UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

VARNOST POSLOVNEGA INFORMACIJSKEGA SISTEMA IN PODATKOV V SKB BANKI

Ljubljana, februar 2005 VANJA VUKAJLOVIĆ

IZJAVA

Študent Vanja Vukajlović izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom prof. dr. Andreja Kovačiča in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne 22.2.2005 Podpis:_____

KAZALO

1 UVOD

Zagotavljanje varnosti informacijskih sistemov in podatkov postaja vse bolj ključno in ga je potrebno nasloviti že v času razvoja. Varnost informacijskih sistemov vidim kot metodologijo in način razmišljanja. Metodologija je po definiciji skupek postopkov, tehnik, metod, ki jih uporabljamo pri reševanju nekega problema. To ne pomeni le ene rešitve, ki odpravi le eno težavo, ampak nudi celovito integrirano rešitev, ki rešuje vse varnostne težave. Vodilo pri zaščiti dela dela temelji na dejstvu, da mora varnost omogočati poslovanje, ne pa ga zavirati. Varnost informacijskih sistemov je kombinacija dobrih poslovnih pravil, dobre varnostne politike, varnostnih načrtov, sodelovanja zaposlenih, sodobne tehnologije in sodelovanja z izkušenimi strokovnjaki ter varovanje samih podatkov.

Varnostna politika je vodilo vodstvene strukture podjetja ali organizacije, ki definira kaj, kako in kdo je odgovoren za varno upravljanje informacij ter se uvaja v vsem podjetju ali organizaciji. To je dokument, ki ga razumejo vsi zaposleni in definira pravila za upravljanje z informacijami in uporabniki teh informacij. Sestavni del varnostne politike pa so tudi varnostni načrti, ki definirajo, na kakšen način se v podjetjih izvaja zaščita zaupnih in kritičnih poslovnih informacij. Varnostne politike temeljijo na standardu BS7799/ISO 17799, v Sloveniji znanem pod imenom PSIST BS7799, in so prilagojene razmeram v organizaciji ali podjetju.

Razvoj računalniškega sistema in interneta danes podjetjem predstavlja tudi nevarnost. Informacijski sistemi in omrežja so lahko tarča mnogih resnih groženj, med drugim računalniškega kriminala, vohunstva, sabotaž, pustošenja in drugih načinov odpovedi ali nesreč. Prihaja tudi do novih poškodb, kot so razvpite grožnje računalniških zanesnjakov, kriminalcev in virusov. Pričakovati je, da se bodo nevarnosti še bolj razširjale, hkrati pa je podjetje zaradi vse večje odvisnosti od računalniških sistemov in storitev še bolj ranljivo. Večja uporaba omrežja pomeni nove priložnosti za nedovoljen dostop do računalniških sistemov.

V diplomskem delu sem se odločil ugotoviti, kako varno je poslovati preko interneta z vidika bančnih storitev. Za elektronsko bančništvo sem izbral Poslovni Skb net, ki je bančno okence Skb banke na internetu. Pred tem pa bom še na splošno opredelil informacijski sistem in poslovno informacijski sistem ter standard PSIST BS7799, ki je vodilo pri vpeljavi informacijske varnosti v informacijski sistem.

Za tako temo diplomske naloge sem se odločil predvsem zaradi njene zanimivosti in aktualnosti, kajti varnost je v današnjih poslovnih informacijskih sistemih zelo pomembna, da lahko uporabnikom in podjetjem zagotavlja zanesljivo, nemoteno in varno delo.

