatu. Storilci za izvajanje zlorab ponavadi izbirajo bančne avtomate točno določenih tipov ali na skriti, odmaknjeni lokaciji, kjer je manjša možnost, da bi bili odkriti. Izogibajo se tudi bančnih avtomatov, ki so že sami opremljeni s kamerami ali je kamera nameščena v okolici bančnega avtomata. Lokacija bančnega avtomata in sama vgraditev pa je pomembna tudi za izogibanje možnosti za klasično kriminaliteto, kot so tatvine celotnih bankomatov, ropi strank, ko dvigujejo denar in druge oblike tatvin in vandalizma.

Redno obveščanje in ozaveščanje strank

Banke same ali v okviru Združenja bank Slovenije permanentno skrbijo za obveščanje in ozaveščanje komitentov o samozaščitnem delovanju in modusih novih zlorab. Na ta način se povečuje preventivna dejavnost samih komitentov in zmanjšujejo možnosti za izvrševanje zlorab. Samo zakritje tipkovnice bančnega avtomata z roko ali denarnico pri vnosu osebne številke, ki jo svetujejo banke komitentom, prepreči in onemogoči storilcem dvig gotovine na bančnem avtomatu s komitentovega računa kljub temu, da so namestili video kamero, saj ne morejo posneti odtipkanih številk.

Ustrezni pogodbeni odnosi s podizvajalci

Prav tako kot pri oskrbi in vzdrževanju naprav na prodajnih mestih, je tudi na področju bankomatne mreže potrebna skrb pri sklepanju pogodb in določitvi medsebojnih razmerij s podizvajalci. Obstajati mora evidenca dostopov v notranjost bančnih avtomatov, evidenca oseb, ki imajo dostop, evidenca serviserjev in evidenca odpravljenih napak. Sama prekinitev delovanja bančnega avtomata je lahko že indic, da gre za zlorabo, prav tako pa lahko storilci tudi takrat, ko je bančni avtomat v okvari in ne dela, izvajajo zlorabe.

Poleg tega je ZBS sprejelo tudi priporočila Mastercarda, namenjena bankam izdajateljicam, ki so:

- obvezna vzpostavitev obveznih dnevnih limitov komitentov in vzpostavitev nižjih limitov
- vzpostavitev sistema parametrov, ki v zgodnji fazi opozarjajo o zlorabah (npr. prekoračeno število poskusov vnosa PIN)
- kontrola pogostosti transakcij v primerjavi z običajnimi navadami komitenta
- vzpostavitev inteligentnih sistemov, ki delujejo po načinu pravil (nevtralna mreža)
- kontrola aktivnosti na bankomatih in POS terminalih v večernih urah, med vikendi, prazniki in v njihovem času
- preverjanje pojavljanja kartic na stop – listah
- preverjati storno in kreditne transakcije na računu (zlorabe fizičnih karakteristik avtomatov)
- osveščanje imetnikov (obveščanje, vzgoja in izobraževanje – finančna kultura)
- stalno prilagajanje programske in strojne opreme bankomatov in POS terminalov

- spremljanje in prepoznavanje neaktivnosti bankomata v času
- video nadzori in najem varnostnih služb
- ustanovitev preiskovalne skupine, ki bo preiskovala kraje in zlorabe (notranja in zunanja)
- zagotavljanje dvojne kontrole in razdeljevanje – ločevanje znanj pri upravljanju s ključi in varnostno tehnologijo
- kontrola vseh kod napak pri bankomatskih zlorabah
- tehnično in fizično spremljanje bankomatov ter preverjanje, da na njih ni nameščene skiming ali podobne naprave
- spremljanje neobičajnih aktivnosti v tujini
- spremljanje nameščanja bankomatov
- trening in nadzor serviserjev bankomatov, da prepoznajo manipulacije na bankomatu, in preprečevanje zlorabe znanj (Združenje bank Slovenije, 2005).

6.2 Vloga uporabnikov

Uporabniki storitev elektronskega bančništva so brez dvoma tisti, ki lahko sami največ naredijo za varnost poslovanja s svojimi kreditnimi in plačilnimi karticami. Zaradi tega je velik del dejavnosti tako bank, kakor tudi policije preko preventivnih ukrepov usmerjen na vlogo in ravnanje uporabnikov storitev. Čeprav je tehnologija elektronskega bančništva na videz in za računalniško podkovanega uporabnika sicer preprosta, pa je za opravljanje transakcij vseeno potrebno osvojiti nekaj znanja s področja uporabe tehnologij za elektronsko komuniciranje in poslovanje. Teh znanj največkrat niso vešči ravno starejši ljudje, ki pogosto tudi zaradi tega in nepazljivosti pri ravnanju in opravljanju storitev elektronskega bančništva postanejo žrtve različnih oblik zlorab. Navajeni so bili namreč zgolj na gotovinsko poslovanje in na preproste bančne storitve kot so hranilne vloge oz. nakazovanje pokojnin na transakcijske račune. V takšnih primerih poslovanja je potrebno zelo malo znanja in spretnosti za to, da na zadovoljiv način opraviš bančno storitev, saj večino dejavnosti izvede bančna uslužbenka. Z informatizacijo bančnega poslovanja so finančne institucije skoraj v celoti prešle na elektronsko poslovanje in ponudile uporabnikom kopico novih storitev in instrumentov, za njihovo uporabo pa je potrebno že določeno znanje. Prav to je razlog, da so starejši nemalokrat žrtve zlorab, saj tudi storilci poznajo pomanjkljivosti določenih starostnih skupin uporabnikov elektronskega bančništva. Prav zaradi tega je ravnanje uporabnikov s

svojo kartico, certifikatom, geslom in ravnanje pri uporabi različnih storitev zelo pomembno za izpostavljenost komitenta kot žrtve zlorabe.

6.2.1 Ravnanje uporabnikov

Uporabniki lahko s svojim ravnanjem preprečijo skoraj vsako izmed zlorab, ki smo jih opisali v opisu in analizi vseh možnih zlorab na področju elektronskega bančništva. Prav tako pa lahko na žalost s slabim ravnanjem omogočijo in storilcem olajšajo izvajanje zlorab oz. jih celo s svojo nepazljivostjo navajajo na zlorabe.

Ravnanje uporabnikov elektronskega bančništva je zaradi tega zelo pomembno v smislu preprečevanja zlorab. Tega se zavedajo tako ponudniki elektronskega bančništva in tudi drugi, ki poskušajo zmanjšati število zlorab in odpraviti možnosti za zlorabe. Še tako popolna tehnična zaščita odpove, če uporabnik samo zaradi nepazljivosti ali malomarnosti omogoči storilcu možnost za dostop do njegovega računa.

Ozaveščenost uporabnikov in njihovo informiranje s strani bank in policije o zlorabah, predvsem pa napotki, na kakšen način se jim s preventivnim ravnanjem izogniti, povzročajo pri uporabnikih tudi večji občutek varnosti in večjo stopnjo zaupanja v elektronsko bančništvo in storitve, ki jih koristijo.

Ponudniki elektronskega bančništva posebno pozornost posvečajo usposabljanju uporabnikov za varno poslovanje. Le-to poteka preko izdajanja različnih brošur, katerih vsebina je varna uporaba elektronskega bančništva, preko obvestil na izpiskih stanja transakcijskih in drugih računov, do obvestil preko medijev, predvsem v primerih, ko se na nekem območju v večjem obsegu pojavijo zlorabe ali se pojavijo poskusi zlorab.

Prav tako policija v okviru svoje dejavnosti, ko zazna na področju, ki ga pokriva, povečanje zlorab ali storilce, preko sredstev javnega obveščanja obvešča uporabnike storitev elektronskega bančništva na povečano pazljivost in skrbnejše ravnanje s plačilnimi instrumenti.

V Sloveniji je v okviru svojih nalog večji del obveščanja in usposabljanja uporabnikov prevzelo Združenje bank Slovenije, prav tako pa posamezne banke in izdajatelji plačilnih in kreditnih kartic skrbijo za varnost poslovanja svojih komitentov.

Uporabniki imajo na voljo navodila za varnejšo uporabo elektronskega bančništva, ki je usklajeno med bankami in drugimi izdajatelji kartic v okviru Odbora za varnost kartičnega poslovanja pri Združenju bank Slovenije. Navodila, ki jih je izdalo Združenje bank Slovenije, so razdeljena na splošni del, nakupovanje s kartico, spletno nakupovanje, uporabo bančnega avtomata in navodila v primeru izgube ali kraje kartice. Vse to so področja, kjer se zgodi večina zlorab oz. pridejo storilci do podatkov o imetnikovi kartici in transakcijskem računu, ki omogočajo nadaljnje zlorabe.

Splošno:

- Uporabnik naj podpiše novo kartico takoj, ko jo prejme, saj je veljavna le podpisana kartica (na hrbtni strani), poleg tega pa na ta način zmanjša možnosti zlorab.
- Staro, neveljavno kartico mora uporabnik čim prej uničiti oz. razrezati, ker tudi takšna omogoča in olajša storilcem izvajanje zlorab.
- Uporabnik mora s kartico ravnati skrbno, imeti jo mora pri sebi, če je to mogoče oz. spravljeno na varnem mestu. Ne sme je puščati na vidnem mestu v avtu, saj to poveča možnost vloma v osebno vozilo in zlorabo kartice. Pri plačevanju na prodajnih mestih uporabnik kartice naj ne bi izpustil kartice iz svojega vidnega polja (praksa pri plačevanju v gostinskih lokalih je žal drugačna, saj povsod nimajo mobilnih POS terminalov).
- Osebno številko (PIN številko) ali geslo si naj uporabnik zapomni in takoj po prejemu uniči ovojnico z zapisano številko.
- Če si številke ne more zapomniti, je ne sme nositi skupaj s kartico ali celo na hrbtni strani kartice, prav tako pa ne smemo doma in nikjer hraniti skupaj kartice in osebnega gesla.
- Kartica je osebna in naj je nihče drug ne bi uporabljal ne za plačevanje na POS terminalih ne za dvigovanje gotovine iz bankomata.
- Osebnega gesla ne smemo zaupati nikomur drugemu, saj s tem omogočamo zlorabe (zlorabe v okviru družine oz. prijateljev).

Nakupovanje s kartico:

- Vsi podatki na kartici sodijo pod tajne in unikatne podatke. Zaradi tega jih na noben način ne posredujemo nobeni drugi osebi, ki bi nas na to zaradi različnih razlogov navajala.

- Preden podpišemo slip (potrdilo) o opravljenem nakupu, preverimo, če se znesek na potrdilu sklada z zneskom nakupa.
- Skrbno ravnajmo s potrdili o opravljenih nakupih, saj vsebujejo veliko podatkov o kartici, ki jih lahko storilci izrabijo.
- Preverjajmo dejansko uporabo kartice in plačil z izpiski prometa, ki ga prejmemo od banke, saj tako ugotovimo dejansko uporabo.
- Ne podpisujemo potrdil z vnaprejšnjimi datumi ali celo neizpolnjenih, saj so lahko predmet zlorabe oz. so plačila izvedena izven dogovora s prodajalcem.

Spletno nakupovanje:

- Pri spletnem nakupovanju se moramo zavedati, da komuniciramo z nekom, ki ga ne poznamo. Zaradi tega ne vpisujemo številk kartic povsod, kjer to od nas zahtevajo, ampak le tam, kjer smo se za nakup odločili. S kartico plačujmo samo na tistih spletnih straneh, ki jih poznamo in so verodostojna in izpolnjujejo minimalne varnostne zahteve.

Uporaba kartice na bančnem avtomatu:

- Pri uporabi bančnega avtomata moramo paziti, da smo pred avtomatom sami in nihče ne more sam ali s tehničnimi pomagali videti osebne številke, ki smo jo odtipkali.
- Bančne avtomate uporabljajte vedno sami in ne sprejemajte pomoči neznancev. O uporabi bančnih avtomatov se posvetujte v banki.
- Uporabljajte tiste bančne avtomate, ki stojijo na obljudenih, ponoči pa na osvetljenih mestih.
- Če na bančnem avtomatu opazite kakršnekoli posebnosti oz. neobičajnosti (kartica gre s težavo v režo, opazne so naprave in stvari, ki jih navadno ni, kamere so neobičajno postavljene, v »oknu« bančnega avtomata se nahaja posoda z reklamnim gradivom…), vzemite kartico in uporabite drug bančni avtomat, svoja opažanja pa sporočite banki ali policiji.
- Če je bančni avtomat nameščen v prostoru, skozi vrata katerih lahko vstopite samo s potegom kartice preko naprave za odklepanje vrat, nikoli ne vnašajte v napravo osebnega gesla, če bi jo le-ta zahtevala.

Ravnanje v primeru izgube, kraje ali preklica kartice:

- V telefon ali drug imenik si vpišite številko, na katero lahko vedno javite izgubo ali tatvino kartice in jo v primeru kraje ali izgube tudi takoj prijavite, da bo banka onemogočila uporabo kartice in opravila blokado nadaljnje uporabe.
- Če sumite, da je bila kartica ukradena, prijavite to policiji.
- Ne nasedajte telefonskim, elektronskim in drugim obvestilom, ki vas obveščajo o domnevni zlorabi vaše kartice in od vas zahtevajo podatke o kartici ali da preko spletnih strani vnašate v »varnostne obrazce« podatke o kartici.

6.2.2 Pomen preventivnega obnašanja uporabnikov

Pomen preventivnega obnašanja uporabnikov je zelo pomemben, saj storilci velikokrat ravno zaradi neznanja, nepazljivosti in celo malomarnosti uporabnikov pridejo do podatkov, ki omogočajo zlorabe. Puščanje plačilne kartice na mestih, kjer jo lahko storilec vzame, presname in nato zlorabi, dajanje podatkov o računih neznanim osebam ali samo malomarno ravnanje s kartico na bančnem avtomatu je že dovolj, da je lastnik kartice žrtev zlorabe in oškodovan za velika finančna sredstva. Zaradi tega je samozaščitno delovanje uporabnika važno za preprečevanje zlorab, čemur se posvečajo tako banke kakor tudi policija.

Najpreprostejša zaščita pri opravljanju storitev na bančnem avtomatu, kjer je potrebno odtipkati osebno številko pred njenim snemanjem z mikro kamero, je prekritje tipkovnice z roko ali denarnico. Na ta način storilci ne dobijo podatka o osebni številki, čeprav pridobijo magnetni zapis kartice z drugo napravo. To jim otežuje zlorabe, saj brez osebne številke ne morejo na preprost način priti do denarja na bančnem avtomatu, ampak lahko plačujejo samo na POS terminalu, kjer se identiteta preverja s podpisom na računu.

V primeru phishinga (ribarjenja) in pharminga (zvabljanja) je najlažji in najboljši način zaščite ravno tako pravilno obnašanje uporabnika in njegova pazljivost pri uporabi elektronskega bančništva. Če se uporabnik zaveda, da svojih podatkov ne sme pošiljati preko elektronskih medijev in ne pozna prejemnika oz. da banka nikoli ne zahteva od uporabnika nobenih pomembnih podatkov (osebno geslo in številka računa), bo poziv nekoga preko elektronske pošte za te podatke preprosto ignoriral in čim prej izbrisal. Če storilci poskušajo priti do osebnih podatkov preko lažnih spletnih strani banke, pa je uporabnik zaščiten (v kolikor se za to odloči) preko osebnega pozdrava (sporočila) na zaslonu, ki si ga lahko individualno določi. S tem je verjetnost, da komunicira z banko, ne s kom drugim, dosti bolj

verjetna, poleg tega pa uporabnika tudi dodatne rubrike (polje za vpis osebnih gesel), ki prej niso bile običajne za bančne strani in izvedbo transakcije, opozorijo na to, da je lahko žrtev zlorabe. V tem primeru ne sme vpisovati zahtevanih drugih podatkov, o lažni spletni strani pa čim prej obvestiti banko ali policijo.

Ustavitev zlorab na posameznem računu, ki se že izvajajo, se mora zgoditi čim prej. Problem je, da za zlorabe največkrat izve uporabnik takrat, ko ne more opraviti transakcije, ker je že nekdo drug prekoračil limit, ki ga je banka odobrila ali komaj takrat, ko pregleduje izpisek transakcij. Da bi zlorabe odkrili takoj, so banke vpeljale možnost obveščanja o izpeljani transakciji preko SMS obvestila, poslanega na mobilni telefon uporabnika kartice. Na ta način je komitent takoj po izvedbi transakcije z njegovo plačilno kartico obveščen o tem. V primeru, če se pojavi obvestilo o transakciji, sam pa je ni opravil, je to znak, da je bila kartica zlorabljena. S takojšnjim obvestilom banki izdajateljici se kartica prekliče in zlorabe ustavijo.

Pravilno in skrbno ravnanje uporabnikov veliko prispeva k zmanjševanju in onemogočanju zlorab. Zaradi tega ravnanja uporabnikov pri preprečevanju zlorab ne smemo zanemariti, ampak mu moramo posvetiti veliko pozornosti, ker zmanjšanja zlorab brez odgovornega obnašanja uporabnikov ne moremo pričakovati.

6.3 Vloga represivnih organov in generalna prevencija

Država s kazensko zakonodajo in svojimi represivnimi organi ureja in skrbi za spoštovanje pravnega reda in prilagajanje družbenim normam. Kakšen vpliv na področje elektronskega plačilnega prometa oz. na število zlorab na tem področju imajo ukrepi države, je pomembno vprašanje, na podlagi katerega država sprejema ukrepe na področju boja proti kriminaliteti in vodi kriminalitetno politiko.

Kako ukrepanje represivnih organov oziroma generalna prevencija vplivata na zlorabe, je vprašanje, ki je za državo, ponudnike elektronskega bančništva in seveda tudi za uporabnike teh storitev zelo pomembno, saj se lahko na podlagi tega odločajo o svojih ravnanjih in ukrepih za dosego čim večje stopnje varnosti (Gradišar M., Lamberger I., 2010).

Vloga represivnih dejavnikov je pomembna zaradi preprečevanja in omejevanja kriminalitete. Država oz. oblast tudi na ta način poizkuša vplivati na kriminaliteto. Tako je eden izmed

dejavnikov zmanjšanja kriminalitete tudi delovanje vseh institucij formalnega družbenega nadzorstva, kar naj bi vodilo k zastraševanju možnih storilcev kaznivih dejanj.
Različne kriminološke teorije govorijo o dejavnikih, na podlagi katerih se storilci odločajo za izvrševanje kaznivih dejanj, brez dvoma pa se zastraševalna vloga kazenskih sankcij povečuje z zvišano možnostjo prijetja in kaznovanja storilca. Zato bi naj grožnja s kaznovanjem odvračala ljudi od izvrševanja kaznivih dejanj, kar predstavlja sestavni del vseh kazenskopravnih sistemov in enega izmed temeljnih elementov preventivnih dejavnosti.

Zastraševanje delimo na dve vrsti. Posebno zastraševanje ali specialna prevencija se nanaša na preprečevanje novih kaznivih dejanj že znanih storilcev. V tem primeru bi naj zastraševalni učinek vplival na kaznovanega storilca, da ne bi nadaljeval z izvrševanjem novih kaznivih dejanj. Generalna prevencija pa ni usmerjena samo na že znane storilce kaznivih dejanj, ampak na vse prebivalce države. Kazenske sankcije in iz tega izhajajoča kazen je opozorilo vsem potencialnim storilcem kaznivih dejanj in predstavlja zastraševalni učinek na vse možne storilce (Meško G., 2002, str. 131 – 132).

Zlorabe bančnih in kreditnih kartic sicer spadajo med gospodarsko kriminaliteto, ki ima svoje znane značilnosti. Ena izmed njih je ravno težavnost preiskovanja zaradi njene kompleksnosti, prikritosti in nevidnosti. Zaradi dobre organizacije storilcev in njihovega transnacionalnega delovanja pa ima tovrstna kriminaliteta pogosto tudi vse zahtevane kriterije, ki opredeljujejo organizirano kriminaliteto[31] in smo jih v Sloveniji prevzeli od EUROPOLA.[32] Zaradi tega je preiskovanje kriminalitete na področju elektronskega bančništva še posebej zahtevno opravilo za preiskovalce, saj govorimo o dobro usposobljenih in organiziranih storilcih (Dobovšek B., 2009).

Organizirani, zlasti transnacionalni kriminal je moderni kriminal, kriminal, ki se še razvija in se pojavlja v vedno novih oblikah, le motiviranost zanj ostaja vedno ista. Organizirani

[31] Dokument št. 6204/2/9 ENFOPOL 35 REV 2 – Poročanje o organizirani kriminaliteti v EU je bil obravnavan v delovni skupini za "policijsko sodelovanje" Sveta EU v okviru pravosodja in notranjih zadev.

[32] V Sloveniji smo za opredeljevanje pojma »organizirana kriminaliteta« prevzeli kriterije Europola, ki zahteva izpolnitev štirih obveznih (1. združba vsaj treh ljudi, 2. deluje v daljšem časovnem obdobju, 3. cilj je premoženjska korist (dobiček) ali družbena moč, 4. izvrševanje težjih kaznivih dejanj (uradno pregonljivih kaznivih dejanj) in dveh od sedmih neobveznih kriterijev (1. uporaba nasilja in /ali korupcije, 2. delovanje na mednarodni ravni, 3. vpletenost v pranje denarja, 4. uporaba notranjih pravil ravnanja, 5. točno določena delitev vlog in nalog za člane, 6. uporaba podjetniškega načina delovanja, 7. vplivanje na medije, gospodarstvo, državno upravo, politiko;

kriminal je lahko tudi gospodarski, kriminal belega ovratnika, podjetniško-poslovni kriminal oziroma transnacionalni kriminal (Pečar J., 1996, str. 14, 15).

Resnična podoba organiziranega kriminala je skrita bolj kot pri katerikoli drugi obliki kriminalitete. Organizirani transnacionalni kriminal sodi v moderno kriminaliteto zlasti zaradi svoje internacionalizacije, ekonomizacije in podjetništva, vdiranja v politiko in gospodarstvo. Hkrati je izredno prilagodljiv, ustvarjalen in iznajdljiv in resen tekmec gospodarstvu in državnim represivnim organom (Pečar J., 1995, str. 319).

Policija je samo ena izmed formalnih institucij družbenega nadzorstva v celotni verigi kazenskega postopka, vendar kar se tiče postopkov in dejavnosti, ki jih izvaja, zelo pomembna za odkrivanje in preiskovanje kriminalitete. Kazenski postopek ima kot rezultat pravnomočno obsodilno sodbo, kar bi naj delovalo na storilca in na potencialne storilce.

Seveda so tudi mnenja o primernosti izrečenih kazni različna. Tako sta poznani retributivistična in utilitaristična teorija, ki govorita o kazenskih sankcijah. Obe upravičujeta kazen z zasluženostjo za že storjeno dejanje, pri tem pa slednja bolj kot prva poudarja vpliv kaznovanja na zastraševanje drugih (Kanduč, Z., 1996, str. 131).

Brez dvoma pa je prisoten vpliv represivnih organov na storilce s področja kriminalitete na tem področju. Dobra zakonodaja, ki ureja delovanje in pooblastila organov na tem področju je pomembna, prav tako pa mora biti ukrepanje vseh institucij od policije do sodišč hitro, saj samo pravočasni ukrepi pozitivno vplivajo na ravnanje storilcev. Pravnomočno zaključenim obsodilnim sodbam morajo slediti tudi odvzemi protipravno doseženih finančnih koristi, saj ta ukrep pomeni, da se kriminal ne izplača, ker prijet storilec od storitve kaznivega dejanja nima koristi (Lamberger I., 2009).

Največji problem našega pravosodja so ravno nenormalno dolgi kazenski postopki, zastaranja kazenskega pregona zaradi preteka časa in relativno malo pravnomočno obsojenih storilcev za gospodarsko kriminaliteto (Lamberger I., 2006).

6.3.1 Ukrepi policije pri odkrivanju in preprečevanju zlorab

Ko policija z lastno dejavnostjo ali po obvestilu banke ali upravljavca bankomatnega omrežja ugotovi, da obstajajo razlogi za sum, da je bilo storjeno kaznivo dejanje, za katerega se

storilec preganja po uradni dolžnosti, je dolžna v skladu s 1. odstavkom 148. člena Zakona o kazenskem postopku ukreniti vse potrebno, da se izsledi storilec kaznivega dejanja, da se storilec ali udeleženec ne skrije ali ne pobegne, da se odkrijejo in zavarujejo sledovi kaznivega dejanja in predmeti, ki utegnejo biti dokaz in se zberejo vsa obvestila, ki bi utegnila biti koristna za uspešno izvedbo kazenskega postopka[33] (Lavtižar A., 2007).

Policija v takšnem primeru izvede ukrepe, kateri so določeni v z Zakonu o kazenskem postopku (ZKP), kot so:

- zbiranje obvestil od oseb
- pregled prevoznih sredstev, potnikov in prtljage
- omejitev gibanja na določenem prostoru
- ugotavljanje istovetnosti oseb in predmetov
- razpis iskanja oseb in stvari, ki se iščejo
- v navzočnosti odgovorne osebe opraviti pregled določenih objektov in prostorov podjetij in drugih pravnih oseb in pregledati določeno dokumentacijo pravne osebe
- izvesti hišno in osebno preiskavo
- pridobitev podatkov o prometu telekomunikacijskih sredstev
- zaseg predmetov
- odvzem prostosti in pridržanje osebe do 48 ur
- zaslišanje osebe
- privedba k preiskovalnemu sodniku.

Ob tem mora policija izvesti še posamezne specifične ukrepe, ki so odvisni od načina izvršitve kaznivega dejanja, in sicer ukrepe v primeru kopiranja magnetnega zapisa plačilnih kartic:

a. na bančnem avtomatu
b. na prodajnem mestu s POS terminalom
c. na prodajnem mestu s strani zaposlenega.

[33] Zakon o kazenskem postopku, 2007, čl. 148

a. *Policijski ukrepi v primeru kopiranja magnetnih zapisov plačilnih kartic na bančnem avtomatu*

Ko policija dobi informacijo, da naj bi bila na bančnem avtomatu nameščena naprava za kopiranje magnetnih zapisov plačilnih kartic, je zelo pomembno, da hitro izvede ustrezne ukrepe za prijetje neznanega storilca, vsi ukrepe pa morajo biti izvedeni učinkovito in načrtovano, saj obstaja velika možnost, da se v takšnem primeru nahaja storilec v bližini bančnega avtomata ter opazuje dogajanje na samem kraju in čaka, da bo snel napravo za presnemavanje magnetnega zapisa in mikro kamero. Zaradi tega je potrebno izvajati ukrepe pazljivo in na način, ki bo omogočal prijetje storilca, saj se ta še nahaja na kraju ali v neposredni bližini bančnega avtomata oz. se bo tja še vrnil.

Specifični policijski ukrepi v primeru nameščene skimming naprave na bančnem avtomatu so:

Napotitev policijske patrulje na kraj in obveščanje drugih policijskih patrulj:

- Na kraj je potrebno napotiti civilna policijska vozila s policisti v civilni obleki. Iz taktičnih razlogov se pri vožnji na kraj ne uporabljajo opozorilni zvočni in svetlobni znaki, saj bi s tem storilce opozorili na svoj prihod, kar bi povzročilo takojšno demontažo in odstranitev kopirne naprave z bančnega avtomata (ta predstavlja materialni dokaz in je hkrati nosilec morebitnih materialni sledi). Prav tako bi storilci s kraja zbežali in bi jih kasneje, ko bi jih prijeli, zelo težko povezali z nastavitvijo kopirne naprave. Tudi če na sami napravi najdemo materialne dokaze, je v primeru, da storilcev ne dobimo na kraju, izredno težka identifikacija, saj gre večinoma za tujce, ki so že nekaj ur po begu lahko v drugi državi.
- Obvestijo se tudi drugi policisti, ki so na terenu, da so pozorni na sumljive osebe in vozila (v večini primerov gre za tuje državljane in vozila, največkrat Romune) in se po potrebi približajo kraju dejanja, da lahko pravočasno zagotovijo dodatno pomoč civilni patrulji za prijetje storilcev.

Opazovanje okolice bančnega avtomata

- Ob prihodu na kraj je potrebno skrbno in previdno pregledati okolico z namenom, da se odkrijejo storilci kaznivega dejanja, povezanega s kopiranjem magnetnega zapisa plačilnih kartic, ugotoviti njihovo število, vozila, ki jih uporabljajo, možne smeri

pobega storilcev s kraja in ostale okoliščine za postavitev zasede in prijetje storilcev. Potrebno je biti pazljiv na parkirana osebna vozila, celo kolesa z motorjem in kolesa, parkirana v bližini bančnega avtomata, saj je lahko v in na njih nameščen sprejemnik za prenos slike z mikro kamere ali se v vozilu nahajajo tudi storilci.

Postavitev zasede v bližini bančnega avtomata

- Če ugotovimo, da je naprava za kopiranje še na bančnem avtomatu, blizu njega postavimo zasedo, da bi prijeli storilce, ki bodo prišli po nasmeščene naprave na njem. Storilci se pri tovrstnih kaznivih dejanjih namreč zadržujejo blizu bančnega avtomata, na katerega so že namestili napravo za kopiranje magnetnega zapisa plačilnih kartic in videokamero za pridobitev PIN številke. Krog, v katerem se storilci zadržujejo, je odvisen od moči oddajnika mikro kamere, nameščene na bančnem avtomatu, ki sproti pošilja podatke s kamere in od konfiguracije in primernosti okolice za parkiranje avtomobila oz. prikritje. Storilci z bančnega avtomata odstranijo napravo za kopiranje magnetnih zapisov, ko dobijo zadostno število podatkov o plačilnih karticah ali ko je polno zaseden pomnilnik spominskega vezja bralne naprave za kopiranje magnetnih zapisov.
- Namen zasede je prijetje storilcev, vendar obstaja dilema, kdaj in koliko časa naj se zaseda izvaja, in kdaj se naj bančni avtomat zavaruje in pristopi k opravljanju kriminalističnega ogleda. Banka namreč v primeru suma, da je na bančnem avtomatu nameščena naprava za kopiranje magnetnih zapisov plačilnih kartic (tehnično izpopolnjeni bančni avtomati lahko tudi sami zaznajo nameščeno napravo), avtomat takoj izklopi iz mreže, da se prepreči možnost zlorab plačilnih kartic. Za storilce je to lahko znak za preplah, zaradi česar ne bodo nikoli izsledeni, zato se je potrebno o času prijetja odločati v odvisnosti od konkretne situacije.
- Pri prijetju storilcev, ki nastavijo naprave za kopiranje magnetnega zapisa na bančni avtomat, mora aktivno sodelovati tudi banka oziroma upravljavec bančnega avtomata. Ta lahko sproti zaradi preventivnih ukrepov blokira vse uporabljene plačilne kartice na takem bančnem avtomatu. Tako se lahko zaseda izvaja vse do trenutka, ko bi storilci prišli po nameščeno napravo in bi bili pri tem prijeti. Zaradi tega je sodelovanje med policijo in bankami tukaj ključnega pomena.

Zavarovanje kraja kaznivega dejanja

- Kriminalistična taktika določa, da se za zavarovanje sledi, ki so na kraju kaznivega dejanja, v tem primeru bančnega avtomata, na katerem je nameščena naprava za kopiranje magnetnega zapisa plačilnih kartic, opravi zavarovanje kraja z namenom, da se prepreči uničenje morebitnih materialnih sledi na bančnem avtomatu in nameščenih napravah za kopiranje magnetnih zapisov. V zavarovanje se vključi tudi bližnja okolica, saj je storilec lahko odvrgel ponarejene kartice, orodje za nameščanje in druge predmete, ki so pomembni za povezavo storilca s kaznivim dejanjem in identifikacijo storilca.

Zavarovanje sledi na nameščenih napravah za kopiranje magnetnih zapisov

- Čeprav mnogo storilcev pri nameščanju naprav za kopiranje magnetnih zapisov že uporablja rokavice, so se lahko pred tem naprav dotikali tudi brez rokavic. Na zunanji in notranji strani nameščenih naprav lahko najdemo sledi papilarnih linij ali biološke sledi storilcev. Zaradi tega se pri opravljanju ogleda vedno uporabljajo zaščitne rokavice, ki preprečujejo kontaminacijo sledi.

Zavarovanje sledi na ponarejenih plačilnih karticah

- Sledi papilarnih linij in biološke sledi storilcev so lahko tudi na ponarejenih plačilnih karticah, ki so jih storilci že uporabili pri dvigovanju denarja z bančnega avtomata, pa jih zaradi napačne PIN številke bančni avtomat zadrži ali pa jih storilci odvržejo, da se znebijo obremenilnega dokaza, ki jih lahko poveže s kaznivim dejanjem. Zaradi tega je tudi pri jemanju ponarejenih plačilnih kartic iz bančnega avtomata potrebno skrbno ravnanje upravljalca in vzdrževalca bankomata in uporaba zaščitnih rokavic oz. prijemanje kartic samo na robovih in paziti, da se sledi ne uničijo in ne kontaminirajo. Na podlagi sodelovanja policije in bank so vzdrževalci bančnih avtomatov obveščeni, na kakšen način ravnajo s takšnimi karticami in kako in komu jih pošljejo.

Pridobitev videoposnetkov nadzornih sistemov

- Za uspešno identifikacijo storilcev, ki niso bili dobljeni na kraju ali za dokazovanje njihove dejavnosti, si lahko pomagamo z video posnetki, če sta bančni avtomat ali

njegova okolica opremljena z video nadzornim sistemom. Ker se posnetki po določenem času presnamejo, je treba pravočasno zavarovati video posnetke, s pomočjo katerih se lahko identificirajo storilci, ugotovi potek izvrševanja kaznivega dejanja, vloge posameznih storilcev in ki služijo kot dokaz v kazenskem postopku. Lahko se izdelajo tudi fotografije storilcev, ki se posredujejo vsem policijskim enotam ali tudi medijem z namenom identifikacije in prijetja storilcev.

Ugotoviti znamko in tip bančnega avtomata

V primeru, ko se nameščanje naprav za kopiranje magnetnih zapisov ponavlja na nekem območju, storilcev pa ne uspemo identificirati in prijeti, si lahko pomagamo tudi s karakteristikami oz. modeli bančnih avtomatov. Oblika in zunanjost bančnih avtomatov se glede na znamko, tip in izdelovalca med seboj razlikujeta. Naprave za kopiranje magnetnih zapisov plačilnih kartic so prilagojene določenemu tipu bančnega avtomata, saj se morajo skladati z njegovim zgledom, da ostanejo neprepoznavne komitentom in se lahko namestijo le na bančni avtomat ustrezne znamke in tipa. Na podlagi pridobljenih podatkov od upravljavca mreže bankomatov se da ugotoviti, kje so lokacije bančnih avtomatov enake znamke in predvidevati, kje se bodo naslednjič pojavili storilci. Preventivno se lahko takšni bančni avtomati pokrijejo z zasedami in se na ta način poizkuša dobiti storilce.

b. *policijski ukrepi v primeru kopiranja zapisov plačilnih kartic na POS terminalu z vgrajeno napravo*

Novejši izmed mogočih načinov za pridobitev zapisov plačilnih kartic je na POS terminalih s pomočjo predhodno vgrajene naprave za kopiranje zapisa. V takšnih primerih začne policija izvajati ukrepe za izsledite storilcev in zavarovanje materialnih dokazov, ko je največkrat s strani banke obveščena o izvedenem kopiranju zapisa na določenem prodajnem mestu. Ukrepi so odvisni od tega, ali je bilo kopiranje opravljeno v preteklem časovnem obdobju ali se še vedno izvaja.

V primeru, če se kopiranje še izvaja, je potrebno takoj ukrepati in izvesti predvidene ukrepe. Prav tako je treba izvesti določene ukrepe v primeru, ko je na kraju zalotena oziroma prijeta oseba, ki je v POS terminal poskušala namestiti ali namestila napravo za kopiranje zapisov.

Specifični ukrepi v primeru kopiranja magnetnih zapisov plačilnih kartic in nameščanja naprav za kopiranje magnetnih zapisov v POS terminale so:

Napotitev policijske patrulje na kraj in obveščanje drugih policijskih patrulj

- Ukrep je podoben kot pri nameščeni kopirni napravi na bančnem avtomatu, saj je tudi v tem primeru potrebno na kraj takoj poslati civilno policijsko patruljo s policisti v civilu in s civilnim službenim vozilom. Prihod v bližino kraja mora biti neopazen, brez zvočnih in svetlobnih signalnih znakov, da pri storilcih ne vzbudi pozornosti in ne povzroči bega storilcev s kraja. Ostale policijske patrulje so ves čas v stiku, da lahko pravočasno priskočijo na pomoč civilni patrulji.

Opazovanje okolice prodajnega mesta, opremljenega s POS terminalom

- Tako kot v primeru naprave za kopiranje magnetnih zapisov, nameščene na bančnem avtomatu, je potrebno tudi v tem primeru pregledati okolico prodajnega mesta z nameščeno napravo za kopiranje magnetnih zapisov. Storilci lahko v tem času v parkiranem osebnem avtomobilu ali kje drugje preko brezžičnega oddajnika s POS terminala na prenosni računalnik, dlančnik ali mobilni telefon sprejemajo prekopirane podatke zapisa plačilnih kartic in uporabljene PIN številke.

Pregled objekta z nameščenimi POS terminali

- Če se izven delovnega časa v prodajalni, predvsem v večjih trgovskih centrih, sproži signalno varnostna naprava in pri pregledu objekta ni opaziti sledov vlamljanja, obstaja velika verjetnost, da je v prodajalni skrit storilec, ki ima namen, da v POS terminal namesti napravo za kopiranje magnetnih zapisov plačilnih kartic. S ciljem, da se izključi navedena možnost in s tem prepreči izvrševanje kaznivih dejanj ter prime morebitnega storilca, je potrebno, da policijska patrulja skupaj z odgovorno osebo ali uslužbencem varnostne službe pregleda notranjost objekta, v katerem se je sprožil alarm. Pri tem je treba pregledati vsa mesta, kjer bi se lahko skrival storilec, preveriti število POS terminalov in ugotoviti, ali je bil izveden poseg v njihovo notranjost. Storilci si lahko na kraju POS terminal tudi prilastijo in ga odnesejo s seboj ter vanj namestijo napravo za kopiranje zapisov. Takšen POS terminal potem zamenjajo s pristnim POS terminalom na izbranem prodajnem mestu. V tem primeru je na kraj

potrebno napotiti še drugo patruljo, ki mora opazovati okolico z namenom, da prepreči pobeg morebitnih storilcev, ki bi se izmuznili prvi patrulji. Storilci lahko za vstop v prodajno mesto tudi izvedejo fingiran vlom, kjer ne odnesejo ničesar ali pa le stvari majhne vrednosti. To je lahko indic, da so vstopili zato, da bi namestili napravo za kopiranje zapisov kartic.

Postavitev zasede

- V primerih, ko ugotovimo, da je naprava za kopiranje zapisov še vedno aktivna v POS terminalu in drugače ni mogoče identificirati storilcev, lahko v notranjosti objekta in njegovi okolici postavimo zasede. Takšen način je primeren predvsem takrat, ko naprava za kopiranje zapisov sproti ne oddaja prekopiranih podatkov z zapisa plačilne kartice in PIN številke, ampak jih hrani v lastnem spominskem mediju. Storilci se morajo po tako nameščeno napravo vrniti, saj v nasprotnem primeru prekopiranih podatkov ne morejo uporabiti za kasnejšo zlorabo bančnih kartic. Za lažje in učinkovitejše delo si lahko pri takem načinu prijetja storilcev pomagamo z video nadzornim sistemom prodajalne, če ga ima.

Zavarovanje kraja in POS terminala

- Ko ugotovimo, da je prodajno mesto opremljeno s POS terminalom, v katerem je vstavljena naprava za kopiranje magnetnih zapisov, je potrebno tak terminal obvezno zaseči in ustrezno zavarovati, da na njem ne uničimo sledi storilcev. Iz enakih razlogov se zavaruje tudi sam kraj kaznivega dejanja, saj lahko storilec med nameščanjem naprave za kopiranje magnetnih zapisov pusti več materialnih sledov.

Zavarovanje sledi na nameščenih kopirnih napravah

- Ko zasežemo POS terminal, ki bi naj imel vgrajeno napravo za kopiranje zapisov, se moramo zavedati, da je to nosilec sledi, predvsem sledi papilarnih linij in bioloških sledi. Sledi so lahko tudi na notranji strani terminala ali na posameznih vgrajenih elektronskih delih. Tudi sami vgrajeni deli oz. tipologija elektronskega vezja nam lahko nakaže, kdo bi lahko bil storilec in pove povezavo z drugimi primeri. Zaradi tega se POS terminal ustrezno pregleda.

Zavarovanje sledi na drugih predmetih

- Storilci za namestitev naprave za kopiranje zapisov kartice v POS terminal potrebujejo orodje in druge predmete, kot so spajkalnik, izvijači, baterijski vrtalnik, lepilni trak, sekundno lepilo, baterijski vložki, svetilka in podobno. S seboj imajo lahko tudi načrt, s pomočjo katerega lahko pravilno namestijo napravo za kopiranje magnetnih zapisov v POS terminal. Te predmete lahko pozabijo ali izgubijo na kraju in s tem pustijo svoje sledi, na podlagi katerih jih je lažje identificirati.

Pridobitev videoposnetkov nadzornih sistemov

- Večina prodajnih mest je danes opremljena z video nadzornim sistemom, predvsem večji trgovski centri, ki neprekinjeno snema dogajanje v posameznih prostorih. S pravočasnim zasegom in pregledom videoposnetkov lahko ugotovimo mnogo koristnih okoliščin o storilcih kaznivega dejanja in izvršitvi ter izvedemo druge ukrepe za identifikacijo storilcev.

c. Policijski ukrepi v primeru kopiranja magnetnih zapisov plačilnih kartic na POS terminalu s strani zaposlenega na prodajnem mestu

Če se s kopiranjem magnetnih zapisov na prodajnem mestu ukvarja zaposleni na prodajnem mestu, se izvajajo podobni ukrepi kot pri prej opisanih načinih pridobivanja podatkov z magnetnega zapisa plačilnih kartic. V vsakem primeru je potrebno izvesti naslednje ukrepe:

Opraviti temeljito analizo izvršenih transakcij zlorabljenih bančnih kartic

- S pomočjo banke je potrebno narediti natančno analizo vseh zlorabljenih plačilnih kartic, da se ugotovi točno mesto opravljenega kopiranja kartic. Za zlorabljene kartice je namreč značilno, da so imele pred izvršitvijo neavtoriziranih transakcij izvedeno legalno transakcijo prek POS terminala na istem ali drugem prodajnem mestu, kjer se je kopiranje magnetnega zapisa tudi izvedlo.

Pridobitev in pregled evidence dela za preteklo obdobje

- Z namenom ugotovitve, kdo od zaposlenih na določenem prodajnem mestu izvršuje kopiranje magnetnih zapisov plačilnih kartic, je potrebno pri odgovorni osebi pridobiti razpored dela vseh zaposlenih za določeno časovno obdobje. S primerjavo razporeda dela in seznama izvršenih pristnih transakciji zlorabljenih plačilnih kartic se lahko točno ugotovi osebo, ki je ob plačilu blaga ali storitev hkrati prekopirala podatke z magnetnega zapisa plačilne kartice oziroma se zoži krog osumljencev.

Zbiranje obvestil o osumljencu

- Ko se na podlagi rezultatov analitične obdelave ugotovi osumljenca, je o njem treba zbrati obvestila, da se ugotovijo druga dejstva in okoliščine, ki potrdijo ali ovržejo sum izvrševanja kopiranja plačilnih kartic. Pri tem je potrebno ugotoviti predvsem osebne lastnosti zaposlenega, njegovo finančno stanje, morebitno zadolženost, pretekla kriminalna dejanja, druženje z operativno zanimivimi osebami in drugo.

Pridobitev prometa telefonskih številk

- Na podlagi odredbe sodišča je potrebno pridobiti izpiske telefonskega prometa telefonskih številk osumljencev in ugotoviti povezave z drugimi osebami, ki bi lahko sodelovale pri zlorabah plačilnih kartic, saj gre v teh primerih največkrat za organizirane storilce, ki imajo točno razdeljene vloge, naloge in svoje mesto v organizaciji.

Zavarovanje naprav za kopiranje magnetnih zapisov in druge opreme

- Za dokazovanje kaznivega dejanja je potrebno zavarovati in zaseči predmete kaznivega dejanja, predvsem napravo za kopiranje magnetnih zapisov plačilnih kartic, računalniško opremo s podatki o plačilnih karticah, programsko opremo za snemanje magnetnih zapisov na plačilne kartice, pa tudi ponarejene plačilne kartice. V skladu z zakonodajo se opravljajo hišne in osebne preiskave na delovnem mestu oz. mestu, kjer je potekalo kopiranje magnetnih zapisov in na kraju, kjer osumljenci prebivajo. Pri tem lahko pridobimo naprave, ki so bile uporabljene pri zlorabah in druge predmete, ki bodo dokaz v kazenskem postopku.