2 INFORMACIJSKI SISTEM

Cilj informacijskega sistema je predelava in obdelava podatkov, s čimer ti pridobijo na vrednosti in uporabnosti ter tako postanejo informacije. Podatek je nevtralno sporočilo o določenem dejstvu, ki še ni ovrednoteno in pripravljeno za sprejem katerekoli poslovne odločitve. Informacija je sporočilo, ki nam pove nekaj novega in mora biti aktualna, za kar so pri sodobnem informacijskem sistemu potrebni računalniki. Informacijo doživljamo šele takrat, ko nam vzbudi določeno predstavo. Da nam je informacija jasna, jo moramo predstaviti z nam razumljivimi podatki (jezik, črke, številke, enote...). Informacije potrebujemo za učinkovitejše odločanje o tem, kaj in kako bomo delali oz. ravnali. V informacijskem sistemu poteka delitev dela med ljudmi in računalniki, ki jih lahko razumemo kot orodje oz. tehnično sredstvo, ki človeku le pomaga pri delu oziroma služi za izvajanje določenih segmentov v procesu obdelave podatkov, tako da se s človekom dopolnjujeta. Računalnik lahko nadomesti človeka le, če zna opravljati samo tiste segmente, ki jih izvede hitreje, bolje in ceneje. V splošnem gre za komplementarnost.

Za izvajanje informacijskih dejavnosti je potrebna informacijska tehnologija; to so stroji in naprave, kot so radio, magnetofon, telefon, telefaks, modem, fotoaparat, kamera, videorekorder, digitalne avdio in video naprave, računalniki, TV, GSM ipd. Informacijske dejavnosti pa so zbiranje, shranjevanje, obdelava in posredovanje informacij. Brez današnje informacijske tehnologije, kot so računalniki, bi si banke težko opomogle, zato uporaba informacijskih sistemov, ki temeljijo na moderni informacijski tehnologiji lahko močno poveča konkurenčno prednost organizacije, njeno učinkovitost in uspešnost. Sodobno zasnovan informacijski sistem omogoča (Gradišar, Resinovič, 2001, str. 387):

- hitrejše, bolj kakovostno delo;
- boljše odločanje, ker poišče, generira in predstavi podatke, ki tvorijo informacijsko podlago za odločanje in boljšo uporabo znanja pri tem;
- boljšo komunikacijo znotraj organizacije ter med organizacijami in njenim okoljem.

V bankah je informacijska tehnologija proizvodna tehnologija banke. Vloga informacijske tehnologije kot proizvodne tehnologije v bančnih procesih je:

- Informatizacija poslovnih aktivnosti strežbe; to so delovne postaje zaposlenih za masovno strežbo (omogočajo hitro posredovanje storitev večjemu številu strank) in delovne postaje za svetovalno strežbo (omogočajo celovito strežbo zahtevnejših in bolj zapletenih storitev).
- Informacijska podpora strank, ki omogoča principe “ samopostrežbe” (angl. Self-service). Stranka je postrežena preko elektronske prodajne poti, tako da sama uporabi izbrano elektronsko prodajno pot.

- Avtomatizacija poslovnih aktivnosti podpore; vlogo poslovnih aktivnosti podpore prevzame računalnik, ki avtomatizirano obdeluje podatke povezane s poslovnimi dogodki, ki so bili zajeti na delovnih mestih strežbe ali s pomočjo elektronskih prodajnih poti.

Računalniki v banki izvajajo operacije s podatki po vnaprej določenem in shranjenem programu. Računalnik skupaj z napravami, ki mu omogočajo komunikacijo z okoljem, tvori računalniški sistem in je del informacijskega sistema, ki vključuje tudi ljudi (Gradišar, Resinovič, 2001, str. 358).

Informacijski sistem tvorijo baza podatkov, ki predstavlja skladišče podatkov, naprave za obdelavo in posredovanje podatkov in ljudje, ki podatke potrebujejo. Naloga sistema je oskrba ljudi z informacijami, ki služijo za kvalitetno odločanje o delu in ravnanju v nekem trenutku. Tak sistem v novejših časih uporablja računalnike za obdelavo in hranjenje podatkov, računalniško omrežje pa za izmenjavo informacij. Lahko ga označimo kot kombinacijo v bazi podatkov shranjenih podatkov, človeških sposobnosti in tehničnih pripomočkov, ki skupaj z ustreznim nizom organizacijskih postopkov proizvajajo informacije za podporo opravljanju, poslovanju in odločanju. Pripomočki so strojna in programska oprema, sistem uporabniških programov, komunikacijsko omrežje, finančna sredstva in strokovno osebje.

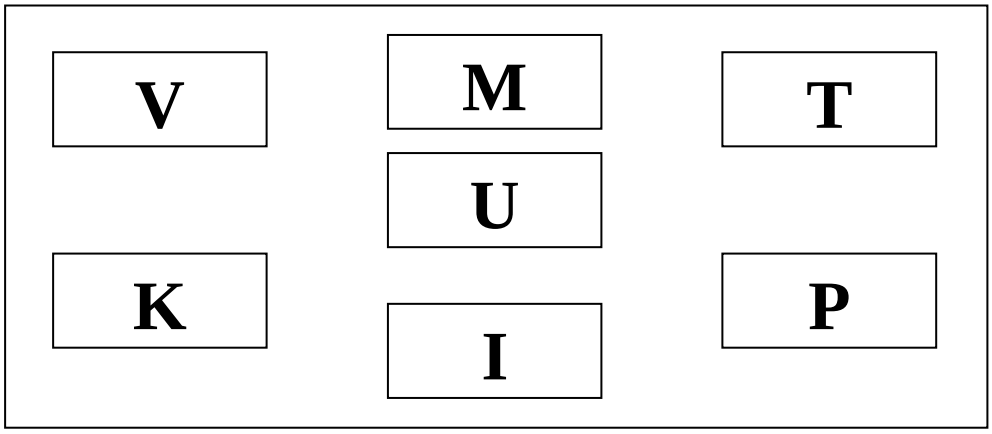
Informacijski sistem lahko nastopa le kot del oziroma podsistem nekega živega organizma ali sistema, na primer poslovnega sistema, in omogoča izvajanje in upravljanje temeljne dejavnosti tega sistema in s tem doseganje ciljev oziroma funkcioniranje. Poslovni sistem je mikroekonomski sistem, katerega temeljni proces je reprodukcijski proces, temeljni cilj pa ekonomski. Je celota medsebojno povezanih komponent, ki omogočajo poslovni proces, to je skupek aktivnosti, ki se izvajajo v poslovnem sistemu in vplivajo na dodano vrednost pri uresničevanju skupnega cilja poslovnega sistema. Pri tem obstajajo tudi medsebojni vplivi med poslovnim sistemom kot zaokroženo celoto in njegovim okoljem. Lahko ga opazujemo kot celoto treh podsistemov: temeljnega, upravljalnega in informacijskega, v katerem potekajo temeljni, upravljalni in informacijski procesi. Na področju finančne institucije oziroma organizacije, kot je banka, ki sestavlja poslovni sistem, se bančni sistem ukvarja s svojim informacijskimim sistemom, v katerem se ustvarjajo, shranjujejo in pretakajo informacije. Doseganje ciljev oziroma sprejemanje odločitev opravlja človek, nekaj pa tudi računalnik s komunikacijami. Celotni sistem je ustvaril in organiziral človek, ki je tudi sam njegov del. Poslovni informacijski sistem je zato informacijski sistem v poslovnem sistemu (Gradišar, Resinovič, 2001, str. 41).

2.1 SESTAVINE INFORMACIJSKEGA SISTEMA

Sistem pomeni urejeno celoto elementov, v kateri vladajo določene zakonitosti. Informacijski sistem zato lahko definiram kot sistem, ki zbira, hrani, obdeluje in dostavlja informacije za organizacijo tako, da je informacija dostopna in uporabna tistim, ki jo želijo uporabiti, vključujoč managerje, osebje, stranke in državljane. Informacijski sistem je sistem človeških

aktivnosti, ki lahko vsebuje (ali pa tudi ne) uporabo računalniških sistemov (Avison, Fitzgerald, 1996, str.13).

Slika1: Vsebinski sklopi elementov IS ali sestavine informacijskega sistema



Vir: Gradišar, Resinovič, 2001, str. 340.