Pridobitev videoposnetkov

- Če je bilo prodajno mesto opremljeno z video nadzorom, je potrebno zaseči videoposnetke, saj se lahko na posnetkih ugotovi, kdo in kdaj je kopiral magnetne zapise kartic. Največkrat pa so zaposleni seznanjeni s tem, katera mesta lokala ali trgovine so pokrita s kamerami in se tistih krajev izogibajo, ko kopirajo magnetne zapise.

Zbiranje obvestil od imetnikov plačilnih kartic

- Pri tem načinu izvrševanja kopiranja magnetnih zapisov plačilnih kartic je zbiranje obvestil pri ugotavljanju okoliščin izvedbe kopiranja magnetnega zapisa za identifikacijo storilca zelo pomembno. Storilec, ki je kartico prekopiral, je bil skoraj gotovo v fizičnem stiku z imetnikom kartice, saj je opravil plačilo blaga ali storitve, ki jo je imetnik koristil, obenem pa še prekopiral magnetni zapis na kartici. S kakovostnim in temeljitim razgovorom z imetnikom zlorabljene plačilne kartice lahko pridemo do osebe, ki je izvršila kopiranje magnetnega zapisa plačilne kartice. Imetnik kartice nam lahko pove podatke o osebnem opisu osebe, ki je ob plačilu rokovala z njegovo plačilno kartico in okoliščine plačila s plačilno kartico. Potrebno je ugotoviti, ali je zaposleni izvedel plačilo prek POS terminala v prisotnosti imetnika kartice ali je kartico odnesel z njegovega vidnega polja, saj je v tem primeru možnost zlorabe največja, še posebej, če ima prodajno mesto tudi prenosni POS terminal.

Prepoznava oseb

- Ukrepi policije poznajo tudi prepoznavo v smislu identifikacije storilcev kaznivih dejanj, ki so neznani, oškodovanec pa bi jih med množico že identificiranih storilcev podobnih kaznivih dejanj lahko prepoznal. Imetniki zlorabljenih plačilnih kartic lahko prepoznajo osebo, ki je opravila kopiranje magnetnega zapisa.

- Druga vrsta prepoznave pa je mogoča, če jo opravi preiskovalni sodnik, katera v pozitivni identifikaciji služi tudi kot dokaz v samem kazenskem postopku.

6.3.2 Kazenska zakonodaja

S 1.11.2008 je v veljavo stopil novi kazenski zakonik (KZ-1). Na področju elektronskega bančništva je prihajalo do tega, da smo nekatere vrste zlorab plačilnih in kreditnih kartic zelo težko kvalificirali kot eno izmed obstoječih kaznivih dejanj iz prejšnjega Kazenskega zakonika, ali smo morali za dejavnosti storilcev, ki so jih vršili na področju gospodarskega poslovanja, uporabiti kazniva dejanja s področja klasične kriminalitete (tatvina, velika tatvina,...) Sprememba zakonodaje pa v nekaterih primerih odpravljajo težave kvalifikacije kaznivega dejanja, saj je uvedba dveh novih členov oziroma kaznivih dejanj zajela dejavnosti, ki jih je bilo pred tem izredno težko kvalificirati kot katero izmed kaznivih dejanj. To kaže na posebno pozornost zakonodajalca za problematiko področja zlorab plačilnih in kreditnih kartic.

Novi kaznivi dejanji s področja zlorab plačilnih in kreditnih kartic sta naslednji:

Uporaba ponarejene bančne, kreditne ali druge kartice po 247. členu KZ

(1) Kdor namesti na bančni avtomat ali aparat za vplačila s kartico napravo za preslikavanje zapisa bančnih ali kreditnih kartic ali njeno prepoznavo pridobi preko plačila na celotnem medmrežju ali jo ponaredi na kakšen drug način ali kdor tako ponarejeno bančno ali kreditno kartico uporabi in si pridobi premoženjsko korist, se kaznuje z zaporom do petih let.
(2) Enako se kaznuje, kdor ponaredi ali uporabi ponarejeno drugo kartico, s katero je mogoče pridobiti premoženjsko korist s pomočjo tehničnih naprav za prepoznavo kartice.
(3) Če je bila z dejanjem iz prvega ali drugega odstavka tega člena pridobljena velika premoženjska korist, se storilec kaznuje z zaporom od enega do osmih let.

V tem členu so zajete vse možne oblike pridobivanja zapisov in podatkov kartic, ponarejanje kartic ali podatkov ter njihova nadaljnja uporaba ali zloraba. Zakonodajalec je v tem členu opredelil kot kaznivo že samo nameščanje naprave za pridobivanje zapisov ali podatkov. Na ta način se rešujejo težave neenotnega tolmačenja zakona, napačna kvalifikacija kaznivih dejanj in pomanjkljiva zakonska opredeljenost glede na število možnih pojavnih oblik dejanja.

Izdelava, pridobitev in odtujitev pripomočkov za ponarejanje po 248. členu KZ

(1) Kdor izdela, si pridobi, proda ali da v uporabo pripomočke za ponarejanje denarja, vrednotnic, vrednostnih papirjev ali napravo za preslikavanje zapisa bančne ali kreditne kartice, se kaznuje z zaporom do dveh let.
(2) Pripomočki za ponarejanje se vzamejo.

Zakonodajalec nadomešča opredeljenost izdelave, pridobivanja in dajanja v uporabo pripomočkov za ponarejanje v 309. členu starega zakona, ki je opredeljeval »Izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje«, kar kaže na posebno pozornost in zavedanje zakonodajalca o teži tovrstne kriminalitete.
Ostala kazniva dejanja, ki so pred 1.11.2008 sankcionirala zlorabe s področja zlorab plačilnih in kreditnih kartic, so ostala nespremenjena. Kaznivo dejanje »Izdaja nekritega čeka in zloraba bančne ali kreditne kartice« je ostalo nespremenjeno, saj kot tako ni predstavljalo nobenih problemov pri zlorabah plačilnih in kreditnih kartic, ki jih storijo imetniki teh kartic. Kaznivo dejanje »Neupravičen poseg v informacijski sistem« po 225. členu KZ pa je zakonodajalec preimenoval v kaznivo dejanje »Napad na informacijski sistem«. Vsebinsko se člen ne razlikuje od predhodnega, razlika je v nekoliko hujši sankciji po 1. odstavku novega člena nasproti stari ureditvi. S spremembo kazenske zakonodaje se bo problem kvalifikacije nekaterih ravnanj storilcev zelo olajšal, saj jih pred tem v nekaterih primerih niti ni bilo mogoče kvalificirati kot kaznivo dejanje, torej prepovedano, danes pa je lahko storilec za to tudi kaznovan oz. obsojen.

6.3.3 Mednarodno sodelovanje pri odkrivanju in preprečevanju zlorab

Zaradi mednarodne razsežnosti izvrševanja tovrstnih kaznivih dejanj je izrednega pomena dobro sodelovanje s tujimi varnostnimi organi, saj se policija brez tega ne more uspešno boriti zoper kriminal. Kopiranje magnetnih zapisov plačilnih kartic se namreč pogosto izvede v eni državi, medtem ko prihaja do zlorab plačilnih kartic v drugi državi, na tujih bančnih avtomatih in POS terminalih. Slovenska policija lahko prek Interpola in Europola na zakonit način zbira in pridobi različne podatke, ki so pomembni za izsledite in identifikacijo storilcev.

Europol

Europol je evropski policijski urad, ustanovljen kot specializirana institucija Evropske unije. Namen in naloga, za katero je bil ustanovljen, je izmenjava informacij o kaznivih dejanjih in večja učinkovitost in sodelovanje med pristojnimi organi držav članic pri preprečevanju in boju zoper posebno škodljive oblike izvrševanja kaznivih dejanj mednarodnega organiziranega kriminala. Europol deluje na področju odkrivanja, preprečevanja in pregona

kaznivih dejanj v Evropski uniji, posebej v boju proti organiziranemu kriminalu in v boju proti delovanju organiziranih kriminalnih družb.

Evropski policijski urad je bil ustanovljen 7. februarja 1992 s podpisom Maastrichtskega meddržavnega sporazuma , ki so ga podpisale države Evropske unije. Začetek delovanja sega v leto 1994, ko je Europol začel z delovanjem kot Služba za droge (ESD). Delovanje je bilo najprej osredotočeno le na boj proti mamilom, vendar so se s časom Europolove pristojnosti širile na druga pomembna področja kriminalitete oz. na druga težja kazniva dejanja, ki so na področju Europske unije postala problematična. Prvega januarja 2002 so bile Europolove pristojnosti razširjene na obravnavo vseh hujših oblik mednarodnega kriminala. Europolovo konvencijo so ratificirale vse države članice EU. Veljati je začela 1. oktobra 1998. Po sprejemu pravnih aktov, povezanih s Konvencijo, je Europol začel opravljati svojo dejavnost v polnem obsegu 1. julija 1999. Sedež Europola se nahaja v Haagu na Nizozemskem.

Europol podpira dejavnosti držav članic pri izmenjavi informacij na naslednjih področjih kriminalitete:

- nezakoniti trgovini s prepovedanimi drogami
- ilegalnimi migracijskimi mrežami
- terorizmu
- nezakoniti trgovini z vozili
- nezakoniti trgovini z ljudmi, vključno z otroško pornografijo
- ponarejanju denarja (ponarejanje evra) in drugih plačilnih sredstev
- nezakoniti trgovini z radioaktivnimi in jedrskimi snovmi
- pranju denarja.

Prednostne naloge Europola vključujejo kazniva dejanja zoper življenje, telesno integriteto in osebne svoboščine, kazniva dejanja s področja finančne oziroma premoženjske in računalniške kriminalitete, kamor sodijo tudi kazniva dejanja s področja zlorab plačilnih kartic, ki imajo tudi večinoma vse znake organizirane kriminalitete.

Europol se lahko vključi v aktivnosti, ko so izpolnjeni določeni pogoji: dejavnost, ki se izvaja, spada v področje kriminalitete in naloge, za katere je bil Europolu dodeljen mandat, potrebna je vpletenost organiziranih kriminalnih združb in prizadetost dveh ali več držav članic s kriminalno dejavnostjo oz. povezanost vsaj dveh ali več držav članic na področjih, kjer se vrši kriminalna dejavnost.

Europol izvaja za države članice naslednje storitve:

V skladu z nacionalno zakonodajo omogoča hitro in neovirano izmenjavo informacij med pooblaščenimi uradniki, predstavniki držav članic (Europol Liaison Officers), ki jih države članice samostojno imenujejo. Državam članicam zagotavlja operativno analitično podporo, pripravlja strateška poročila (npr. ocene ogroženosti) in analizira razne pojavne oblike kriminalitete na osnovi informacij in koristnih spoznanj, pridobljenih s strani držav članic ali pridobljenih iz drugih virov, zagotavlja strokovno in tehnično podporo pri preiskavah in operacijah znotraj EU, upoštevaje nadzor in pravno suverenost posameznih držav na svojih ozemljih.

Poleg tega Europol analizira določene pojavne oblike kaznivih dejanj s ciljem iskanja najboljših preiskovalnih praks ter s tem skrbi za poenotenje preiskovalnih tehnik v državah članicah.

S podpisom bilateralnih sporazumov z Republiko Češko, Estonijo, Evropsko centralno banko, Evropskim nadzornim centrom za drogo in odvisnost od drog, Islandijo, Interpolom, Madžarsko, Norveško, Poljsko, Slovenijo in Svetovno carinsko organizacijo, je Europol izboljšal mednarodno sodelovanje na področju odkrivanja in preprečevanja mednarodnega kriminala. Poleg tega je Europol odprl svojo pisarno tudi v Washingtonu (www.policija.si).

Interpol

Interpol predstavlja mednarodno združenje kriminalističnih policij (ICPO - International Criminal Police Organization). Članstvo združuje trenutno 186 držav. Sedež Interpola se nahaja v Lyonu v Franciji. Slovenija je polnopravna članica Interpola postala leta 1992.

Tako kot naloga Europola, je tudi naloga Interpola kot mednarodne organizacije zagotavljanje in realizacija sodelovanja med kriminalističnimi policijami ne glede na razlike v pravnih sistemih držav. Interpol deluje na principu vzpostavljanja in razvoja institucij, ki z medsebojnim sodelovanjem prispevajo v boju proti kriminalu. Vsaka država, članica Interpola, ima v policiji specifično službo, ki zagotavlja sodelovanje in komunikacijo z Interpolom in odgovori na zaprosila od lokalnih domačih in tujih policij in pravosodnih organov. Takšna služba se imenuje nacionalni centralni biro (NCB) in se v Sloveniji nahaja v Ljubljani. Pri nas je nacionalni centralni biro Interpola organiziran v okviru GPU UKP

(Generalne policijske uprave - Uprave kriminalistične policije). V tem okviru deluje SMPS (Sektor za mednarodno policijsko sodelovanje), v sklopu katerega se nahaja oddelek Interpol (Ljubljana), saj se načeloma nacionalni centralni biroji poimenujejo po glavnem mestu države, kjer delujejo.

Primarna naloga Interpola Ljubljana je posredovanje zaprosil za podatke, vezane na policijske preiskave v Sloveniji, ustreznim NCB-jem po svetu in obratno. Na nacionalnem nivoju je Interpol Ljubljana zadolžen za spremljanje in zagotavljanje ustreznih standardov, ki jih narekuje članstvo v organizaciji. Omogoča tudi aktivno vlogo Slovenije v mednarodnem združenju. Za zagotavljanje hitrega in nemotenega delovanja je Interpol Ljubljana vključen v različne komunikacijske mreže (www.policija.si).

Interpol posveča veliko vlogo tudi zlorabam na področju plačilnih in kreditnih kartic, saj v njegovih evidencah hrani in obdeluje tudi podatke o spornih (presnetih, ukradenih ali kako drugače zlorabljenih) karticah. Velika vloga Interpola je tudi na področju usposabljanja oziroma pretoka informacij o novih zlorabah na tem področju in seznanjanja držav članic o novih modusih storitev zlorab.

Policija se lahko kosa v boju s storilci kaznivih dejanj le z dobrim sodelovanjem in učinkovitim pretokom informacij med kriminalisti in policisti. Ker gre v primeru zlorab kartic večinoma za transnacionalno kriminaliteto, je nujno potrebno tudi mednarodno policijsko sodelovanje, saj so brez sodelovanja storilci vedno korak ali dva pred policijo in »roko pravice«.

6.3.4 Sodelovanje policije z bankami in izdajatelji plačilih kartic

Sodelovanje med policijo in bankami je obvezen proces pri preprečevanju, odkrivanju in preiskovanju tovrstnih kaznivih dejanj. Banke in procesni centri so tisti, ki policiji posredujejo ustrezne podatke za izsledite storilcev in pomagajo pri ugotavljanju prodajnih mest, na katerih se opravlja kopiranje magnetnih zapisov plačilnih kartic. Največkrat je ravno banka tista, ki v okviru svojih nadzornih mehanizmov odkrije zlorabo, ali pa se nanjo obrne njen komitent, ki je na izpisku prometa njegove kartice ugotovil, da je bila njegova kartica zlorabljena. Tudi procesni centri so pomembni kot vir informacij o zlorabah, saj se pri procesiranju transakcij prav tako ugotovijo zlorabe.

V smislu bančne tajnosti in zaupnosti bančnega poslovanja je vsaka informacija, ki jo vodijo banke o poslovanju komitenta, podvržena strogim določilom o varovanju teh informacij, ki se ne posredujejo medijem in javnosti, brez odredbe sodišča pa tudi ne policiji. Zaradi tega je sodelovanje s policijo lahko tudi na tem področju oteženo, saj bi policija lahko v primeru zlorab do podatkov, ki jih vodijo banke, lahko dostopala samo z odredbo sodišča, kar pa z vidika pravočasnega in hitrega ukrepanja lahko pomeni oviro pri preiskovanju zlorabe in možnost, da storilec zlorabe ni dobljen. Ker na področju kartičnega poslovanja obstaja skupen interes bank in izdajateljev kartic in policije, da se zlorabe odkrijejo in storilci kaznujejo, prihaja do različnih oblik sodelovanja, ki pa seveda mora biti v skladu z zakonodajo.
V Sloveniji policija in Združenje bank Slovenije (v nadaljevanju ZBS) sodelujeta na področju kartičnega poslovanja v okviru Priporočil za ravnanje bank v primeru suma zlorab na bančnih avtomatih in POS terminalih, ki določa načine medsebojnega obveščanja in sodelovanja. Dokument je bil usklajen med bankami in policijo in dokaj natančno določa postopke, ki jih izvedejo banke v primerih sumov zlorab in tudi, kako in kdaj obveščajo policijo, ki mora v takih primerih hitro in na primeren način ukrepati v smislu kriminalističnih pravil, da odkrije in dobi storilca kaznivega dejanja. Sporočanje podatkov o zlorabljenih karticah poteka v skladu z zakonodajo, ki določa bančno tajnost in se policiji ne pošiljajo podatki o komitentih banke in lastnikih kartic, ampak samo podatki o zlorabljenih karticah in mestih zlorab, ki so pogoj za hiter odziv policije in uspešno preiskavo zlorabe. Vse druge podatke, ki se nanašajo na osebne podatke in finančno poslovanje komitenta, lahko policija pridobi od banke samo na podlagi odredbe sodišča.

Sodelovanje med bankami in policijo je pomembno tudi na področju usposabljanja, saj je samo področje elektronskega bančništva že samo po sebi izredno kompleksno, poleg tega pa storilci z vedno novimi tehnično-tehnološkimi sredstvi poskušajo in tudi uspešno izvršujejo zlorabe. Zaradi tega je usposabljanje in seznanjanje tako bančnih uslužbencev, ki skrbijo za varnost elektronskega bančništva, kot tudi preiskovalcev v policiji z novimi načini prevar in novosti na tem področju, nujno. Takšna usposabljanja so tako organizirana večkrat letno oz. takrat, ko se za to pojavi potreba.

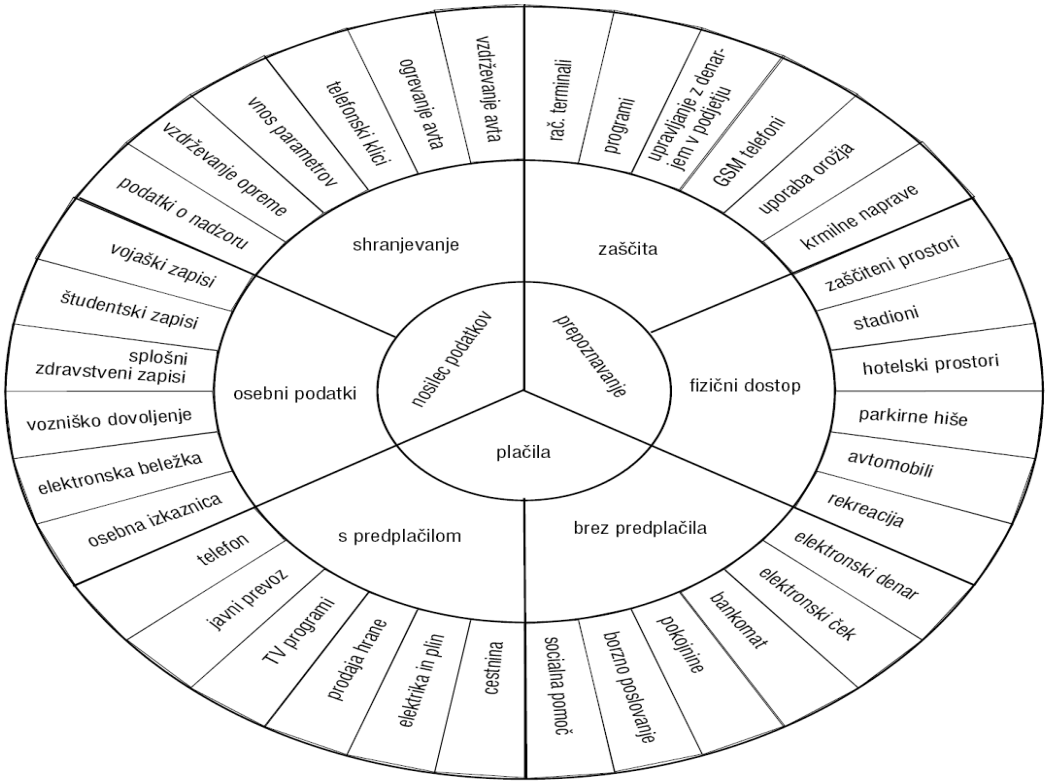
6.4 Novi vidiki zaščite plačilnih sistemov pred zlorabami

Vsaka od novih metod preprečevanja je bila učinkovita le ob njeni uvedbi. Raznovrstne zaščite je uspešno presegla tehnologijo tistih, ki so jo zlorabili. Za preprečitev novih zlorab je nujen hiter razvoj nove zaščite. Pri tem je potrebno realno oceniti učinek uvedbe nove tehnologije.

6.4.1 Pametna kartica

Zgodovina nastanka prve »pametne kartice« sega v leto 1974, ko so v Franciji (R. Moreno) magnetni kartici dodali čip, s čimer je nastala prva pametna kartica. Do prve večje komercialne uporabe pametnih kartic je prišlo v letu 1985, ko so francoske banke poslale na trg 16 milijonov pametnih kartic. Naslednje leto je francoski Telekom izdal in dal v uporabo 7 milijonov pametnih kartic, namenjenih za plačilo telefonskih storitev v javnih govorilnicah. Število in uporaba pametnih kartic se je iz leta v leto povečevala. Tako je bilo v letu 2002 takšnih kartic že 4,7 milijarde. Pametna kartica se od klasične kartice z magnetnim zapisom razlikuje v tem, da je sposobna shraniti večjo količino podatkov in lahko govorimo o malem računalniku na kartici. Najpomembnejši razlog za uporabo pametnih kartic je vsekakor varnost shranjenih podatkov in zaščita podatkov drugih računalniških sistemov pred zlorabami. Pametna kartica lahko sprejema, shranjuje in procesira podatke ter omogoča uporabo različnih aplikacij. Poleg plačevanja se uporabljajo tudi v mobilnih telefonih GSM kot SIM kartica, predplačniškemu telefoniranju, nadomeščajo zdravstvene izkaznice, osebne izkaznice, na njih pa lahko shranimo tudi digitalne certifikate. Področja uporabe kartic so prikazana na sliki št. 21.

Slika 21: Področje uporabe »pametnih kartic«



Tehnologija pametnih kartic omogoča hranjenje in prenos informacij v integriranem vezju, ki je vgrajeno v kartico. V njej lahko shranimo šifrirni ključ oz. digitalno potrdilo. Tehnologija omogoča varno izmenjavo podatkov in komunikacijo preko kontaktov, ki se nahajajo na kartici, za kar potrebujemo še poseben čitalnik za kartice, ki se poveže z računalniškim sistemom. "Inteligenca" pametne kartice se skriva v majhnem čipu, spravljenem na plastični kartici. Na čip gre malo manj kot dvajset tipkanih strani računalniškega besedila (do 64 KB). Varen je pred magnetnimi polji, škoditi pa mu utegnejo le zelo močne elektrostatične motnje. Prednost čipa pred magnetnimi trakovi je v tem, da ne omogoča le branje podatkov, temveč je na čip podatke možno tudi zapisovati. Prav omenjena lastnost omogoča razvoj novih bančnih produktov, kot npr. "elektronske denarnice" (Abanka Vipa d.d., 1999: 16).

Do danes se je pametna kartica razvijala in posodabljala. Nekaj več kot trideset let po prvem patentu pametne kartice poznamo različne oblike kartic. Glede na njihovo vlogo in dostopanje do podatkov na njih jih delimo na:

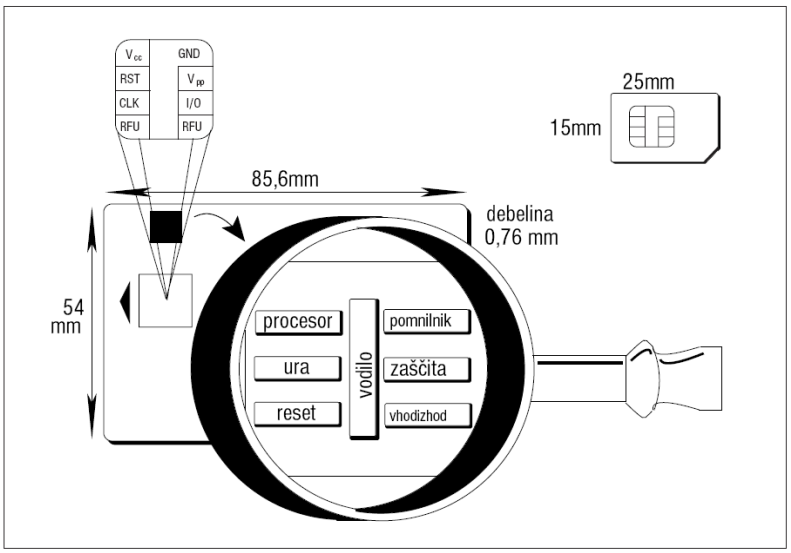
- kontaktne

- brezkontaktne
- kombinirane.

Kartice lahko delimo tudi glede na velikost spomina in glede na prisotnost pomnilnika, ki se je s časom in razvojem tehnologije, tudi zaradi potreb, povečeval. Naredili so že tudi pametne kartice z vgrajenim monitorjem in kartice z vgrajenim čitalnikom prstnih odtisov. Kartice z vgrajenim mikroprocesorjem prekašajo mikroprocesorsko hitrost hišnega računalnika IBM XT/PC, najnovejše s kripto-soprocesorjem pa so po procesorski hitrosti hitrejše od 50 MHz računalnika PC 486. Omenjeni podatki kažejo na možnosti in potencial pametnih kartic in njihov razvoj in uporabo tudi v prihodnje.

Čipne kartice delujejo na skupnem standardu, imenovanem EMV. Gre za skupino standardov, ki so jih razvili Europay, MasterCard in Visa, opisuje pametne kartice za uporabo v plačniških sistemih. Napisani so tako, da omogočajo uporabo kartic različnih bank na istem bankomatu, ne da bi pri tem banka morala razkriti interni sistem plačevanja. Standardiziran je tudi v ISO 7816 standardu. Čeprav sam čip na pametni kartici zagotavlja identifikacijo v sistemu oziroma čitalniku, pa je čipna kartica, izdana s strani bančne institucije, navadno opremljena tudi z magnetnim trakom za primere uporabe na čitalni stezi magnetnega zapisa terminala, če ta ni opremljen s čitalnikom čipnih kartic. Takšna rešitev bistveno ne pripomore k povečanju varnosti, saj je kot predmet napada še vedno lahko magnetni trak oz. napis na njem.

Slika 22: Sestava »pametne kartice«



Elektronsko vezje pametne kartice je sestavljeno iz (slika št. 22):

- CPU (Central Processing Unit – procesor), izvaja aplikacije kartice, procesira shranjene podatke, opravlja odločitve in je odgovoren za naziv »pametna« kartica
- RAM (Random Acces Memory – začasni pomnilnik), shranjuje podatke in jih briše po izključitvi enote iz sistema
- ROM (Read Only Memory – stalni pomnilnik), podatki so stalni, se ne brišejo, shranjuje tudi operacijski sistem
- EEPROM (Electronically Erasable Programmable Read-Only Memory-shranjena vsebina se da elektronsko zbrisati in nanovo zapisati), uporablja se le v redkih sistemih
- Elektronsko vezje sestavljajo še klasični elementi (vodila, vhodno-izhodna enota, reset).

Pri tem je za izdajatelja in uporabnika pametnih kartic najbolj pomembna zaščita podatkov na njej. Zlorabe preprečuje trojni sistem preverjanja. Prvi je ta, da kartica preveri , ali je terminal, preko katerega poteka plačilo, pravi. Drugi je, da terminal preveri avtentičnost kartice. Nazadnje se preveri, ali je imetnik kartice tudi njen lastnik. Ob PIN kodi kot metodi identifikacije imetnika, ki jo je neprevidnim lastnikom še vedno mogoče ukrasti, obstajajo tudi drugačne oblike nadzora. Gre za biometrične tehnike. To so primerjave prstnih odtisov, očesne mrežnice, geometrije rok ali podpisov. Čitalna naprava preveri, ali je biometrični podatek na kartici enak temu, kar kaže uporabnik. (Newton, 1996: 17)

Pametna kartica je dražja od magnetne zaradi svoje inteligence, pa tudi zdrži precej dlje (nekaj let). Prednost pametne kartice pred magnetno je tudi možnost dodatnega zapisovanja podatkov. Uporaba pametne oziroma čip kartice v plačilnem in finančnem sistemu je možna na mnogih področjih, omejena pa je samo z višino sprejemljivih stroškov za njeno uvedbo. Poglavitni načini njene uporabe so (Abanka Vipa d.d., 1999: str.16-17):

- kot plačilno sredstvo, saj se pri zamenjavi z običajnimi plačilnimi sredstvi čip kartica pojavlja kot elektronska čekovna knjižica, elektronski potovalni ček, elektronska denarnica, elektronski žeton in podobno
- dvig gotovine na bančnih avtomatih
- plačevanje obveznosti ali jamstvo za plačilo
- prenos sredstev iz zunanjega vira v kartico (npr. sredstva na tekočem računu se prenesejo v elektronsko denarnico)

- avtorizacija pristopa, kar pomeni odpiranje vrat v bančne sefe ali trezorje, pri vstopu v mrežo pa za prenos sredstev ali pregledovanje stanj na računih
- elektronski podpis, ki se uporablja za preverjanje identitete, verodostojnosti in pooblastil prejemnika in pošiljatelja v sistemu elektronske izmenjave podatkov
- prenos datotek, na primer v funkciji elektronskega notesa za shranjevanje transakcij in podrobnosti, pomembnih za imetnika.

Čeprav ni možno zagotoviti, da se ne bodo tudi te kartice nekoč množično ponarejale, se poleg bank zanje zanimajo tudi pošte in telekomunikacijski sistemi. V njej je namreč možno združiti več funkcij.

Pametne kartice bi naj v bodočnosti v celoti nadomestile kartice z magnetnim zapisom. Pri nas banke že od leta 2004 izdajajo pametne kartice, vendar so še vedno opremljene tudi z magnetno stezo. Banke morajo ob uveljavitvi nove tehnologije ustrezno nadgraditi tudi POS terminale in bančne avtomate, kar je dolgotrajno in povezano z visokimi stroški. Na terminalih in bančnih avtomatih, ki še niso posodobljeni, se transakcija opravlja še vedno preko branja magnetnega zapisa in je zloraba kljub pametni kartici še vedno možna (Bizovičar M., 2007, str. 42).

Pametne kartice izpolnjujejo EMV[34] standard, ki pa velja samo za Evropo. Kljub izboljšavam zaščite na pametni kartici pa 100% zaščite pred zlorabami v elektronskem bančništvu ne bomo dosegli. Razlog je tudi v tem, da se za zamenjavo kartic z magnetnim zapisom za pametne kartice z mikroprocesorjem odločajo le izdajatelji kartic v Evropi, Amerika pa takšne zamenjave še ne predvideva, saj se odločanje o tem izvaja na osnovi razmerja med škodo, povzročeno z zlorabami in stroški zamenjave tehnologije (Cost – Benefit). V ZDA, iz katerih prihajajo tudi vse najbolj razširjene licenčne kartice (VISA, EUROCARD, AMERICAN EXPRES, DINNERS…) očitno zaenkrat še ni padla odločitev za zamenjavo tehnologije, ki bi močno zmanjšala možnost zlorab. Zaradi tega (Kranjec S., 2006, str. 18) se bo za ves plačilni promet s karticami do nadaljnjega (vsaj do leta 2010) uporabljal še dvojni sistem zapisovanja in branja podatkov na magnetni stezi in v integrirano vezje (če upoštevamo še alfa - numerični zapis na sami kartici, pa celo trojni sistem zapisa).

[34] Združenje EMV (Europay, Mastercard in Visa), ki so največji izdajatelji kartic, je razvilo standard za pametne kartice

Od začetka leta 2005 je v veljavi mehanizem, ki varuje banke, ki so sisteme za standard EMV že nadgradile. V primeru zlorab pokrije škodo tista stran, ki s tehnologijo EMV še ni opremljena. Če lastnik pametne kartice dvigne denar na bančnem avtomatu, ki še ni nadgrajen na tehnologijo EMV in pride do zlorabe, krije škodo banka, ki je lastnica bančnega avtomata (Bizovičar M., 2007, str. 42).

6.4.2 Varnost

Na samem področju varnosti plačevanja s pametnimi karticami pomenita razvoj in uvedba teh kartic velik napredek. Visoka stopnja varnosti temelji na naslednjih dejstvih:

- s pametne kartice je sicer možno prekopirati vsebino, ni pa možno prekopirati zasebnega ključa, zaradi česar so podatki neuporabni
- pametna kartica omogoča izkazovanje verodostojnosti in procesiranje kriptografskih algoritmov – zaščitnih elementov na sami kartici.

.

Izkazovanje verodostojnosti uporabnika je ena najpomembnejših komponent zagotavljanja varnosti. Pri pametnih karticah je ta izkazana s številko PIN (Personal Identification Number) ali pa z uporabo biometričnih metod. Za uporabo kartice moramo poznati PIN. V primeru tatvine kartice ima storilec le nekaj poizkusov uganitve pravilnega PIN-a, nato pa se kartica sama trajno zaklene ali pa je na bančnem avtomatu odvzeta. Kartico ob prijavi lahko zaklene tudi njen izdajatelj oziroma pooblaščeni nadzorni center. Še večjo varnost pa uporabniku kartice omogočajo biometrične metode, ki za izkazovanje verodostojnosti zahtevajo preverjanje prstnega odtisa ali očesne šarenice. Omenjeni biometrični podatki so predhodno shranjeni v spominu kartice. Procesor, stalni in začasni spomin kartice omogočajo tudi različne kriptografske tehnike, kot so šifriranje, dešifriranje podatkov ter procesiranje kriptografskih algoritmov in šifrirnih ključev. Zaradi teh lastnosti je pametna kartica postavljena v sam vrh varnega elektronskega poslovanja.

Na to mesto kartico postavlja uporaba javnega in zasebnega ključa, ki sta shranjena na kartici, in zmožnost procesiranja podatkov. Ključa sta matematično sorodna, a se med seboj toliko razlikujeta, da je na podlagi enega ključa nemogoče odkriti drugega. Zasebni ključ se na kartico zapiše ob personalizaciji kartice s strani izdajatelja in se nikoli ne zbriše, sistem pa zagotavlja, da se zasebni ključ tudi nikoli ne prenese oziroma prekopira s kartice. Kartica se identificira v sistemu s certifikatom, ki vsebuje podatke o imetniku in sami kartici ter javnim ključem, ki je sicer javno znan. Strežnik banke na podlagi pridobljenega certifikata in javnega ključa z uporabo algoritma kriptira simetrični ključ, tega pa lahko dekriptira le uporabnik

oziroma kartica pošiljateljica z zasebnim ključem. Ta proces se opravi z uporabo procesorja, stalnega spomina (zasebni ključ) in delavnega spomina. Z uporabo dekriptiranega simetričnega ključa se vzpostavi varna povezava terminala s strežnikom.

Znano je, da ključa, dolžine 128 bitov, s pomočjo metode preizkusa vseh možnih kombinacij z osebnim računalnikom ne najdemo v nekaj milijonih let, pametne kartice, uporabljene v bančništvu, pa navadno uporabljajo ključ, dolžine 192 bitov (Jerman Blažič, 2001).

Profesor računalniške znanosti Adi Shamir iz Weizmann Institute of Science v ZDA in eden vodilnih strokovnjakov s tega področja je leta 2006 na konferenci varnostnih sistemov predstavil in dokazal, da je možna tudi zloraba pametne kartice in razbitje oz. dekripcija tako javnega kakor tudi zasebnega ključa pametne kartice. Njegov pristop temelji na preučevanju delovanja procesorja čipa kartice in nihanja napetosti ob identifikacijskem postopku oziroma protokolu. Predstavljene so bile tudi možnosti uporabe mobilnih telefonov za zlorabe kartic, in sicer na način, da mobilni telefon po razbitju varnostnih ključev simulira plačilno kartico in se namesto kartice za plačilo uporablja telefon. Trenutno še ni podatka, da bi bil opisan pristop dejansko uporabljen v praksi (O'Connor, 2006).

Poleg uporabe varnostnih sistemov in tehnologij pa je za varno poslovanje zelo pomembno tudi fizično varovanje. Tu je mišljeno fizično varovanje dostopa do vitalnih delov informacijskega sistema in komunikacijske opreme. Tega se tvorci sistemov sicer zelo dobro zavedajo, saj jim le zavarovani in drugim nepoznani sistemi zaščite prinašajo denar, razkritje teh skrbno varovanih podatkov pa bi gotovo pomenilo najhujšo možno obliko zlorabe.

Kljub opevanim varnostnim značilnostim pametnih kartic in napredku, kateremu ni moč oporekati, pa se je potrebno zavedati, da napadi na varnostne sisteme v današnjem času niso nič nenavadnega in da nam tudi pametne kartice ne zagotavljajo 100% varnosti.

6.4.3 Razvoj uporabe pametnih kartic

Kartice z magnetnim zapisom so se v bančništvu v glavnem uporabljale kot bankomatne in kreditne kartice, za dvigovanje gotovine na bankomatih ali bankah in plačevanje na POS terminalih. Z napredkom tehnologije in uvedbo pametnih kartic pa so se pojavili novi načini uporabe. Banke so se začele nagibati k uvedbi elektronskih denarnic. Medtem ko so bankomatne kartice namenjene za takojšnje plačilo, kreditne za odloženo plačilo, so elektronske denarnice predplačniške. To pomeni, da ob izdaji kartica vsebuje določen znesek,

ki se ob vsakem plačilu zmanjša. Uporaba je podobna kot pri telefonskih karticah. Takšne kartice so z uporabo navadno omejene samo na naprave izdajatelja kartice, npr. plačevanje parkirnine in drugih storitev. O pravi elektronski denarnici pa lahko govorimo, ko s takšno denarnico lahko plačujemo na raznih mestih, predvsem manjše zneske, in ko ni potrebno preverjanje vsake transakcije. Elektronske denarnice so tesno povezane s pravim denarjem. Da bi bile elektronske denarnice povsem ekvivalentne denarju, morajo omogočati transakcije med karticami. S tem lastnikom omogočajo nakazovanje denarja sorodnikom, prijateljem in ponudnikom storitev, ki niso vključeni v mrežo trgovcev, katerim je kartica primarno namenjena. Z dokončno uvedbo elektronskih denarnic med vse prebivalstvo bi tako papirnati denar lahko popolnoma zamenjal plastičnega oziroma e-denar.

Najpreprostejše denarnice so za enkratno uporabo, kvalitetnejše in izpopolnjene pa že omogočajo vnovično polnjenje, pogosto kar na bankomatih ali pa na posebnih napravah na bankah. Prav tako lahko naprednejše kartice nosijo podatke, s katerimi se uporabnik identificira, enostavnejše pa ponavadi ne.

Tehnologija že dopušča uporabo pametnih kartic kot elektronskih denarnic, vendar se množična uporaba predvsem pri velikih zneskih ne bo uveljavila zaradi dveh razlogov. Prvi je možnost pranja denarja, saj bi brez vzpostavljene evidence nakupa predplačniških kartic ali njihovih polnjenj lahko prišlo na preprost način do prikrivanja izvora denarja iz nezakonitih dejavnosti. Drug problem je v potrošništvu in zadolženosti prebivalstva, ki s plačilnimi in kreditnimi karticami porablja finančna sredstva, ki jih dejansko še nima in jih še mora pridobiti. Predplačniške kartice bi namreč zahtevale, da uporabnik denarna sredstva ob nakupu že ima.

Zaradi zagotovitve varnih elektronskih transakcij se zanimanje za pametne kartice pojavlja tudi na tem področju. Proizvajalci tehnologije in lastnika licence za Viso in Mastercard so razvili enoten standard SET (Secure Electronic Transactions), ki omogoča avtentikacijo in celovitost transakcije s kreditnimi karticami. Ta standard za elektronske transakcije uporablja številko računa, serijsko številko kartice in datum veljavnosti. Na ta način ščiti podatke, ne preprečuje pa možnosti zlorab ukradenih kartic ali ukradenih podatkov o številki računa, številki kartice in datumu poteka, ker ne zahteva, da je kartica prisotna med transakcijo. SET tako preprečuje vnos nepravilnih in lažnih podatkov, ne more pa opravljati identifikacije uporabnika. Uporabniku nudi tudi anonimnost v razmerju do banke, pri kateri ima račun, saj njegova banka ne pridobi podatka o vrsti nakupa. Po drugi strani je komitent varen tudi pred

zlorabo s strani prodajnega mesta, saj trgovec ne pridobi osebnih podatkov o uporabniku in njegovem računu. Pametne kartice se danes uporabljajo tudi pri elektronskem bančništvu za shranjevanje certifikatov, ki so danes nujni za vzpostavitev varne povezave med uporabnikom in banko. Največja razlika v uporabnosti med pametnimi in karticami z magnetnim zapisom je v uporabnosti pri elektronskem poslovanju in v možnosti hranjenja podatkov v spominskem mediju.

V Sloveniji in tudi drugod v svetu se pametne kartice uporabljajo v elektronskem bančništvu, v zdravstvu, za plačila v telefonskem prometu v javnih govorilnicah, mobilni telefoniji (SIM kartice) in v različnih oblikah trgovinskih kartic (PETROL, MERCATOR PIKA…).

6.4.4 Tehnične zaščite bančnih avtomatov

Pri nas je nameščenih več različnih bančnih avtomatov, različnih proizvajalcev in tipov. Med bolj zvenečimi imeni proizvajalcev so IBM, NEC, Olivetti. Sprva so se nameščali raznovrstni bančni avtomati, v zadnjem času pa je zaradi različnih razlogov opaziti poenotenje tako proizvajalcev kot tipov avtomatov.

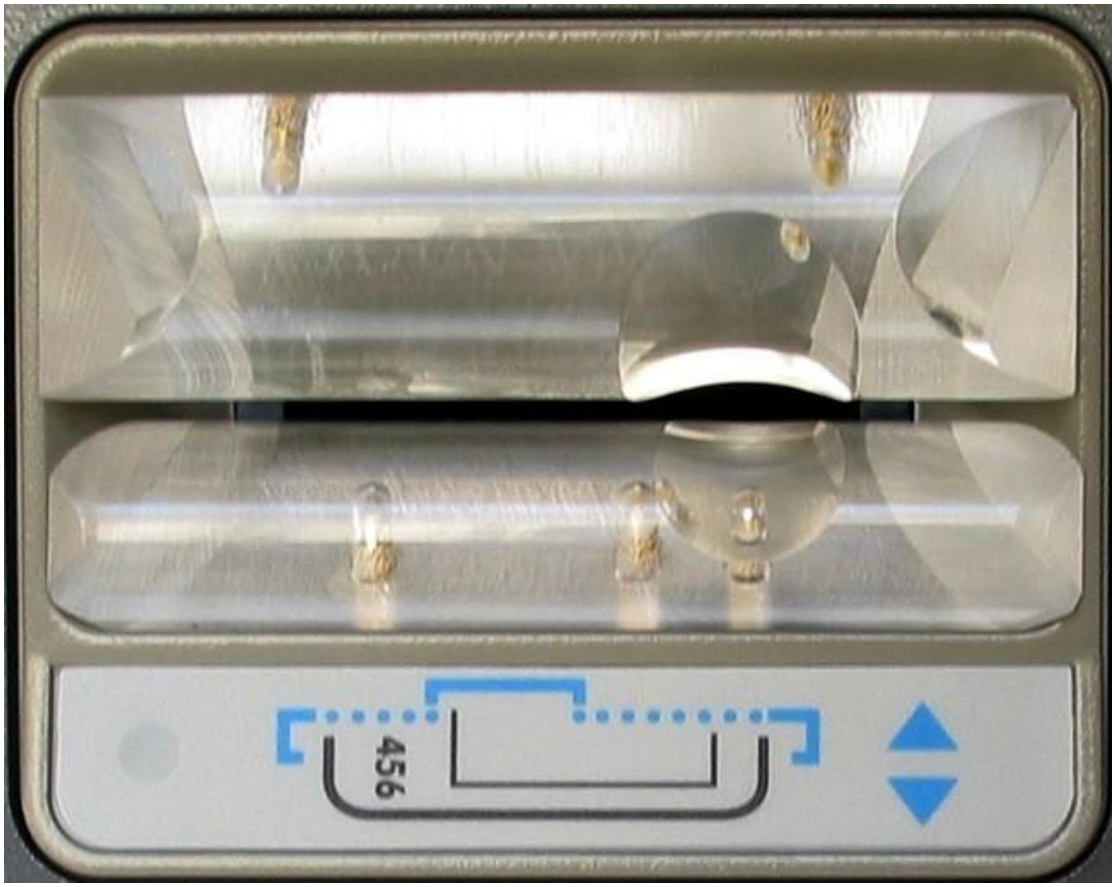
Zagotavljanje varnosti bančnega avtomata in preprečevanja vdiranja v notranjost bančnih avtomatov in nameščanja naprav za kopiranje magnetnih zapisov in mikro kamer mora proizvajalec izvesti s samo konstrukcijo in varovalnimi mehanizmi. Tako so elementi bančnega avtomata skrbno skriti za enodelnim zunanjim oklepom bančnega avtomata iz debelejše pločevine. Vsi deli bančnega avtomata, ki so se v prejšnjih izvedbah dali izvleči (tipkovnica, monitor, čitalec kartice in posamične plošče zunanje oplate, pričvrščene z zunanjimi vijaki), plošče iz plastike in tanke pločevine so se izkazali kot lahka tarča napadalcev. Zaradi tega so proizvajalci na podlagi analiz zlorab, vdorov in tatvin bančnih avtomatov umaknili vse nepotrebne in štrleče elemente. Danes je večina bančnih avtomatov izvedena z gladkimi stenami, iz katerih ne štrlijo nobeni deli, potrebni za izvedbo transakcije. Vsi deli na bančnem avtomatu so pritrjeni tako, da njihova zamenjava od zunaj ni možna, kar zelo otežuje nameščanje dodatnih naprav, kakor tudi zamenjavo delov bančnega avtomata z deli, ki bi omogočali storilcem izvajanje zlorab. V bančnih avtomatih je nameščenih tudi mnogo naprav, ki dodatno omogočajo večjo varnost pred vdori. Tako je bančni avtomat opremljen s stikali, ki v primeru odpiranja izklopijo bančni avtomat iz omrežja in preprečijo njegovo delovanje in izplačilo denarja.