Elemente slehernega IS-a s slike 1 lahko razdelimo na 7 vsebinskih sklopov:

- **Vhodni blok (V).** Vhodni blok predstavlja množica vnosnih form, preko katerih poteka vnos podatkov. Vnos je lahko računalniško podprt, tako da je forma prikazana na zaslonu, ali pa ni računalniško podprt in zahteva ročni vpis na papir.
- **Metode (M).** Sklop proceduralnih, logičnih, matematičnih metod, s katerimi se obdelujejo podatki, da bi prišli do želenih rezultatov. Tipični postopki obdelave podatkov so zajemanje, razvrščanje, urejanje, računanje, sumiranje, arhiviranje, iskanje, reproduciranje, komuniciranje, preverjanje.
- **Tehnika (T).** Informacijska tehnologija temelji na tehničnih sredstvih in omogoča dejansko transformacijo podatkov.
- **Podatkovna baza (P).** Podatkovna baza hrani podatke v določeni podatkovni strukturi.
- **Izhodni blok (I).** Izhodni blok mora prikazovati izhodne informacije. Pogoj za transformacijo podatkov v informacije je poleg obdelave podatkov tudi ustrezen način prikaza informacij, saj postane podatek informacija takrat, ko za uporabnika postane uporaben. Če je uporabna informacija v prikazu skrita ali nejasno prikazana, za uporabnika ne predstavlja nobene uporabnosti.
- **Kontrolni blok (K).** Kontrolni mehanizmi informacijskega sistema morajo zagotavljati preverjanje vhodnih podatkov in izločati tiste nepravilne vnosne podatke, ki so nepotrebni ali napačni za ustrezen zapis v podatkovno bazo.
- **Udeleženci (U).** Udeleženci so ljudje, ki skrbijo in upravljajo z informacijskim sistemom ter uporabljajo izhode informacijskega sistema.

2.2 VRSTE INFORMACIJSKIH SISTEMOV

Informacijski sistem lahko med seboj primerjamo na podlagi dveh značilnosti, spremenljivk, ki sta del slehernega IS-a (Gradišar, Resinovič, 2001, str. 364):

- **Stopnja strukturiranosti problemov, ki jih IS-i rešujejo.** Strukturiranost problema pomeni stopnjo entropije (mera za neurejenost sistema) sistema, ki za nas predstavlja problem. Problem, ki ga želimo rešiti, lahko definiramo kot informacijo, ki jo želimo, ali izhodno informacijo proučevanega sistema. Za dobro strukturiranost problema morajo biti elementi, ki predstavljajo vhodne podatke sistema, ter njihove povezave, znani. Problem lahko definiramo tudi kot enačbo, s katero odvisne elemente pretvorimo v rešitev problema.

- **Nivo usklajevanja dela.** IS-i se med seboj ločijo po številu udeležencev, ki z njihovo pomočjo usklajujejo aktivnosti, ki jih izvršujejo. Usklajevanje lahko poteka med aktivnostmi enega človeka, delovne skupine, organizacije ali skupine organizacij.

Klasifikacija bančnega informacijskega sistema razvršča ta sistem na tri plasti podsistemov:

- **Informacijski podsistemi strežbe**, ki jih ločimo v dve skupini:

    1. Informacijske podsisteme bančnih enot – ti podpirajo osebno strežbo tako standardiziranih kot tudi individualno oblikovanih bančnih storitev; pri tem upoštevajo učinkovitost strežbe (hitrost), dodano vrednost svetovanj in informatiziranje gotovinskega poslovanja.
    2. Informacijske podsisteme elektronskih prodajnih poti – ti podpirajo samopostrežbo bančnih strank; pri tem upoštevajo dosegljivost bančne storitve, enostavnost uporabe, zanesljivost delovanja in varnost.

- **Informacijski podsistemi podpore** – so povezani z operativnimi postopki delovanja banke, ki so za stranke nevidni in so povezani zlasti z evidentiranjem (knjiženjem).
  Informacijske podsisteme podpore ločimo v tri skupine:

    1. Informacijski podsistemi, v katerih se izvaja potrebna podpora posamezni bančni storitvi, ki ni neposredno povezana s strežbo.
    2. Informacijski podsistemi, ki omogočajo horizontalno in vertikalno povezovanje in avtomatizacijo bančnih procesov.
    3. Informacijski podsistemi, ki so v funkciji informatizacije raznih notranjih del poslovanja banke, kot je npr. kadrovsko področje.

- **Informacijski podsistemi managementa** – so povezani z upravljanjem banke.
  Informacijske podsisteme managementa ločimo v tri skupine:

1. Informacijski podsistemi za obvladovanje tveganj.
2. Informacijski podsistemi za upravljanje odnosov s strankami.
3. Informacijski podsistemi za upravljanje donosnosti in drugih vidikov kontrolinga (opredelitev vizije, poslanstva in ciljev banke, določanje ukrepov za uresničenje načrtovane donosnosti, sestava planov, optimalna uporaba razpoložljivih virov itn.)

2.3 RAZVOJ INFORMACIJSKEGA SISTEMA

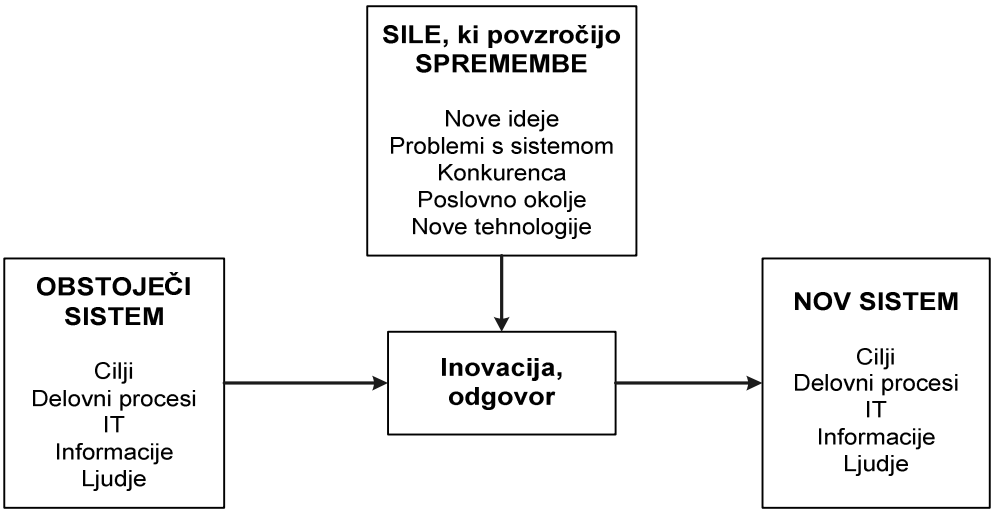
Pri izgradnji oziroma prenovi informacijskega sistema lahko uporabimo tradicionalni tehnološki ali strateški pristop.

Tradicionalni pristop temelji na preslikavi poslovnih in delovnih postopkov v aplikativne rešitve, s čimer je zanemarjena ideja o prenovi poslovanja in največ, kar lahko dosežemo s tehnološkim postopkom, je dvig učinkovitosti izvajanja obstoječih poslovnih postopkov (Kovačič, 1997, str. 2). Z vključitvijo prvih računalnikov v informacijske sisteme je postala preslikava rutinskih ročnih postopkov v aplikativne rešitve možna ter je povzročila veliko znižanje stroškov procesa. Prvi IS-i so najprej skrbeli za obdelavo podatkov, pozneje pa za obdelavo procesov. IS, ki poleg grobe preslikave izvaja tudi analize podatkov, se imenuje IS za podporo odločanja, pojavil pa se je v sedemdesetih letih 20.stoletja.