Za preprečevanje nameščanja skimming naprav na bančne avtomate se uporabljajo tudi posebne ploščice, ki se montirajo na ščitnik čitalnika kartic. Sestavljene so iz zgornjega in spodnjega dela, ki sta zaobljena in s svojo obliko preprečujeta nameščanje skimming naprave, saj ni ravnih ploskem za pritrditev. Sama debelina ploščic je takšna, da pri izmetu kartice iz bančnega avtomata gleda iz reže samo toliko kartice (1-2 mm), da jo komitent lahko vzame. Če bi bilo pred režo nameščena naprava za skimming, kartice iz reže ne bi bilo mogoče vzeti in uporabnik bi bil s tem opozorjen, da je nekaj narobe.

Ploščice za zaščito so pritrjene s štirimi vijaki, od katerih je eden slep in povezan na stikalo za izklop bančnega avtomata. Če bi prišlo do vdora v bančni avtomat in demontaže varovalne ploščice, bi se ob zasuku slepega vijaka bančni avtomat izključil. Položaj slepega vijaka ni vedno enak in ga določi vzdrževalec bančnega avtomata. Primer takšne vrste zaščite je prikazan na sliki št. 23.

Obstajajo pa že tudi lažne naprave za zaščito pred skimmingom, ki so na bančni avtomat samo prilepljene, vijaki pa niso povezani s stikalom za izklop. S temi napravami bi naj preventivno zagotavljali varnost in odvračali storilce, vendar ob visokem tehničnem znanju storilci kaj hitro ugotovijo in prepoznajo lažne naprave za zaščito. Takšne snamejo in namestijo skimming napravo, ker bančni avtomat nima zaščite, ki bi nameščeno napravo zaznala in izključila delovanje.

Slika 23: Bančni avtomat z napravo, ki preprečuje nameščanje skimming naprav



Vir: Europol 2006

Še bolj tehnološko dovršeni način zaščite pred nameščanjem skimming naprav je elektronski. Optični senzorji in infrardeči žarki kontrolirajo ustje čitalnika kartic. Če je žarek neprekinjen, ostaja bančni avtomat vklopljen, če pa z namestitvijo naprave za skimming žarek prekinemo, se bančni avtomat izključi.

Za dodatno tehnično varovanje bančnih avtomatov se lastniki odločajo predvsem na podlagi stroškov in koristi, ki se vidijo v zmanjšanju zlorab, saj stroški namestitve dodatne naprave niso zanemarljivi.

Velik napredek v varnosti bančnih avtomatov pomeni tudi stalna povezanost bančnih avtomatov v omrežje, ki omogoča stalni nadzor nad delovanjem bančnih avtomatov in spremljanje prometa, saj upravljavec omrežja bančnih avtomatov zagotavlja tudi 24 urno delovanje nadzornih centrov. Zaradi pogostih fizičnih vdorov v trezorje bančnih avtomatov in

tatvine celotnih bančnih avtomatov pa tudi pri nas načrtujejo zaščito denarja v bančnem avtomatu z barvo, ki bo v primeru tatvine obarvala denar (http://www.mojevro.si/252874 Finance, 2009) in ga naredila prepoznavnega in neuporabnega za storilca.

V skladu s podpisanimi priporočili med Združenjem bank Slovenije in policijo nadzorni center ob izklopu, napaki, napačnem delovanju ali drugi zaznani nepravilnosti, ki kaže na zlorabo na bančnem avtomatu, v sklopu bančnih varnostnih sistemov, obvešča policijo.

Zaščitni ukrepi in dejavnosti proizvajalcev bančnih avtomatov in njihovih lastnikov za zagotavljanje varnosti so varovani in javnosti nedostopni.

6.4.5 Nova metoda ocenjevanja informacijskega tveganja (IBRA)

V nalogi smo s proučevanjem poslovanja na področju elektronskega bančništva, analizami zlorab in proučevanja varnostnih in zaščitnih mehanizmov na preventivnem in represivnem področju prišli do celovitega varnostnega modela za preprečevanje zlorab. Iz varnostnega modela je razvidno, da se je zagotavljanju varnosti na področju elektronskega bančništva potrebno lotiti celovito. Ukrepi za doseganje višje stopnje varnosti so pomembni za zmanjšanje in preprečevanje zlorab, poleg tega pa znižujejo tudi nevarnost, da bi nastala nematerialna škoda za finančno institucijo iz naslova slabega imagea, ki lahko za finančno institucijo pomeni odliv komitentov in zmanjšanje prometa, v najslabšem primeru pa tudi propad finančne institucije. Pri proučevanju zlorab na področju elektronskega bančništva smo ugotovili, da vse škode ni mogoče finančno ovrednotiti, težave pa so tudi s pridobivanjem podatkov o zlorabah. Zaradi tega je težavno določiti, kolikšna je škoda, ki jo utrpijo finančne institucije z zlorabami, prav tako pa nimamo kakovostnih podatkov za namen ocenjevanja varnostnih modelov finančnih institucij. Problematiko zagotavljanja varnosti finančnih institucij smo preverjali pri zaposlenih z vprašalniki in intervjuji. Iz odgovorov je razvidno, da je na področju elektronskega bančnega poslovanja zelo pomembna varnost informacijskih sistemov, kakor tudi grožnje in ranljivosti, ki jih prinašajo druge okoliščine, v katerih delujejo bančni informacijski sistemi. Varnostni model obvladovanja zlorab pokaže, da na varnost vpliva mnogo dejavnikov in je zato na področje varnosti potrebno gledati celovito in da na tem področju veljajo določene posebnosti, na katere moramo biti še posebej pozorni (zaupnost podatkov, izgube sredstev zaradi slabega imagea, mednarodni kriminal in vpliv uporabnikov). Zaradi tega se je pokazala potreba po metodi ocenjevanja informacijskega tveganja, ki bi ugotovljene posebnosti upoštevala in bi bila prilagojena specifičnostim bančnega poslovanja.

Zato smo najprej proučili obstoječe metode za ocenjevanje informacijskih tveganj in na podlagi teh v nadaljevanju oblikovali novo metodo, ki je prilagojena ocenjevanju informacijskega tveganja bančnih informacijskih sistemov.

Za naš obravnavani model celovite varnosti smo na podlagi obstoječih metod in konceptov izdelave ocen tveganja izdelali novo metodo ocenjevanja informacijskega tveganja. Metoda IBRA (Information Bank Risk Analysis) ima za glavni cilj postavljeno analizo groženj in njihovo zmanjšanje, s tem pa tudi zmanjšanje tveganja. Metoda temelji na tem, da poskušamo na podlagi ocenjevanja groženj in ranljivosti sistema z vidika preventivnih in represivnih dejavnikov oceniti tveganje sistema in na podlagi odzivov sistema te vrednosti zmanjšati. Stroški informacijske varnosti namreč pomenijo pomembno postavko v skupnih stroških poslovanja organizacije in vodstva se na podlagi stroškov in koristi, ki nastanejo, odločajo za nove vrste zaščite. Glavni rezultat povečane varnosti informacijskih sistemov je zmanjšanje tveganj sistema. Če je sistem preveč izpostavljen grožnjam in ranljiv, se pojavljajo stroški, ki nastanejo zaradi izgube sredstev, posledic dogodkov in zmanjšanja ugleda (imagea) tako storitve (plačilni promet) kakor tudi institucije (banke). Posebej finančne institucije morajo biti pozorne na zagotavljanje »dobrega imena«, kajti v nasprotnem primeru lahko pride zaradi nezaupanja do izgube komitentov, deleža trga ali v najslabšem primeru tudi do propada institucije. Za izgube iz tega področja je tudi značilno, da jih je težko ali celo nemogoče vrednostno zajeti in ovrednotiti. Poleg tega smo pri zbiranju kvantitativnih podatkov naleteli na bančno tajnost, saj banke ne izdajajo podatkov, ki so predmet poslovanja, prav tako pa se podatki o zlorabah posameznih bank nikjer centralno ne zbirajo in obdelujejo.

Zaradi tega smo za ocenjevanje tveganja za našo metodo uporabili kvalitativni pristop. Metoda tudi ni statična metoda, kajti spremembe razmer na področju elektronskega bančništva so izredno dinamične in se spreminjajo zaradi vpliva različnih dejavnikov na tem področju. Vse spremembe na področjih groženj in ranljivosti sistema morajo spremljati tudi odzivi sistema z ukrepi za povečanje varnosti. S tem se seveda spremeni tudi ocena tveganja v spremenjenih okoliščinah. Nova metoda ocenjevanja tveganja je usmerjena v ocenjevanje potencialnih groženj in dogodkov, ki bi imeli za posledico izgubo in stroške na vseh treh področjih.

Značilnosti metode IBRA so:

- ocenjuje tveganja z vidika preventivno – represivnih dejavnikov, ki vplivajo na varnost sistema
- za zbiranje podatkov uporablja ankete, intervjuje in sestanke
- tveganje opredeljuje kot tveganje izgube sredstev, zaščite in izgubo dobrega imena (imagea banke)
- deluje v realnem času in dinamično obravnava dejavnike tveganja
- na osnovi povratne zanke odzivi modela vplivajo tako na nevarnosti kot na grožnje
- zahteva dobro poznavanje procesov.

Grožnje

Grožnja pomeni določen tok dogodkov, ki izkorišča ranljivost sistema in povzroči nek dogodek, ki ima za posledico povzročeno škodo (Goldberg Y., 2005). Ta je lahko v primeru metode IBRA poleg izgube sredstev tudi izguba dobrega imena finančne institucije. Poznamo namerne in nenamerne grožnje. Namerne grožnje imajo za sabo določen cilj, ki je lahko materialna korist ali zgolj povzročanje škode.

Sodobne metodologije za analizo tveganj so zelo obsežne in lahko vsebujejo več sto različnih vrst groženj od zlonamernih sistemskih operaterjev, inženirjev, hekerjev do različnih tehničnih in tehnoloških napak in izpadov, v končni fazi pa lahko grožnje za finančne sisteme predstavlja tudi terorizem oz. vojna na nekem področju ali pa naravne nesreče, na pojav katerih ne moremo vplivati.

V naši metodi smo glavne grožnje, ki so specifične za bančne informacijske sisteme, razvrstili na naslednje (Gradišar, M., Lamberger, I., 2010):

- zlorabe uporabnikov
- zlorabe uporabniške identitete s strani zunanjih oseb
- nepooblaščena uporaba aplikacij
- uporaba in namestitev škodljive programske in strojne opreme
- nameščanje in napadi z računalniškimi virusi in trojanskimi konji
- zlorabe in spremembe logističnih poti do uporabnika
- zlorabe s strani pogodbenih uporabnikov (trgovcev)
- namestitev in uporaba lažnih sredstev (tujkov) v sistemih

- tatvine s strani zunanjih oseb z lažno ali prevzeto identiteto pravega uporabnika
- lažne tehnične okvare in zlorabe opreme
- namerno povzročanje škode s strani zaposlenih
- namerno povzročanje škode s strani zunanjih oseb (hekerji)
- sodelovanje zaposlenih z zunanjimi osebami pri zlorabah
- posredovanje informacij o delovanju in zaščiti sistema zunanjim osebam s strani zaposlenih
- posredovanje informacij o delovanju in zaščiti sistema zunanjim osebam s strani pogodbenih partnerjev
- neavtorizirani vdori v sistem.

Poleg vseh naštetih groženj seveda na sistem delujejo tudi povsem splošne grožnje: od naravnih nesreč, vojn in terorističnih napadov, ki pa jih podrobneje v modelu nismo obravnavali, saj predstavljajo splošne grožnje in kot take imajo vpliv na vse modele ocenjevanja tveganj. V naši metodi smo zajeli predvsem grožnje, ki so specifične za naš varnostni model.

Ranljivost

Ranljivost je škoda, ki jo povzroči uresničenje grožnje. Pomeni (Goldberg Y., 2005), da se lahko zaradi določenih slabosti celotnega sistema ali posameznega dela poseže v normalno funkcioniranje in delovanje sistema in tako doseže okvara oz. zloraba sistema za določene cilje storilca, ki so lahko materialne narave (premoženjska korist) ali nematerialne narave (dokazovanje in postavljanje pred ostalimi).

Informacijske sisteme lahko ogrožajo vse vrste groženj, ki so poznane, od specifičnosti sistema pa je odvisno, katere grožnje so bolj verjetne. Nove grožnje prinaša tudi razvoj in razmah informacijskih sistemov, opreme in povezovanje lokalnih mrežnih sistemov v medmrežja. S tem se povečuje tudi število uporabnikov, kar poleg koristi (mrežne eksternalije) prinaša tudi večje možnosti za ranljivosti sistema. Večjo ranljivost zato lahko pričakujemo zaradi (EBIOS, 2004):

- geografske razširjenosti in možnosti dostopa kjerkoli
- možnosti dostopa zunanjih oseb
- možnosti uporabe storitev brez neposrednega nadzora zaposlenih
- potrebe po določenem znanju uporabe informacijske tehnologije pri uporabnikih

- izpostavljenosti opreme namernim poškodbam in tatvinam
- manipuliranja uporabnikov storitev s strani tretjih oseb
- nedorečene in zastarele zakonodaje
- možnosti visokih zaslužkov s povzročanjem namernih zlorab.

Zadnji dejavnik ranljivosti je v našem modelu varnosti tudi najpomembnejši, saj se zlonamerni uporabniki ravno zaradi njega odločajo za zlorabe, ker je možno z zelo malo vloženimi sredstvi pridobiti velike zaslužke in premoženjske koristi.

Ocenjevanje tveganja

Po opredelitvi groženj in ranljivosti sistema nas zanima tudi, koliko potencialne škode nam lahko povzročijo posamezne grožnje, ki lahko izrabijo določeno ranljivost sistema. Ocenjevanje tveganja pri varovanju informacijske tehnologije je sistematičen proces, ki ga uporabljamo za določitev možnosti, da informacijski sistem utrpi posledice zaradi izgube sredstev, izgube dobrega imena (imagea) in povečanih stroškov zaščite sistema.

Določitev in ocenjevanje tveganja informacijskih sistemov zahteva dobro razumevanje okolja sistema. Zato moramo zbrati informacije, ki so povezane s tveganjem in sistemom. Rezultati ocene tveganja kažejo, kaj je resnično pomembno za varovanje in varnost informacijskega sistema in samo organizacijo. Ocena tveganja se uporablja pri podpori sprejema tveganja in izboru stroškovno ugodnih kontrol in zaščit.

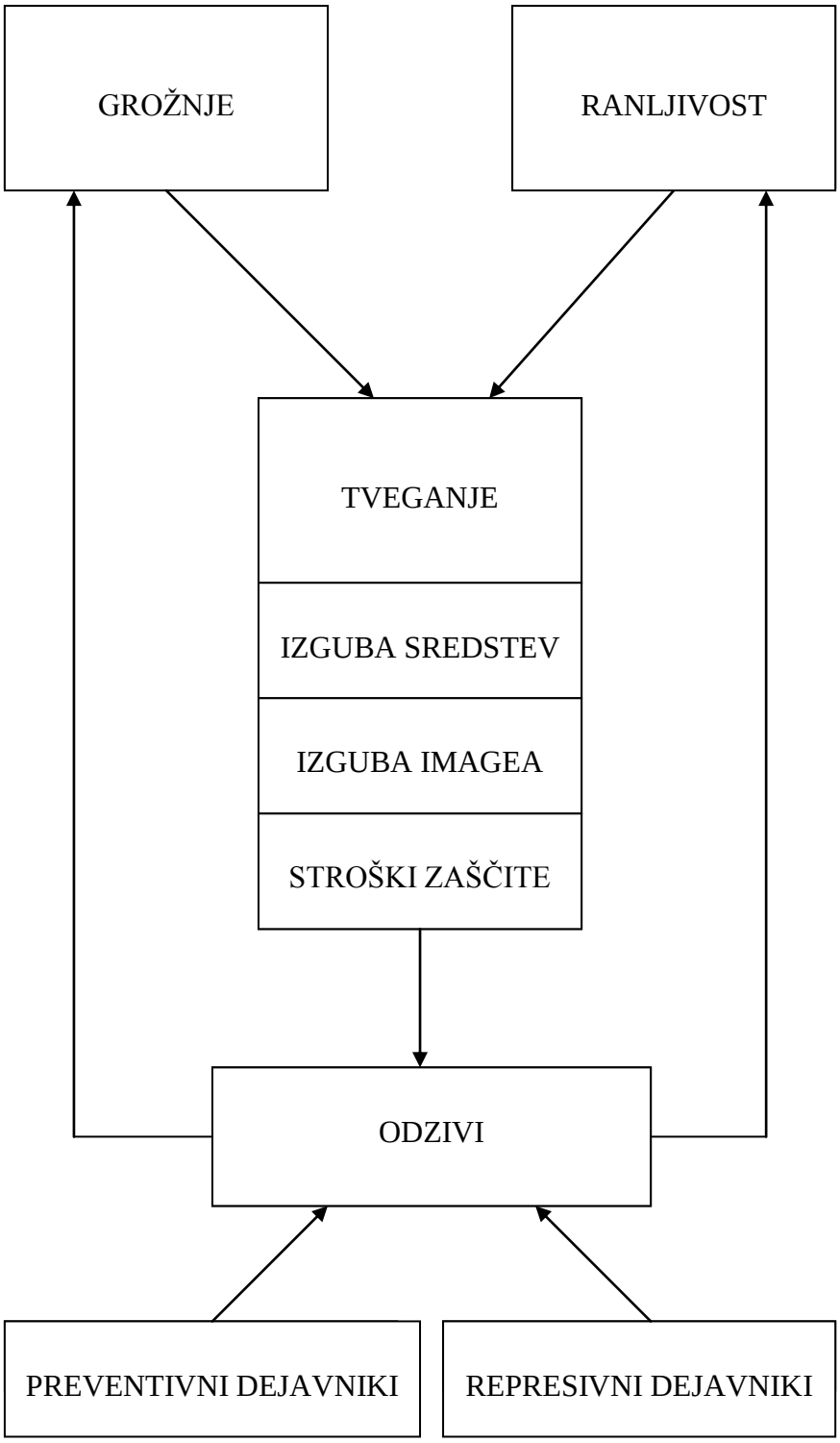
Odzivi

Odzivi sistema so lahko postopki, ukrepi na organizacijskem področju ali nova, izpopolnjena sredstva in tehnologije, ki zmanjšujejo ranljivost sistema na osnovi prepoznanih groženj, ranljivosti in ocene tveganja.

Dobri in kakovostni ukrepi sistem zaščitijo pred grožnjami in lahko kratkoročno možnosti posameznih groženj tudi skoraj popolnoma izključijo oz. onemogočijo. Vendar moramo biti pozorni na prilagajanje storilcev zlorab novim varnostnim mehanizmom, ki jih lahko z novim znanjem ali tehnologijo ponovno obidejo in ponovno povzročajo škodo. Zaradi tega ima metoda IBRA tudi povratno zanko, ki vedno preverja možnosti potencialnih novih groženj in sprememb v ranljivosti sistema. Gre za dinamično spremljanje groženj in ranljivosti in na

osnovi sprememb z odzivi zmanjševanje enih in drugih in s tem povečevanje varnosti sistema. Na sliki št. 24 je prikazana medsebojna povezanost dejavnikov tveganja metode IBRA.

Slika 24: Medsebojna povezanost dejavnikov tveganja (IBRA)



Koraki metode IBRA

Metoda IBRA poteka v osmih korakih:

1. Začetek: zavedanje o problemih in nevarnostih informacijske varnosti

V tem koraku določimo, kaj želimo doseči, kakšni so naši nameni in cilji in kaj bi se lahko zgodilo, če v proces ne gremo. Upoštevamo in predvidimo tudi vse dejavnike, ki lahko vplivajo na proces. Ta korak izvajajo vodje, ki so odgovorni za področje varnosti v organizaciji v sodelovanju in obveščanju vodstva organizacije.

2. Določitev zahtev:

Določimo zahteve v zvezi z varnostjo sistema, ki so lahko informacijske, pravne, organizacijske ali druge. Zahteve se določajo v skladu s potrebami varnosti sistema ob sodelovanju zaposlenih na področju varnosti informacijskih sistemov in vodstva organizacije, saj se lahko zahteve nanašajo tudi na druga področja, ne zgolj na informacijsko varnost.

3. Ocena vpliva preventivnih in represivnih dejavnikov

V tem koraku ocenjujemo preventivne dejavnike in represivne dejavnike, njihovo težo in vpliv na postavljene zahteve in ocenimo izgube, ki so lahko na več področjih. Gre za izgube sredstev, izgube zaradi stroškov zaščite in izgube zaradi slabega imena organizacije. Ta korak izvaja izvajalec metode.

4. Anketiranje

Dejavnike iz prejšnjega koraka preoblikujemo v anketne vprašalnike, oblikujemo možne odgovore, določimo vrednosti za posamezen odgovor in izvedemo anketo. Izvajanje tega koraka je v pristojnosti izvajalca metode.

5. Ocena rezultatov in analiza odgovorov

V tem koraku ocenjujemo in analiziramo dobljene odgovore na postavljena vprašanja in dobimo rezultat metode v obliki ocene tveganja in priporočil in ukrepov za odpravo tveganja. Korak izvaja izvajalec metode, ki si lahko pomaga tudi z mnenji analitikov.

6. Izvedba novih kontrol

Gre za korak, kjer nameščamo in testiramo nove ukrepe in kontrole v sistem. Na osnovi rezultatov iz vprašalnikov se izvajalec ankete o ukrepih in kontrolah posvetuje s strokovnjaki s področja informacijske varnosti v organizaciji ali zunanjimi strokovnjaki.

7. Upravljanje in nadzor

Upravljanje sistema pomeni zagotavljanje delovanje kontrol in spremljanje odzivov sistema ter sporočanje in dokumentiranje incidentov. V tem koraku je pomembna vloga in sodelovanje zaposlenih za prepoznavanje, dokumentiranje in obveščanje predpostavljenih o incidentih.

8. Potrjevanje

Na osnovi rezultatov potrjujemo smotrnost ukrepov in delovanje novih kontrol za zmanjšanje tveganja. Potrjevanje poteka na osnovi dobljenih rezultatov iz predhodnega koraka, kjer sodelujejo zaposleni, v zadnjem koraku pa se izvajalec metode in vodstvo odločata o smotrnosti in uspešnosti novih kontrol in ukrepov za zmanjševanje tveganja.

Primerjava metode IBRA z drugimi metodami

Prednosti metode IBRA v primerjavi z drugimi so v tem, da je primerna za področje preučevanja tveganja informacijskih sistemov bank, ker obsega grožnje, ranljivosti in tveganja, ki so značilna za bančno poslovanje. Zaradi bančnih tajnosti ni mogoče pridobiti podatkov o povzročenih škodah zaradi zlorab, zato je zastavljeni model kvalitativen in ne zahteva kvantitativnih podatkov za oceno tveganja.

Metoda upošteva tudi škodo, ki jo lahko povzročijo zlorabe, saj poleg izgube sredstev pride tudi do izgube komitentov ali neuporabe določenih storitev zaradi izgube ugleda bančne institucije. Takšna škoda lahko presega ostale izgube oz. je lahko usodna tudi za obstoj same banke.

Na osnovi znanja, ki ga imajo zaposleni v organizaciji, se lahko z metodo IBRA na dokaj enostaven način ocenijo tveganja in grožnje sistema. Ker ne uporabljamo kvantitativnih metod, ne potrebujemo programske opreme in algoritmov za preračunavanje številčnih podatkov. Zaradi specifičnosti modela, ki je naravnan na banke, podatke pridobivamo od zaposlenih, ki delajo na področju varnosti informacijskih sistemov in že morajo imeti

določeno znanje o delovanju in varnostnih mehanizmih informacijskega sistema. Zato dobimo tudi kvalitetne podatke, saj jih zbiramo od tistih, ki so za varnost tudi zadolženi v okviru zaposlitve oz. statusa delovnega mesta in bi varnostne zahteve morali tudi obvladovati.

Metoda je dinamična, saj na osnovi povratne vezave in dejavnosti vpliva na spreminjanje groženj in ranljivosti. Če do zmanjšanja tveganja ne pride ali če se tveganje celo poveča, se zažene nov cikel in nove dejavnosti za zmanjšanje tveganja. To se izvaja tako dolgo, da ukrepi privedejo do še obvladljivega tveganja in s tem optimalnemu razmerju med stroški varovanja in stroški zlorab.

Banka oz. druge finančne institucije, ki se ukvarjajo z elektronskim bančništvom, lahko z zastavljenim modelom ocenjevanja tveganja na dokaj preprost način in brez visokih stroškov pridejo do ocene tveganja in glede na to sprejmejo ukrepe za omejevanje in zmanjšanje tveganja. Seveda metoda zahteva od sodelujočih določen nivo znanja in poznavanje problematike zlorab na tem področju, a zaradi kvalitativne vrste metode ne potrebujemo številčnih podatkov, do katerih je zelo težko priti zaradi bančne tajnosti in zaradi nesistematičnosti zbiranja, obdelave in njihovega posredovanja oz. primerjave med različnimi bankami in sistemi.

Metodo IBRA smo z drugimi metodami primerjali še po ključnih kriterijih: vrsti metode, številu sredstev, ki jih ocenjuje, sodelujočih, rezultatih in potrebnih izkušnjah za izvedbo.

Vrsta metode

Metoda IBRA je kvalitativna metoda in za njeno izvedbo ne potrebujemo številčnih podatkov. To predstavlja v našem primeru prednost pred drugimi metodami, ki zahtevajo samo ali tudi številčne podatke (CRAMM, ISRAM, EBIOS, MEHARI). Zaradi specifike bančnega poslovanja in množice finančnih transakcij in podatkov je relevantne podatke o zlorabah izredno težko opredeliti, jih obdelati in zbrati. Poleg tega naletimo na problem tajnosti podatkov, ki so vsi opredeljeni kot bančna tajnost in je v primeru obdelovanja teh podatkov s strani zunanjih institucij problematično samo posredovanje podatkov. Zaradi nezadostne pazljivosti lahko namreč vplivajo na image institucije, če pridejo v neprave roke.

Ocena za eno sredstvo ali več

Metoda je celovita in se ocena tveganja vrši za celoten sistem elektronskega bančnega poslovanja, za kar je tudi namenjena. Metoda ne ocenjuje tveganja samo za določena sredstva, saj smo z našim varnostnim modelom ugotovili, da je varnost potrebno obravnavati celovito. Ocena tveganja se izvaja za celotno organizacijo, kar pa ne pomeni slabosti v primerjavi z metodami, ki lahko ocenjujejo tveganje tudi samo za eno sredstvo (CRAMM, OCTAVE, BPIRM, EBIOS, MEHARI).

Sodelujoči

Sodelujoči pri pridobivanju vhodnih podatkov pri tej metodi so zaposleni, ki delajo na področju varnosti informacijskih procesov. V organizaciji se lahko sami odločijo, če se med sodelujoče vključi tudi management. Vključevanje je smiselno takrat, ko nam management lahko da zadovoljive podatke o problematiki varnosti v organizaciji in ni samo upravljavsko povezan s tem področjem, ampak tudi strokovno. Ker je metoda kvalitativna, ne potrebujemo številčnih podatkov in vključevanja drugih zaposlenih, ki bi bili s pridobivanjem, razvrščanjem in analiziranjem podatkov dodatno obremenjeni pri svojem rednem delu. Prednosti te metode so, da imajo sodelujoči znanje in vedenje o varnosti informacijskih sistemov in nam dajo kakovostne odgovore na zastavljena vprašanja z vprašalniki, poleg tega pa ni dodatno obremenjeno večje število zaposlenih v organizaciji. Druge metode lahko za daljše časovno obdobje precej obremenijo zaposlene in odgovorne (management) v organizaciji (CRAMM, 2001), zato je lahko ta metoda zelo pozitivno sprejeta ravno zaradi nizke dodatne obremenitve zaposlenih.

Rezultat

Po analizi odgovorov dobimo rezultat v dokaj preprosti obliki. Rezultat je ocena tveganja in priporočila in ukrepi, ki vodijo k zmanjšanju tveganja. Sama analiza ni dolgotrajna in lahko do rezultata pridemo dokaj hitro in s tem tudi do želenega rezultata tveganja. Ker je metoda dinamična, se s povratno povezavo novi ukrepi preverjajo in analizira njihov vpliv na varnost informacijskega sistema.

Potrebne izkušnje

Sama metoda IBRA je dokaj preprosta za uporabo in ne zahteva posebnih znanj zaposlenih, saj se izvaja s preprostimi vprašalniki. Zato posebne priprave na uporabo metode niso potrebne in ni potrebno izobraževanje zaposlenih za uporabo orodja, kot to zahtevajo nekatere druge metode (CRAMM, OCTAVE, EBIOS in MEHARI). Zahteva metode je ta, da imajo sodelujoči določeno znanje in izkušnje na področju informacijske varnosti, zato je metoda namenjena ravno temu krogu zaposlenih v organizaciji.

Preverjanje metode IBRA pri potencialnih uporabnikih

Uporabnost metode IBRA, ki je namenjena ocenjevanju tveganj bančnih informacijskih sistemov, smo preverili še z izvedbo intervjujev pri osebah, ki v bankah skrbijo za varnost informacijskih sistemov.

Za namen naše naloge smo uporabili strukturirani intervju. Vnaprej pripravljena vprašanja so bila postavljena vsem osebam, ki so sodelovale v intervjuju enako in v istem vrstnem redu. Intervjuji so bili izvedeni spomladi leta 2011. Vprašanim so bili cilji in namen intervjuja predstavljeni pred postavljanjem vprašanj. S pomočjo Združenja bank Slovenije smo opravili intervju z osebami, ki skrbijo za varnost informacijskih sistemov v štirih slovenskih bankah, katerih tržni delež po bilančni vsoti predstavlja 41,2% in še z osebo na Združenju bank Slovenije, ki je na združenju zadolžena za področje plačilnega prometa.

Vsem smo zastavili naslednja vprašanja:

1. Pomembna zahteva informacijskih sistemov, še posebej bančnih, je njihova varnost. Ali je potrebno in na kakšen način v vaši instituciji poteka ocenjevanje varnosti informacijskih sistemov?
2. Kakšne vrste škode lahko povzroči banki nezadostna zaščita informacijskega sistema?
3. Bančni informacijski sistemi so izpostavljeni grožnjam, ki vplivajo na tveganja in varnost poslovanja. Obstaja več metod za ocenjevanje tveganja informacijske varnosti (CRAMM, OCTAVE, ISRAM, BPIRM, EBIOS, MEHARI). Ali bi bila potrebna za ocenjevanje tveganja bančnih informacijskih sistemov posebna metoda, ki bi bila prilagojena bančnemu poslovanju?

4. Poznamo kvalitativne, kvantitativne in kombinirane metode za ocenjevanje tveganj informacijske varnosti. Vsaka vrste metode ima svoje prednosti in slabosti. Slabosti kvantitativnih so odvisnost od kakovosti podatkov, zahtevana in dolgotrajna uporaba, težavnost denarnega vrednotenja sredstev, težavnost vrednotenje kontrol, nekaterih stroškov ni mogoče ovrednotiti. Slabosti kvalitativnih metod sta lahko subjektivnost in nenatančnost. Katera vrsta metode za ocenjevanje tveganja bi bila po vaše za banke najboljša?
5. Ali bi bila obdelava, zbiranje in analiziranje številčnih podatkov o zlorabah na področju elektronskega bančništva za namen ocenjevanja tveganja varnosti informacijskega sistema banke mogoča z vidika obremenitve zaposlenih, točnosti podatkov, hitrosti pridobitve, ovrednotenja vse škode (image banke) in bančne tajnosti (če bi ocenjevanje tveganja izvajala zunanja institucija)?
6. Kvantitativne metode ocenjujejo tveganja na podlagi obdelave številčnih podatkov, vendar je rezultat odvisen od kakovosti podatkov, izognemo pa se subjektivnemu vplivu ocenjevalcev. Ali bi bila kvantitativna metoda primerna za ocenjevanje tveganja bančnih informacijskih sistemov?
7. Kvalitativne metode ne zahtevajo številčnih podatkov, ampak ocenjujejo tveganja s pomočjo podatkov, ki jih pridobijo z anketami, vprašalniki in intervjuji od zaposlenih, ki morajo dobro poznati procese. Ali bi bila takšna metoda primerna za banko in ali bi se lahko na ta način ocenile grožnje, ranljivosti in tveganja bančnega informacijskega sistema?
8. Kdo vse od zaposlenih bi moral sodelovati pri pridobivanju podatkov o varnosti informacijskega sistema?
9. Ocenjevanje tveganja informacijske varnosti je dolgotrajen postopek, povezan s povečanimi obremenitvami zaposlenih in dodatnimi stroški. Po katerih kriterijih in zaradi česa bi se odločali za ocenjevanje tveganja?
10. Je ocenjevanje tveganja informacijskega sistema enkratno dejanje v nekem časovnem obdobju ali je potrebno tveganje ocenjevati sprotno in se prilagajati razmeram na področju varnosti?
11. Katere prednosti za banko bi lahko pomenila metoda za ocenjevanje tveganja informacijskih sistemov, ki bi bila prilagojena posebnostim bančne varnosti?
12. Ocenjevanje tveganja pomeni za institucijo tudi dodatne stroške, le ti pa nastanejo tudi zaradi dodatnih ukrepov varovanja informacijskih sistemov. Katere slabosti oz. nevarnosti še lahko predvidevate v primeru, če bi za ocenjevanje tveganj uporabljali metodo, ki bi bila prilagojena posebnostim bančnega poslovanja?

13. Bi ocenjevanje tveganja izvajali zaposleni ali bi to prepustili zunanji instituciji? Kakšne bi bile prednosti ali slabosti?

Podatke, pridobljene z intervjuji, smo analizirali z metodo nekvantitativne analize (Miles, Huberman, 1994). Dobljeni so bili naslednji rezultati analize:

1. Prilagojene metode niso v uporabi, ampak ocenjevanje informacijske varnosti poteka na različne načine: od revizijskih pregledov, priprav ocen tveganja, preverjanja ranljivosti in možnosti vdora, do izvajanja nadzora nad omrežjem.
2. Povzročena škoda zaradi slabe zaščite je lahko finančna, poleg tega pa je poudarjena tudi škoda zaradi zmanjšanja ugleda banke oz. nematerialna izguba.
3. Poleg uveljavljenih metod, ki so namenjene za ocenjevanje tveganja informacijske varnosti, obstaja potreba za prilagojenimi metodami, ki bi bila prilagojena bančnemu poslovanju.
4. Glede vrste metode se je več intervjuvancev opredelilo za kvalitativno metodo. Kot razlog so izpostavili težavno pridobivanje podatkov, vrednotenje nematerialne škode in kompleksna in dolgotrajna analiza številčnih podatkov pri kvantitativnih metodah.
5. Kvantitativne podatke o zlorabah bi v okviru poslovanja banke bilo mogoče obdelovati, zbirati in analizirati, problematični so podatki o nematerialni škodi in zahteve o varovanju bančne tajnosti. Če bi ocenjevanje tveganja izvajala zunanja institucija, bi bilo potrebno zagotoviti spoštovanje tajnosti podatkov.
6. Kot primerne metode za ocenjevanje tveganja bank je kvantitativne metode ocenil samo en intervjuvanec. Največji zadržki za uporabo kvantitativnih metod se porajajo zaradi nezmožnosti natančne opredelitve škode oz. zaradi kompleksnosti in dolgotrajnosti kvantitativnih metod.
7. Glede uspešnosti uporabe kvalitativnih metod za ocenjevanje tveganja je mnenje intervjuvancev takšno, da so te metode primerne za ocenjevanje tveganja bančnih institucij, saj lahko v krajšem času pridemo do rezultata in se hitreje posvetimo sanaciji stanja in ukrepom za zagotovitev večje varnosti. Poleg tega se izognemo težavnemu pridobivanju številčnih podatkov in vrednotenja nematerialne škode.
8. Krog sodelujočih, ki bi morali po mnenju intervjuvancev sodelovati pri pridobivanju podatkov o varnosti, je naslednji: od zaposlenih, vodstva banke, notranjih revizorjev, do lastnikov.
9. Ker ocenjevanje tveganja in s tem povezani ukrepi pomenijo zmanjšanje poslovne škode in s tem stroškov iz naslova zlorab, bi se banke odločale za ocenjevanje tveganj

s stroškovnega vidika. Dodatni kriteriji pa so še: večje spremembe informacijskih sistemov, ugotovljeni varnostni incidenti, zamenjava upravitelja in vzdrževalcev informacijskih sistemov, povečanje obsega poslovanja in glede na zmanjšan ugled banke zaradi povečanja zlorab.

10. Ocenjevanje tveganja bi moralo potekati stalno oz. periodično kot del procesa upravljanja. V praksi je to težko izvedljivo in se ocenjevanje izvaja predvsem takrat, ko se zaznajo nove grožnje, periodično pa enkrat v letu.
11. Prilagojene metode za ocenjevanje tveganja bančnih informacijskih sistemov bi pomenile hitrejši odziv na grožnje, boljšo učinkovitost, pozitiven vpliv na bančno poslovanje, primerne rezultate, lažje ugotavljanje povezljivosti groženj in ranljivosti informacijskih sistemov.
12. Če bi metoda za ocenjevanje tveganja, prilagojena bančnim informacijskim sistemom, zajemala vse vidike tveganj, ki veljajo tudi za ostale organizacije, intervjuvanci ne navajajo pomanjkljivosti ali slabosti metode.
13. Ocenjevanje tveganja bi glede na dobljene odgovore sodilo v domeno zaposlenih, kjer kot razlog navajajo ravno zaupnost informacij, pri vzpostavitvi sistema in zagotavljanju informacijske podpore zaradi bolj kakovostnega zagotavljanja virov in znanja, pa lahko sodeluje tudi zunanja institucija. Kot prednost zunanje institucije vidijo večjo objektivnost, nevarnost pa v določilih finančne stimulacije za opravljeno delo.

Glede na rezultate, dobljene z analizo odgovorov, smatramo, da smo potrdili ustreznost nove metode za ocenjevanje tveganja informacijskih sistemov. V odgovorih smo zaznali potrebo po metodi, ki bi bila prilagojena bančnemu poslovanju. Pri ocenjevanju tveganj in izdelavi ocene bi moral sodelovati večji krog udeležencev, uspešnost in potreba po ocenjevanju tveganja pa je odvisna od stroškov metode (pogostost uporabe) in od pojavljanja varnostnih incidentov, ki vplivajo tudi na ugled banke. Kvalitativna metoda je bila ocenjena kot primernejša zaradi različnih razlogov, pri čemer so najpomembnejši zlasti težavnost vrednotenja nematerialnih stroškov, dolgotrajnosti kvantitativnih metod in zahteve o varovanju bančne tajnosti v primeru zunanjih izvajalcev. Problematična je tajnost podatkov zaradi konkurenčnosti bank, zato bi zunanje institucije uporabili samo pri vzpostavitvi informacijskega sistema in zagotavljanju informacijske podpore, samo ocenjevanje tveganja pa bi opravljali zaposleni v banki.

6.4.6 SWOT analiza

Na osnovi dobljenih rezultatov z intervjuji, smo metodo IBRA testirali tudi s SWOT analizo.

SWOT ANALIZA METODE IBRA	
PREDNOSTI: • fleksibilna metoda • prilagojenost okoliščinam • prilagojenost potrebam • zagotovitev skladnosti zahtev • hiter odziv na spremembe • ocenjuje tveganja z vseh vidikov • namenjena tistim, ki skrbijo za varnost • ne zahteva visokih stroškov • jasna definicija ciljev	SLABOSTI: • ne vključuje številčnih vrednosti • ne upošteva vpliva uporabnikov storitev • primerna za omejen krog organizacij
PRILOŽNOSTI: • večja odzivnost • večja varnost	NEVARNOSTI: • naraščanje stroškov varovanja • odločanje na podlagi subjektivnih mnenj

Prednosti metode so v njeni prilagojenosti specifičnosti bančnega poslovanja, saj zajema specifične nevarnosti. Je fleksibilna in se lahko prilagaja spremembam v poslovanju in novim potrebam na področju zagotavljanja varnosti. Metoda je namenjena vsem tistim, ki skrbijo za varnost poslovanja in skupaj z vodstvom tudi definirajo varnostne zahteve in cilje, ki so točno določeni. Metoda ocenjuje tveganja z vseh vidikov, saj smo v nalogi ugotovili, da je z varnostnim modelom potrebno varnost zagotavljati celovito. Ocenjevanje tveganja informacijskih sistemov poteka z vprašalniki, kar ne zahteva visokih stroškov uporabe metode in dolgotrajnega usposabljanja zaposlenih za njeno uporabo.

Kot nove priložnosti metode štejemo večjo odzivnost na področju zagotavljanja varnosti, saj se lahko zaradi boljše prilagodljivosti in fleksibilnosti hitreje odzovemo na spremembe, ki se dogajajo na področju zagotavljanja varnosti elektronskega bančništva in s tem doseženo večjo varnost.

Slabosti nove metode so te, da je primerna samo za določen krog organizacij, saj je prilagojena bančnemu poslovanju. Ker je metoda kvalitativna, ne upošteva številčnih podatkov, katerim smo se načrtno izognili zaradi težavnosti njihovega pridobivanja in vrednotenja. Prav tako metoda ne upošteva vpliva uporabnikov storitev, kar je v primeru bančnega poslovanja težko zagotoviti zaradi velikega števila storitev, ki jih banke izvajajo in množice njihovih uporabnikov.

Nevarnost metode IBRA lahko pomeni naraščanje stroškov varovanja, če so cilji previsoko zastavljeni ali se precenijo nevarnosti, ki grozijo sistemu, saj metoda upošteva subjektivna mnenja udeležencev, ki ocenjujejo tveganje informacijskega sistema z metodo IBRA.

Kot vidimo iz SWOT analize metode za ocenjevanja tvegana IBRA, so prednosti te metode prevladujoče. Namenjena je za finančne organizacije, kjer je pomembna visoka stopnja varnosti poslovanja, saj grožnje ne vplivajo samo na izgubo realnega premoženja, ampak tudi na izgubo dobrega imena, kar lahko vodi tudi do prenehanja organizacije.

6.5 Preverjanje varnostnega modela v praksi

Ustreznost varnostnega modela smo preizkusili tudi z izvedbo ankete in intervjujev med zaposlenimi, ki v bankah in drugih finančnih institucijah delajo na področju varnosti elektronskega bančništva. Rezultati ankete, ki smo jo izvedli z vprašalnikom, so predstavljeni v posebnem poglavju.

Dodatno smo opravili tudi intervjuje pri osebah iz bank, ki so zadolžene za zagotavljanje varnosti v bankah in so tudi člani skupine, ki se pri ZBS ukvarja z zagotavljanjem varnosti elektronskega bančništva.

Intervjuji kot metoda raziskovanja so dokaj pogosti kot ena izmed možnosti zbiranja podatkov. Glavna prednost intervjuja pred anketami je osebni pogovor in stik med izpraševalcem in vprašanim, kar nam omogoča doseganje bolj kakovostnih rezultatov. Pri fenomenoloških raziskavah uporabljamo poglobljene intervjuje z odprtimi vprašanji in strukturiranimi vprašanji pri pozitivističnem pristopu.

Obstaja več tipologij raziskovanja in vrst intervjujev. Tako poznamo (Saunders M., Lewis P. in Thornhill A., 1997):

- strukturiran intervju
- polstrukturiran intervju
- nestrukturiran intervju.

Drugi ločijo (Healey M. J in Rawlinson M. B., 1994) samo:

- standardiziran intervju in
- nestandardiziran intervju.

Prav tako pa obstaja tudi razdelitev na (Robson C.,1993):

- intervjuje, ki jih usmerja vprašanec in
- intervjuje, ki jih usmerja spraševalec.

Navedena razvrščanja se ponekod tudi prekrivajo. Strukturirani intervju je oblika vprašalnika, v katerem so vsa vprašanja pripravljena vnaprej. V osebni komunikaciji z vprašanim pa so zapisana in zastavljena vsem vprašanim enako. Na enak način se zapisujejo tudi odgovori na postavljena vprašanja. Polstrukturirani in nestrukturirani intervjuji so nestandardizirani. Vprašanja se razlikujejo glede na intervjuvance, kar je odvisno od tega, kaj vprašani o določeni temi vedo in znajo in kakšen je njihov položaj v okolju. Nestrukturiran intervju ponavadi uporabljamo takrat, ko o sami temi raziskovanja ne vemo veliko. Pogovor je zato neformalen in je lahko različno dolg pri različnih vprašanjih. Vprašanja niso pripravljena vnaprej, moramo pa poznati cilj intervjuja. Vprašani sam govori o temi, vpraševalec pa posluša in ne usmerja pogovora s podvprašanji. Takšne vrste intervjujev imenujemo tudi poglobljeni intervjuji, usmerja pa jih vprašanec.

Kadar zbiramo podatke z intervjuji, lahko izkoristimo možnost izbire in kombinacije različnih vrst vprašanj. Omogočeno nam je postavljanje odprtih, zaprtih in polodprtih vprašanj. Odprta vprašanja omogočajo odgovore, ki niso z ničemer omejeni in lahko vprašani odgovarja tako, kakor sam želi. Pogoste vprašalnice, ki se pojavljajo pri odprtih vprašanjih so: kaj, kako in zakaj. Za boljše razumevanje odgovora lahko s podvprašanji dosežemo večjo kvaliteto intervjuja. Zaprta vprašanja v glavnem postavljamo v strukturiranih intervjujih.

Za raziskovalno nalogo smo uporabili strukturirani intervju. Vnaprej pripravljena vprašanja so bila postavljena vsem osebam, ki so sodelovale v intervjuju enako in v istem vrstnem redu. S

podvprašanji smo poskušali vzpodbuditi vprašane, da so o temi povedali še več. Pogovarjali smo se z ljudmi, ki so pri nas dolga leta delali na področju elektronskih plačilnih sistemov in so jim zlorabe teh sistemov poznane oz. tudi aktivno delajo na preprečevanju teh zlorab. Intervjuji so bili izvedeni v jeseni leta 2009. Vpraševalec se je najprej pripravil na intervju, izbral cilje in vprašanja. Vprašanim so bili cilji in namen intervjuja predstavljeni pred postavljanjem vprašanj. Zaprošeno je bilo njihovo dovoljenje za delno uporabo njihovih osebnih podatkov. S pomočjo Združenja bank Slovenije smo opravili intervju z naslednjimi osebami:

- Slavko Cimprič, vodja področja poslovanja s privatnimi komitenti, Združenje bank Slovenije, s plačilnimi sistemi se poklicno ukvarja okoli 20 let
- Mateja Plestenjak, spremljava zlorab (višji referent spremljave zlorab), Oddelek spremljave poslovanja, Bankart d.o.o., na področju kartičnega poslovanja 15 let
- Vedran Šubic, strokovni svetovalec, Abanka Vipa d.d., 14 let dela na kartičnem področju
- Gojmir Nabergoj, poslovni svetovalec v sektorju organizacije in kadrov, procesni center Intesa San Paolo d.d., 20 let na področju kartičnih sistemov
- NN (imena ne želi objaviti), NLB d.d., kartično poslovanje.

Izbranim osebam smo postavili enaka vprašanja, ki so bila naslednja:

1. Kaj menite o spreminjanju in posodabljanju zlorab na področju elektronskih plačilnih sistemov z razvojem na tehnično-tehnološkem področju, nove storitve?
2. Ali lahko preprečujejo zlorabe samo banke?
3. Katere institucije vključiti v sistem in na katerih področjih?
4. Kako se mora sistem zaščite prilagajati na spremembe problematike področja in nove oblike zlorab?
5. Ali je lahko preprečevanje zlorab uspešno, če posamezne institucije vsaka zase izvaja ukrepe in aktivnosti?
6. Ali je za preprečevanje zlorab dovolj samo visoka zagrožena kazen za storilce in stroga zakonodaja za kršitelje? Kako je s preventivno zaščito sistemov?
7. Kateri bi bili po vašem ključni dejavniki, ki omogočajo učinkovito preprečevanje zlorab?
8. Ali je potrebno tudi v organizacijskih in tehnoloških rešitvah upoštevati rešitve, pomembne za varnost poslovanja in kako?
9. Je pri zagotavljanju varnosti pomembna tudi mednarodna dimenzija in kako?

10. Kakšen vpliv ima tehnično-tehnološki razvoj na področje in ukrepe zaščite informacijskih sistemov pred zlorabami?
11. Kaj menite o bodočnosti zaščite elektronskih plačilnih sistemov pred zlorabami in kako jo uspešno poskušati zagotavljati?

Da dobimo iz intervjujev tudi praktične rezultate za raziskavo, je potrebno dobljene podatke analizirati. Kvalitativni podatki, ki smo jih z intervjuji dobili, imajo drugačen pomen kot kvantitativni podatki, saj ne izhajajo iz številk, ampak iz besed. Zaradi tega obstajajo za analizo tudi posebne metode, ki so namenjene analiziranju kvalitativnih podatkov. Kvalitativne podatke večinoma dobimo pri fenomenološkem raziskovanju, lahko pa tudi pri pozitivističnem raziskovanju.

Pri analizi kvalitativnih podatkov naletimo na naslednje probleme:

- kako naj dolga besedila skrčimo na velikost, ki bo obvladljiva za analizo in interpretacijo
- kako naj različne podatke strukturiramo
- kako naj podatke različno interpretiramo, sestavimo grafe ali preglednice in ne izgubimo s tem pomena podatkov.

Za rešitev navedenih problemov obstajajo različne možnosti izvedbe nekvantitativnih ali kvalitativnih metod. Neformalna metoda je metoda, s katero raziskovalec iz prebranih podatkov ugotavlja, kateri odgovori in dejanja se ponavljajo. Ta ponavljanja si izpisuje v procesu krčenja in selekcije. Predstavi in prešteje tista dejanja ali podatke, ki so bili zelo pogosti ali zelo redki, sam pa se odloči, na kakšen način bo to počel. Pri neformalni metodi moramo biti pazljivi, da v procesu selekcije ne zapostavimo ali izpustimo podatkov, ki so vsebinsko bogati in pomembni. Da bi se temu izognili, neformalno metodo kombiniramo z drugimi metodami.

Analiza vsebine[35] je metoda, s katero formalno, z uveljavljenim načinom, strukturiramo kvalitativne podatke. Primerna je za zelo dolga oz. obsežna besedila. S to analizo besedilo pretvorimo v številčne spremenljivke in jih nato obdelamo s kvantitativnimi metodami.

[35] Angleško »content analysis.

Pregledana mreža[36] je metoda analize, kjer razumevanja in pojmovanja ljudi o dogodkih in procesih, ki so predmet študije, predstavimo v obliki matematičnih predstavitev. Za to metodo se moramo pripraviti že pred izvedbo intervjujev, saj moramo natančno vedeti, katera individualna razumevanja in pojmovanja bomo zbirali.

Pri metodah nekvantitativne analize številke in frekvence niso cilj, ampak so namenjene vsebinski obdelavi podatkov. Cilj je čim bolj verodostojen, a skrčen prikaz značilnosti, vzrokov in posledic, ki jih vprašani posvečajo posameznim procesom in pojavom (Hussey, J., Hussey R., 1997).

Metodo splošnega analitičnega[37] postopka sta razvila Miles in Huberman (1994). Uporablja se lahko pri vsaki metodologiji in je natančna in sistematična, sproti pa lahko preverjamo kriterije kredibilnosti.
Podatke, pridobljene z intervjuji, smo analizirali z metodo nekvantitativne analize. Dobljeni so bili naslednji rezultati analize:

1. Kriminaliteta, povezana s plačilnim prometom, se spreminja in prilagaja spremembam na tem področju. Storilci se prilagajajo spremembam in so vedno bolj organizirani, povezani in delujejo na sofisticiran način in se prilagajajo novim tehničnim in tehnološkim rešitvam.
2. Zlorab ne morejo preprečevati in se proti njim boriti samo banke ali druge institucije iz tega področja, ampak je potreben skupen boj in izmenjava informacij. Potrebno je formirati model ali sistem, ki bo preprečeval zlorabe.
3. V sistem je potrebno vključiti banke, procesne centre, prodajna mesta, policijo in druge institucije, katerih področje je boj proti zlorabam na področju elektronskega bančništva. Potrebno je sprejeti učinkovite varnostne ukrepe na informacijskih sistemih, urediti in definirati nadzor sistemov, sporočanje, obveščanje in povezovanje različnih institucij, ki skrbijo za varnost plačilnih sistemov.
4. Varnostni sistem se mora prilagajati in odzivati na spremembe na tem področju in se prilagajati novim, kompleksnejšim načinom zlorab. Biti mora odziven.

[36] Angleško »repertory grid«.

[37] Angleško »general analytical procedure«.

5. Samostojno ukrepanje posameznih institucij je seveda potrebno, a se lahko najboljše rešitve dosežejo le v primeru celovitega zagotavljanja varnosti z zastavljenim modelom, v katerem sodelujejo različne institucije.
6. Za varnostni model so bolj pomembni preventivni dejavniki, ki omejujejo možnosti izvrševanja zlorab, če pa do njih vseeno pride, pa so na voljo represivni dejavniki, ki pa imajo manjši pomen na izvrševanje zlorab.
7. Izobraževanje uporabnikov, informiranje javnosti o novih zlorabah, zaščita in varna uporaba elektronskih sistemov, znanje v institucijah in preprečevanje, da le to pride v roke storilcev, spremljanje in analiziranje dogodkov in ustrezno ukrepanje, so ključni dejavniki, ki jih je potrebno upoštevati v varnostnem modelu.
8. Potrebna so enotna pravila ukrepanja, uporaba enotne opreme, uravnotežen prenos varnosti na tehnično – tehnološke rešitve.
9. Varnostni model mora upoštevati tudi mednarodno dimenzijo, saj je večina storitev internacionalnih, prav tako pa so tudi zlorabe mednarodne. Tudi povezovanje sistemov je nujno v tej smeri.
10. Razvoj zaščitnih mehanizmov je odziv na izvedene zlorabe, upoštevati pa moramo tudi stroškovni vidik, saj so tehnično – tehnološke rešitve praviloma povezane z visokimi stroški.
11. Novim varnostnim elementom in načinom zaščite se bodo storilci prilagodili. Popolne varnosti ne bomo nikoli uspeli zagotoviti, samo učinkovit varnostni model pa lahko zagotovi znižanje zlorab na tem področju.

Z analizo dobljeni rezultati potrjujejo zastavljene hipoteze, ki smo jih postavili na začetku naloge.

7 EMPIRIČNO PREVERJANJE MODELA

7.1 Utemeljitev raziskovalnega problema

V vsem razvitem svetu obstaja problem zlorab plačilnih kartic in spletnega bančništva. Podatki, do katerih je sicer zaradi bančnih tajnosti težko priti, kažejo, da se zlorabe dogajajo kljub nekaterim ukrepom, ki so jih institucije, ki delujejo na področju varnosti, že sprejele. Kako uspešni so ti ukrepi, pa je vprašanje, na katerega odgovora ne poznamo, saj v medijih od časa do časa zasledimo objave o zlorabah, ki so se zgodile in se še dogajajo. Problem je tudi nepovezanost institucij in njihovih ukrepov, ki lahko zaradi nekoordinacije dosežejo manjšo korist ali so celo neuspešni. Pri pregledu razmer na tem področju ugotavljamo, da v Sloveniji nismo osamljeni pri pojavljanju zlorab na področju elektronskega bančništva. Po nekaterih statističnih podatkih zlorabe pri nas ne izstopajo iz povprečja razvitega sveta. Večina zlorab se zgodi na način, ko storilci pridejo iz drugih držav in zlorabijo tuje plačilne kartice. V nalogi smo si za cilj postavili preveritev delovanja celovitega modela za zagotavljanje varnosti na področju elektronskega bančništva. Model bomo preverjali pri zaposlenih v bančnih institucijah, ki skrbijo za varnost plačilnega prometa in imajo bogate izkušnje z zagotavljanjem varnosti. Postavljene hipoteze se nanašajo na celovit varnostni model za zagotavljanje varnosti poslovanja na področju elektronskega bančništva. S preverjanjem postavljenih hipotez bomo iskali dokaz za delovanje modela, katerega bomo preverjali z izvedbo ankete in podkrepili z intervjuji s kompetentnimi ljudmi iz bank. Na področje zlorab namreč država in drugi udeleženci lahko vplivajo na različne načine, z represivnimi in preventivnimi ukrepi. Kakšne rezultate na področju varnosti prinesejo eni in drugi ukrepi in dejavniki, kakor tudi njihovo kombiniranje, so vprašanja, na katera smo želeli dobiti odgovore v nalogi. Prav tako smo hoteli ugotoviti, ali je možno varnost tega področja finančnega poslovanja zagotoviti zgolj z ukrepi, ki jih uvajajo posamezne institucije, ali so rezultati bolj kakovostni, če se varnost zagotavlja s sodelovanjem in povezovanjem institucij, ki delujejo na tem področju.

7.1.1 Cilji naloge

V nalogi smo skušali ugotoviti, kateri dejavniki vplivajo na zlorabe na področju elektronskega plačilnega prometa s plačilnimi in kreditnimi karticami. Na osnovi analiz načinov zlorab, ki se

dogajajo na tem področju in zbranih podatkov o številu in obsegu zlorab, storilcih in tehnično-tehnoloških in organizacijskih možnostih zaščit, smo naredili celovit varnostni model preprečevanja zlorab. Model smo testirali z anketo in izvedbo intervjujev, ki smo jih opravili pri zaposlenih v bankah, ki delajo na področju elektronskega plačilnega prometa. Z anketo in intervjuji smo potrdili postavljene hipoteze in s tem tudi delovanje celovitega modela za zagotavljanje varnosti. Ugotovili smo povezave med varnostjo informacijskih sistemov in ocenjevanjem tveganj informacijskih sistemov. Zato smo na osnovi dobljenih rezultatov pri preverjanju zastavljenega varnostnega modela koncipirali novo metodo za ocenjevanje informacijskih tveganj IBRA, ki je prilagojena specifičnostim bančnega poslovanja. Metodo IBRA smo testirali z izvedbo novih intervjujev s strokovnjaki v bankah, ki delajo na področju zagotavljanja varnosti bančnih informacijskih sistemov.

Hipoteze raziskovanja

H1. Gospodarska kriminaliteta, kamor spada področje elektronskih plačilnih sistemov, se neprestano spreminja in posodablja.

H2. Za preprečevanje zlorab je potrebno izdelati učinkovit varnostni model, ki bo zmanjšal možnost zlorab.

H3. Za zmanjšanje zlorab je potrebno sprejeti učinkovite varnostne ukrepe na samih informacijskih sistemih, urediti in definirati nadzor sistemov, sporočanje, obveščanje in povezovanje različnih institucij, ki skrbijo za varnost plačilnih sistemov.

H4. Varnostni model mora biti zasnovan tako, da bo omogočal takojšnje odzive na spremembe problematike področja in se bo lahko fleksibilno prilagajal novim, kompleksnejšim oblikam zlorab.

H5. Uspešno in učinkovito preprečevanje zlorab v elektronskih plačilnih sistemih je mogoče le ob celovitem modelu zagotavljanja varnosti.

H6. Varnostni model mora zajemati tudi preventivne dejavnike varnosti, saj lahko tudi na ta način zmanjšamo možnosti zlorab.

H7. Na uresničevanje modela celovite varnosti vpliva nekaj ključnih dejavnikov, ki zagotavljajo uspešno in učinkovito preprečevanje zlorab.

H8. Celovito varnost je potrebno uravnoteženo prenesti na organizacijske in tehnološke rešitve.

H9. Celovit varnostni model mora upoštevati mednarodno dimenzijo.

H10. Sprememba tehnologije zaščite posameznih delov sistemov in celote se

mora prilagajati in nadgrajevati z razvojem tehnično – tehnoloških novosti na področju zaščit sistemov.

H11. Samo kompleksna obravnava vseh vidikov in institucij, ki delujejo na področju elektronskih plačilnih sistemov, lahko prinese učinkovit varnostni model, ki bo lahko zmanjšal možnosti zlorab. Zavedati pa se moramo, da popolne varnosti na tem področju ni možno doseči, predvsem ne dolgoročno, brez ažurnega prilagajanja varnostnega modela novim razmeram.

7.2 Uporabljena metoda, instrumentarij in opis vzorca

7.2.1 Opis vzorca

V raziskavi je sodelovalo 43 zaposlenih iz različnih bank, izdajateljev in procesorjev, ki se ukvarjajo s področjem elektronskega plačilnega prometa z bančnimi in kreditnimi karticami. V okviru raziskave so bili opravljeni tudi trije intervjuji z najbolj kompetentnimi ljudmi, ki se ukvarjajo s tem področjem v Sloveniji. Z anketnimi vprašalniki oz. odzivi nanje je bilo pokritih okoli 80% zaposlenih v bankah in drugih institucijah, ki se ukvarjajo s področjem varnosti in ki dnevno delajo na tem področju.

Struktura anketirancev glede na spol je bila 57,6% moških in 42,4% žensk. Starostna struktura anketirancev je bila naslednja: od 30-39 let jih je bilo 37,7%, od 40-49 let jih je bilo 32,6% in od 50-59 let 25,6%. V kategorijo pod 30 in nad 60 let sta se uvrstila samo dva anketiranca oz. skupaj 4,6%.

Stopnja izobrazbe anketirancev je bila naslednja: 30,2% srednja izobrazba, 11,6% višja izobrazba, 20,9% visoka izobrazba, 32,6% univerzitetna izobrazba in 4,7% magisterij in doktorat znanosti.

Glede na dolžino delovne dobe so se anketiranci razvrstili v naslednje skupine: 0 do 10 let 9,3%, 11 do 19 let 34,9%, 20 do 29 let 27,9% in 30 do 39 let 27,9%.

Glede na dobo zaposlitve na področju kartičnega poslovanja se anketiranci razvrščajo v naslednje skupine: 0 do 10 let 44,2%, 11 do 19 let 39,5%, 20 do 29 let 11,6% in 30 do 39 let 4,7%.

7.2.2 Uporabljen instrumentarij

V raziskavi bo uporabljen tudi vprašalnik. Predvidena so zaprta vprašanja, kjer so vsi možni odgovori v naprej predvideni, in odprta vprašanja, kjer odgovori niso vnaprej določeni. Zaprta vprašanja lahko sestavimo tako, da omogočajo večje razlikovanje, kjer je ena izmed najbolj običajnih oblik znana kot Likertova lestvica. Anketiranca tako prosimo, da na vprašanje obkroži enega izmed npr. petih odgovorov, ki kažejo intenzivnost strinjanja ali nestrinjanja z začetno izjavo. Za merjenje vseh neodvisnih in odvisnih spremenljivk v raziskovalnem

modelu bomo uporabili vprašanja zaprtega tipa in ponudili odgovore v obliki Likertove lestvice. Zaprta vprašanja lahko anketiranci hitro izpolnijo in jih je enostavno analizirati, a so lahko dobljeni podatki površni (Easterby-Smith, 2005). Vprašalnik bo zajemal razumljiva vprašanja, ki bodo povezana in si bodo sledila glede na tematiko in občutljivost.

Predmet raziskovanja bodo zaposleni v bankah in drugih institucijah, ki se ukvarjajo z varnostnimi vidiki elektronskih plačilnih sistemov. Pri nas nastopajo kot izdajatelji plačilnih kartic tako banke kot tudi drugi ponudniki, ki so skoraj vsi člani Združenja bank Slovenije. Ta tudi v okviru Odbora za varnost kartičnega poslovanja združuje interese članov in vodi dejavnosti za čim bolj varen model. Pričakujemo, da bo odstotek vrnjenih vprašalnikov visok, saj gre tukaj za zaključen krog ljudi, ki imajo tudi interes, da se zagotovi varnost sistema.

Kumar (2005) poudarja, da bo odstotek vrnjenih vprašalnikov visok, če jih posredujemo zaključeni množici. Prednost takšnega načina posredovanja vprašalnikov je, da je izvedba cenejša, kljub temu pa je zagotovljena večja avtonomija. Dodaja, da je odstotek vrnjenih vprašalnikov odvisen od več dejavnikov: interesa vzorčne skupine o vsebini študije, zgledu in dolžini vprašalnika, kakovosti spremnega besedila in metodologiji, ki je bila uporabljena za pošiljanje vprašalnika. Da bi zagotovil čim večji odstotek vrnjenih vprašalnikov, bo le – ta poslan preko Združenja bank Slovenije, kar bo pripomoglo k višjemu odstotku vrnjenih izpolnjenih vprašalnikov.

Podatke bomo statistično obdelali v skladu z nameni in predvidevanji raziskave s pomočjo statističnega programskega paketa SPSS za Windows (deskriptivna statistika).

Anketni vprašalnik je sestavljen iz več vsebinskih sklopov. Sestavljen je bil vprašalnik z več spremenljivkami, z njimi pa smo ugotavljali vpliv različnih dejavnikov na možnosti in izvrševanje zlorab na področju kartičnega poslovanja v Sloveniji med zaposlenimi na področju elektronskega plačilnega prometa pri nas.

Kot *neodvisne spremenljivke* je bilo uporabljenih več osebnih podatkov anketiranih oseb, in sicer spol, starost, stopnja izobrazbe, skupna delovna doba in delovna doba na področju kartičnega poslovanja.

7.2.3 Opis postopka

Anketiranje smo izvedli spomladi leta 2008. Vprašalniki so bili poslani in tudi izpolnjeni v elektronski obliki, kar je olajšalo in pospešilo izpolnjevanje vprašalnikov, prav tako pa je bil odziv anketiranih večji. Anketirancem je bila zagotovljena anonimnost in zaupnost njihovih odgovorov.

Sodelovanje v raziskavi je bilo prostovoljno. Podatke smo analizirali s pomočjo programa za statistično obdelavo podatkov (SPSS).

7.3 Merski inštrumentarij

Stališča anketirancev do zlorab na področju elektronskega plačilnega prometa smo proučevali s pomočjo vprašalnika, ki je vseboval vprašanja – trditve v obliki Likertove lestvice. Odločili smo se za petstopenjsko intervalno lestvico. Nad vprašalnikom smo zapisali, katero področje obravnava posamezen sklop vprašanj, ki so bile razdeljene v tri sklope in pozvali anketirance, da na vprašanja odgovorijo tako, da s poudarjenim tekstom ali drugo barvo označijo številko odgovora s katerim se strinjajo ali ne strinjajo.

1 – sploh se ne strinjam
2 – ne strinjam se
3 – sem nevtralen, ne vem
4 – se strinjam
5 – popolnoma se strinjam

Vprašalnik je bil najprej pregledan in testiran na Združenju bank Slovenije, tako glede vsebine in strokovnosti vprašanj, kakor tudi glede na obseg vprašalnika in možnostjo podaje odgovorov anketirancev glede na znanje, ki ga posedujejo, kakor tudi na možnost podaje odgovorov zaradi zadržanosti od dela, saj bi vprašalnike izpolnjevali v službenem času in se predpostavljeni z dalj časa trajajočim izpolnjevanjem vprašalnika in odsotnostjo od dela ne bi strinjali. Po pregledu je bil vprašalnik z nekaterimi spremembami akceptiran s strani Združenja bank Slovenije, dobili smo dovoljenje za anketiranje in vprašalnik smo lahko poslali anketirancem.

7.3.1 Objektivnost

Vprašalnik je anonimen, anketiranci pa so ga izpolnjevali na delovnih mestih. Vprašalniki so jim bili poslani v elektronski obliki zaradi hitrejše in lažje komunikacije. Izpolnjeni vprašalniki so bili poslani kontaktni osebi na Združenju bank Slovenije, ki jih je posredovala izvajalcu raziskave. Na ta način izvajalec raziskave ni bil seznanjen z identiteto anketirancev, ki bi se videla iz pošiljateljevega elektronskega naslova, kar pomeni večjo objektivnost ankete. V samem vprašalniku so bila napisana pravila izpolnjevanja, namen vprašalnika in raziskave in zagotovilo o popolni anonimnosti anketirancev. Čas izpolnjevanja vprašalnika ni bil omejen, predviden čas izpolnjevanja (izostanek od dela) je bil predviden na 15 minut.

7.3.2 Zanesljivost

Za ugotavljanje zanesljivosti vprašalnika smo uporabili metodo notranje konsistentnosti ocenjevalne lestvice. Za prikaz merske značilnosti smo izračunali koeficient zanesljivosti *Cronbach alfa,* ki se giblje v intervalu od 0 do 1, najnižja ustrezna meja zanesljivosti pa je 0,7.

Tabela 10: Cronbach's Alpha

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0,870	0,897	54

Tabela 10 zgoraj kaže vrednost Cronbachovega koeficienta α, ki v našem primeru znaša 0,870. Ker je njegova vrednost večja od 0,8, lahko zaključimo, da je naša lestvica dovolj zanesljiva. V tabeli vidimo še, koliko bi znašal ta koeficient na standardiziranih spremenljivkah ter koliko spremenljivk je bilo vključenih v analizo.

Na Cronbachov koeficient α vpliva število spremenljivk vprašalnika; več kot je spremenljivk, večja je zanesljivost. V analizi Inter-Item Correlation Matrix smo uporabili 54 spremenljivk (demografske podatke smo izpustili), zato je dobljena tabela malce preobsežna, da bi jo

predstavili tukaj. Korelacijski koeficienti med posameznimi spremenljivkami kažejo, da je korelacija med spremenljivkami ponekod sorazmerno močna, ponekod pa tudi šibka oziroma negativna. Zaradi vsega tega pa je lažje izbrati posamezne sklope povezanih spremenljivk.

Nadalje smo dobili korelacijski koeficient med posamezno spremenljivko ter vsemi spremenljivkami vprašalnika. Iz Tabele Item-Total Statistics je to razvidno v stolpcu Item-Total Correlation. Če je lestvica zanesljiva, morajo spremenljivke dobro kolerirati s celoto, t.j., če je vrednost njenega korelacijskega koeficienta v tem stolpcu manjša od 0,3, je priporočljivo, da jo izločimo iz vprašalnika. V zadnjem stolpcu ista tabela (Item-Total Statistics) prikazuje vrednost Cronbachovega koeficienta (Cronbach's Alpha if Item Deleted). Tu vidimo vrednosti Cronbachovega koeficienta α, če posamezna spremenljivka vprašalnika ne bi bila vključena v vprašalnik. Vrednosti v tem stolpcu ne smejo biti večje od vrednosti Cronbachovega koeficienta α v prejšnji tabeli, ki v našem primeru znaša 0,870. Če je kateri izmed elementov večji, ga je priporočljivo izločiti iz nadaljnjih analiz ter s tem omogočiti večjo zanesljivost lestvice. Ugotovili smo, da je vrednost tega koeficienta višja ravno pri nekaterih izmed tistih spremenljivk, kjer smo opazili že odstopanje pri analizi korelacijskega koeficienta. Tako bomo zgoraj naštete spremenljivke izločili iz vprašalnika ter zagotovili tudi zanesljivost naše lestvice.

Z analizo zanesljivosti vprašalnika smo ugotovili, da bomo zaradi boljše zanesljivosti izločili določena vprašanja in v nadaljevanju faktorsko analizo izvedli brez teh vprašanj.

7.3.3 Veljavnost

Veljavnost smo ugotavljali s *faktorsko analizo.*

7.3.4 Občutljivost

Občutljivost je podana s petstopenjsko lestvico odgovorov oz. ocenami od 1 - 5.

7.3.5 Postopki statistične obdelave

Rezultati so bili obdelani s statističnim programom SPSS 16.0.

Najprej smo izračunali opisne statistike, s katerimi smo opisali vzorec, mediane, standardne odklone in variance spremenljivk, ki smo jih merili s pet-stopenjsko lestvico. Ugotovljene so bile merske značilnosti ocenjevalne lestvice (objektivnost, zanesljivost in veljavnost) z izračunom *Cronbach alfa* in *faktorske analize*.

8 PREDSTAVITEV REZULTATOV RAZISKAVE

V nadaljevanju predstavljamo rezultate, ki smo jih dobili s pomočjo anketiranja bančnih uslužbencev, ki delajo na področju plačilnih in bančnih kartic. Vprašalnik je sestavljen iz treh sklopov vprašanj. V prvi sklop spadajo vprašanja, ki se nanašajo na splošno varnost področja brezgotovinskega plačilnega prometa in razvoj tega področja v prihodnosti. Drugi sklop vprašanj obravnava preventivne dejavnike, ki vplivajo na varnost brezgotovinskega načina poslovanja, tretji sklop vprašanj pa se nanaša na represivne dejavnike, ki vplivajo na to področje. Na koncu vprašalnika so vprašanja, ki se nanašajo na demografske podatke o anketirancih.

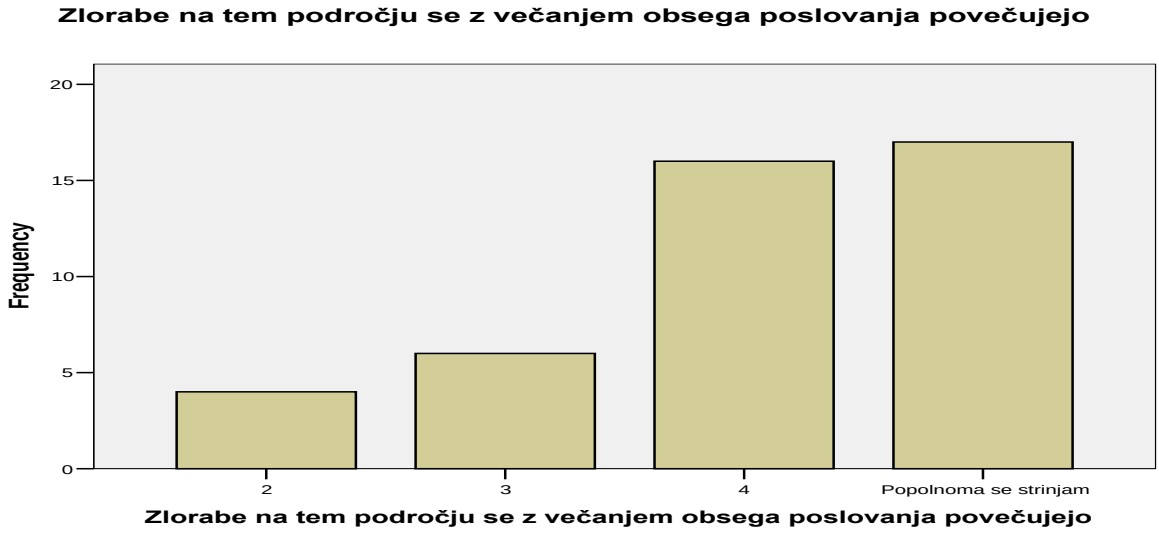
8.1 Splošna varnost in razvoj področja

Vprašanja iz tega sklopa se nanašajo na ugotavljanje stanja varnosti na področju brezgotovinskega plačilnega prometa, vrst in velikosti potencialnih ogrožanj varnosti poslovanja in razvoju področja.

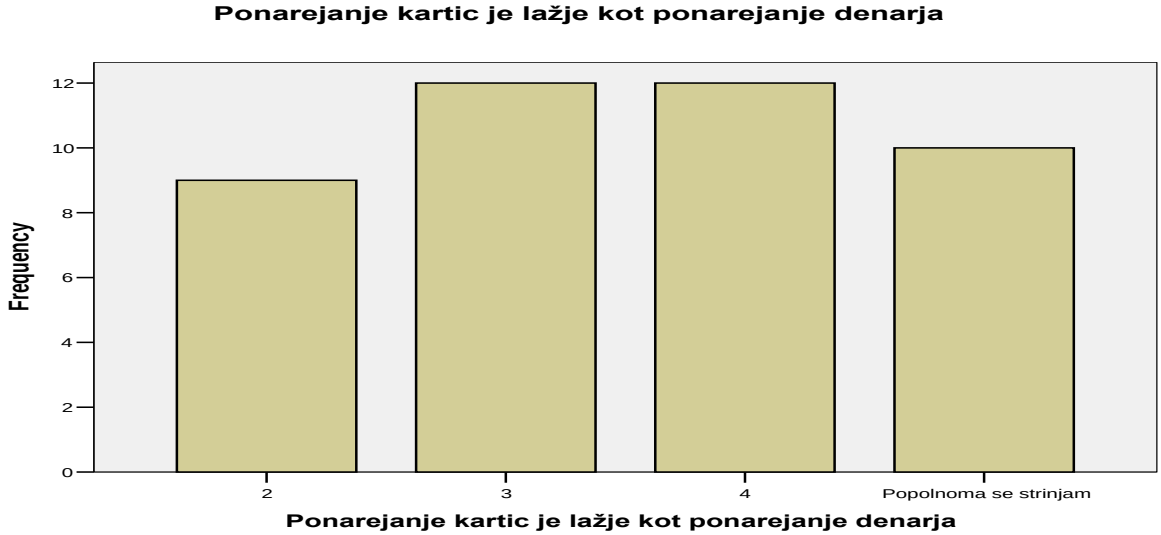
8.1.1 Opisne statistike

S trditvijo »brezgotovinski plačilni promet se bo v prihodnje povečeval« se je popolnoma strinjalo 86% anketirancev. Aritmetična sredina je znašala 4,79, noben od anketirancev se ni opredelil za možnost nestrinjanja s trditvijo in odgovora, da se s trditvijo ne strinja, ni izbral. Standardni odklon je znašal 0,559, varianca pa 0,312.

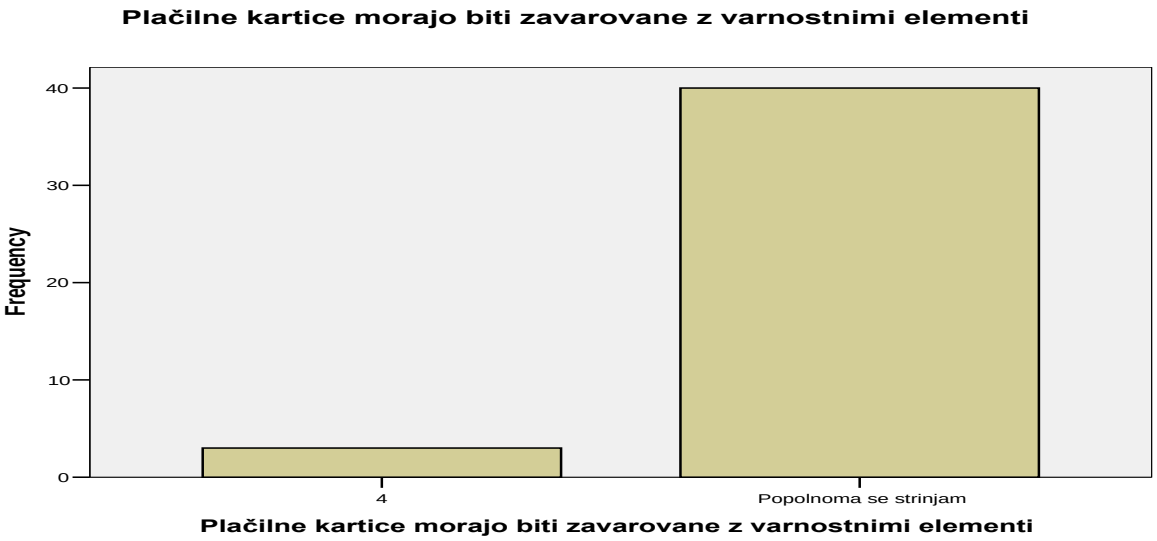
Trditev »zlorabe na tem področju se z večanjem obsega poslovanja povečujejo« je dosegla aritmetično sredino 4,07. Od 43 veljavnih odgovorov se je s trditvijo popolnoma strinjalo 39,5% anketirancev, takšnih, ki se s trditvijo sploh niso strinjali, ni bilo. Standardni odklon je znašal 0,961, varianca pa 0,924.



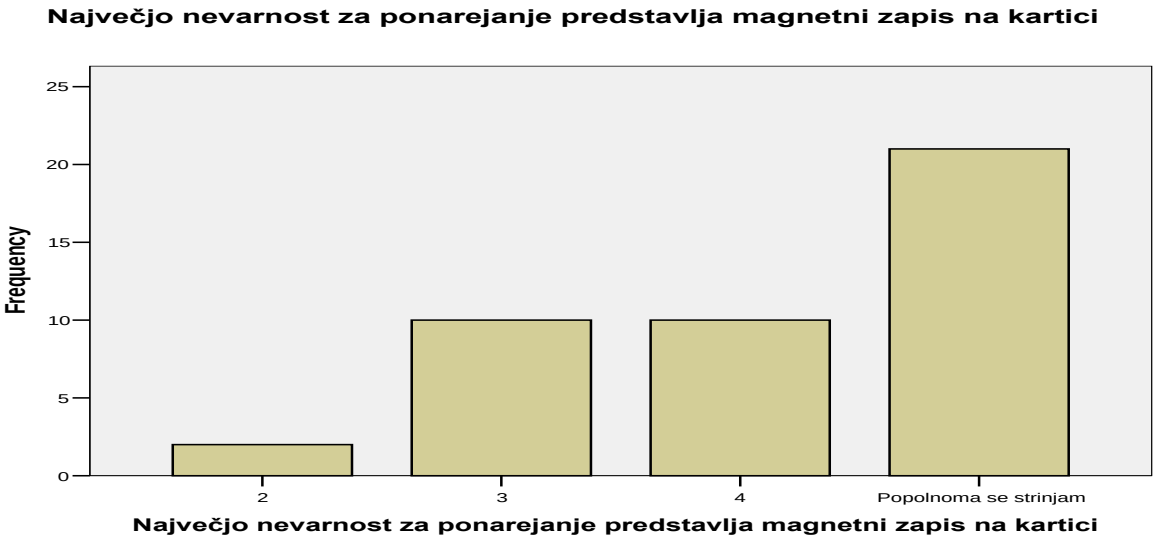
Na trditev »ponarejanje kartic je lažje kot ponarejanje denarja« je s popolnoma se strinjam odgovorilo 23,3% vprašanih, z oceno 4 pa 27,9% vprašanih. Aritmetična sredina je znašala 3,53. Standardni odklon je znašal 1,077, varianca pa 1,159.



Trditev »plačilne kartice morajo biti zavarovane z varnostnimi elementi« je dosegla aritmetično sredino 4,93. S trditvijo se je popolnoma strinjalo 93% vprašanih. Odgovorov v smeri nestrinjanja s trditvijo ni bilo. Standardni odklon je znašal 0,258, varianca pa 0,066.

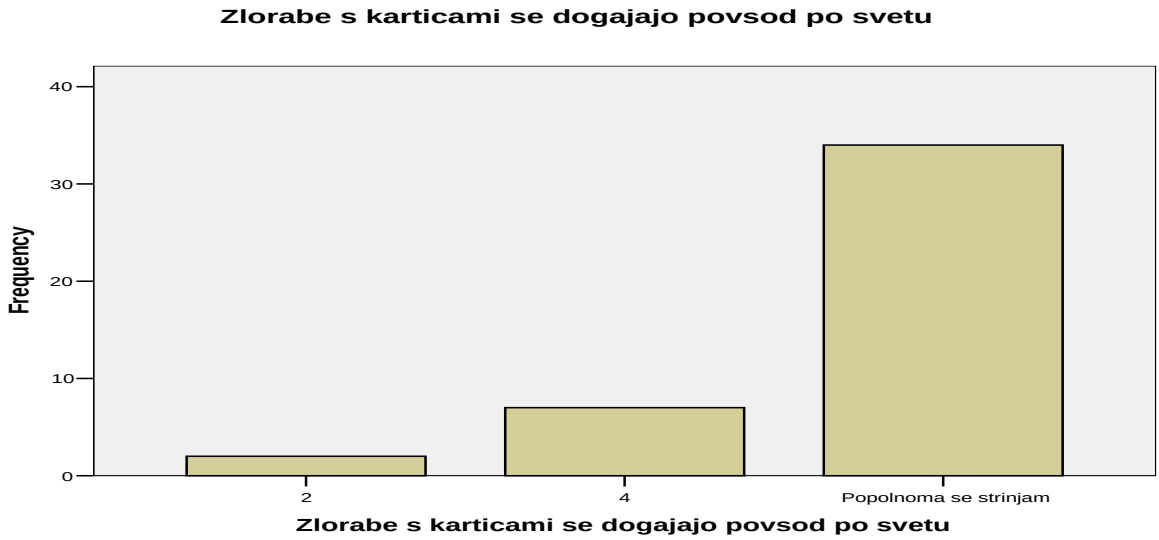


Na trditev »največjo nevarnost za ponarejanje predstavlja magnetni zapis na kartici« je z odgovorom popolnoma se strinjam odgovorilo 48,8% vprašanih, aritmetična sredina je bila 4,16. Standardni odklon je znašal 0,949, varianca pa 0,901.

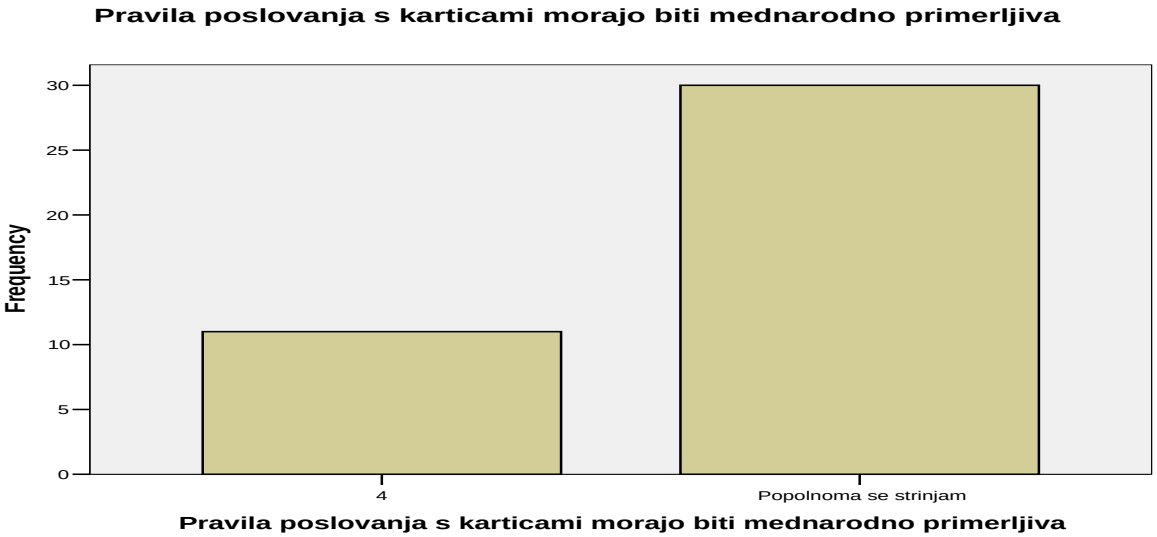


S trditvijo »pravila poslovanja uporabnikov s karticami morajo biti jasno določena« se je popolnoma strinjalo 88,4% vprašanih, aritmetična sredina je znašala 4,88. Odgovorov nestrinjanja s trditvijo ni bilo. Standardni odklon je znašal 0,324, varianca pa 0,105.