Strateški pristop temelji na možnostih, ki jih ponuja informacijska tehnologija in stremi k najučinkovitejši uporabi informacijskega sistema z namenom doseči strateško prednost na nekem področju. (Kovačič, 1997, str. 2; Alter, 1995, str. 288-298). V začetku devetdesetih so se pojavili strateški IS-i, ki so omogočali primerjavo, spremljanje in analizo poslovanja posameznih delov organizacije v povezavi z zunanjim okoljem (Groznik, Kovačič, 2001, str. 12).

Dinamika poslovnega okolja, ter predvsem s tem povezane nove tehnološke možnosti, je razlog za nujnost stalnega spreminjanja informacijskega sistema podjetja, da bi dosegli spreminjajoče se organizacijske cilje. Načrtovanje in razvoj IS-a tako postaneta iterativna procesa s stalnim prilagajanjem na spremembe okolja ter izkoriščanjem novih tehnoloških možnosti.

Slika 2: Razvoj novega informacijskega sistema



Vir: Alter, 1992, str. 10.

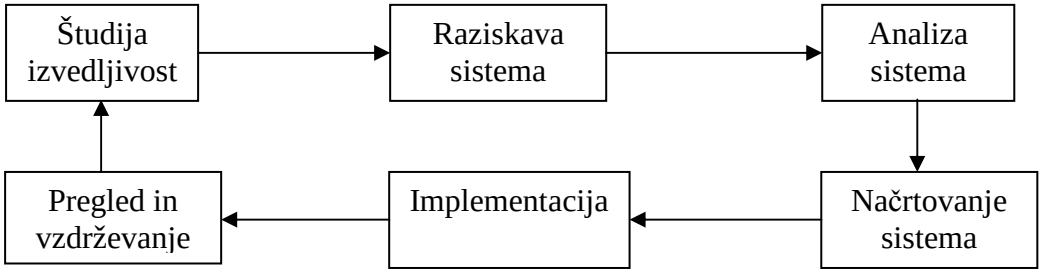
Splošna načela izgradnje IS so (Avison, Shah, 1997, str. 306):

- sodelovanje uporabnikov,
- jasno definiran problem,
- določene morajo biti posamezne faze in aktivnosti,
- določena morajo biti pravila za skladen razvoj IS-a in ustrezna dokumentacija,
- stalno je potrebno preverjati izvedljivost projekta,
- možnost razširitve ter spremembe IS-a.

2.4 ŽIVLJENJSKI CIKEL RAZVOJA INFORMACIJSKEGA SISTEMA

Ena od metodologij razvoja IS-a je življenjski cikel razvoja IS-a. Razvili so jo v Veliki Britaniji konec šestdesetih let in predstavlja podlago za mnogo drugih danes razvitih metodologij. Faze metodologije so prikazane na sliki 3.

Slika 3: Faze tradicionalnega življenjskega cikla razvoja informacijskega sistema



Vir: Razvojno življenjski cikel, 2004.

Postopki so naslednji:

- V študijo izvedljivosti spadajo postopki, in sicer: rezultat obstoječe situacije, analiza zahtev, možne rešitve in izdelava poročila.

- Ko je poročilo izdelano in odločitev sprejeta, pričnemo z raziskavo sistema. Prejšnji informacijski sistem prikažemo z raznimi pripomočki, kot so npr. diagram tokov podatkov, diagram strukture poročanja v organizaciji, intervjuji itd. Postopek oziroma tehnika raziskovanja je v proučevanju obstoječih dokumentov, intervjujev, razni vprašalniki in opazovanje obstoječih načinov dela.

- V fazi analize sistema poskušamo odkriti vzroke obstoječih problemov, vzroke uporabe določenih metod dela ter poskušamo izboljšati delovanje sistema.

- V fazi načrtovanja izdelamo podatkovno strukturo sistema, definiramo operacije, potrebne za obdelavo podatkov, načine testiranja ter načine zaščite sistema.
- V fazi implementacije nakupimo ustrezno strojno in programsko opremo ter opravimo vso potrebno kodiranje programov oziroma namestimo kupljeno programsko opremo.