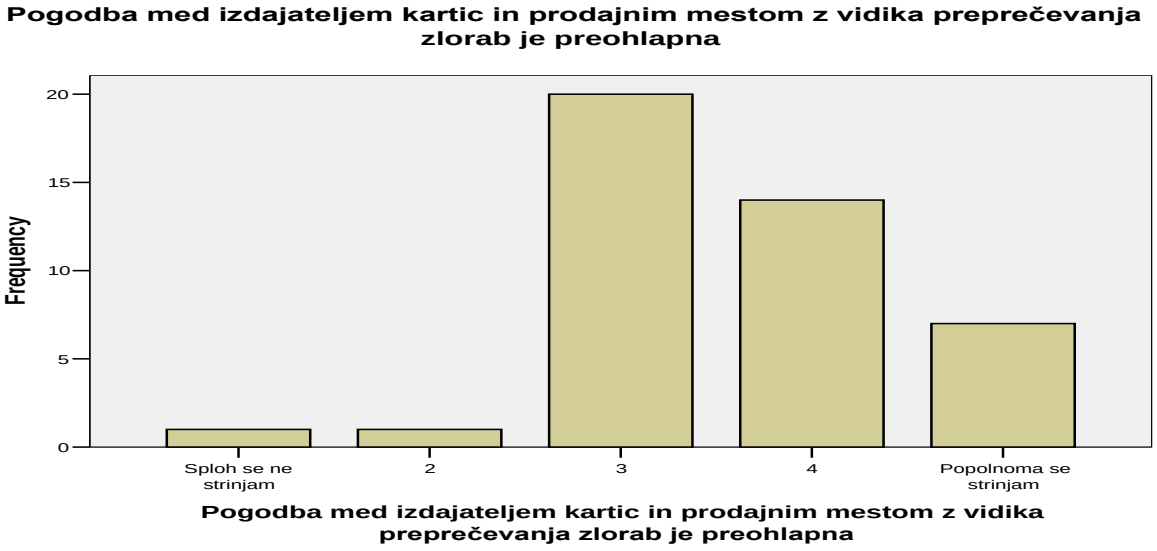
Trditev »zlorabe s karticami se dogajajo povsod po svetu« je dosegla aritmetično sredino 4,70%. Z odgovorom popolnoma se strinjam je odgovorilo 79,1% vprašanih. Standardni odklon je znašal 0,708, varianca pa 0,502.



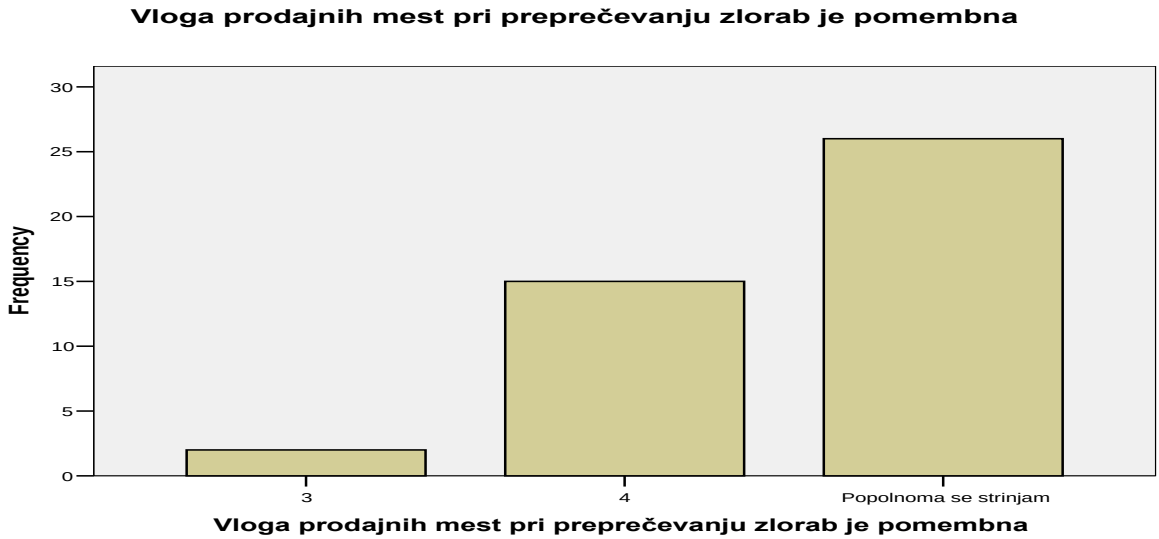
Na trditev »pravila poslovanja s karticami morajo biti mednarodno primerljiva« je z odgovorom popolnoma se strinjam odgovorilo 69,8% vprašanih. Aritmetična sredina je znašala 4,73. Odgovorov nestrinjanja s trditvijo ni bilo. Standardni odklon je znašal 0,449, varianca pa 0,201.



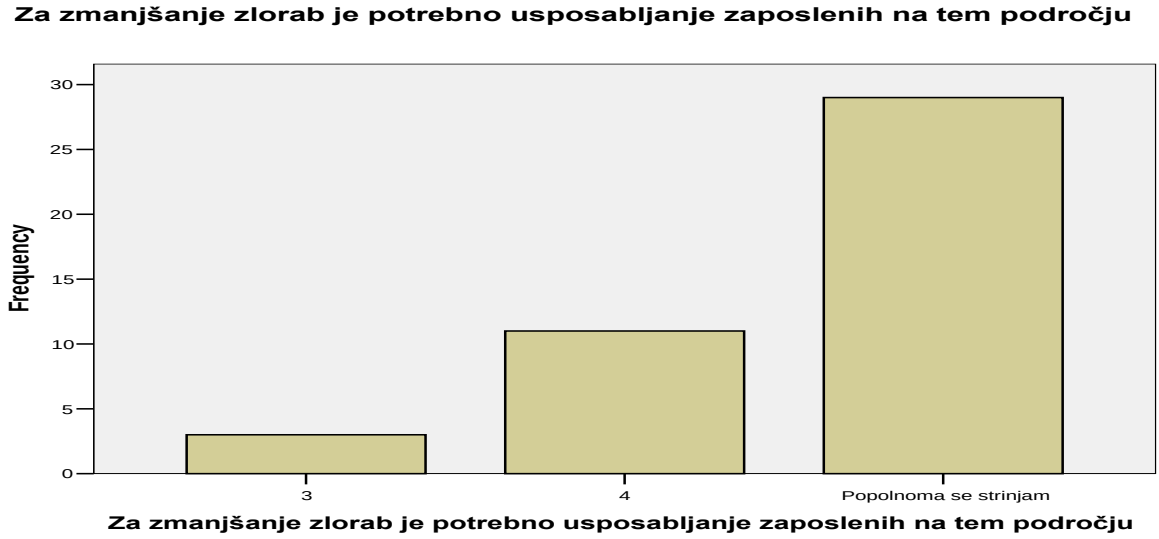
S trditvijo »pogodba med izdajateljem kartic in prodajnim mestom z vidika preprečevanja zlorab je preohlapna« se je popolnoma strinjalo 16,3% vprašanih, največ, 46,5 procentov se je odločilo za odgovor »se strinjam«. Aritmetična sredina znaša 3,58. Standardni odklon je znašal 0,879, varianca pa 0,773.



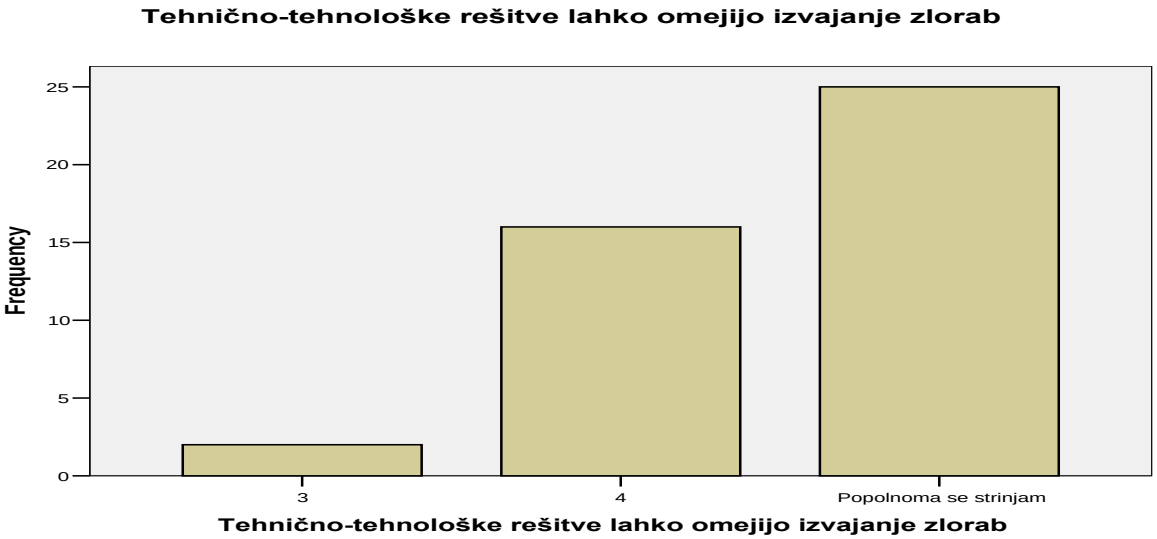
Na trditev »vloga prodajnih mest pri preprečevanju zlorab je pomembna« je kar 60,5% vprašanih odgovorilo s popolnoma se strinjam, tistih, ki se s trditvijo ne bi strinjali, ni bilo. Aritmetična sredina je znašala 4,56. Standardni odklon je znašal 0,590, varianca pa 0,348.



S trditvijo »za zmanjšanje zlorab je potrebno usposabljanje zaposlenih na tem področju« se je popolnoma strinjalo 67,4% vprašanih, aritmetična sredina je znašala 4,60. Odgovorov vprašanih, ki se ne bi strinjali s trditvijo, ni bilo. Standardni odklon je znašal 0,623, varianca pa 0,388.

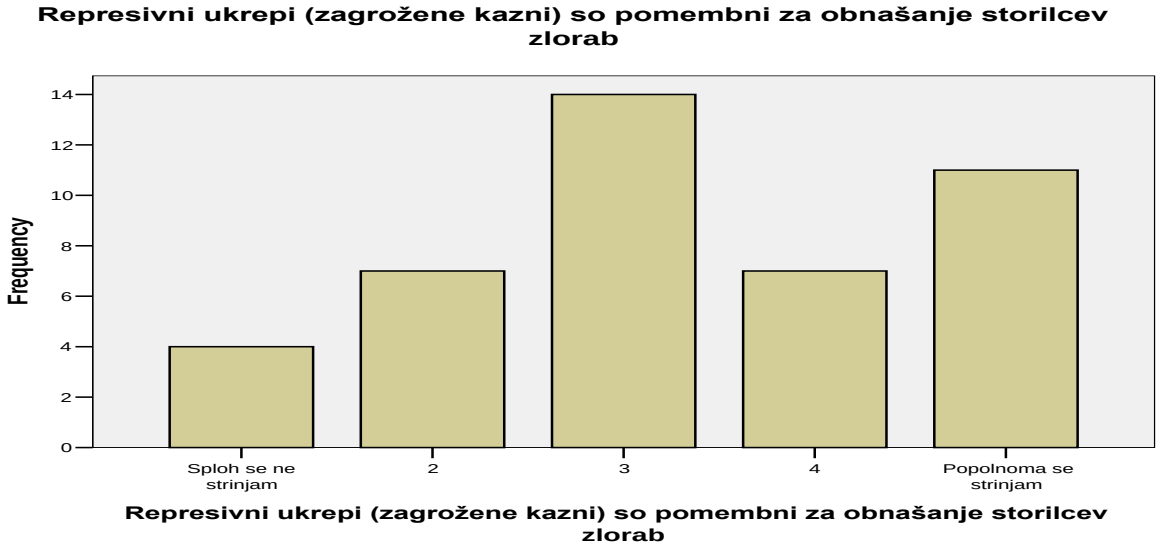


S trditvijo »tehnično-tehnološke rešitve lahko omejijo izvajanje zlorab« se je popolnoma strinjalo 58,1% vprašanih. Aritmetična sredina je znašala 4,53. Odgovorov vprašanih, ki se ne bi strinjali s trditvijo, ni bilo. Standardni odklon je znašal 0,592, varianca pa 0,350.



Na trditev »varnost poslovanja je odvisna tudi od organizacijskih rešitev« je z odgovorom popolnoma se strinjam odgovorilo 46,5% vprašanih, aritmetična sredina je znašala 4,33. Samo 2,3% vprašanih se s trditvijo ni strinjalo. Standardni odklon je znašal 0,754, varianca pa 0,569.

Trditev »represivni ukrepi (zagrožene kazni) so pomembni za obnašanje storilcev zlorab« je dosegla aritmetično sredino 3,33. Skupaj se je s trditvijo popolnoma strinjalo 25,6%, večinoma se je strinjalo 16,3%, strinjalo se je 32,6% vprašanih. S trditvijo se ni strinjalo 16,3% vprašanih, sploh se ni strinjalo 9,3% vprašanih. Standardni odklon je znašal 1,286, varianca pa 1,653.



Aritmetične sredine ($\bar{x}$), standardni odkloni (SD) in variance (V), ki smo jih dobili z analizo, so prikazani v tabeli.

Tabela 11: Splošna varnost in razvoj področja

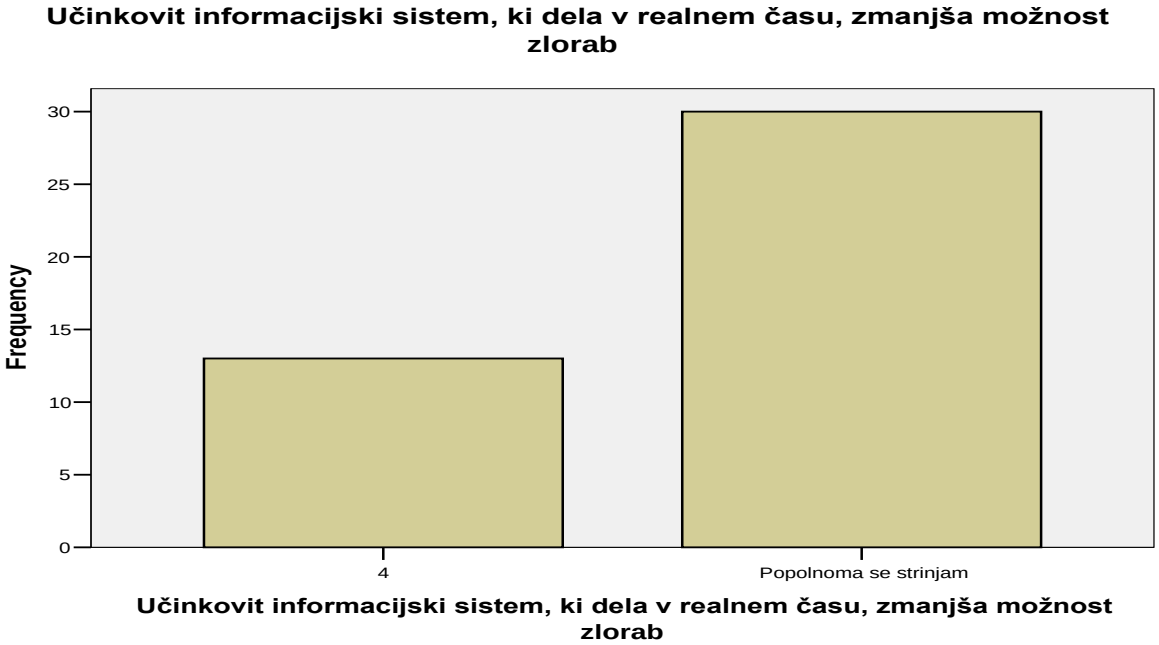
Vprašanje	$\bar{x}$	SD	V
a1: Brezgotovinski plačilni promet se bo v prihodnje povečeval	4,79	0,559	0,312
a2: Zlorabe na področju se z večanjem obsega poslovanja povečujejo	4,07	0,961	0,924
a3: Ponarejanje kartic je lažje kot ponarejanje denarja	3,53	1,077	1,159
a4: Plačilne kartice morajo biti zavarovane z varnostnimi elementi	4,93	0,258	0,066
a5: Največjo nevarnost za ponarejanje predstavlja magnetni zapis	4,16	0,949	0,901
a6: Pravila poslovanja uporabnikov morajo biti jasno določena	4,88	0,324	0,105
a7: Zlorabe s karticami se dogajajo povsod po svetu	4,70	0,708	0,502
a8: Pravila poslovanja s karticami morajo biti mednarodno primerljiva	4,73	0,449	0,201
a9: Pogodba med izdajateljem in prodajnim mestom je preohlapna	3,58	0,879	0,773
a10: Vloga prodajnih mest pri preprečevanju zlorab je pomembna	4,56	0,590	0,348
a11: Za zmanjšanje zlorab je potrebno usposabljanje zaposlenih	4,60	0,623	0,388
a12: Tehnično-tehnološke rešitve lahko omejijo izvajanje zlorab	4,53	0,592	0,350
a13: Varnost poslovanja je odvisna tudi od organizacijskih rešitev	4,33	0,754	0,569
a14: Represivni ukrepi so pomembni za obnašanje storilcev zlorab	3,33	1,286	1,653

8.2 Preventivni dejavniki, ki vplivajo na varnost poslovanja

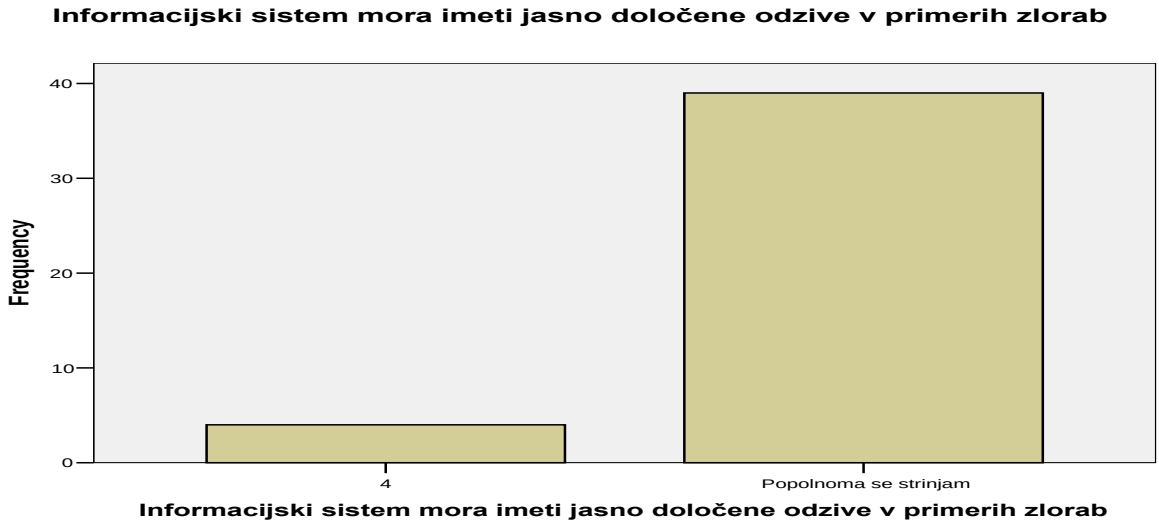
Vprašanja s tega sklopa vprašalnika se nanašajo na preventivne dejavnike, ki lahko preprečujejo možnosti zlorab.

8.2.1 Opisne statistike

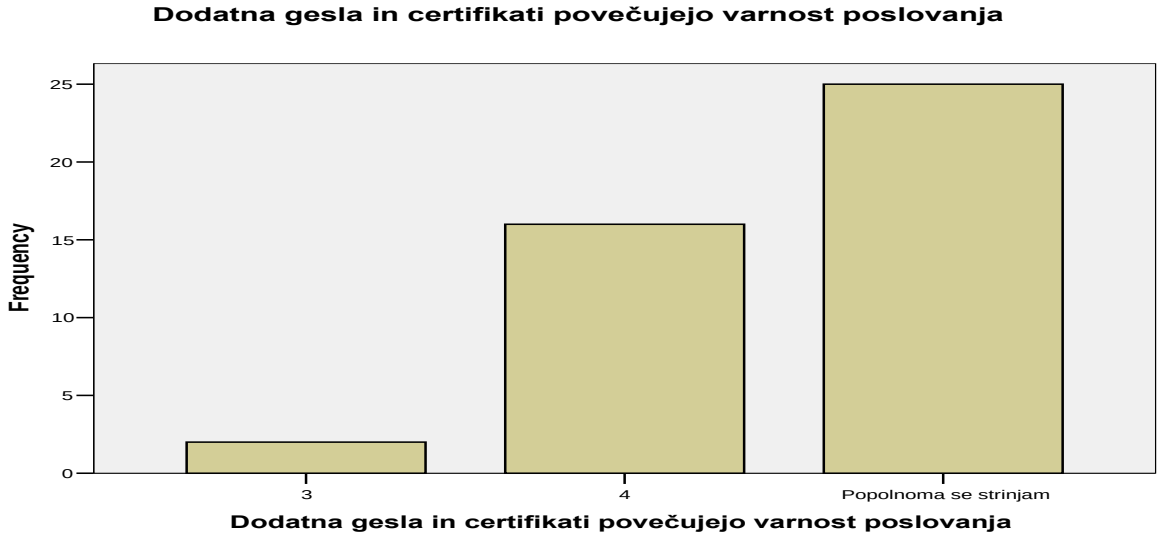
Na trditev » učinkovit informacijski sistem, ki dela v realnem času, zmanjša možnost zlorab« je z odgovorom popolnoma se strinjam odgovorilo 69,8% vprašanih in večinoma se strinjam 30,2%. Drugih odgovorov ni bilo, aritmetična sredina je bila 4,70. Standardni odklon je znašal 0,465, varianca pa 0,216.



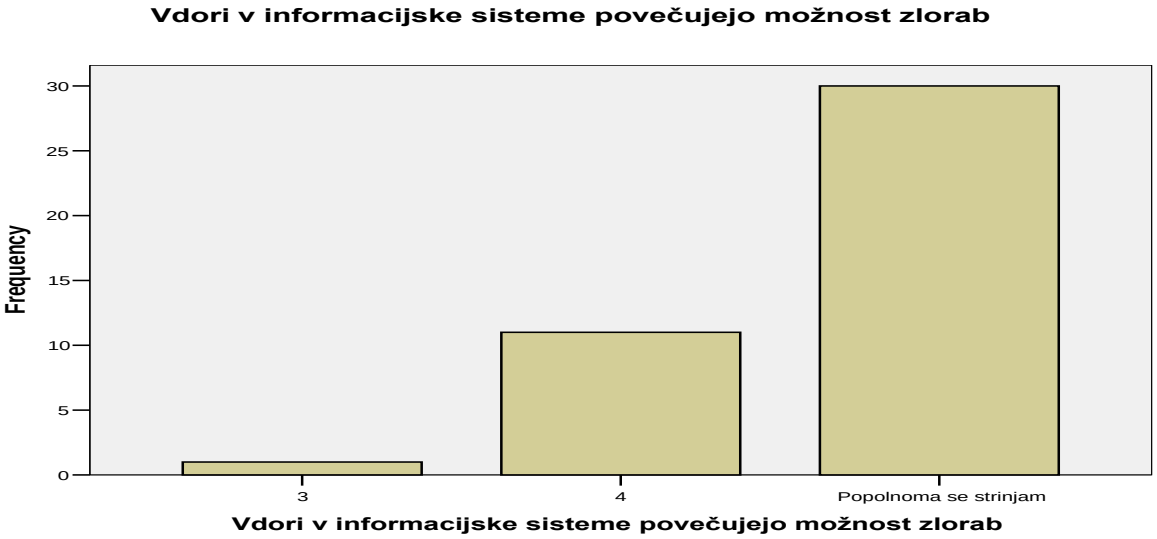
Na trditev »informacijski sistem mora imeti jasno določene odzive v primeru zlorab« je z odgovorom popolnoma se strinjam odgovorilo 90,7% vprašanih, nestrinjanj s trditvijo ni bilo, aritmetična sredina je znašala 4,91. Standardni odklon je znašal 0,294, varianca pa 0,086.



S trditvijo »dodatna gesla in certifikati povečujejo varnost poslovanja« se je popolnoma strinjalo 58,1% vprašanih, večinoma pa 37,2%. Aritmetična sredina je znašala 4,53. Standardni odklon je znašal 0,592, varianca pa 0,350.



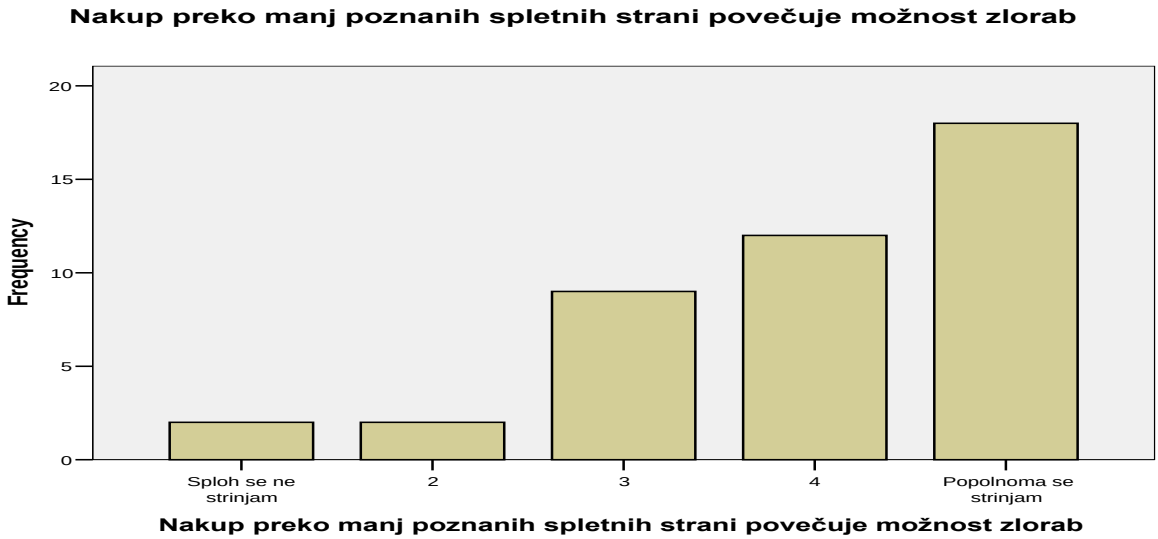
Trditev »vdori v informacijske sisteme povečujejo možnost zlorab« je dosegla aritmetično sredino 4,69. S trditvijo se je popolnoma strinjalo 69,8%, večinoma pa 25,6% vprašanih. Noben anketiranec ni izrazil nestrinjanja s trditvijo. Standardni odklon je znašal 0,517, varianca pa 0,268.



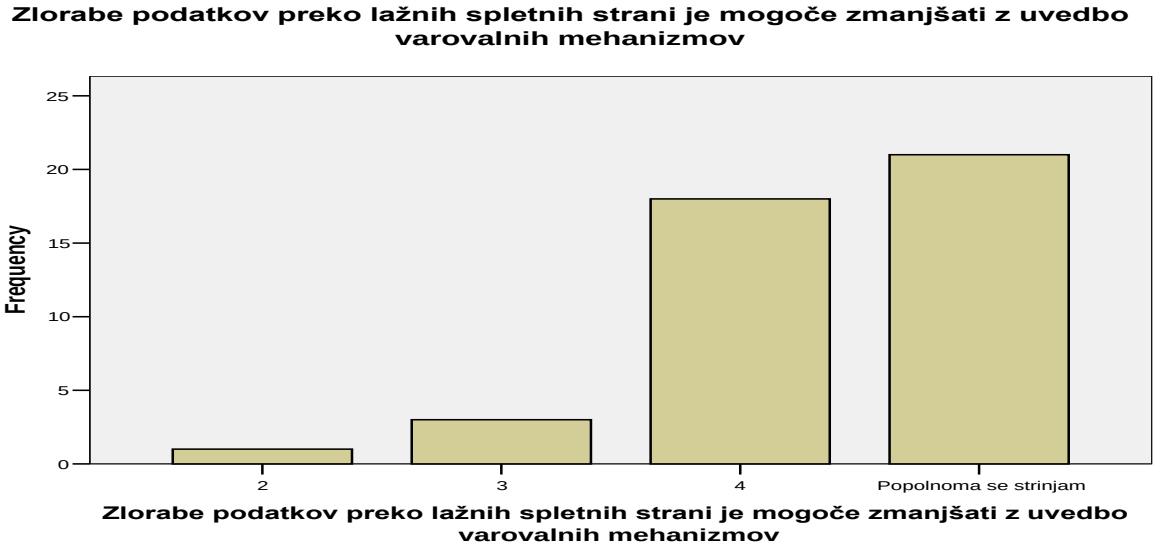
S trditvijo »največjo nevarnost predstavljajo uporabnikovi operacijski sistemi in slaba zaščita pred virusi« se je popolnoma strinjalo 18,6% vprašanih, večinoma strinjalo 37,2% in strinjalo 27,9% vprašanih. Aritmetična sredina je znašala 3,58. Standardni odklon je znašal 0,982, varianca pa 0,963.

Na trditev »pošiljanje podatkov uporabnikov preko e-pošte lahko poveča možnost zlorab (fishing)« je z odgovorom popolnoma in večinoma se strinjam odgovorilo skupaj odgovorilo 90,7% vprašanih. Aritmetična sredina je znašala 4,37. Noben anketiranec trditvi ni nasprotoval. Standardni odklon je znašal 0,655, varianca pa 0,430.

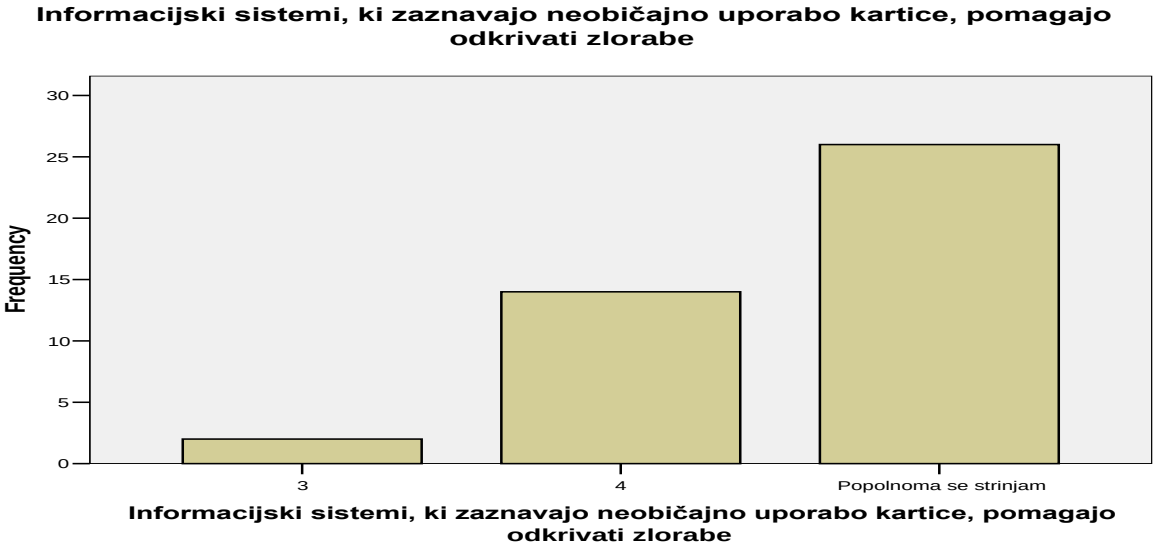
Trditev »nakup preko manj poznanih spletnih strani povečuje možnost zlorab« je dosegla aritmetično sredino 3,98. Z odgovorom popolnoma se strinjam je odgovorilo 41,9% vprašanih, s trditvijo se jih je večinoma strinjalo 27,9%. Standardni odklon je znašal 1,123, varianca pa 1,261.



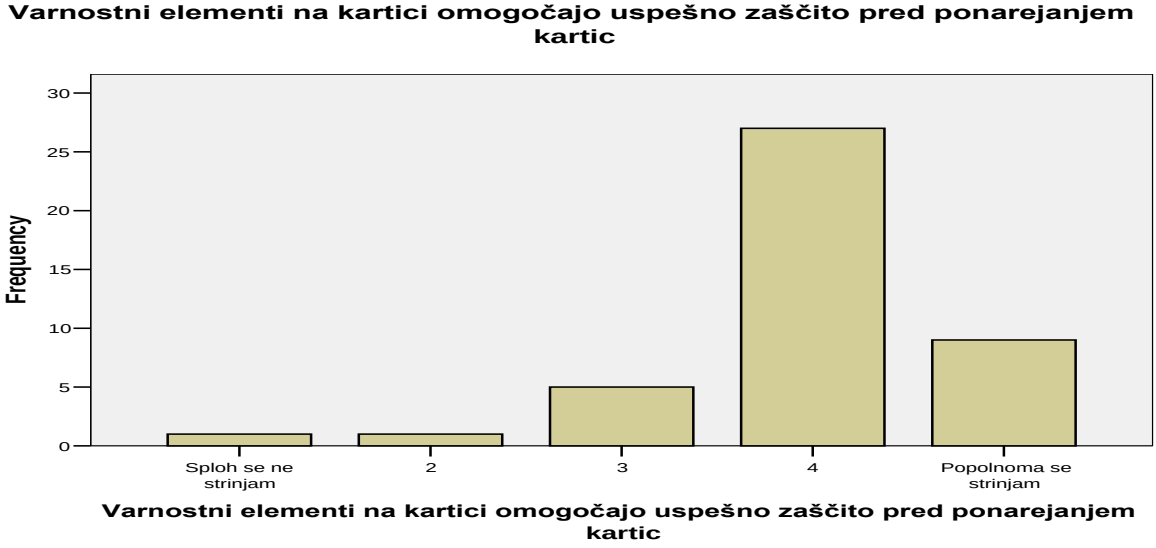
Na trditev »zlorabe podatkov preko lažnih spletnih strani je mogoče zmanjšati z uvedbo varovalnih mehanizmov« je z odgovorom popolnoma se strinjam odgovorilo 48,8% vprašanih, delež tistih, ki se s trditvijo niso strinjali je 9,3%. Aritmetična sredina je znašala 4,37. Standardni odklon je znašal 0,725, varianca pa 0,525.



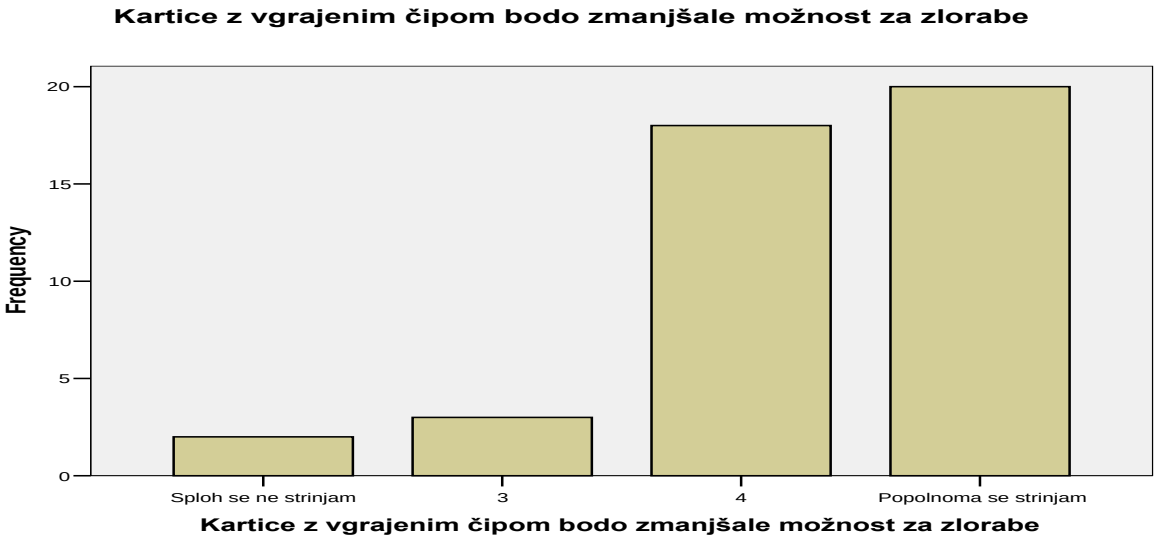
S trditvijo »informacijski sistemi, ki zaznavajo neobičajno uporabo kartice, pomagajo odkrivati zlorabe« se je popolnoma strinjalo 60,5% in večinoma strinjalo 32,6% vprašanih. Aritmetična sredina je zanašala 4,57. Standardni odklon je znašal 0,590, varianca pa 0,348.



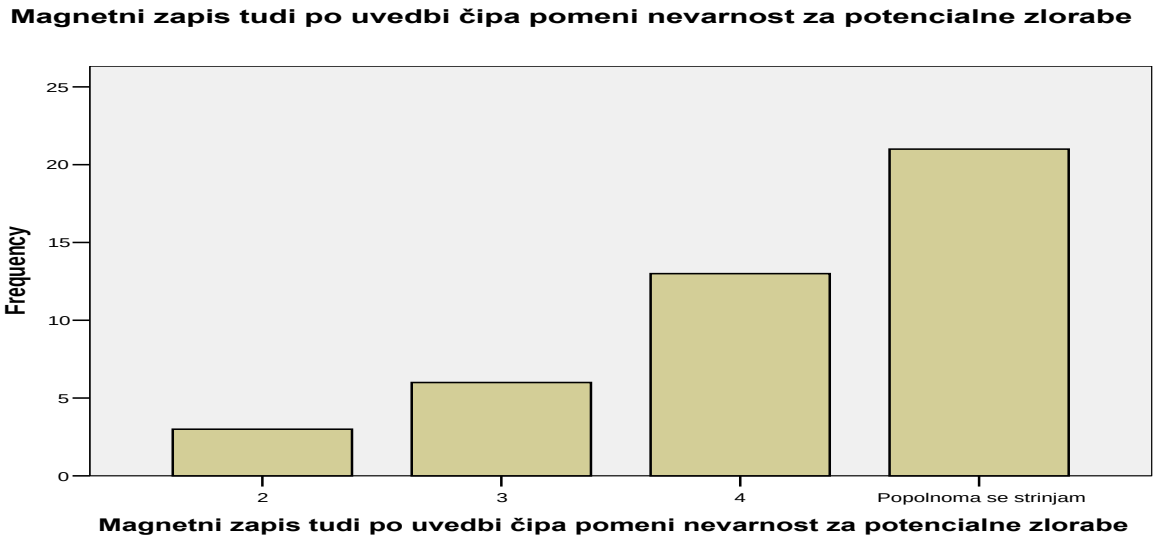
Trditev »varnostni elementi na kartici omogočajo uspešno zaščito pred ponarejanjem kartic« je dosegla aritmetično sredino 3,98. Večina anketiranih se je odločila za odgovor večinoma se strinjam (62,8%) in popolnoma se strinjam (20,9%). Nestrinjanje je izrazilo samo 4,7% vprašanih. Standardni odklon je znašal 0,801, varianca pa 0,642.



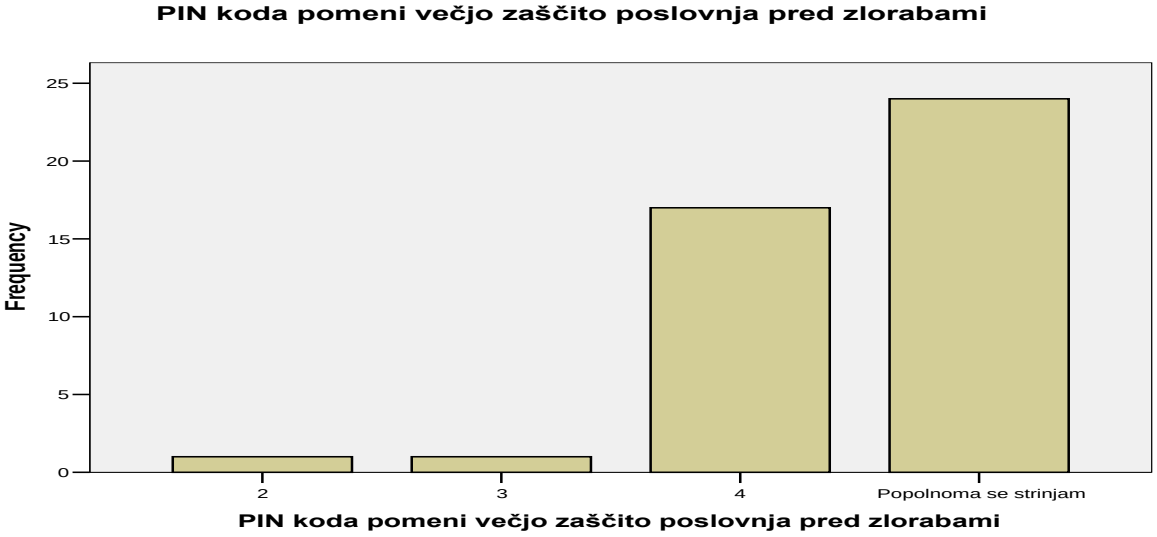
Na trditev »kartice z vgrajenim čipom bodo zmanjšale možnost za zlorabe« je kar 46,5% vprašanih odgovorilo z odgovorom popolnoma se strinjam, 41,9 pa z odgovorom večinoma se strinjam. 11,6% vprašanih se s trditvijo ni strinjalo. Aritmetična sredina je znašala 4,26. Standardni odklon je znašal 0,954, varianca pa 0,909.



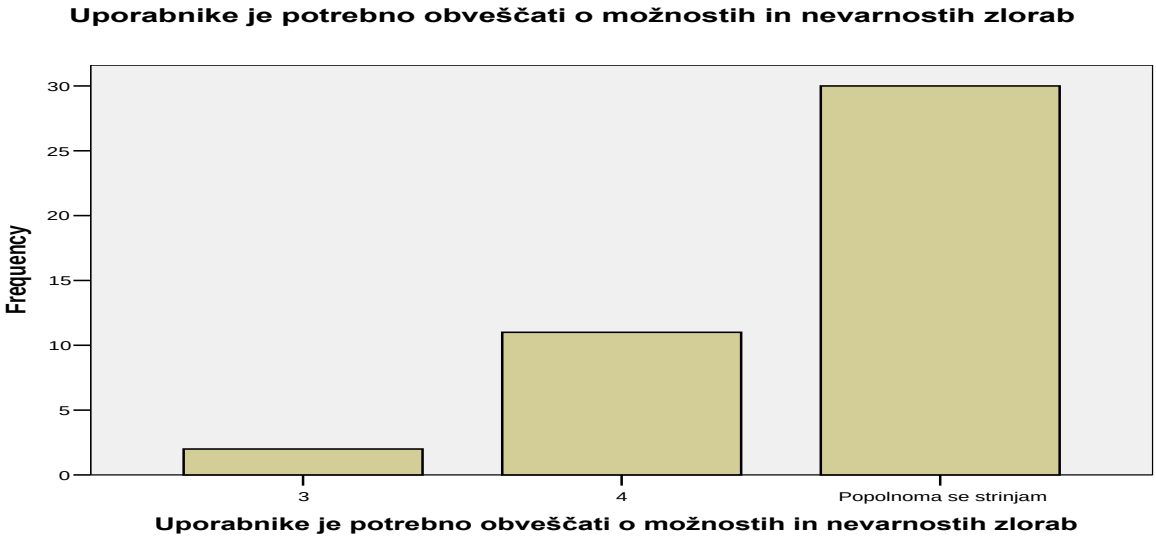
Na trditev »magnetni zapis tudi po uvedbi čipa pomeni nevarnost za potencialne zlorabe« se je popolnoma in večinoma strinjalo skupaj 79,0% vprašanih, aritmetična sredina je znašala 4,21. Standardni odklon je znašal 0,940, varianca pa 0,884.



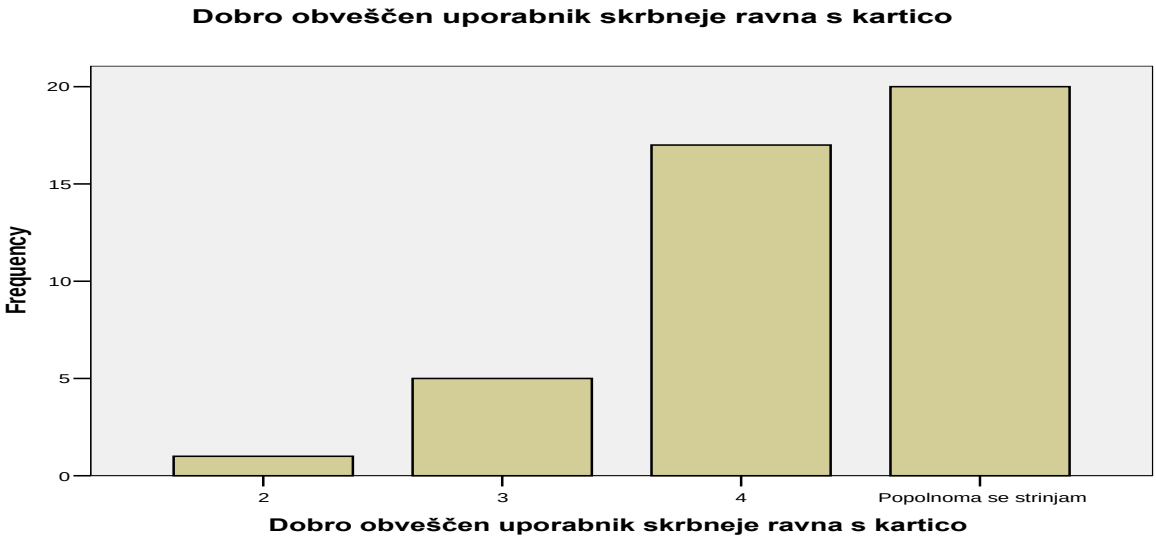
S trditvijo »PIN koda pomeni večjo zaščito poslovanja pred zlorabami« se je popolnoma strinjalo 55,8% in večinoma strinjalo 39,5% vprašanih. Aritmetična sredina je bila 4,49. Standardni odklon je znašal 0,668, varianca pa 0,446.