- Po vseh fazah izgraditve informacijskega sistema ga ponovno pregledamo. Ugotovimo skladnost delovanja informacijskega sistema z načrtovanimi zahtevami ter skladnost dejanskih stroškov z načrtovanimi.

2.5 STRATEŠKO NAČRTOVANJE INFORMACIJSKEGA SISTEMA

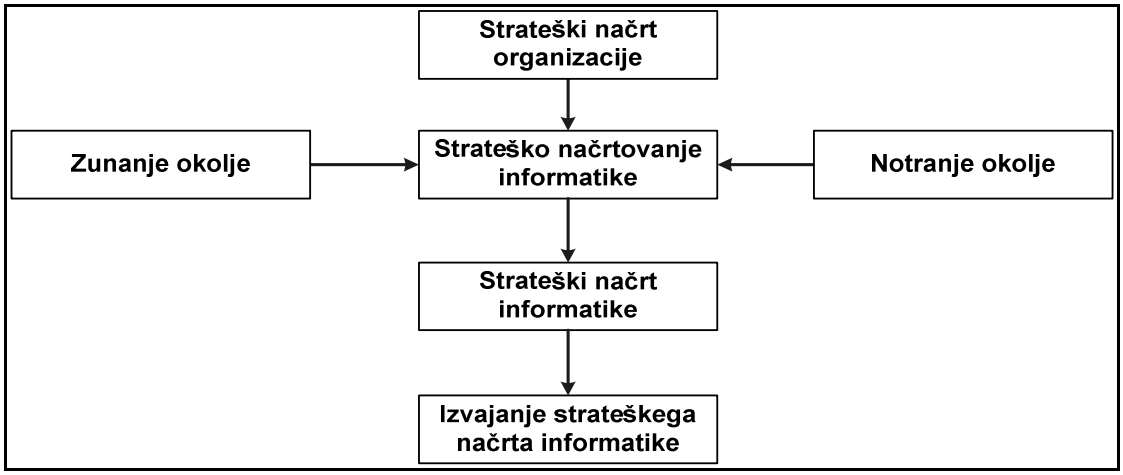
Razvoj informacijskega sistema je projekt, ki mora biti ustrezno načrtovan, če želimo, da bo uporabljen v praksi (Kovačič, Vintar, 1994, str. 176). Pot do konkurenčne prednosti je določena v strateškem načrtu podjetja. Del strateškega načrta je strateški načrt informatike. Proces izdelave strateškega načrta informatike imenujemo strateško načrtovanje informatike. Strateški načrt informatike je lahko določen z različnimi orodji, kot so profil prednosti in slabosti, profil poslovnih možnosti in nevarnosti, ključni dejavniki poslovnega uspeha, itn. Strateški načrt funkcijskega področja informatike mora biti usklajen z strateškim načrtom celotne organizacije.

Ko razvijemo vrsto možnih funkcionalnih strategij v podjetju, se takoj postavi vprašanje, katera funkcionalna strategija je primarna in katera drugotnega pomena (Pučko, 1999, str. 278). Za doseganje sinergijskih učinkov različnih funkcionalnih strategij je potrebna koordinacija planiranja.

Strateški informacijski sistem postaja vedno pomembnejše orodje za dosego konkurenčne prednosti podjetja, vendar je zaradi kompleksne tehnologije in zelo hitrih sprememb v okolju

izredno težko zagotavljati skladnost med izvajanjem strateškega načrta informatike ter izhodišči poslovnega strateškega načrtovanja.

Slika 4: Proces strateškega načrtovanja informatike



Vir: Groznik, Kovačič, 2001, str. 12.

3 STANDARD BS7799

Informacije in podatki, ki so v informacijskem sistemu shranjeni, so ključnega pomena pri vodenju podjetja oziroma organizacije in zagotavljanju nemotenega poslovnega procesa. Dobro varovani informacijski sistemi omogočajo hitrejšo izmenjavo podatkov teh informacij, s tem pa tudi povečajo zanesljivost delovnega procesa in povečajo konkurenčnost. Informacijsko varnost v informacijskem sistemu nam omogoča tudi standard, v Sloveniji znan pod imenom PSIST BS7799.