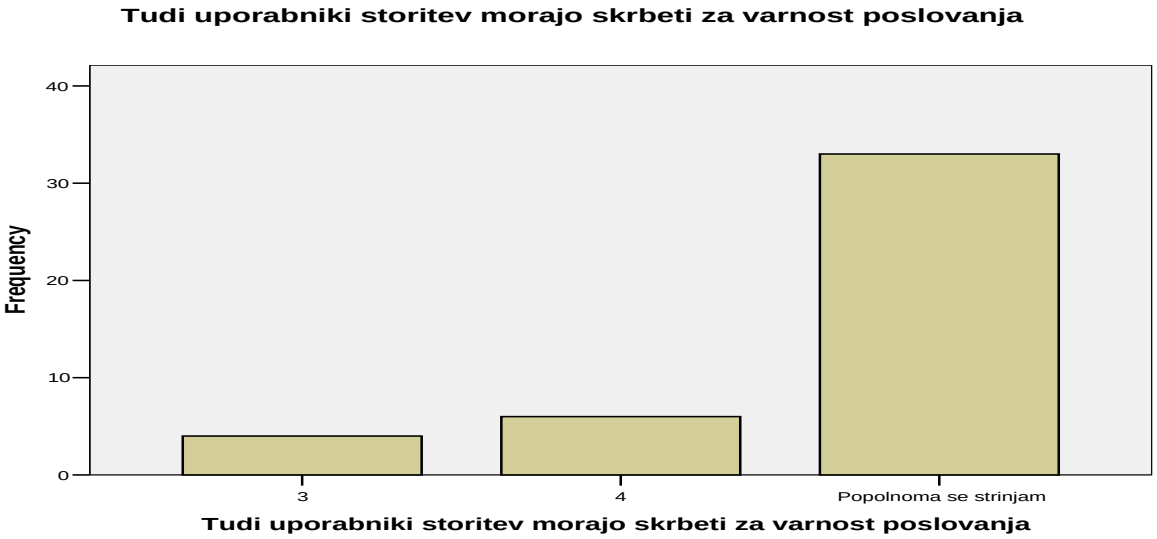
S trditvijo »uporabnike je potrebno obveščati o možnostih in nevarnostih zlorab« se je popolnoma strinjalo 69,8% in večinoma strinjalo 25,6% vprašanih. Nestrinjanja s trditvijo vprašani niso izražali. Aritmetična sredina je znašala 4,65. Standardni odklon je znašal 0,573, varianca pa 0,328.



Trditev »dobro obveščen uporabnik skrbneje ravna s kartico« je dosegla aritmetično sredino v višini 4,30. S trditvijo se je popolnoma strinjalo 46,5% in večinoma strinjalo 39,5% anketirancev. Tistih, ki se s trditvijo niso strinjali, je bilo skupaj 2,3%. Standardni odklon je znašal 0,773, varianca pa 0,597.

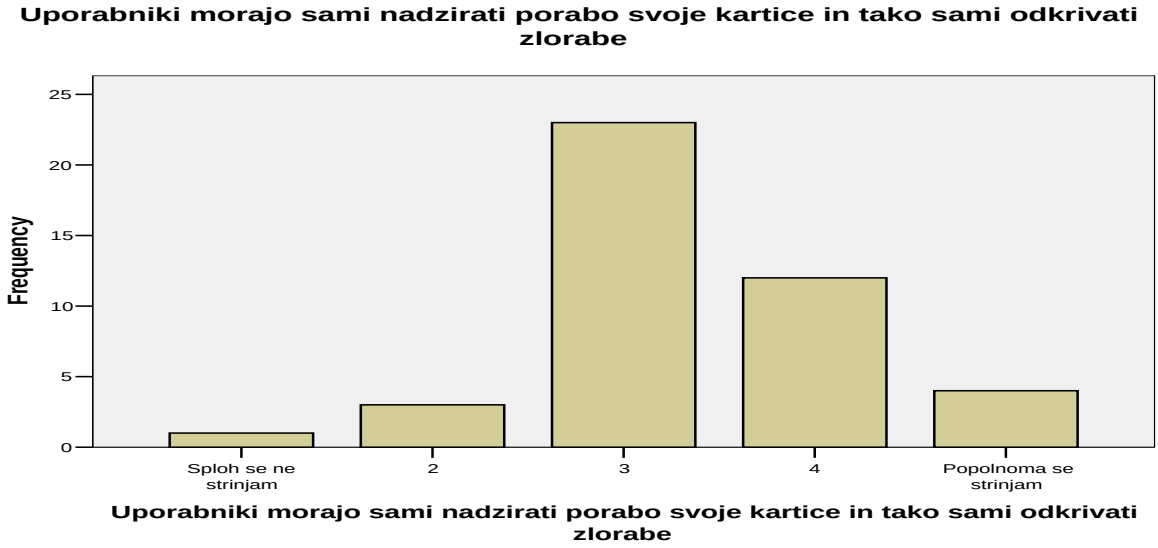


Na trditev »tudi uporabniki storitev morajo skrbeti za varnost poslovanja« je z odgovorom popolnoma se strinjam odgovorilo 76,7% anketirancev. Aritmetična sredina je dosegla vrednost 4,67. Anketirancev, ki se s trditvijo ne bi strinjali, ni bilo. Standardni odklon je znašal 0,644, varianca pa 0,415.

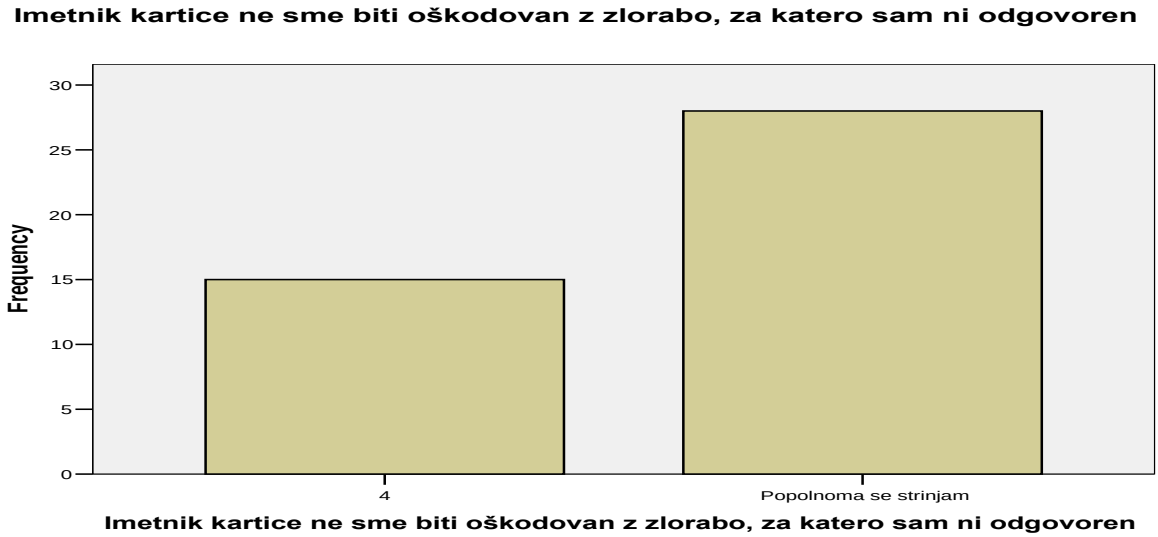


Na trditev »obnašanje uporabnika ima vpliv na možnost zlorab« je z odgovorom popolnoma se strinjam odgovorilo 41,9% in večinoma se strinjam 30,2% vprašanih. Za nestrinjanje se ni odločil nihče. Aritmetična sredina je znašala 4,20. Standardni odklon je znašal 0,813, varianca pa 0,661.

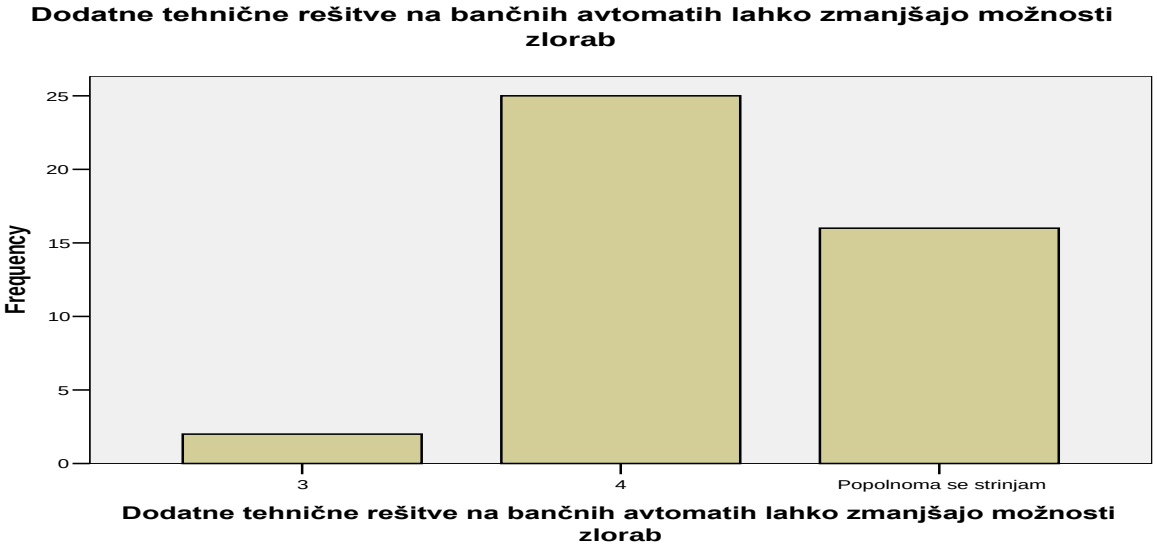
Trditev »uporabniki morajo sami nadzirati porabo svoje kartice in tako sami odkrivati zlorabe« je dosegla aritmetično sredino v višini 3,35. Kar 53,5% vprašanih se je s trditvijo strinjalo, vendar je bil delež tistih, ki so se popolnoma strinjali samo 9,35% in tistih, ki so se večinoma strinjali 27,9%. Negativnih odgovorov oz. tistih, ki se s trditvijo niso strinjali, je bilo skupaj 9,3%. Standardni odklon je znašal 0,842, varianca pa 0,709.



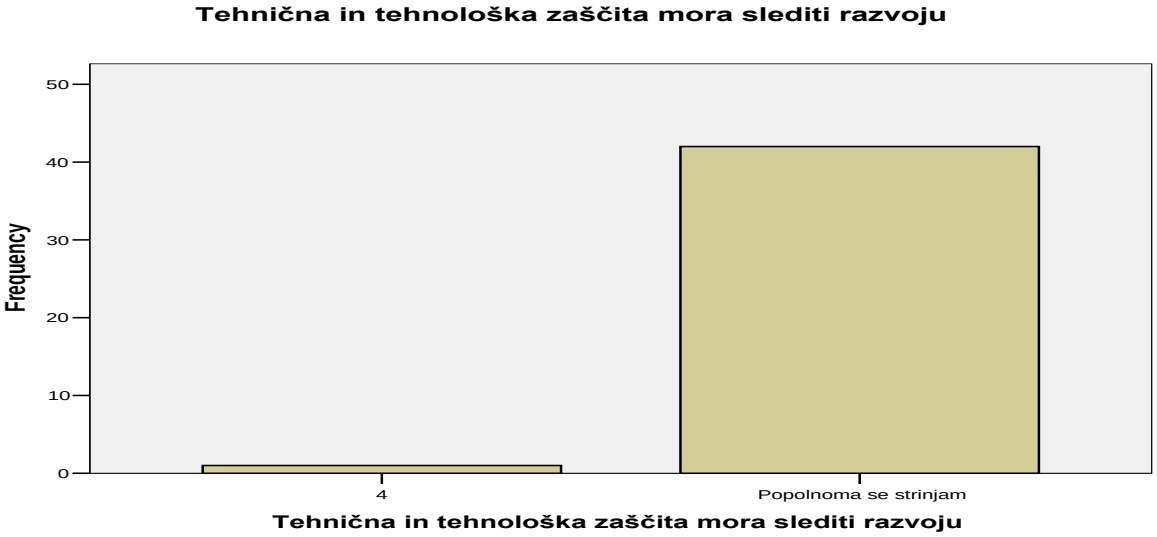
S trditvijo »imetnik kartice ne sme biti oškodovan z zlorabo, za katero sam ni odgovoren« se je popolnoma strinjalo 65,1% vprašanih in večinoma strinjalo 34,9% vprašanih. Drugih odgovorov ni bilo, zato je trditev dosegla tudi visoko aritmetično sredino 4,65. Standardni odklon je znašal 0,482, varianca pa 0,233.



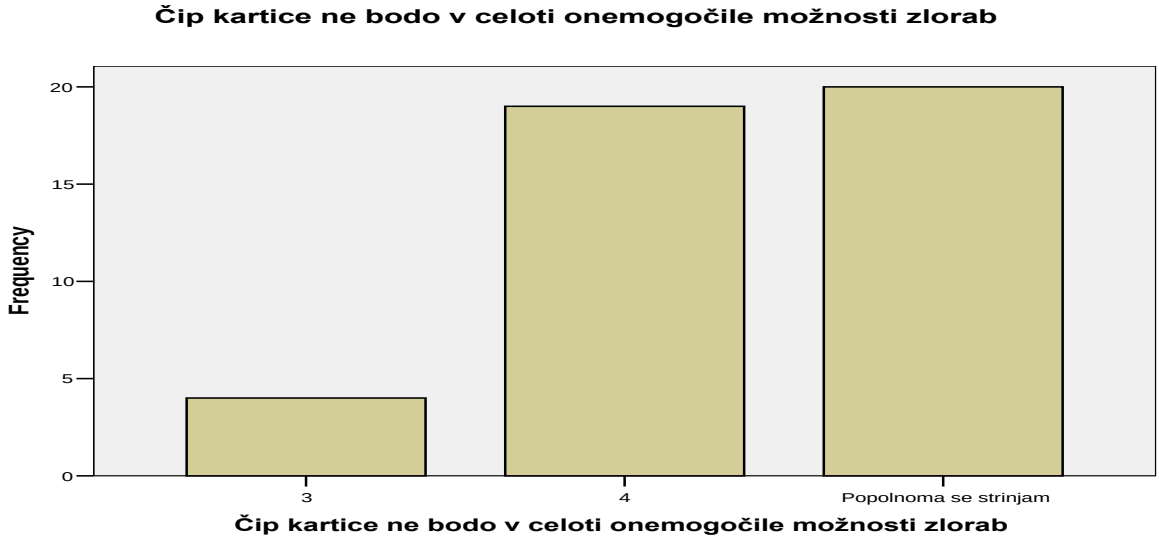
S trditvijo »dodatne tehnične rešitve na bančnih avtomatih lahko zmanjšajo možnosti zlorab« se je popolnoma strinjalo 37,2% in večinoma strinjalo 58,1% vprašanih. Anketirancev, ki se s trditvijo ne bi strinjali, ni bilo. Aritmetična sredina je znašala 4,33. Standardni odklon je znašal 0,566, varianca pa 0,320.



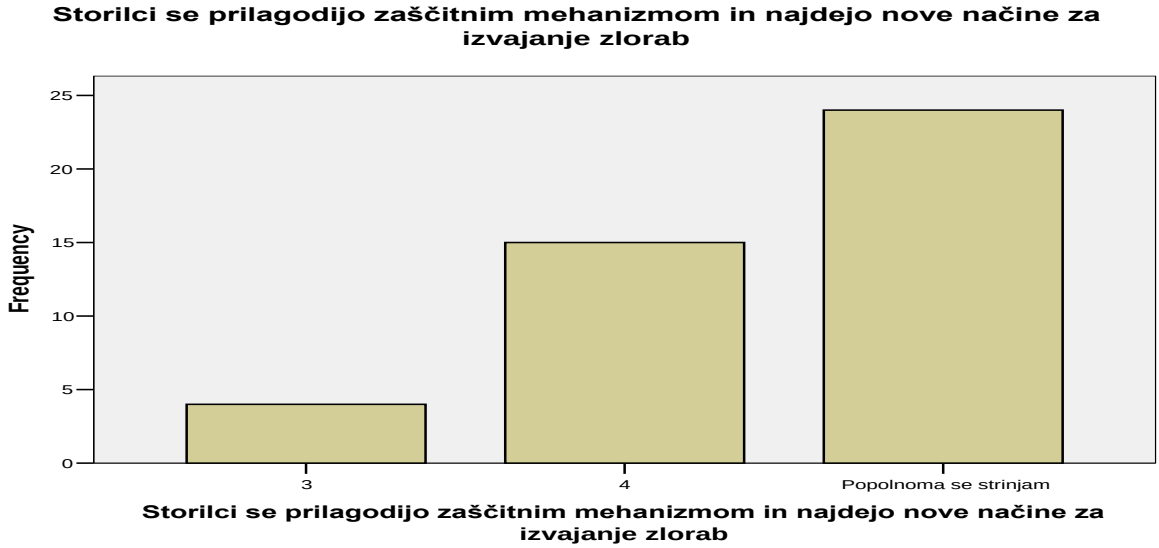
Na trditev »tehnična in tehnološka zaščita mora slediti razvoju« je z odgovorom popolnoma se strinjam odgovorilo 79,7% vprašanih, negativnih odgovorov ni bilo. Dosežena aritmetična sredina je znašala 4,98. Standardni odklon je znašal 0,152, varianca pa 0,023.



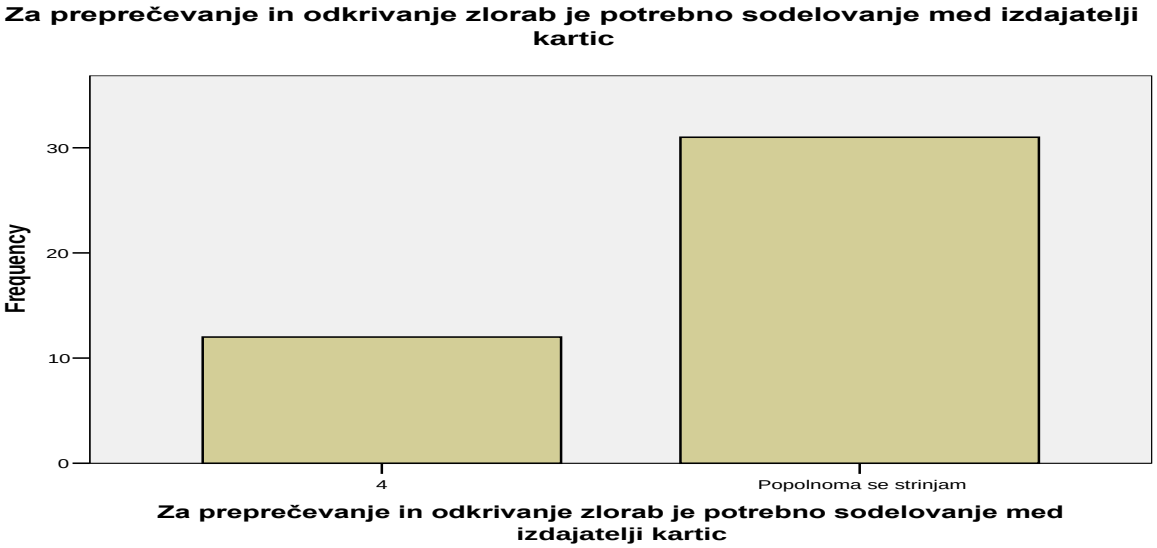
Trditev »čip kartice ne bodo v celoti onemogočile možnosti zlorab« je dosegla aritmetično sredino v višini 4,37. S takšno trditvijo se je popolnoma strinjalo 46,5% vprašanih, tistih, ki se s trditvijo ne bi strinjali, ni bilo. Standardni odklon je znašal 0,655, varianca pa 0,430.



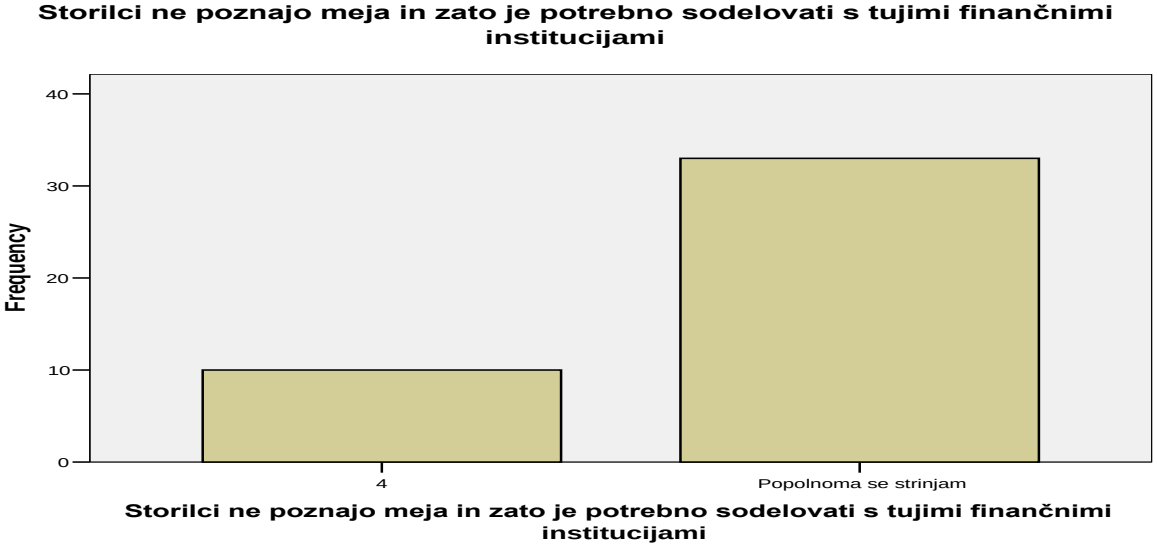
S trditvijo »storilci se prilagodijo zaščitnim mehanizmom in najdejo nove načine za izvajanje zlorab« se je popolnoma strinjalo 55,8% in večinoma strinjalo 34,9% vprašanih. Negativnih odgovorov ni bilo, aritmetična sredina je znašala 4,47. Standardni odklon je znašal 0,667, varianca pa 0,445.



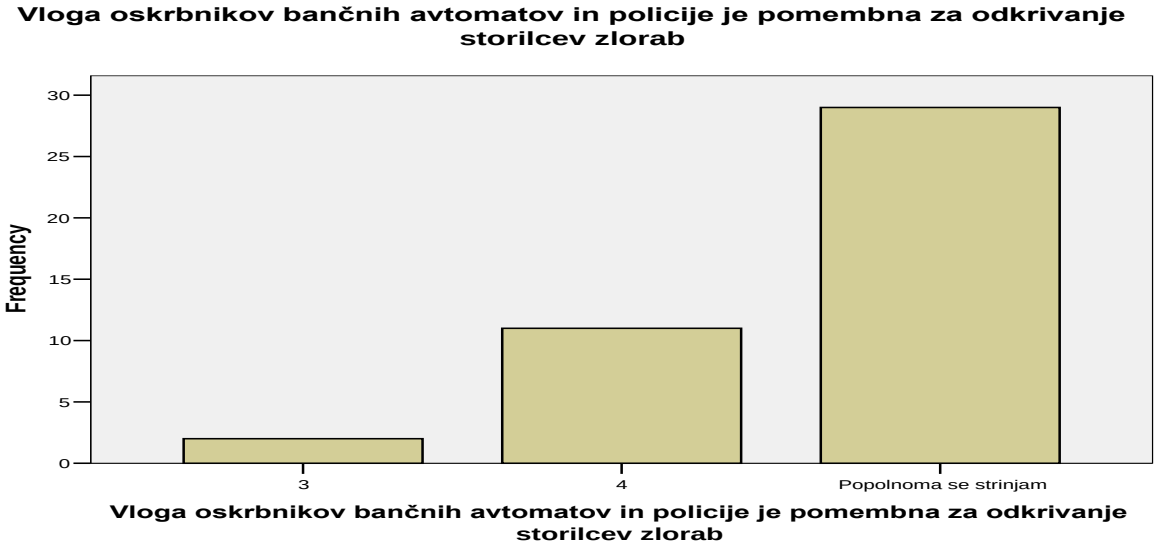
Na trditev »za preprečevanje in odkrivanje zlorab je potrebno sodelovanje med izdajatelji kartic« je z odgovorom popolnoma se strinjam odgovorilo 72,1% vprašanih in večinoma se strinjam ostalih 27,9%. Drugih odgovorov ni bilo izbranih, aritmetična sredina pa je znašala 4,72. Standardni odklon je znašal 0,454, varianca pa 0,206.



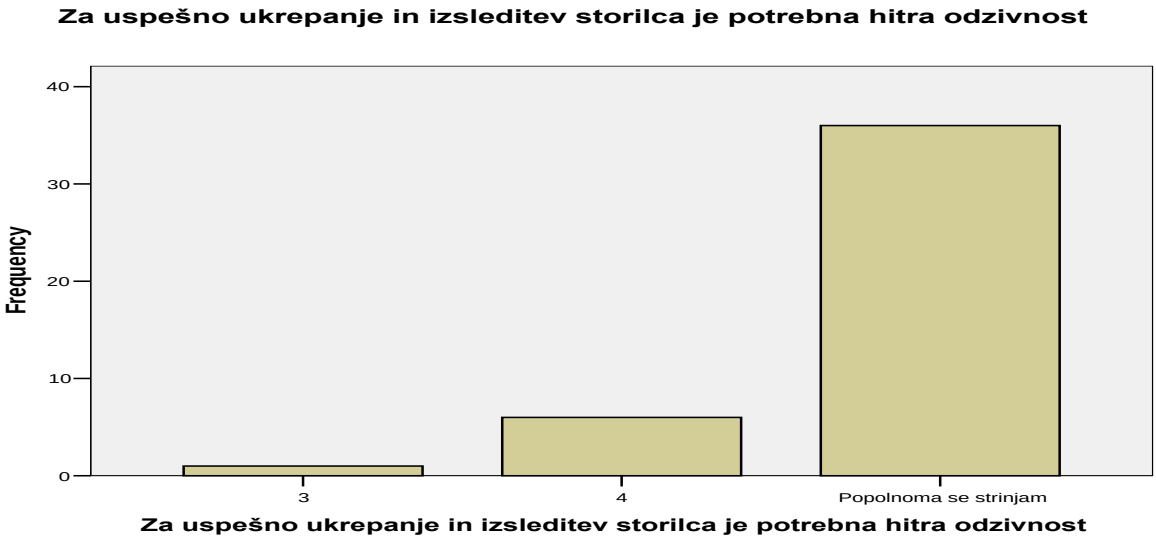
Trditev »storilci ne poznajo meja in zato je potrebno sodelovati s tujimi finančnimi institucijami« je dosegla aritmetično sredino v višini 4,77. Vprašani so se s trditvijo popolnoma strinjali v 76,7% in večinoma strinjali v 23,3%. Negativnih odgovorov ni bilo. Standardni odklon je znašal 0,427, varianca pa 0,183.



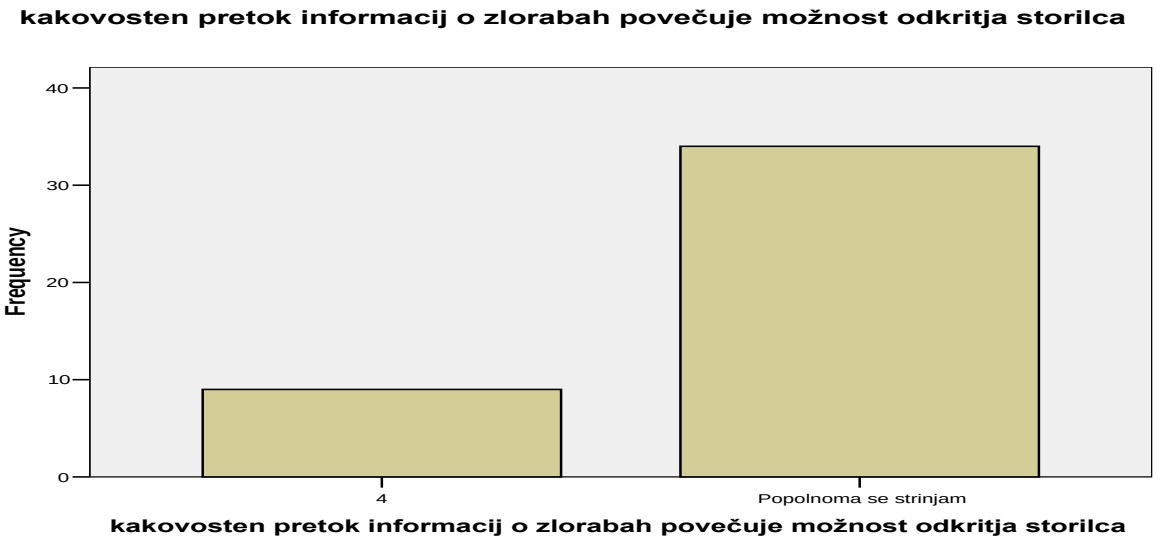
Trditev »vloga oskrbnikov bančnih avtomatov in policije je pomembna za odkrivanje storilcev zlorab« je dosegla aritmetično sredino v višini 4,64. Kar 67,4% vprašanih se je s trditvijo popolnoma strinjalo, 25,6% se jih je večinoma strinjalo. Negativnih odgovorov oz. tistih, ki se s trditvijo niso strinjali, ni bilo. Standardni odklon je znašal 0,577, varianca pa 0,333.



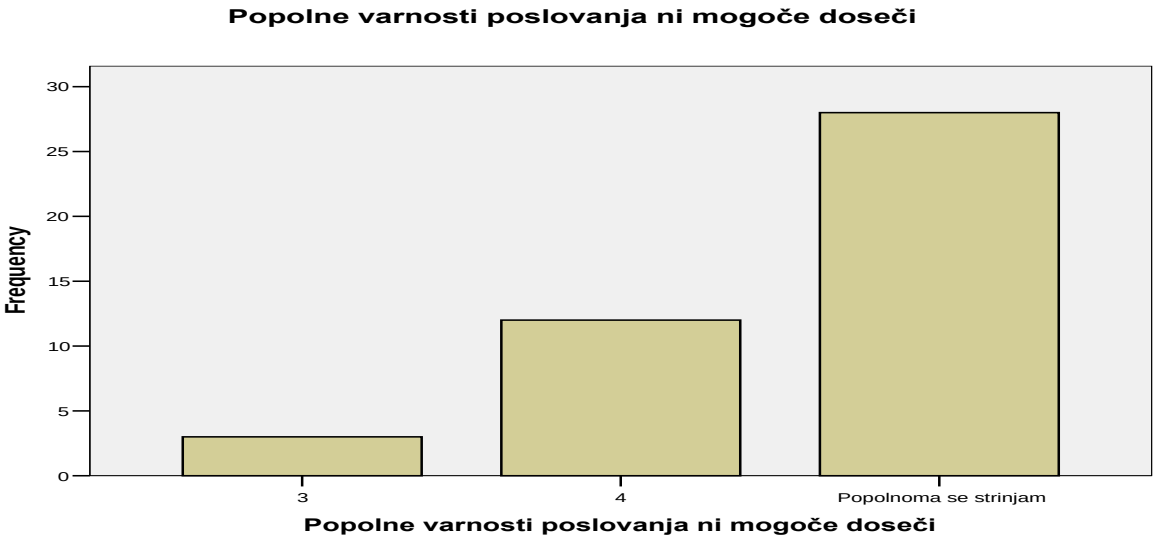
S trditvijo »za uspešno ukrepanje in izsledite storilca je potrebna hitra odzivnost« se je popolnoma strinjalo 83,7% vprašanih, večinoma pa 14% vprašanih. Trditev je dosegla aritmetično sredino v višini 4,81. Standardni odklon je znašal 0,450, varianca pa 0,203.



Na trditev »kakovosten pretok informacij o zlorabah povečuje možnost odkritja storilca« je z odgovorom popolnoma se strinjam odgovorilo 79,1% vprašanih. Večinoma se strinjam je odgovorilo ostalih 20,9% vprašanih. Odgovor je dosegel visoko aritmetično sredino v višini 4,79. Standardni odklon je znašal 0,412, varianca pa 0,169.



Trditev »popolne varnosti poslovanja ni mogoče doseči« je dosegla aritmetično sredino v višini 4,58. S trditvijo se je popolnoma strinjalo 65,1% vprašanih, večinoma pa 27,9% vprašanih. Negativnih odgovorov oz. nestrinjanja s trditvijo ni bilo. Standardni odklon je znašal 0,626, varianca pa 0,392.



Aritmetične sredine ($\bar{x}$), standardni odkloni (SD) in variance (V), ki smo jih dobili z analizo, so prikazani v tabeli.

Tabela 12: Preventivni dejavniki

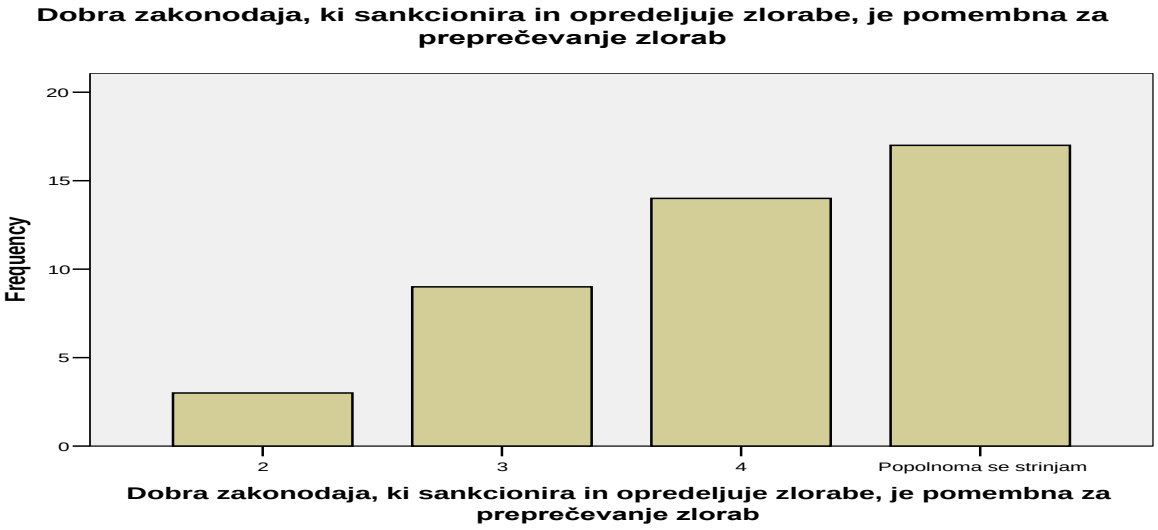
Vprašanje	$\bar{x}$	SD	V
b1: Učinkovit informacijski sistem zmanjša možnosti zlorab	4,70	0,465	0,216
b2: Informacijski sistem mora imeti jasno določene odzive	4,91	0,294	0,086
b3: Dodatna gesla in certifikati povečujejo varnost poslovanja	4,53	0,592	0,350
b4: Vdori v inf. sisteme povečujejo možnosti zlorab	4,69	0,517	0,268
b5: Največjo nevarnost predstavljajo uporabnikov OS in slaba zaščita	3,58	0,982	0,963
b6: Pošiljanje podatkov uporabnikov preko el. pošte poveča možnost zlorab	4,37	0,655	0,430
b7: Nakup preko manj poznanih spletnih strani povečuje možnosti zlorab	3,98	1,123	1,261
b8: Zlorabe pod. lažnih splet. st. je mogoče zmanjšati z uvedbo varov. meh.	4,37	0,725	0,525
b9: IS, ki zaznavajo neobičajno uporabo kartice, pomagajo odkrivati zlorabe	4,57	0,590	0,348
b10: Varnostni el. na kartici omogočajo uspešno zaščito pred ponarejanjem	3,98	0,801	0,642
b11: Kartice z vgrajenim čipom bodo zmanjšale možnosti za zlorabe	4,26	0,954	0,909
b12: Magnetni zapis tudi po uvedbi čipa pomeni nevarnost za pot. zlorabe	4,21	0,940	0,884
b13: PIN koda pomeni večjo zaščito poslovanja pred zlorabami	4,49	0,668	0,446
b14: Uporabnike je potrebno obveščati o možnostih in nevarnostih zlorab	4,65	0,573	0,328
b15: Dobro obveščen uporabnik skrbneje ravna s kartico	4,30	0,773	0,597
b16: Tudi uporabniki storitev morajo skrbeti za varnost poslovanja	4,67	0,644	0,415
b17: Obnašanje uporabnika ima vpliv na možnost zlorabe kartice	4,20	0,813	0,661
b18: Uporabniki morajo sami nadzirati porabo svoje kartice in odkrivati zlorabe	3,35	0,842	0,709
b19: Im. kart. ne sme biti oškodovan z zlorabo, za katero ni sam odgovoren	4,65	0,482	0,233
b20: Dodatne tehnične rešitve na BA lahko zmanjšajo možnosti zlorab	4,33	0,566	0,320
b21: Tehnična in tehnološka zaščita mora slediti razvoju	4,98	0,152	0,023
b22: Čip kartice ne bodo v celoti onemogočile možnosti zlorab	4,37	0,655	0,430
b23: Storilci se prilagodijo zašč. Meh. in najdejo nove načine za izvajanje zlorab	4,47	0,667	0,445
b24: Za prepr. in odkrivanje zlorab je potrebno sodelovanje med izd. kartic	4,72	0,454	0,206
b25: Storilci ne poznajo meja, potrebno je sodelovati s tujimi fin. institucijami	4,77	0,427	0,183
b26: Vloga oskrb. BA in policije je pomembna za odkrivanje storilcev zlorab	4,64	0,577	0,333
b27: Za uspešno ukrepanje in izsledite storilca je potrebna hitra odzivnost	4,81	0,450	0,203
b28: Kakovosten pretok informacij o zlorabah povečuje možnost odkritja storilca	4,79	0,412	0,169
b29: Popolne varnosti poslovanja ni mogoče doseči	4,58	0,626	0,392

Represivni dejavniki, ki vplivajo na varnost poslovanja

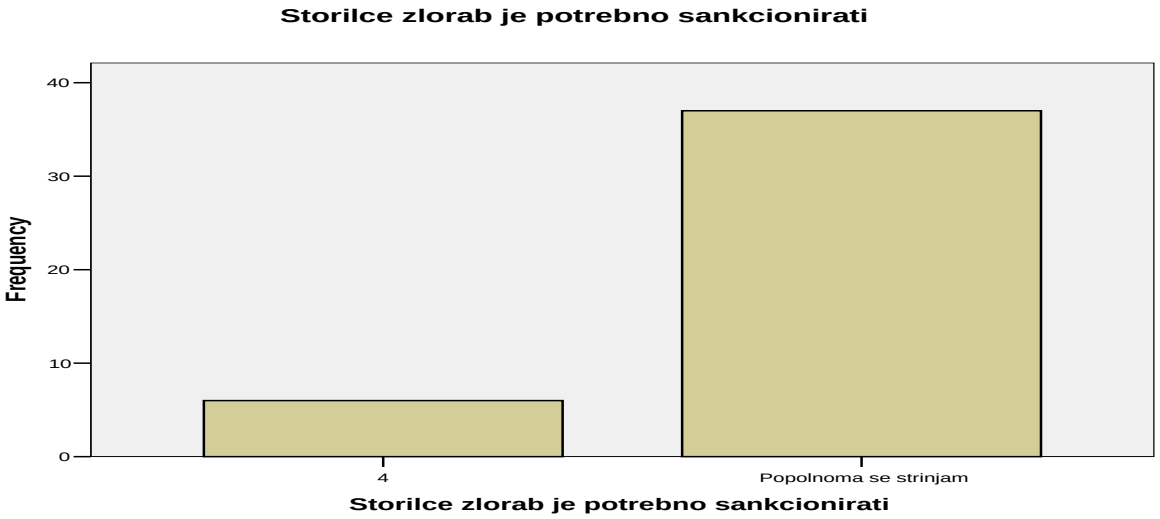
Represivni dejavniki v vprašalniku zajemajo ukrepe in dejavnosti, ki vplivajo represivno na storilce zlorab.

8.2.2 Opisne statistike

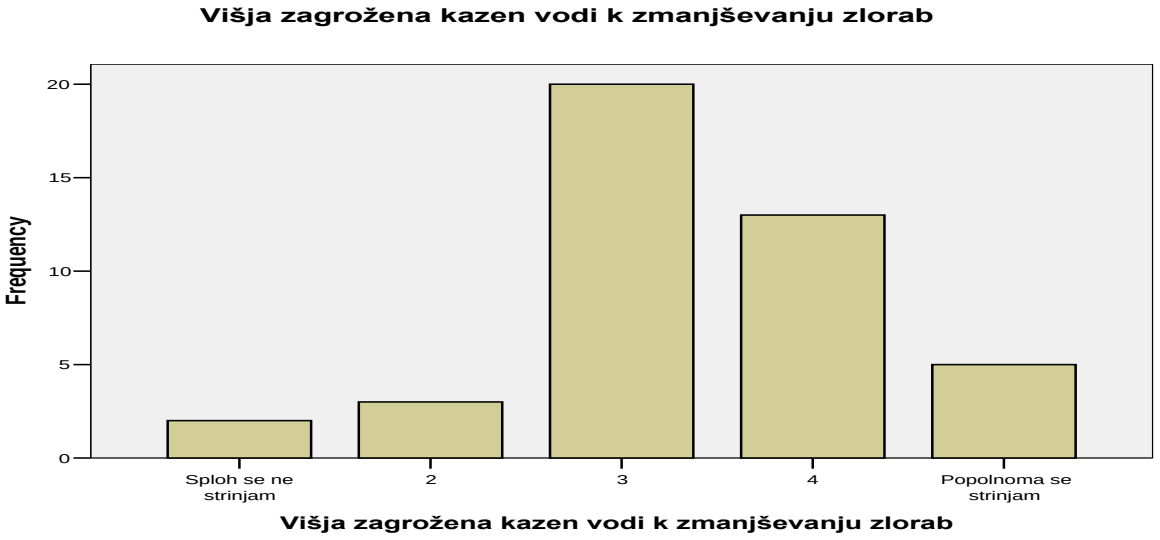
Trditev »dobra zakonodaja, ki sankcionira in opredeljuje zlorabe, je pomembna za preprečevanje zlorab« je dosegla aritmetično sredino v višini 4,05. S trditvijo se je popolnoma strinjalo 39,5% vprašanih, večinoma strinjalo 32,6% vprašanih. Takšnih, ki se s trditvijo niso strinjali, je bilo 7,0%. Standardni odklon je znašal 0,950, varianca pa 0,903.



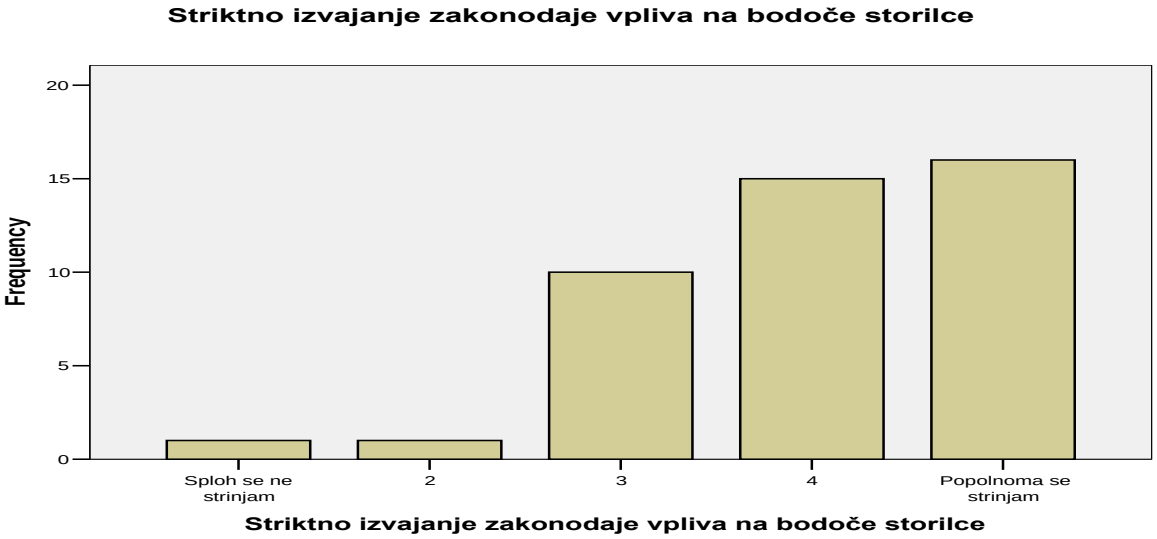
Na trditev »storilce zlorab je potrebno sankcionirati« je z odgovorom popolnoma se strinjam odgovorilo 86,0% in večinoma se strinjam 14% vprašanih. Aritmetična sredina je znašala 4,86. Standardni odklon je znašal 0,351, varianca pa 0,123.



S trditvijo »višja zagrožena kazen vodi k zmanjšanju zlorab« se je popolnoma strinjalo 11,6% vprašanih, večinoma strinjalo 30,2% vprašanih, strinjalo 46,5% vprašanih. Takšnih, ki se jih s trditvijo ni strinjalo oz. sploh ni strinjalo, je bilo skupaj 11,6%. Aritmetična sredina je dosegla 3,37. Standardni odklon je znašal 0,952, varianca pa 0,906.



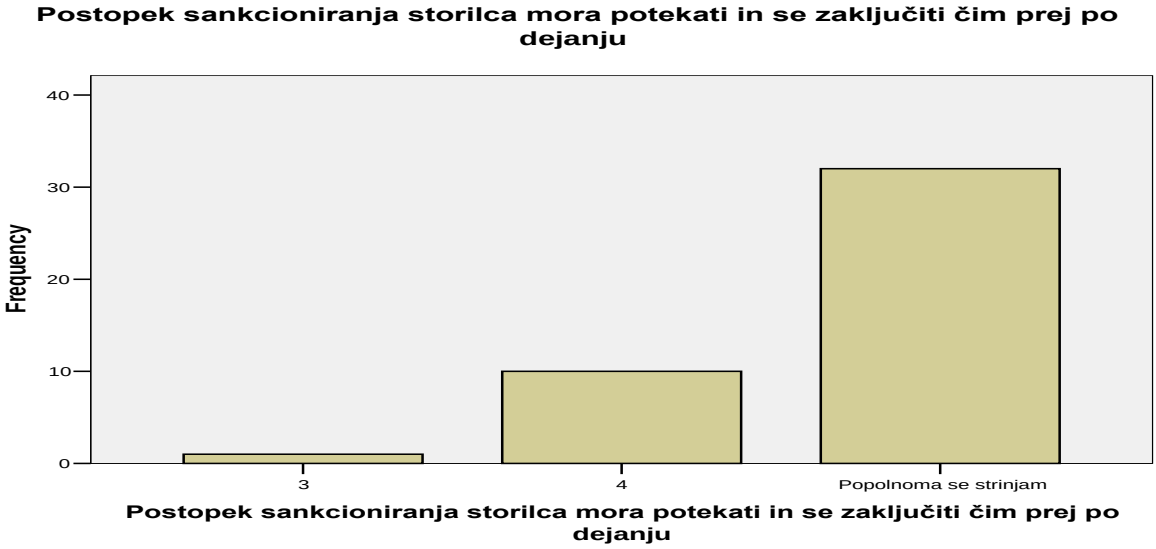
S trditvijo »striktno izvajanje zakonodaje vpliva na bodoče storilce« se popolnoma strinja 37,2% vprašanih, večinoma strinja 34,9%, tistih, ki se s trditvijo ne strinjajo, pa je skupaj 4,7%. Trditev je dosegla aritmetično sredino v višini 4,02. Standardni odklon je znašal 0,963, varianca pa 0,928.



Trditev »povečanje števila odkritih storilcev vpliva na zmanjševanje izvrševanja zlorab« je dosegla aritmetično sredino v višini 3,84. S trditvijo se je popolnoma strinjalo 27,9% vprašanih, večinoma se je strinjalo 32,6% vprašanih. Takšnih, ki se s trditvijo niso strinjali, je bilo 4,7%. Standardni odklon je znašal 0,898, varianca a pa 0,806.

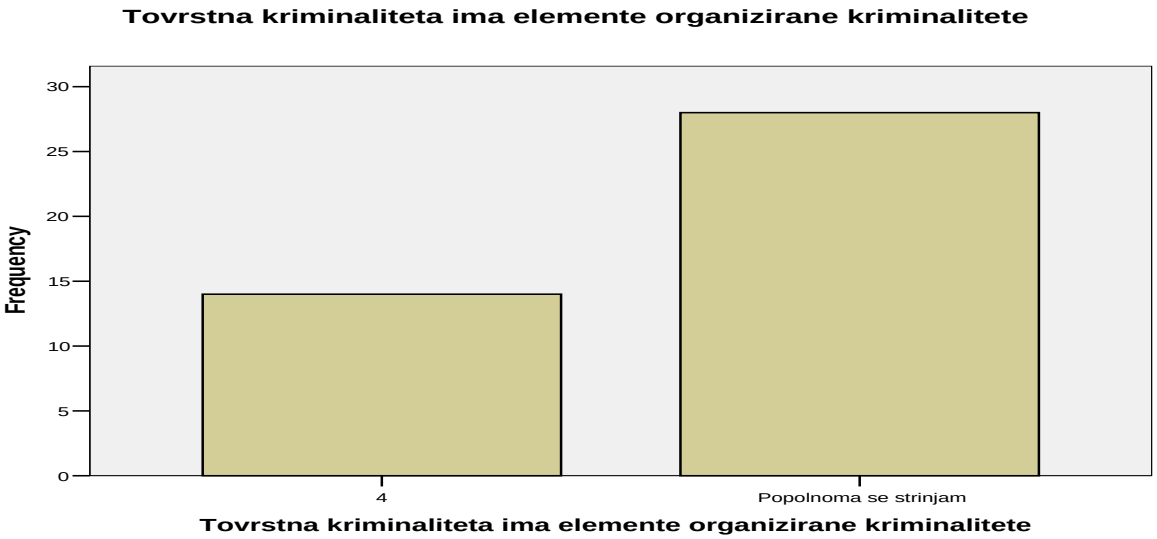
Na trditev »veliko število obsojenih storilcev vpliva na zmanjšanje števila tistih, ki se odločajo za zlorabe« je z odgovorom popolnoma se strinjam odgovorilo 25,6% vprašanih, večinoma se strinjam je odgovorilo 34,9% in strinjam se 32,6%. Takšnih, ki se s trditvijo niso strinjali, je bilo skupaj 7%. Trditev je dosegla aritmetično sredino v višini 3,77. Standardni odklon je znašal 0,972, varianca pa 0,945.

S trditvijo »postopek sankcioniranja storilca mora potekati in se zaključiti čim prej po dejanju« se je popolnoma strinjalo 74,4% vprašanih in večinoma strinjalo 23,3% vprašanih. Takšnih, ki se s trditvijo ne bi strinjali, ni bilo. Trditev je dosegla aritmetično sredino v višini 4,72. Standardni odklon je znašal 0,504, varianca pa 0,254.



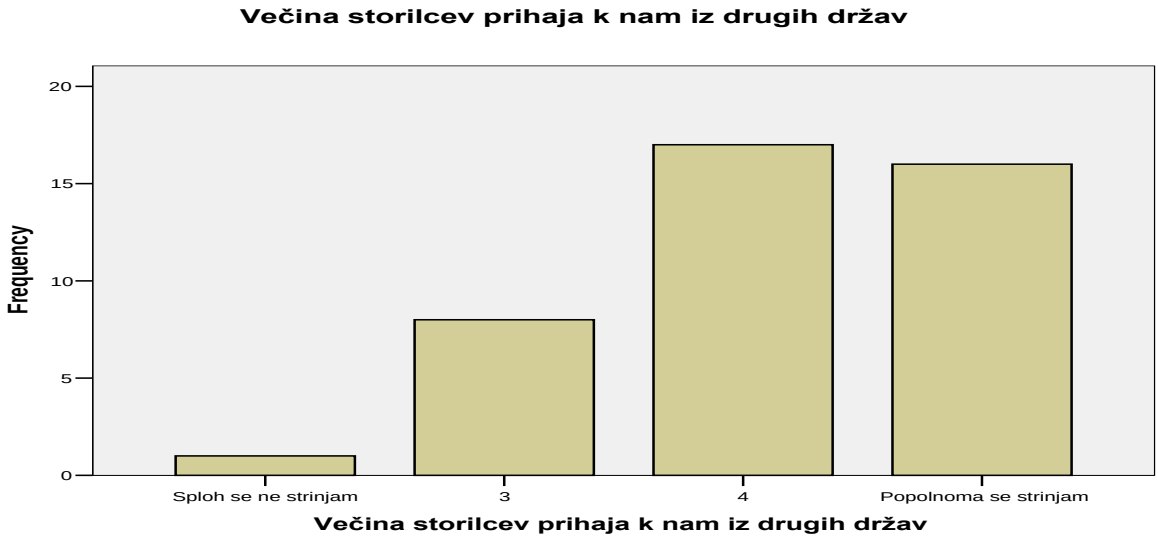
Trditev »storilci na tem področju so zelo dobro organizirani« je dosegla aritmetično sredino 4,55. S trditvijo se je popolnoma strinjalo 58,1% in večinoma strinjalo 34,9% vprašanih. Tistih, ki se s trditvijo niso strinjali, ni bilo. Standardni odklon je znašal 0,593, varianca pa 0,351.

S trditvijo »tovrstna kriminaliteta ima elemente organizirane kriminalitete« se je popolnoma strinjalo 65,1% vprašanih in večinoma strinjalo 32,6% vprašanih. Trditev je dosegla aritmetično sredino v višini 4,67. Odgovorov, ki se s trditvijo ne bi strinjali, ni bilo. Standardni odklon je znašal 0,477, varianca pa 0,228.



Na trditev »storilci ne smejo obdržati premoženjske koristi, ki so jo z zlorabo pridobili« je z odgovorom popolnoma se strinjam odgovorilo 95,3% vprašanih in večinoma se strinjam 4,7%. Takšnih, ki se s trditvijo ne bi strinjali, ni bilo, trditev pa je dosegla zelo visoko aritmetično sredino v višini 4,95. Standardni odklon je znašal 0,213, varianca pa 0,045.

S trditvijo »večina storilcev prihaja k nam iz drugih držav« se je popolnoma strinjalo 37,2% vprašanih, večinoma strinjalo 39,5% vprašanih in strinjalo 18,6% vprašanih. Takšnih, ki se s trditvijo niso strinjali, je bilo 2,3%. Trditev je dosegla aritmetično sredino v višini 4,12. Standardni odklon je znašal 0,889, varianca pa 0,790.



Aritmetične sredine ($\bar{x}$), standardni odkloni (SD) in variance (V), ki smo jih dobili z analizo, so prikazani v tabeli.

Tabela 13: Represivni dejavniki

Vprašanje	$\bar{x}$	SD	V
c1: Dobra zakonodaja, ki sankcionira zlorabe, je pomembna za preprečevanje zlorab	4,05	0,950	0,903
c2: Storilce zlorab je potrebno sankcionirati	4,86	0,351	0,123
c3: Višja zagrožena kazen vodi k zmanjšanju zlorab	3,37	0,952	0,906
c4: Striktno izvajanje zakonodaje vpliva na bodoče storilce	4,02	0,963	0,928
c5: Povečanje števila odkritih storilcev vpliva na zmanjševanje izvrševanja zlorab	3,84	0,898	0,806
c6: Št. obsojenih storilcev vpliva na zmanjšanje št. tistih, ki se odločajo za zlorabe	3,77	0,972	0,945
c7: Postopek sankcioniranja storilca mora potekati in se zaključiti čim prej po dejanju	4,72	0,504	0,254
c8: Storilci na tem področju so zelo dobro organizirani	4,55	0,593	0,351
c9: Tovrstna kriminaliteta ima elemente organizirane kriminalitete	4,67	0,477	0,228
c10: Storilci ne smejo obdržati premoženjske koristi, ki so si jo z zlorabo pridobili	4,95	0,213	0,045
c11: Večina storilcev prihaja k nam iz drugih držav	4,12	0,889	0,790

8.3 Faktorska analiza

S pomočjo faktorske analize bomo na podlagi večjega števila opazovanih spremenljivk in z upoštevanjem odvisnosti med njimi opredelili manjše število novih spremenljivk, ki so povezane po skupnih lastnostih. Te nove množice spremenljivk se imenujejo faktorji.
Cilji faktorske analize so naslednji (Sharma 1996, 99):

- določiti majhno število skupnih faktorjev, ki najbolje pojasnjujejo povezave med opazovanimi spremenljivkami
- opredeliti vsebinsko najprimernejše faktorje
- oceniti faktorske uteži, komunalitete in specifične variance opazovanih spremenljivk
- pojasniti vsebino skupnih faktorjev.

Glede na sestavo samega vprašalnika na tri vsebinske sklope (splošna varnost in razvoj področja, preventivni dejavniki, represivni dejavniki) smo s faktorsko analizo skušali tudi preveriti, če se posamezne, neposredno merjene spremenljivke povezujejo v podobne sklope. Zato smo izbrali 3 faktorje.

Najprej smo preverili primernost podatkov za izvedbo faktorske analize. Izločiti je bilo potrebno veliko spremenljivk (nekaj zaradi nenormalne porazdelitve, nekaj zaradi prenizkih komunalitet – pod 0,4), ostalo jih je 18. Glede na to, da je brezgotovinsko poslovanje sestavljeno iz več med seboj prepletenih delov, lahko pričakujemo, da bodo dobljeni faktorji med seboj korelirali, na podlagi česar sklepamo, da bo ustreznejšo faktorsko strukturo pokazalo poševno rotiranje, zato izberemo Direct Oblimin rotacijo.

8.3.1 Zanesljivost vprašalnika

Zanesljivost vprašalnika smo izračunali s pomočjo Cronbachovega koeficienta α. V vprašalniku je bila uporabljena 5-stopenjska Likertova lestvica (od 1 – sploh se ne strinjam, do 5 – popolnoma se strinjam). Cronbachov koeficient α smo izračunali za celoten vprašalnik oziroma za 18 spremenljivk, ki smo jih v nadaljevanju upoštevali pri faktorski analizi. Vrednost Cronbachovega koeficienta α znaša 0,848, zato lahko zaključimo, da je naš vprašalnik dovolj zanesljiv.

8.3.2 KMO in Bartlettov test

Primernost vzorca smo preverili s Kaiser-Meyer-Olkinovo mero (KMO) statistične ustreznosti in Bartlettovim testom. KMO mera ustreznosti vzorca nam pokaže, ali so podatki ustrezni za faktorsko analizo. Višja kot je mera KMO, bolj so podatki ustrezni. Optimalno je, da je KMO večja od 0,8, še sprejemljiva mera pa je med 0,5 in 0,6; pod 0,5 podatki niso ustrezni za faktorsko analizo. V našem primeru znaša KMO 0,618 (tabela 14), kar pomeni, da faktorsko analizo lahko izvedemo. Nekoliko nižjo vrednost lahko pripišemo velikosti vzorca (N = 41), ki je dokaj nizka, vendar pa je vprašalnik rešilo 80 % strokovnjakov s tega področja v Sloveniji. Bartlettov test pa preverja, ali je korelacijska matrika enotska (v praksi bi to pomenilo, da med spremenljivkami zveza ne obstaja). Če je stopnja statistične značilnosti manjša od 0,05, potem lahko rečemo, da matrika ni enotska (med spremenljivkami zveza obstaja) in da so podatki ustrezni za nadaljnjo analizo. Tako je tudi v našem primeru (tabela 14) in so vse korelacije med spremenljivkami statistično pomembne.

Tabela 14: Rezultati KMO in Bartlettovega testa

Kaiser-Meyer-Olkinova mera ustreznosti vzorca		0,618
Bartlettov test	Approx. χ^2	427,937
	df	153
	Sig.	0,000

8.3.3 Komunaliteta

Komunalitete nam prikazujejo, kakšna je pojasnjenost pojasnjevalne spremenljivke s faktorji. Večja, kot je korelacijska vrednost, boljši je faktor (Mencinger, 2005). Vrednost naj ne bi padla pod 0,4 oziroma 40 %. Vrednosti komunalitet naših 18 spremenljivk so prikazane v tabeli 15.

Tabela 15: Komunalitete

	Začetna	Ekstrahirana
Varnost poslovanja je odvisna tudi od organizacijskih rešitev.	1,000	0,560
Nakup preko manj poznanih spletnih strani povečuje možnost zlorab.	1,000	0,688
Informacijski sistem mora imeti jasno določene odzive v primerih zlorab.	1,000	0,412
Uporabnike je potrebno obveščati o možnostih in nevarnostih zlorab.	1,000	0,467
Tudi uporabniki storitev morajo skrbeti za varnost poslovanja.	1,000	0,541
Za preprečevanje in odkrivanje zlorab je potrebno sodelovanje med izdajatelji kartic.	1,000	0,714
Storilci ne poznajo meja in zato je potrebno sodelovati s tujimi finančnimi institucijami.	1,000	0,745
Vloga oskrbnikov bančnih avtomatov in policije je pomembna za odkrivanje storilcev zlorab.	1,000	0,484
Kakovosten pretok informacij o zlorabah povečuje možnost odkritja storilca.	1,000	0,402
Dobra zakonodaja, ki sankcionira in opredeljuje zlorabe, je pomembna za preprečevanje zlorab.	1,000	0,552

Storilce zlorab je potrebno sankcionirati.	1,000	0,565
Višja zagrožena kazen vodi k zmanjševanju zlorab.	1,000	0,685
Striktno izvajanje zakonodaje vpliva na bodoče storilce.	1,000	0,683
Povečanje števila odkritih storilcev vpliva na zmanjševanje izvrševanja zlorab.	1,000	0,757
Veliko število obsojenih storilcev vpliva na zmanjšanje števila tistih, ki odločajo za zlorabe.	1,000	0,737
Storilci na tem področju so zelo dobro organizirani.	1,000	0,747
Tovrstna kriminaliteta ima elemente organizirane kriminalitete.	1,000	0,712
Večina storilcev prihaja k nam iz drugih držav.	1,000	0,554

Iz tabele številka 15 je razvidno, da nobena spremenljivka ne pade pod vrednost 0,4, zato lahko vseh teh 18 spremenljivk povežemo s skupnimi faktorji. Največ skupne variance je pojasnjene pri spremenljivki »Povečanje števila odkritih storilcev vpliva na zmanjšanje števila tistih, ki odločajo za zlorabe« (75,7 %), najmanj pa pri spremenljivki »Kakovosten pretok informacij o zlorabah povečuje možnost odkritja storilca« (40,2 %).

8.3.4 Celotna pojasnitev variance

V tabeli 16 so prikazane vrednosti celotne pojasnjene variance. Izbrali smo metodo glavnih komponent, 3 faktorje ter Direct Oblimin rotacijo.

Tabela 16: Celotna pojasnjena varianca

	Začetna lastna vrednost			Ekstrahirani seštevek kvadratov			Rotirani
Faktorji	Skupaj	% variance	Kumulativni %	Skupaj	% variance	Kumulativni %	Skupaj
1	5,709	31,718	31,718	5,709	31,718	31,718	4,339
2	3,003	16,682	48,400	3,003	16,682	48,400	3,847
3	2,290	12,724	61,124	2,290	12,724	61,124	3,867
4	1,160	6,447	67,571				
5	1,009	5,607	73,178				
6	0,803	4,460	77,638				
7	0,743	4,128	81,766				
8	0,623	3,464	85,229				
9	0,572	3,178	88,407				
10	0,509	2,829	91,236				
11	0,348	1,936	93,172				
12	0,331	1,840	95,012				
13	0,275	1,528	96,540				
14	0,213	1,181	97,721				
15	0,174	0,967	98,688				
16	0,106	0,588	99,276				
17	0,080	0,445	99,721				
18	0,050	0,279	100,000				

Tri faktorje smo izbrali zato, ker smo skušali ugotoviti, če se posamezne, neposredno merjene spremenljivke, povezujejo v podobne sklope, kot smo jih predvideli z vprašalnikom. Če bi izbrali kriterij začetnih lastnih vrednosti (= 1), bi dobili 5 faktorjev, vendar pa je med 3. in 4. faktorjem večji skok v odstotku pojasnjene variance, poleg tega pa s tremi izločenimi faktorji pojasnimo kar 61,124 % celotne variance. Prvi faktor pojasni 31,718 % variance, drugi 16,682 %, tretji pa 12,724 %. Ostalo varianco (38,876 %) lahko pripišemo specifičnim faktorjem, katerih ne moremo pojasniti z vključenimi spremenljivkami.

8.3.5 Matrika faktorskih uteži

Na osnovi matrike faktorskih uteži smo združili spremenljivke v nove tri faktorje ter jih tudi na novo poimenovali. V tabeli 17 so prikazane faktorske uteži posameznih spremenljivk v tistem stolpcu, katerega faktorju pripadajo.

Tabela 17: Matrika faktorskih uteži

Zap. št. sprem. glede na sklop iz vprašalnika	Ime spremenljivke	Faktorji		
		1	2	3
b24	Za preprečevanje in odkrivanje zlorab je potrebno sodelovanje med izdajatelji kartic.	0,863		
b25	Storilci ne poznajo meja in zato je potrebno sodelovati s tujimi finančnimi institucijami.	0,862		
c11	Večina storilcev prihaja k nam iz drugih držav.	0,632		
a13	Varnost poslovanja je odvisna tudi od organizacijskih rešitev.	0,618		
b2	Informacijski sistem mora imeti jasno določene odzive v primerih zlorab.	0,587		
b28	Kakovosten pretok informacij o zlorabah povečuje možnost odkritja storilca.	0,556		
c5	Povečanje števila odkritih storilcev vpliva na zmanjševanje izvrševanja zlorab.		0,864	
c4	Striktno izvajanje zakonodaje vpliva na bodoče storilce.		0,840	
c6	Veliko število obsojenih storilcev vpliva na zmanjšanje števila tistih, ki odločajo za zlorabe.		0,829	
c3	Višja zagrožena kazen vodi k zmanjševanju zlorab.		0,753	
c11	Dobra zakonodaja, ki sankcionira in opredeljuje zlorabe, je pomembna za preprečevanje zlorab.		0,508	
b7	Nakup preko manj poznanih spletnih strani povečuje možnost zlorab.			0,792
c2	Storilce zlorab je potrebno sankcionirati.			0,716
c9	Tovrstna kriminaliteta ima elemente organizirane kriminalitete.			0,711
c8	Storilci na tem področju so zelo dobro organizirani.			0,675
b14	Uporabnike je potrebno obveščati o možnostih in nevarnostih zlorab.			0,675
b16	Tudi uporabniki storitev morajo skrbeti za varnost poslovanja.			0,640
b26	Vloga oskrbnikov bančnih avtomatov in policije je pomembna za odkrivanje storilcev zlorab.			0,401

Iz tabele 17 je razvidno, da drugi faktor v celoti ustreza sklopu c, zato ga poimenujemo kar REPRESIVNI DEJAVNIKI, prvi in drugi faktor pa delno ustrezata drugemu, delno tretjemu sklopu. Tretji faktor ima višje vrednosti faktorskih uteži glede spremenljivk, ki opisujejo zlorabe, zato poimenujemo ZLORABE, prvi faktor pa se nanaša bolj na preprečevanje zlorab, zato ga tudi poimenujemo PREPREČEVANJE ZLORAB.

Prvi faktor PREPREČEVANJE ZLORAB pojasni torej 31,718 % variance, vanj pa smo uvrstili naslednje spremenljivke:

- Za preprečevanje in odkrivanje zlorab je potrebno sodelovanje med izdajatelji kartic.
- Storilci ne poznajo meja in zato je potrebno sodelovati s tujimi finančnimi institucijami.
- Večina storilcev prihaja k nam iz drugih držav.
- Varnost poslovanja je odvisna tudi od organizacijskih rešitev.
- Informacijski sistem mora imeti jasno določene odzive v primerih zlorab.
- Kakovosten pretok informacij o zlorabah povečuje možnost odkritja storilca.

Drugi faktor REPRESIVNI DEJAVNIKI pojasni 16,682 % variance, vanj pa smo uvrstili naslednje spremenljivke:

- Povečanje števila odkritih storilcev vpliva na zmanjševanje izvrševanja zlorab.
- Striktno izvajanje zakonodaje vpliva na bodoče storilce.
- Veliko število obsojenih storilcev vpliva na zmanjšanje števila tistih, ki odločajo za zlorabe.
- Višja zagrožena kazen vodi k zmanjševanju zlorab.
- Dobra zakonodaja, ki sankcionira in opredeljuje zlorabe, je pomembna za preprečevanje zlorab.

Tretji faktor ZLORABE pa pojasni 12,724 % variance, vanj pa smo uvrstili naslednje spremenljivke:

- Nakup preko manj poznanih spletnih strani povečuje možnost zlorab.
- Storilce zlorab je potrebno sankcionirati.
- Tovrstna kriminaliteta ima elemente organizirane kriminalitete.
- Storilci na tem področju so zelo dobro organizirani.
- Uporabnike je potrebno obveščati o možnostih in nevarnostih zlorab.
- Tudi uporabniki storitev morajo skrbeti za varnost poslovanja.

- Vloga oskrbnikov bančnih avtomatov in policije je pomembna za odkrivanje storilcev zlorab.

8.3.6 Korelacije med faktorji

V tabeli 18 so prikazane korelacije med faktorji, ki pa so statistično značilne.

Tabela 18: Korelacije med faktorji

		PREPREČEVANJE ZLORAB	REPRESIVNI DEJAVNIKI	ZLORABE
PREPREČEVANJE ZLORAB	Pearson Correlation	1	,456**	,397**
	Sig. (2-tailed)		,002	,008
	N	43	43	43
REPRESIVNI DEJAVNIKI	Pearson Correlation	,456**	1	,335*
	Sig. (2-tailed)	,002		,028
	N	43	43	43
ZLORABE	Pearson Correlation	,397**	,335*	1
	Sig. (2-tailed)	,008	,028	
	N	43	43	43

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Vidimo, da so vse korelacije med faktorji pozitivne in statistično značilne. Najbolj sta povezana faktorja PREPREČEVANJE ZLORAB in REPRESIVNI DEJAVNIKI (R = 0,456), sledi povezava med faktorjema ZLORABE in PREPREČEVANJE ZLORAB (R = 0,397) in nato še med faktorjema ZLORABE in REPRESIVNI DEJAVNIKI (R = 0,335). Glede na vrednosti Pearsonovega koeficienta (R) lahko rečemo, da je povezanost med faktorji srednja.

8.3.7 Analiza variance

- **primerjava faktorjev glede na spol**

Tabela 19: Skupna statistika

Spol		Povpr. vrednost	Stand. odklon	N
Moški	PREPREČEVANJE ZLORAB	4,62	0,401	22
	REPRESIVNI DEJAVNIKI	3,87	0,792	22
	ZLORABE	4,41	0,504	22
Ženski	PREPREČEVANJE ZLORAB	4,63	0,365	14
	REPRESIVNI DEJAVNIKI	3,74	0,681	14
	ZLORABE	4,83	0,258	14

Tabela 20: Testiranje enakosti aritmetičnih sredin

	Wilks' Lambda	F	df1	df2	Sig.
PREPREČEVANJE ZLORAB	1,000	0,010	1	34	0,919
REPRESIVNI DEJAVNIKI	0,993	0,229	1	34	0,635
ZLORABE	0,807	8,112	1	34	0,007

Iz tabele 20 je razvidno, da so statistično pomembne razlike glede na spol samo pri faktorju ZLORABE, saj je vrednost $\alpha < 0,05$. Iz tabele 19 vidimo, da se ženske bolj strinjajo s trditvami o zlorabah (povpr. vrednost je 4,83) kot moški (povpr. vrednost je 4,41).

- **Primerjava faktorjev glede na starost**

Analiza variance ni pokazala nobene statistično pomembne razlike glede na starost.

- **Primerjava faktorjev glede na izobrazbo**

Analiza variance ni pokazala nobene statistično pomembne razlike glede na izobrazbo.

- **Primerjava faktorjev glede na skupno delovno dobo**

Analiza variance ni pokazala nobene statistično pomembne razlike glede na skupno delovno dobo.

- **Primerjava faktorjev glede na delovno dobo na področju kartičnega prometa**

Analiza variance ni pokazala nobene statistično pomembne razlike glede na delovno dobo na področju kartičnega prometa.

8.4 Preverjanje hipotez

V nalogi smo si zastavili naslednje hipoteze:

H1. Gospodarska kriminaliteta, kamor spada področje elektronskih plačilnih sistemov, se neprestano spreminja in posodablja.

Tako celotno področje gospodarske kriminalitete, kakor tudi področje kriminalitete na področju elektronskih plačilnih sistemov, se s časom, predvsem zaradi novih tehnično – tehnoloških rešitev, neprestano spreminja in posodablja. Na področju zlorab elektronskega bančništva smo priče vedno novih načinov izvajanja zlorab, ki se prilagajajo novim zaščitnim mehanizmom oz. novi organizaciji preprečevanja zlorab in zaščit elektronskih sistemov.
Hipotezo smo preverjali z vprašanjem »Storilci se prilagodijo zaščitnim mehanizmom in najdejo nove načine za izvajanje zlorab«. Hipotezo bomo potrdili, če bo povprečna vrednost vsaj 3,5 (merjeno na lestvici od 1-5).
Postavili smo ničelno in nasprotno hipotezo:
H_0: Storilci se prilagodijo zaščitnim mehanizmom in najdejo nove načine za izvajanje zlorab ($\mu \geq 3{,}5$).
H_1: Storilci se ne prilagodijo zaščitnim mehanizmom in ne najdejo novih načinov za izvajanje zlorab ($\mu < 3{,}5$).
Ničelno hipotezo (in s tem tudi našo) bomo sprejeli, če je povprečna ocena μ celotne populacije strokovnjakov, ki je določala vzorčni okvir, najmanj 3,5.

Stopnja pomembnosti tega testa kot tudi vseh nadaljnjih bo α = 0,05. Statistično izvedbo tega testa naslonimo na statistiko (t-test): $t = \frac{\bar{X} - 3}{s}\sqrt{n}$, ki je zaradi velikega vzorca (>30)

standardizirana normalna slučajna spremenljivka. V njej je $\bar{X}$ aritmetična sredina vzorca, s standardni odklon, n pa velikost vzorca.

Povprečna ocena podatkov vzorca je $\bar{X} = 4,47$ in standardni odklon $s = 0,667$, velikost vzorca pa $n = 43$ (toliko je odgovorov na postavljeno trditev), medtem ko je 95 % interval zaupanja za $\bar{X}$ enak (4,26; 4,67). Ničelno hipotezo bomo zavrnili, če bo vrednost statistike testa hipoteze padla pod kritično vrednost standardizirane normalne slučajne spremenljivke . Iz podatkov vzorca izračunamo vrednost $t = 9,485$, kar je nad kritično vrednostjo in zato ničelne hipoteze ne zavrnemo. Postavljeno hipotezo lahko torej v celoti potrdimo.

H2. Za preprečevanje zlorab je potrebno izdelati učinkovit varnostni model, ki bo zmanjšal možnost zlorab.

Za zmanjšanje zlorab je potreben učinkovit varnostni model, ki zajema različne dejavnike, ki vplivajo na možnost izvrševanja zlorab. V samem vprašalniku je bilo postavljenih več vprašanj, ki opredeljujejo učinkovitost in potrebnost zastavljenega modela v praksi pri preprečevanju zlorab. S faktorsko analizo smo ta vprašanja povezali v skupen faktor PREPREČEVANJE ZLORAB, na katerega lahko naslonimo testiranje hipoteze. Hipotezo bomo potrdili, če bo povprečna vrednost faktorja vsaj 3,5 (merjeno na lestvici od 1 do 5).

H_0 in H_1 se torej glasita:

H_0: Za preprečevanje zlorab je potrebno izdelati učinkovit varnostni model ($\mu \geq 3,5$).

H_1: Za preprečevanje zlorab ne potrebujemo učinkovitega varnostnega modela ($\mu < 3,5$).

Ničelno hipotezo (in s tem tudi našo) bomo sprejeli, če je povprečna ocena μ celotne populacije strokovnjakov, ki je določala vzorčni okvir, najmanj 3,5.

Stopnja pomembnosti tega testa je α = 0,05. Statistično izvedbo tega testa naslonimo na statistiko (t-test): $t = \frac{\bar{X} - 3}{s}\sqrt{n}$, ki je zaradi velikega vzorca (>30) standardizirana normalna slučajna spremenljivka. V njej je $\bar{X}$ aritmetična sredina vzorca, s standardni odklon, n pa velikost vzorca.

Povprečna ocena podatkov vzorca (faktorja PREPREČEVANJE ZLORAB) je $\bar{X} = 4,61$ in standardni odklon $s = 0,385$, velikost vzorca pa $n = 43$, medtem ko je 95 % interval zaupanja za $\bar{X}$ enak (4,49; 4,73). Ničelno hipotezo bomo zavrnili, če bo vrednost statistike testa hipoteze padla pod kritično vrednost standardizirane normalne slučajne spremenljivke .

Iz podatkov vzorca izračunamo vrednost $t = 18,903$, kar je nad kritično vrednostjo in zato ničelne hipoteze ne zavrnemo. Našo postavljeno hipotezo lahko torej v celoti potrdimo.

H3. Za zmanjšanje zlorab je potrebno sprejeti učinkovite varnostne ukrepe na samih informacijskih sistemih, urediti in definirati nadzor sistemov, sporočanje, obveščanje in povezovanje različnih institucij, ki skrbijo za varnost plačilnih sistemov.

Ukrepi, ki smo jih opisali v varnostnem modelu preprečevanja zlorab in se nanašajo na zaščito varnostnih sistemov pred zlorabami, potrjujejo, da samo učinkoviti ukrepi lahko zmanjšajo možnosti za zlorabe. Prav tako je definiran tudi nadzor nad sistemi, obveščanje in povezovanje med različnimi službami in institucijami pa je pri nas predpisan celo v posebnih priporočilih, ki so jih sprejeli vsi udeleženci, ki skrbijo za varnost poslovanja. V vprašalniku smo postavili več vprašanj vezanih na to tematiko (tehnično-tehnološki in organizacijski dejavniki), potrjevanje H3 pa bomo vezali na vprašanje »Informacijski sistem mora imeti jasno določene odzive v primerih zlorab«. Hipotezo bomo potrdili, če bo povprečna vrednost spremenljivke vsaj 3,5 (merjeno na lestvici od 1 do 5).

H_0 in H_1 se torej glasita:

H_0: Informacijski sistem mora imeti jasno določene odzive v primerih zlorab ($\mu \geq 3,5$).

H_1: Ni potrebno, da ima informacijski sistem jasno določene odzive v primerih zlorab ($\mu < 3,5$).

Ničelno hipotezo (in s tem tudi našo) bomo sprejeli, če je povprečna ocena μ celotne populacije strokovnjakov, ki je določala vzorčni okvir, najmanj 3,5.

Statistično izvedbo tega testa naslonimo na statistiko (t-test): $t = \frac{\bar{X} - 3}{s}\sqrt{n}$, ki je zaradi velikega vzorca (>30) standardizirana normalna slučajna spremenljivka. V njej je $\bar{X}$ aritmetična sredina vzorca, s standardni odklon, n pa velikost vzorca.

Povprečna ocena podatkov vzorca je $\bar{X} = 4,91$ in standardni odklon $s = 0,294$, velikost vzorca pa $n = 43$, medtem ko je 95 % interval zaupanja za $\bar{X}$ enak (4,82; 5,00). Ničelno hipotezo bomo zavrnili, če bo vrednost statistike testa hipoteze padla pod kritično vrednost standardizirane normalne slučajne spremenljivke (pri α = 0,05). Iz podatkov vzorca izračunamo vrednost $t = 31,392$, kar je močno nad kritično vrednostjo in zato ničelne hipoteze ne zavrnemo. Našo postavljeno hipotezo torej v celoti potrdimo.

H4. Varnostni model mora biti zasnovan tako, da bo omogočal takojšnje odzive na spremembe problematike področja in se bo lahko fleksibilno prilagajal novim, kompleksnejšim oblikam zlorab.

Že pri prvi postavljeni hipotezi, ki govori o stalnem spreminjanju načinov izvrševanja zlorab na tam področju, smo ugotovili, da hipoteza drži. Pri spremenljivih in novih načinih izvrševanja zlorab je potreben tudi takšen varnostni model, ki bo omogočal sprotne odzive na spremembe in se z dodatnimi ukrepi zaščite prilagajal novim oblikam zlorab. Hipotezo lahko v celoti potrdimo, saj smo tudi na postavljena vprašanja dobili odgovore, ki hipotezo potrjujejo. Tako smo na postavljeno vprašanje »tehnična in tehnološka zaščita mora slediti razvoju« dobili visoko povprečno vrednost odgovorov v višini 4,98 in standardnim odklonom 0,152. Hipotezo smo preverili še s t-testom: $t = \frac{\bar{X} - 3}{s}\sqrt{n}$, ki je zaradi velikega vzorca (>30) standardizirana normalna slučajna spremenljivka ($\bar{X}$ je aritmetična sredina vzorca, s standardni odklon, n pa velikost vzorca).

Za testiranje hipoteze smo zopet postavili H_0 in H_1:

H_0: Tehnična in tehnološka zaščita morata slediti razvoju ($\mu \geq 3{,}5$).

H_1: Ni potrebno, da tehnična in tehnološka zaščita sledita razvoju ($\mu < 3{,}5$).

95 % interval zaupanja za $\bar{X}$ je enak (4,93; 5,02). Ničelno hipotezo bomo zavrnili, če bo vrednost statistike testa hipoteze padla pod kritično vrednost standardizirane normalne slučajne spremenljivke (pri α = 0,05). Iz podatkov vzorca izračunamo vrednost $t = 63{,}500$,kar je močno nad kritično vrednostjo in zato ničelne hipoteze ne zavrnemo. Našo postavljeno hipotezo torej v celoti potrdimo.

H5. Uspešno in učinkovito preprečevanje zlorab v elektronskih plačilnih sistemih je mogoče le ob celovitem modelu zagotavljanja varnosti

Hipotezo lahko potrdimo, saj smo z vprašalnikom preverjali delovanje zastavljenega modela, ki vključuje različne dejavnike, v praksi. Odgovori na postavljena vprašanja s precej visokimi povprečnimi vrednostmi odgovorov so potrdili, de je učinkovito preprečevanje zlorab možno le ob celovitem modelu zagotavljanja varnosti.

Hipotezo smo preverili na podlagi treh spremenljivk, in sicer:

- Za zmanjšanje zlorab je potrebno usposabljanje zaposlenih na tem področju.
- Tehnično-tehnološke rešitve lahko omejijo izvajanje zlorab.

- Varnost poslovanja je odvisna tudi od organizacijskih rešitev.

Hipotezo smo preverili s t-testom: $t = \frac{\bar{X} - 3}{s}\sqrt{n}$ za vsako posamezno spremenljivko.

H_0 in H_1 se torej vežeta na vse tri trditve in velja:

H_0: $\mu \geq 3{,}5$

H_1: $\mu < 3{,}5$

Ničelno hipotezo bomo zavrnili, če bo vrednost statistike testa hipoteze padla pod kritično vrednost standardizirane normalne slučajne spremenljivke (pri α = 0,05).

V tabeli 21 so prikazane povprečne vrednosti, standardni odkloni, 95 % intervali zaupanja ter t vrednosti za posamezno spremenljivko (N = 42).

Tabela 21: Izvedba t-testa za H5

			95 % interval zaupanja		
	Povpr. vrednost	Stand. odklon	Spodnja meja	Zgornja meja	t
Za zmanjšanje zlorab je potrebno usposabljanje zaposlenih na tem področju.	4,60	0,627	4,40	4,79	11,635
Tehnično-tehnološke rešitve lahko omejijo izvajanje zlorab.	4,55	0,593	4,36	4,73	11,472
Varnost poslovanja je odvisna tudi od organizacijskih rešitev.	4,33	0,754	4,10	4,57	7,159

Iz tabele 21 lahko razberemo, da pri vseh treh spremenljivkah vrednost t ne pade pod kritično vrednost, zato lahko našo hipotezo v celoti potrdimo.

H6. Varnostni model mora zajemati tudi preventivne dejavnike varnosti, saj lahko tudi na ta način zmanjšamo možnosti zlorab.

Sestavni del zastavljenega modela so preventivni dejavniki. V vprašalniku je bilo o vplivu preventivnih dejavnikov zastavljenih več vprašanj (od c1 – c11). Večina odgovorov je preventivnim dejavnikom dala veliko težo pri zmanjševanju možnosti zlorab. S faktorsko analizo smo dobili tudi skupen faktor REPRESIVNI DEJAVNIKI, na katerega lahko vežemo preverjanje hipoteze. Povprečna vrednost faktorja je 3,82 in standardni odklon 0,705. Hipotezo smo preverili še s t-testom: $t = \frac{\bar{X} - 3}{s}\sqrt{n}$, ki je zaradi velikega vzorca (>30)

standardizirana normalna slučajna spremenljivka ($\bar{X}$ je aritmetična sredina vzorca, s standardni odklon, n pa velikost vzorca).

Za testiranje hipoteze smo zopet postavili H_0 in H_1:

H_0: Uspešno in učinkovito preprečevanje zlorab v elektronskih plačilnih sistemih je mogoče le ob celovitem modelu zagotavljanja varnosti ($\mu \geq 3{,}5$).

H_1: Za uspešno in učinkovito preprečevanje zlorab v elektronskih plačilnih sistemih ni potrebno vzpostaviti celovitega modela zagotavljanja varnosti ($\mu < 3{,}5$).

95 % interval zaupanja za $\bar{X}$ je enak (3,61; 4,04). Ničelno hipotezo bomo zavrnili, če bo vrednost statistike testa hipoteze padla pod kritično vrednost standardizirane normalne slučajne spremenljivke (pri α = 0,05). Iz podatkov vzorca izračunamo vrednost $\mathbf{t = 3{,}019}$, kar je nad kritično vrednostjo in zato ničelne hipoteze ne zavrnemo. Našo postavljeno hipotezo torej v celoti potrdimo.

H7. Na uresničevanje modela celovite varnosti vpliva nekaj ključnih dejavnikov, ki zagotavljajo uspešno in učinkovito preprečevanje zlorab.

Kot smo ugotovili v modelu celovite varnosti, obstajajo trije ključni dejavniki, ki najbolj vplivajo na varnost poslovanja in na učinkovitost preprečevanja zlorab. To so: izdajatelji kartic, uporabniki, preventivno – kurativni ukrepi in novi načini tehnično – tehnološke zaščite elektronskih sistemov.

Hipotezo smo preverili na podlagi naslednjih spremenljivk:

- *Izdajatelji kartic*

- Za preprečevanje in odkrivanje zlorab je potrebno sodelovanje med izdajatelji kartic.

- *Uporabniki*

- Uporabnike je potrebno obveščati o možnostih in nevarnostih zlorab.
- Dobro obveščen uporabnik skrbneje ravna s kartico.
- Tudi uporabniki storitev morajo skrbeti za varnost poslovanja.
- Obnašanje uporabnika ima vpliv na možnost zlorabe kartice.

-

Preventivno-kurativni ukrepi

- Dobra zakonodaja, ki sankcionira in opredeljuje zlorabe, je pomembna za preprečevanje zlorab.
- Storilce zlorab je potrebno sankcionirati.

- *Tehnično-tehnološke zaščite*

- Dodatne tehnične rešitve na bančnih avtomatih lahko zmanjšajo možnosti zlorab.
- Tehnična in tehnološka zaščita morata slediti razvoju.

Hipotezo smo preverili s t-testom: $t = \frac{\bar{X} - 3}{s}\sqrt{n}$ za vsako posamezno spremenljivko.

H_0 in H_1 se torej vežeta na vse trditve in velja:

H_0: $\mu \geq 3{,}5$

H_1: $\mu < 3{,}5$

Ničelno hipotezo bomo zavrnili, če bo vrednost statistike testa hipoteze padla pod kritično vrednost standardizirane normalne slučajne spremenljivke (pri $\alpha = 0{,}05$).

V tabeli 22 so prikazane povprečne vrednosti, standardni odkloni, 95 % intervali zaupanja ter t vrednosti za posamezno spremenljivko (N = 42).

Tabela 22: Izvedba t-testa za H7

			95 % interval zaupanja		
	Povpr. vrednost	Stand. odklon	Spodnja meja	Zgornja meja	**t**
Za preprečevanje in odkrivanje zlorab je potrebno sodelovanje med izdajatelji kartic.	4,73	0,449	4,59	4,87	17,641
Uporabnike je potrebno obveščati o možnostih in nevarnostih zlorab.	4,66	0,575	4,48	4,84	13,185
Dobro obveščen uporabnik skrbneje ravna s kartico.	4,29	0,782	4,05	4,54	6,810
Tudi uporabniki storitev morajo skrbeti za varnost poslovanja.	4,68	0,650	4,48	4,89	11,950
Obnašanje uporabnika ima vpliv na možnost zlorabe kartice.	4,20	0,813	3,94	4,45	5,475
Dobra zakonodaja, ki sankcionira in opredeljuje zlorabe, je pomembna za preprečevanje zlorab.	4,05	0,947	3,75	4,35	3,772
Storilce zlorab je potrebno sankcionirati.	4,85	0,358	4,74	4,97	25,445
Dodatne tehnične rešitve na bančnih avtomatih lahko zmanjšajo možnosti zlorab.	4,33	0,566	4,15	4,50	9,569
Tehnična in tehnološka zaščita morata slediti razvoju.	4,98	0,152	4,93	5,02	63,500

Iz tabele 22 lahko razberemo, da pri vseh spremenljivkah vrednost t ne pade pod kritično vrednost, zato lahko našo hipotezo v celoti potrdimo.

H8. Celovito varnost je potrebno uravnoteženo prenesti na organizacijske in tehnološke rešitve.

Hipotezo lahko potrdimo, saj je v modelu celovite varnosti pomemben poudarek dan tudi organizacijskim in tehnološkim rešitvam, katere se morajo stalno prilagajati novim načinom zlorab in tehnično – tehnološkemu napredku. Značilnost našega varnostnega modela je ravno organiziranost institucij, ki delujejo na tem področju v okviru Združenja bank Slovenije - Odbora za kartično poslovanje, Delovne skupine za varnost kartičnega poslovanja, katerega zunanji član je tudi policija. Prav tako so tudi vsi ukrepi in postopki ukrepanja vseh sodelujočih natančno določeni v protokolu, varnostni model pa zajema tudi tehnološke rešitve, ki preprečujejo zlorabe.

Hipotezo smo preverili na podlagi dveh spremenljivk, in sicer:

- Tehnično-tehnološke rešitve lahko omejijo izvajanje zlorab.
- Varnost poslovanja je odvisna tudi od organizacijskih rešitev.

Rezultati t-testa za ti dve spremenljivki sta prikazani že v tabeli 21 pri H5. Vidimo, da lahko hipotezo zopet potrdimo.

H9. Celovit varnostni model mora upoštevati mednarodno dimenzijo.

Iz zastavljenega modela in analize zlorab vidimo, da ima značaj zlorab na področju elektronskega bančništva značaj mednarodnega kriminala, saj storilci največkrat prihajajo iz drugih držav in zlorabljajo pri nas kartice imetnikov iz tujine. Zaradi tega je potrebno povezovanje izdajateljev kartic (bank) in tudi vseh institucij, ki preiskujejo in preprečujejo zlorabe. Banke so tako povezane in sodelujejo z domačimi bankami preko Združenja bank Slovenije, kakor tudi mednarodno s tujimi bankami in lastniki licenc tujih kartic. Policija preko Europola in Interpola sodeluje z drugimi policijami, saj brez mednarodnega sodelovanja in upoštevanje mednarodne dimenzije ni mogoče omejevati, še manj pa preiskovati zlorab na tem področju. Hipotezo lahko v celoti potrdimo. Preverili smo jo na podlagi treh spremenljivk, in sicer:

- Večina storilcev prihaja k nam iz drugih držav.
- Za preprečevanje in odkrivanje zlorab je potrebno sodelovanje med izdajatelji kartic.
- Storilci ne poznajo meja in zato je potrebno sodelovati s tujimi finančnimi institucijami.

Hipotezo smo preverili s t-testom: $\mathbf{t = \frac{\bar{X} - 3}{s}\sqrt{n}}$ za vsako posamezno spremenljivko.

H_0 in H_1 se torej vežeta na vse tri trditve in velja:

H_0: $\mu \geq 3{,}5$

H_1: $\mu < 3{,}5$

Ničelno hipotezo bomo zavrnili, če bo vrednost statistike testa hipoteze padla pod kritično vrednost standardizirane normalne slučajne spremenljivke (pri $\alpha = 0{,}05$).

V tabeli 23 so prikazane povprečne vrednosti, standardni odkloni, 95 % intervali zaupanja ter t vrednosti za posamezno spremenljivko (N = 42).

Tabela 23: Izvedba t-testa za H9

			95 % interval zaupanja		
	Povpr. vrednost	Stand. odklon	Spodnja meja	Zgornja meja	**t**
Večina storilcev prihaja k nam iz drugih držav.	4,12	0,889	3,84	4,40	4,513
Za preprečevanje in odkrivanje zlorab je potrebno sodelovanje med izdajatelji kartic.	4,71	0,457	4,57	4,86	17,641
Storilci ne poznajo meja in zato je potrebno sodelovati s tujimi finančnimi institucijami.	4,79	0,415	4,66	4,92	19,443

Iz tabele 23 lahko razberemo, da pri nobeni spremenljivki ne pade vrednost t pod kritično vrednost, zato lahko hipotezo v celoti potrdimo.

H10. Sprememba tehnologije zaščite posameznih delov sistemov in celote se mora prilagajati in nadgrajevati z razvojem tehnično – tehnoloških novosti na področju zaščit sistemov.

Elektronsko bančništvo je relativno nova storitev in uporablja napredne informacijske tehnologije. Zaradi potrebne in zahtevane večje varnosti pri opravljanju plačilnega prometa in prenosu finančnih transakcij po informacijskih sistemih je zahtevana visoka stopnja varnosti sistemov in naprav, ki omogočajo opravljanje transakcij (bančni avtomati, POS terminali, plačilne kartice…). Zato je na področju elektronskega bančništva uporabljena tudi najnovejša zaščitna tehnologija, seveda v obsegu, ki še opravičuje stroške. Velik doprinos k višji stopnji varnosti prinaša tudi tako imenovan pametna kartica z mikroprocesorjem, ki bo po zamenjavi celotne tehnologije in opustitvi magnetnega zapisa zmanjšala možnosti zlorab. Odgovori na vprašanja iz vprašalnika, ki se nanašajo na tehnično zaščito in pametne kartice, so potrdili pomembnost tehnično – tehnološke zaščite in novosti na tem področju. Hipotezo lahko zato potrdimo.

Hipotezo smo preverili na podlagi naslednjih spremenljivk:

- Dodatna gesla in certifikati povečujejo varnost poslovanja.
- Zlorabe podatkov preko lažnih spletnih strani je mogoče zmanjšati z uvedbo varovalnih mehanizmov.

- Informacijski sistemi, ki zaznavajo neobičajno uporabo kartice, pomagajo odkrivati zlorabe.
- Varnostni elementi na kartici omogočajo uspešno zaščito pred ponarejanjem kartice.
- Kartice z vgrajenim čipom bodo zmanjšale možnosti za zlorabe.

Hipotezo smo preverili s t-testom: $t = \frac{\bar{X} - 3}{s}\sqrt{n}$ za vsako posamezno spremenljivko.

H_0 in H_1 se torej vežeta na vseh pet spremenljivk in velja:

H_0: $\mu \geq 3{,}5$

H_1: $\mu < 3{,}5$

Ničelno hipotezo bomo zavrnili, če bo vrednost statistike testa hipoteze padla pod kritično vrednost standardizirane normalne slučajne spremenljivke (pri $\alpha = 0{,}05$).

V tabeli 24 so prikazane povprečne vrednosti, standardni odkloni, 95 % intervali zaupanja ter t vrednosti za posamezno spremenljivko (N = 42).

Tabela 24: Izvedba t-testa za H10

			95 % interval zaupanja		
	Povpr. vrednost	Stand. odklon	Spodnja meja	Zgornja meja	**t**
Dodatna gesla in certifikati povečujejo varnost poslovanja.	4,55	0,593	4,36	4,61	11,472
Zlorabe podatkov preko lažnih spletnih strani je mogoče zmanjšati z uvedbo varovalnih mehanizmov.	4,36	0,727	4,13	4,58	7,893
Informacijski sistemi, ki zaznavajo neobičajno uporabo kartice, pomagajo odkrivati zlorabe.	4,57	0,590	4,39	4,76	11,763
Varnostni elementi na kartici omogočajo uspešno zaščito pred ponarejanjem kartice.	4,02	0,749	3,79	4,26	3,901
Kartice z vgrajenim čipom bodo zmanjšale možnosti za zlorabe.	4,29	0,944	3,99	4,58	5,198

Iz tabele 24 lahko razberemo, da pri vseh spremenljivkah vrednost t ne pade pod kritično vrednost, zato lahko našo hipotezo v celoti potrdimo.

H11. Samo kompleksna obravnava vseh vidikov in institucij, ki delujejo na področju elektronskih plačilnih sistemov, lahko prinese učinkovit varnostni model, ki bo lahko zmanjšal možnosti zlorab. Zavedati pa se moramo, da popolne varnosti na tem področju ni možno doseči, predvsem ne dolgoročno, brez ažurnega prilagajanja varnostnega modela novim razmeram.

Zastavljen model pri nas kompleksno in v celoti obravnava varnost elektronskih informacijskih sistemov in njegovo zaščito pred zlorabami. Samo na tak način lahko pričakujemo ugodne rezultate in zmanjšanje zlorab. Kljub temu pa se vsi, ki skrbijo za varnost na tem področju zavedajo, da popolne zaščite ni in da se bodo zlorabe na tem področju nadaljevale in dogajale še vnaprej, ker bo zaradi vedno več finančnih transakcijah in sredstvih, ki se opravijo in prelivajo preko informacijskih sistemov, vedno obstajal interes storilcev, da nekaj teh sredstev pridobijo zase na nezakonit način. Zaradi tega morajo vsi udeleženci varnostnega modela nenehno bdeti nad spremembami na varnostnem področju in prilagajati model novim razmeram. Hipotezo lahko v celoti potrdimo. Hipotezo smo preverili na podlagi naslednjih spremenljivk:

- Za preprečevanje in odkrivanje zlorab je potrebno sodelovanje med izdajatelji kartic.
- Storilci ne poznajo meja in zato je potrebno sodelovati s tujimi finančnimi institucijami.
- Popolne varnosti poslovanja ni mogoče doseči.

Hipotezo smo preverili s t-testom: $t = \frac{\bar{X} - 3}{s}\sqrt{n}$ za vsako posamezno spremenljivko.

H_0 in H_1 se torej vežeta na vse tri spremenljivke in velja:

H_0: $\mu \geq 3{,}5$

H_1: $\mu < 3{,}5$

Ničelno hipotezo bomo zavrnili, če bo vrednost statistike testa hipoteze padla pod kritično vrednost standardizirane normalne slučajne spremenljivke (pri $\alpha = 0{,}05$).

V tabeli 25 so prikazane povprečne vrednosti, standardni odkloni, 95 % intervali zaupanja ter t vrednosti za posamezno spremenljivko (N = 42).

Tabela 25: Izvedba t-testa za H11

			95 % interval zaupanja		
	Povpr. vrednost	Stand. odklon	Spodnja meja	Zgornja meja	**t**
Za preprečevanje in odkrivanje zlorab je potrebno sodelovanje med izdajatelji kartic.	4,72	0,454	4,58	4,86	17,641
Storilci ne poznajo meja in zato je potrebno sodelovati s tujimi finančnimi institucijami.	4,77	0,427	4,64	4,90	19,443
Popolne varnosti poslovanja ni mogoče doseči	4,58	0,392	4,39	4,77	11,326

Iz tabele 25 lahko razberemo, da pri vseh treh spremenljivkah vrednost t ne pade pod kritično vrednost, zato lahko našo hipotezo v celoti potrdimo.

SKLEP

Ena od značilnosti gospodarske kriminalitete je ravno njeno spreminjanje s časom oz. z razvojem tehnike, tehnologije in storitev. Prav na področju raziskovalne teme, ki smo jo izbrali za preučevanje, to še kako velja. Področje elektronskega plačilnega prometa je v nekaj letih doživelo nesluten razvoj. Zaradi prednosti pred klasičnimi načini plačevanja storitev in blaga se je dokaj hitro uveljavilo tudi pri konservativno naravnanih komitentih, ki niso dovzetni za spremembe v svojih navadah. Prav področje elektronskega plačilnega prometa je zaradi svoje kompleksnosti in zahtevnosti še posebej kritično za spremembe navad komitentov, saj predvsem starejši, tudi računalniško neuki komitenti, z določenim strahom in odporom sprejemajo nove načine poslovanja. Seveda se v ospredju elektronskega bančništva ne pojavljajo zgolj njegove prednosti, ampak se od časa do časa pojavijo tudi ekscesi oz. negativne posledice tehnično – tehnološkega napredka na tem področju. Mislimo seveda na vse mogoče zlorabe, ki se pri nas in v svetu dnevno dogajajo na tem področju. Razlogi, zakaj je to področje še posebej na udaru tistih, ki bi radi brez veliko truda prišli do zaslužka, so seveda različni in jih je več. Prvi med njimi je dejstvo, da se preko elektronskih plačilnih sistemov v negotovinski obliki pretaka velika količina finančnih sredstev. Ob dejstvu, da se obseg gotovinskega plačevanja povsod v svetu zmanjšuje, poleg tega pa so zaščite pred ponarejanjem denarja vse bolj kompleksne in raznovrstne, se storilci seveda odločajo za kriminal na tistem področju, kjer je to omogočeno. Zakaj omogočeno? Zato, ker se zaradi hitrega napredka, želje po čim nižjih stroških in visokem dobičku vse pogosteje vsaj v prvi fazi uvajanja novosti zanemari varnost poslovanja in preprečevanje zlorab. Zaradi tega in zaradi preprostega dejstva, da 100% varnosti ne moremo doseči na nobenem področju človeškega delovanja ne z organizacijskimi, tehničnimi, niti fizičnimi načini varovanja, je prav, da o varnosti govorimo in se ji posvečamo, iščemo rešitve, ki bodo omogočile razmeroma varno poslovanje na področju elektronskih plačilnih sistemov in poskušamo omejiti zlorabe na nizko stopnjo in s tem zmanjšati škodo.

V nalogi smo sledili namenu ugotavljanja dejavnikov, ki vplivajo na varnost poslovanja in na izvajanje raznovrstnih zlorab na tem področju. Na osnovi analize zlorab, njihovega razvrščanja in ugotavljanja vzrokov, ki zlorabe omogočajo, smo opredelili model, ki bi zlorabe zmanjševal oz. jih preprečeval. V modelu so zajeti tako represivni, kakor tudi preventivni dejavniki. Uporabnost modela v praksi smo testirali z anketo med upravljavci varnostnih sistemov v bankah in finančnih institucijah oz. osebami, ki skrbijo za varnost

elektronskih plačilnih sistemov. Poleg ankete smo opravili tudi intervjuje z več strokovnjaki iz tega področja, ki dolga leta v svoji delovni karieri skrbijo za razvoj in tudi varnost elektronskih plačilnih sistemov in so sodelovali tudi pri njihovem uvajanju. Na osnovi rezultatov, ki smo jih dobili, smo opravili analizo odgovorov in preverjali zastavljene hipoteze.

Pri raziskavi smo se soočali z različnimi težavami. Vsi podatki, ki jih banke in druge finančne institucije vodijo in obdelujejo, spadajo med bančne tajnosti, ki so strogo varovane. Področje zlorab v finančnih institucijah je »tabu« tema, ki naj ne bi prišla v javnost, kar brez dvoma vpliva na obnašanje komitentov, ki se lahko zaradi skrbi za svoje finančne vložke odločijo za drugega ponudnika finančnih storitev. Varnost poslovanja namreč vpliva na izbiro finančne institucije komitenta, ki bo skrbela za njegova finančna sredstva, ki pomenijo tudi njegovo življenjsko eksistenco. Zaradi tega vse finančne institucije skrbno varujejo podatke o poslovanju, del katerih so tudi podatki o znesku povzročene škode z različnimi zlorabami pri poslovanju. Ker finančne institucije tržijo tudi licenčne produkte (predvsem na področju kartičnega prometa), so podatki o zlorabah pomembni tudi za imetnika licence, ki na ta način spremlja trženje svojih produktov z željo po čim manjšem številu zlorab. Po drugi strani so podatki o zlorabah pomembni tudi za finančno institucijo, saj se na podlagi števila in vrste zlorab odloča o sredstvih, ki jih bo namenila za zagotavljanje varnosti poslovanja. Podatki o zlorabah se zato v finančnih institucijah vodijo in obdelujejo, vendar se ne zbirajo centralno. Tako nimamo podatkov, koliko je v nekem geografskem področju dejansko zlorab. Pri nas poslovne banke, ki razen nekaterih drugih institucij večinoma delujejo na tem področju, prostovoljno sodelujejo tudi na področju zagotavljanja varnosti v okviru Združenja bank Slovenije. To sodelovanje seveda ne pomeni tudi analize in zbiranja števila in zneska zlorab, saj je to občutljiv podatek in lahko za konkurenco pomeni tudi način za doseganje konkurenčne prednosti. Zaradi tega pri nas in tudi v tujini ni mogoče pridobiti podatka o škodi, povzročeni z zlorabami. Tudi lastniki licenc (EMV) teh podatkov niso pripravljeni dati na razpolago, ne medijem, ne znanstvenikom ali stroki za namene analiz. Kljub temu smo do delnih podatkov, ki se nanašajo na število in zneske zlorab pri elektronskem plačilnem prometu, uspeli priti. Čeprav je lastnik podatkov le – te predstavil na seminarju, zaprtem za javnost in izrazil pripravljenost za posredovanje tudi drugih podatkov, so kasneje naša zaprosila (ob zagotovitvi, da bodo podatki uporabljeni zgolj za znanstveno obravnavo in brez navajanja imena vira) naletela na gluha ušesa, izgovarjanje na nujne službene obveznosti in končno na molk in neodzivanje na naša pisma. Zaradi tega so podatki predstavljeni brez

navajanja vira, gre pa za enega izmed tujih lastnikov licence na področju kartičnega poslovanja.

Tudi podatki o zlorabah, ki jih obravnava policija v okviru predkazenskega postopka, so pomanjkljivi, saj zaradi načina vodenja evidenc po kaznivih dejanjih ne moremo priti do podatkov o vseh zlorabah, ki se zgodijo na področju elektronskih plačilnih sistemov in jih obravnava policija. Gre pa za manjše število zlorab, kot pa se jih dejansko zgodi, saj policija ne obravnava vseh, ker ne dobi prijave banke ali komitenta, sama pa za sum zlorabe ne izve. Zato podatki policije niso toliko pomembni in odločujoči za našo raziskavo. Zlorabe pa se dogajajo in so problem tako za lastnike licenc, bančne institucije, nadzorstvene in represivne institucije in organe ter seveda uporabnike storitev. Da je problematika zlorab na tem področju pereča, kažejo tudi aktivnosti bank na področju zagotavljanja varnosti, ki se kažejo navzven v obveščanju in ozaveščanju uporabnikov oz. komitentov, prav tako pa interes za sodelovanje s policijo, ki ga na drugih področjih (notranja kriminaliteta v bankah, kjer so storilci zaposleni v bankah) ni zaslediti.

Pri raziskovanju tega področja smo naleteli tudi na probleme z literaturo in pomanjkanjem znanstvenih dognanj na ožjem področju znanstvenega dela, ki se nanaša na zlorabe. Dokaj zadovoljivo se znanost posveča bančnemu poslovanju, elektronskim plačilnim sistemom in različnim tehničnim načinom zaščite, tudi varnosti poslovanja. Prav malo pa je znanstvenih del, ki bi se ukvarjala z različnimi vrstami zlorab na tem področju, njihovemu preprečevanju in sankcioniranju. Smo na področju preiskovanja finančne, gospodarske kriminalitete, ki je po povzročeni škodi najbolj nevarna oblika kriminalitete in lahko ogrozi tudi finančne sisteme držav. Manjko na tem področju smo zato poizkušali zapolniti z dognanji tega dela na strokovnem in znanstvenem področju in različnimi strokovnimi dognanji policije in drugih organov na področju preiskovanja in preprečevanja gospodarske kriminalitete.

Zelo veliko pomoč pri testiranju zastavljenega modela smo imeli v Združenju bank Slovenije, še posebej pri g. Cimpriču, preko katerega smo prišli do strokovnjakov iz tega področja, zaposlenih v bankah. Brez pomoči Združenja verjetno raziskava v bankah sploh ne bi bila mogoča, saj zaradi zaupnosti poslovanja ne bi bile pripravljene v sodelovanje. Seveda pa smo s tem rešili tudi logistične in organizacijske težave pri pošiljanju vprašalnikov in njihovem vračanju, prav tako pa pri opravljanju intervjujev oz. iskanjem kompetentnih oseb, strokovnjakov s tega področja.

Pri analizi zlorab na področju elektronskega bančništva smo se srečali z obsežnim in mukotrpnim delom. Za gospodarsko kriminaliteto je namreč značilno, da je produkt novih tehnologij in se nenehno razvija in spreminja moduse izvrševanja kriminalnih dejanj. Dober primer tega posodabljanja in spreminjanja oblik je ravno področje elektronskega bančništva. Z razvojem tega področja smo bili priča tudi razvoju novih oblik izvrševanja kriminalnih dejanj od najpreprostejših, ki ne zahtevajo veliko znanja in spretnosti, kakor tudi ne dodatnih pripomočkov in naprav, pa vse do takšnih, ki so v svoji izvedbi kompleksne, sofisticirane in izvedene s tehnično – tehnološko dovršenimi pripomočki in napravami. Dokaz kompleksnosti tega področja zlorab je tudi sprememba kazenske zakonodaje, saj obstoječi opisi kaznivih dejanj niso bili več dovolj za nove oblike manipulacij s kreditnimi in plačilnimi karticami. Zlorab, ki se pojavljajo na tem področju, je tudi glede na obliko izvedbe ogromno. Z ugotavljanjem skupnih značilnosti smo jih uspeli strniti v določene skupine, ki jih je prav tako veliko, kar kaže na veliko zanimanje kriminala za to področje poslovanja finančnih institucij.

Rezultati raziskave in doktorskega dela so pokazali številne ugotovitve. Po našem mnenju je zelo pomembna ta, da se zoper kriminal oz. zlorabe na področju elektronskega bančništva ni dovolj boriti samo na enem področju, samo z ukrepi ene institucije. V modelu preprečevanja zlorab je zato udeleženih več institucij, ki z različnim ukrepanjem le skupaj lahko dosegajo pomembne rezultate pri preprečevanju zlorab. Samo represivni vidik v smislu odkrivanja in lovljenja storilcev je preživet in neučinkovit. Zaradi različnih razlogov je zelo malo storilcev tudi odkritih, še manj pa sankcioniranih in to ne vodi k zmanjševanju zlorab zaradi vpliva »zastraševanja« na potencialne nove ali ponovne storilce v smislu generalne ali specialne prevencije, da se ne bi odločali za izvrševanje kaznivih dejanj. Slaba preiskanost tega področja je ravno dodatna vzpodbuda za storilce, ki se na podlagi »cost – benefit« metode odločajo za izvrševanje kriminala na tem področju, ker omogoča velike zaslužke z malo vloženega kapitala oz. je možnost »izgube« v smislu zagroženih kazni zelo malo verjetna.

Zelo pomembno je zaradi tega področje preventivnih dejavnikov, ki z vsemi svojimi ukrepi in aktivnostmi otežuje možnosti za izvajanje zlorab. Veliko vlogo, morda celo največjo, igrajo tukaj ravno uporabniki storitev elektronskega bančništva. Njihovo skrbno ali neskrbno ravnanje in uporaba plačilnih instrumentov je namreč največkrat tisti dejavnik, ki storilcem omogoča ali preprečuje izvrševanje zlorab. Zaradi tega je obnašanje in ravnanje uporabnikov zelo pomemben člen v modelu preprečevanja zlorab in tudi področje, ki se mu banke in drugi izdajatelji zelo posvečajo.

Seveda so za učinkovito preprečevanje zlorab pomembni tako preventivni kakor tudi represivni dejavniki, vendar je vloga prvih pomembnejša v smislu preprečevanja zlorab in ustvarjanja pogojev poslovanja na področju elektronskega bančništva, ki zagotavljajo večjo stopnjo varnosti poslovanja in zmanjševanje zlorab. Če pa do zlorab kljub temu pride, saj se moramo zavedati, da 100% varnosti ni mogoče doseči, so tukaj represivni dejavniki, ki morajo že izvršene zlorabe preiskati, najti in izslediti storilce, ki morajo biti za svoja dejanja sankcionirani s predpisanimi kaznimi (zaporne ali denarne), odvzeta pa jim mora biti tudi premoženjska korist, ki so jo dosegli v nasprotju z določili zakonov. Pozabiti seveda ne smemo tudi na oškodovance, ki največkrat direktno za škodo, ki jo utrpijo, sami niso direktno odgovorni ali jim krivde zaradi neskrbnega ravnanja ni moč dokazati. Potrebno jim je povrniti izgubo sredstev, ki so jo utrpeli, kar je pomembno tako z vidika zadovoljstva komitenta s storitvami in odnosom banke, kakor tudi z vidika poslovne bonitete in »imagea« banke do komitentov oz. javnosti.

Na osnovi spoznanj, pridobljenih z raziskavo, smo oblikovali metodo za ocenjevanje informacijskega tveganja, ki je prilagojena bančnemu poslovanju. Glede na zahtevnost in specifičnost bančnega poslovanja smo se odločili za kvalitativno metodo IBRA, ki upošteva problematiko težavnosti vrednotenja vseh stroškov oz. izgub poslovanja bank, bančne tajnosti in zaupnosti podatkov. Z intervjuji smo metodo IBRA testirali v bankah in dobili pozitivne rezultate o primernosti zastavljene metode. Metoda je zasnovana na osnovi zahtev bančnega poslovanja in bi jo lahko uporabili za ocenjevanje tveganja informacijske varnosti.

LITERATURA

Abanka Vipa. (2003). Katalog kartic, ki jih izdaja banka,

Abanka Vipa. (2000). Zlorabe trgovcev-pomoč pri iskanju zlorab,

Abanka Vipa. (1999). Plačilne kartice. Seminar, Ljubljana,

Activa, (2009). Zgodovina pametnih kartic, http://www.activa-card.com/pametnaKartica/zgodovina.asp?content=05, 22.07.2009,

Alberts, C.et. al. (2003). Introduction to the OCTAVE Approach. Network Systems Survivability Program. Carnegie Mellon University,

Ambrož, M., Mihalič, T., Ovsenik, M., (2000) Varnostna kultura in sistem varovanja v Organizaciji. V: Varstvoslovje, 2 (3), Ljubljana,

Banka Slovenije, (2010), Banke v Sloveniji, http://www.bsi.si/poslovanje-bank-in-podjetij.asp?MapaId=521, , 11.03.2010,

Bilten Banke Slovenije. (2011). Letnik XX št. 3, Ljubljana,

Bedjanič, R., Lorenz, K. (1997). Elektronsko bančništvo. V: Bančni vestnik št. 12, str. 57 – 59,

Berndt, H. (1995). Elektronisches Geld – Geld der Zukunft?, V: Spk, letnik 112,

Bilten Banke Slovenije, junij 2009: Letnik XVIII št. 6,

Birkelbach, J. (1996). Homebanking: Neue Sicherheitskonzepte fuer das Internet vorgestellt – »Der Kunde ist jetzt das Hauptrisiko«, V: HB, št. 167, str. 40,

Bizovičar, M. (2007). Čip je varnejši od magnetne steze, V: Delo – FT, 46:42, Ljubljana,

Bobek, D. (1989). Sodobna banka, EPOK, Založba Obzorja Maribor,

Bobek, D. (1992). Organiziranje in poslovanje bank, EPF Maribor,

Bobek, S. (1993). Informatika za ekonomiste, EPF Maribor,

Borak, N. (1997). Strokovno posvetovanje o bančništvu – banke in tveganja, V: Zveza ekonomistov, Ljubljana,

Bračun, F., Cetinski, A. (1998). Elektronsko poslovanje v SKB banki d.d. V: Organizacija, Kranj, št. 3, str. 144,

Bračun, F. (1997). Praktične izkušnje pri uvajanju e- bančništva. V: Banke in tveganje, Zveza ekonomistov Slovenije, Ljubljana, str. 149 – 154,

Braun, G. (2002). Information Security Risk Analisys and Modeling, BWI-paper, Vrije Universiteit, Amsterdam,

Brueckner, M. (1997). Hypobank stoesst als Vorreiter der Telearbeit in Kreditinstituten an grenzen, V: HB, št. 23, str. 26,

Cerar, G. (2004). Nevarni bankomati, V: Mladina, Ljubljana,

Cetinski, A. (1999). Elektronsko poslovanje v bančništvu, V: Izboljšanje konkurenčnosti z elektronskim poslovanjem, Kranj, Moderna organizacija,

Clough, B (1997). Plastic Fraud. Intersec, št. 7, 1997, str. 289-292,

Coles, s. R., Moulton, R. (2003). Operationalizing IT Risk Management Computers and Security, Volume 22,

Cowichan, D. (2000). Computer, Internet and Network System Security, Canada, Parmar,

Deisinger, M. (2002). Kazenski zakonik s komentarjem: Posebni del. Nova slovenska zakonodaja, Ljubljana,

Dobovšek, B. (2009). Transnacionalna kriminaliteta, V: Fakulteta za varnostne vede, Univerza v Mariboru, študijsko gradivo,

Duclaux, D. (1996). The call of the web. V: ABA, 88. zvezek, št. 4, str. 20 – 22,

EBIOS MEMO: 4 March 2004.

http://www.ssi.gouv.fr/en/confidence/documents/methods/ebiosv2-memento-2004-02-04_en.pdf,

Enders, M. (1994). Entwiklungslinien der Bankorganisation. V: DBk, št. 1,

Europol. (2006). Slovenia police in collaboration with Europol, Training seminar – Other means of payment fraud. Haag, Europol,

Easterby-Smith, M., THORPE R., LOWE A.: Raziskovanje v managementu. Koper: Univerza na Primorskem, Fakulteta za management Koper, 2005,

GAO: Information Security Risk Assessment, Practices of Leading Organizations, 1999.

Glogovšek, J. (2008). Bančni management. Maribor, Pivec, str. 566,

Golob, R. (1997). Sistem zaščite in varovanja oseb in premoženja. Ljubljana, samozaložba,

Goldberg, Y. (2005). Practical Threat Analysis for the SoftwareIndustry, PTA Technologies,

Gradišar, M. (2003). Uvod v informatiko, V: Ekonomska fakulteta, Ljubljana,

Gradišar, M., Jaklič, J., Talij, D., Baloh, P. (2005). Osnove poslovne informatike, V: Ekonomska fakulteta, Ljubljana,

Gradišar, M., Jaklič, J., T., Turk, P. (2007). Osnove poslovne informatike, V: Ekonomska fakulteta, Ljubljana,

Gradišar, M., Lamberger, I. (2010). Vpliv represivnih dejavnikov na zlorabe kreditnih in plačilnih kartic v Sloveniji, V: Revija za kriminalistiko in kriminologijo, št. 1, letnik 61, str. 15 – 28, Ljubljana,

Gradišar, M., Lamberger, I. (2011) Celovit sistem zaščite elektronskih plačilnih sistemov pred zlorabami. Bančni vestnik, , letnik 60, št. 3, str. 13-20, tabele,

Healey M. J in Rawlinson M. B., (1994). Interviewing techniques in business and management research. V: Principles and practice in business and management research, ur. V. J. Wass in P. E. Wells, str. 123-146. Dartmouth: Aldershot,

Hevner, A. R.; March, S. T.; Park, J. & Ram, (2004). S. Design Science in Information Systems Research. MIS Quarterly, 28, 75-106.

Holbrook, P., Reynolds, J., (1991). Site Security Handbook, Network Working Group,

Hussey, J., Hussey R., 1997. Business research: a practical guide for undergraduate and postgraduate students. London: MacMillan Business,

Iglič, D. (1998). Upravljanje s tveganji kartičnega poslovanja. Prikazi in analize, let. 6, št. 3, september 1998, str. 54-58,

Ivanovič, Ž. (1995). Preprečevanje zlorab kreditnih kartic v luči nove zakonodaje. Bančni vestnik, let. 44, št. 4, 1995, str. 41- 44,

Jurak, U. (1996). Plastični denar. Slovenski almanah 1996, str. 183-185,

Jerman Blažič, B. (2001). Elektronsko poslovanje na internetu. V: Gospodarski vestnik, Ljubljana, 206 str.,

Jouas, J., Roule, J. (2007). MEHARI 2007 Overview. Club de la Securite de L' Information Francais, Clusif,

Jurišić, A., Trojar, A. (1997). Pametna kartica. Uporabna informatika, št. 1, 1997, str. 37-45,

Kajić, M., (1999). Varnostna politika in načrtovanje ukrepov za izredne razmere pri varovanju IS. V: Organizacija, letnik 32, št. 7, Moderna organizacija, Kranj,

Kalakota, R., Whiston, A. (1997). Electronic Commerce. A Manager' s guide. V: Addison – Wesley Longman, XVI, 431 str.,

Kanduč, Z. (1996). Utilitarne in retributivne zamisli o upravičenosti kaznovanja. V: Revija za kriminalistiko in kriminologijo, Ljubljana 47, str. 122 – 133,

Karabacak, B. Sogukpinar, I. (2005). ISRAM: Information Security Risk Analisys Method. Computers and Security, Volume 24,

Kazenski zakonik (KZ-1). /Uradni list RS, št. 55/2008 z dne 04.06.2008/,

Kazenski zakonik (KZ). /Uradni list RS, št. 95/2004 z dne 27.08.2004/,

Kos, G. (2007). Poslovanje z bankomati je več kot le dvigovanje gotovine, Delo – FT, str. 40,

Košir, A. (2008). Rezultati projekta SEPA, Bančni vestnik 4/08, april, Združenje bank Slovenije, Ljubljana,

Kovačič, M. (1997). Storitve elektronskega bančništva. Banke in tveganje, V: Zbornik III Strokovnega posvetovanja o bančništvu, Portorož, Zveza ekonomistov Slovenije, str. 155 – 165,

Kranjec, S. (2006). Bančne kartice bodo dobile tudi čipe, Finance 237, str. 18, Ljubljana,

Krivec, V. (2008). Plastična doba, Mag, Ljubljana,

Kumar, R. (2005). Research methodology. London, Thousand Oaks (CA), New Delhi, Sage Publications,

Lamberger, I. (2005). Mednarodne finančne goljufije, V: DVORŠEK, A., SELINŠEK, L. (ur.). Problematika finančnega kriminala v Sloveniji, Pravna fakulteta, Maribor, str. 87-100,

Lamberger, I. (2006). Učinkovitost preiskovanja in zatiranja gospodarske kriminalitete, V: Zbornik povzetkov, Raznolikost zagotavljanja varnosti, 7. slovenski dnevi varstvoslovja, Fakulteta za varnostne vede, Maribor, str. 1073 – 1080,

Lamberger, I. (2007). Varnostni vidiki elektronskih plačilnih sistemov s poudarkom na zlorabah, V: Zbornik povzetkov, Varnost v sodobni družbi groženj in tveganj, 8. slovenski dnevi varstvoslovja, Fakulteta za varnostne vede, Maribor, 5 str.,

Lamberger, I. (2008a). Kako preprečevati zlorabe v elektronskem plačilnem prometu, V: TURK, I. (ur.). Zbornik referatov. 40. simpozij o sodobnih metodah v računovodstvu, financah in reviziji, 16.-18. april 2008, Portorož, Ljubljana, Zveza ekonomistov Slovenije: Zveza računovodij, finančnikov in revizorjev Slovenije,

Lamberger, I. (2008b). Slovenski informacijski sistem bonitet komitentov bank in hranilnic kot preventivni dejavnik za preprečevanje goljufij v bančništvu, V: Zbornik povzetkov, Javna in zasebna varnost, 9. slovenski dnevi varstvoslovja, Fakulteta za varnostne vede, Maribor,

Lamberger, I. (2009). Vpliv represivnih organov in generalne prevencije na področju zlorab kreditnih in plačilnih kartic, V: Zbornik povzetkov, 10. slovenski dnevi Varstvoslovja, Fakulteta za varnostne vede, Ljubljana,

Lasbaher, A. (1997). Nasveti izdajateljev. Kapital, št. 164, str. 48-50,

Lavtižar, A. (2007). Ukrepi policije v primerih kopiranja magnetnih zapisov plačilnih kartic, Fakulteta za varnostne vede, Ljubljana,

Logar, R. (1998). Plačilni sistemi: Kaj je dobro vedeti o njih. V: Slovenski inštitut za revizijo, Zveza računovodij, finančnikov in revizorjev Slovenije,

Lunt, P. (1995). What will dominate the home?, V: ABA, 87. zvezek, št.

Lunt, P. (1996). Welcome tosfnb.com. The paradigm just shifed, V: ABA, 87. zvezek, št. 12, str 41 – 42.

Makarovič, B. (2001). Internet in pravo, V: Založba Pasadena, Ljubljana,

Markovič, D. (1997). Računalniška kriminaliteta. Pravna praksa, 16 (14/15), str. 38-41,

Meško, G. (2002). Osnove preprečevanja kriminalitete, V: MNZ, Visoka policijsko-varnostna šola, Ljubljana.

Miles, M.B, Huberman, A.M., 1994. Qualitativedata analysis. Thousand Oaks: Sage.

Miš Svoljšak I. (1997). Osnove trženja finančnih storitev, V: Združenje bank Slovenije, Maribor, str. 23.

Miš Svoljšak I. (1998). Do denarja kjerkoli – kadarkoli. V: PC Kapital (priloga revije Kapital), Maribor, str 7 – 8,

Moulton R., Moulton M. (1996). V: Electronic Communications Risk Managenent, A Checklist for Business Managerrs, Computers & Security, 15, str. 377 – 386,

Nabergoj, G. (2007). Kartično poslovanje v pogojih enotnega območja plačil v evrih. V: Bančni vestnik 07/2007, Združenje bank Slovenije, Ljubljana,

Newton, J. (1996). Card Fraud. Lafferty Publications Ltd, Dublin, 1996, str. 162-167,

NLB Klik, (2010). Varno poslovanje s plačilnimi karticami, http://www.nlb.si/varno-poslovanje-s-placilnimi-karticami, 25.5.2010,

Obligacijski zakonik (OZ-UPB1). /Uradni list RS, št. 97/07 z dne 24.10.2007/,

O' Connor, N. (2006). Semantic Multimedia [Elektronski vir] V: First International Conference on Semantic and Digital Media Technologies, SAMT, Athens, Greece, December 6-8, 2006, Proceedings,

Odar, M. (1993). Finančno poslovanje: Kreditne kartice. Informacije o knjigovodstvu in stroki. Revija za računalništvo in finance, 20 (12), str. 110 -119,

Osojnik M. (2002). Skrivnosti elektronskega poslovanja, V: Gospodarska zbornica Slovenije, International Trade Center,

Pavlič G. (2004). Plačevanje prek elektronske banke, Podjetnik, junij 2004, Podjetje RR, Ljubljana,

Pavlin, F. (1996). Seminarska naloga: Goljufije v zvezi s kreditnimi karticami. Visoka policijsko-varnostna šola, Ljubljana,

Pavliha, M. (2002). Zakon o elektronskem poslovanju in elektronskem podpisu s komentarjem, V: GV Založba, Ljubljana, 222 str.,

Pečar, J. (1996). Družbeno nadzorstvo in organizirani kriminal. V: Revija za kriminalistiko in kriminologijo, Ljubljana 47, str. 14 – 24,

Pečar, J. (1995). Organizirani in transnacionalni kriminal. V: Revija za kriminalistiko in kriminologijo, Ljubljana 46, str. 319 – 328,

Power, R. (1998). How NOT to build a firewall. Computer Security Institute, (URL: http://www.spirit.com/CSI/Papers/hownot.htm), 13.05.2009,

Pucihar, A., Gričar, J. (2000). Izraba informacijske tehnologije za elektronsko poslovanje, V: Organizacija, Kranj, 3, str. 207 – 212,

Pukmajster, V. (2001). Diplomsko delo: Sistemske in organizacijske spremembe v Abanki d.d. Ljubljana na področju plačilnega prometa. Ekonomska fakulteta, Ljubljana,

Robson C. (1993). Real world research. Oxford: Blackwell,

Saunders, M., Lewis P. in Thornhill A., (1997). Research methods for business students. London, Pitman,

SET Secure Electronic Transaction. Book 1: Business Description. (1997). Mastercard – Visa, http://www.ccc.cs.lakeheadu.ca/set/set_bk1.pdf, 19.08.2009,

Schueller, B. (1995). Organisation und Technologie des Wertpapier und Devisengeschaeftes. V: J. H. v Stein J. Terrahe (izd.): Handbuch Bankorganization, 2. izd., Wiesbaden,

Sharma, S. (1996). Applied multivariate techniques. New York, Wiley,

Šalamun, A. (2007). Večino POS terminalov upravljajo… V: Finance 65, str. 18, Ljubljana,

Šavnik, J. (2007). Tehnično ozadje zlorab plačilnih kartic s pravnimi kvalifikacijami. Ljubljana, SKP PU Ljubljana,

Shon, H. (2006). Information risk management http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1178861,00.html, 15.03.2010,

Širaj, M. (2008). Enotno območje plačil v evrih – SEPA. V: Pravna praksa št. 5, GV Ljubljana,

Škrlec, I. (2002). E-poslovanje in uporaba formata XML. V: Finance, Ljubljana, str. 18,

STA, (2009). Američan obtožen kraje podatkov 130 milijonov kreditnih kartic http://www.mojevro.si/255226/Ameri%E8an_obto%BEn_kraje_podatkov-130_milijonov_kreditnih_kartic, 18.08.2009,

Šteblaj, A. (1999). Uporaba sodobnih plačilnih instrumentov v Sloveniji v prvem polletju 1999. Prikazi in analize, let. 7, št. 3, september 1999, str. 41 -59,

Toplišek, J. (1998). Elektronsko poslovanje, V: Založba Atlantis, Ljubljana, 336 str.,

Trampuš, M., Ciglarič, M., Vidmar, T. (2005). Formalizacija varnostnih politik, V: Elektrotehniški vestnik, 72(5): 309-315, Ljubljana,

Trstenjak, M. (2006). Nov pravni okvir za plačilne storitve, Bančni vestnik 3/2006, Združenje bank Slovenije, Ljubljana,

Tulloch, M. (2005). Zvijače za Windows server, Ljubljana : Pasadena,

N.N. (1996). Das Internet Banking wird immer beliebter, V: BZ št. 159, str. 4, B. Orr: How to get your bank on the www, V:ABA, 88. zvezek, št. 4, str. 22 in WGZ – Bank: Internet als Vertriebungsweg fuer Bankdienstleistungen, str. 7,

Vidmar, T. (2002). Informacijski – komunikacijski sistem, Založba Pasadena, Ljubljana,

Vrešak, S. (1997). Internet in elektronsko bančništvo, V: Bančni vestnik, Ljubljana, št. 12, str. 60-63,

ZBS-Združenje bank Slovenije. (2002). Ponaredki in druga kriminalna dejanja pri kartičnem poslovanju. Seminar, Policijska akademija Tacen, 6.3.2002,

Zupančič, M. (1998). Zlorabe plačilnih kartic pri elektronskem poslovanju. Analiza, 2/1998, MNZ, Ljubljana,

Vaishnavi, V., Kuechler, W. (2004). "Design Research in Information Systems" January 20, 2004, last updated August 16, 2009. URL: http://desrist.org/design-research-in-information-systems

Wilson, R., Backhouse, J. (2005). Re-conceptualising IS Security: Insight from a criminological perspective. Department of Information Systems, London School of Economics and Political Science,

Zakon o kazenskem postopku (ZKP-UPB-4). /Uradni list RS, št. 32/2007 UPB-4 z dne 10.04.2007/,

Zakon o bančništvu (Zban-1-UPB5). /Uradni listi RS, št. 99/2010 z dne 07.12.2010/,

Zakon o Banki Slovenije (ZBS-1-UPB1). /Uradni list RS, št. 72/2006 z dne 11.7.2006/,

Zakon o deviznem poslovanju (ZDP-2A). /Uradni list RS, št. 85/2009 z dne 30.10.2009/,

Zakon o policiji (Zpol-UPB7). /Uradni list RS, št. 66/2009, z dne 21.08.2009/.