3.1 KAJ JE STANDARD?

Standard je (Standard varovanja informacij po standardu BS 7799, 2004):

- dokumentiran dogovor, ki vsebuje tehnične specifikacije ali druge natančne zahteve, ki naj bodo stalno uporabljane kot pravila oziroma smernice;
- definicija karakteristik, ki zagotovijo skladnost materialov, proizvodov, procesov in storitev.

Slovenija je **vstopila v Evropsko unijo 1. maja 2004** in mora izvajati tudi ukrepe na področju varnosti informacij. To omogoča slovenskim gospodarskim družbam in organizacijam poslovanje na enakovreden način s tujimi partnerji. Vodilna svetovna organizacija za omenjena področja je British Standards Institution (BSi), ki je leta 2002 izdala novo izdajo standarda BS 7799-2:2002.

Kratica BS pomeni, da gre za britanske standarde, 7799 je prepoznavna številka standarda, številka 2 pomeni, da gre za drugi del tega standarda, 2002 pa je letnica izdaje.

V letu 2003 je bil v Sloveniji standard sprejet kot **slovenski standard (SIST)**. Objavljen je v dveh delih:

- SIST BS 7799-2:2003 – Sistemi za upravljanje varovanja informacij – Specifikacija z napotki za uporabo.
- SIST ISO/IEC 17799:2003 - Informacijska tehnologija – Kodeks upravljanja varovanja informacij.

Za finančne institucije je Banka Slovenije leta 2003 izdala sklep, da morajo banke za opravljanje bančnih storitev upoštevati slovenska standarda SIST BS 7799-2:2003 in SIST ISO/IEC 17799:2003. Poleg bank in v ostalih organizacijah morajo standard upoštevati tudi v državni in javni upravi za varovanje in zaščito informacij.

3.2 VELJAVNOST MEDNARODNIH STANDARDOV V SLOVENIJI

Za veljavnost mednarodnega standarda v posamezni državi je potrebno izpeljati določen postopek. V Sloveniji je zato zadolžen Slovenski inštitut za standardizacijo SIST, ki je ustanovljen po zakonodaji, usklajeni z zakonodajo Evropske unije. Naloga SIST-a je, da izdaja standarde, ki veljajo za področje Republike Slovenije. Hkrati preverja skladnost z zahtevami v naši državi za mednarodne ali druge standarde. Ti se lahko privzamejo ali pa prevedejo.

3.3 NALOGA STANDARDA BS 7799/ISO 17799

Poslovanje v skladu s standardom BS 7799/ISO 17799 zagotavlja upravljanje varnosti informacij. Pod tem pojmom razumemo zaupnost, celovitost in dostopnost informacij. Zaupnost zagotavlja, da je določena informacija dostopna samo tistemu, ki mu je namenjena. Celovitost zagotavlja točnost in popolnost informacije ter metod obdelave teh. Dostopnost zagotavlja, da imajo avtorizirani uporabniki dostop do informacije in s tem povezanih sredstev, kadarkoli je to potrebno.

3.4 SORODNOST STANDARDA BS 7799

Pridobljen certifikat po standardu BS 7799/ISO 17799 organizacijam zagotavlja varnost pri posredovanju in shranjevanju informacij. Je orodje stalnega izboljševanja poslovnega procesa v smislu upravljanja varnosti informacij. Vzpostavljen notranji sistem je potrebno namreč vzdrževati ter ga stalno izboljševati. Ravno v tem je ta standard soroden s standardi ISO 9000 (kakovost), 14000 (okolje), 18000 (zdravje zaposlenih). Omenjeni standardi se zbližujejo tudi

po svoji strukturi z namenom zniževanja stroškov pri vzpostavitvi in vzdrževanju dveh ali več standardov v istem podjetju.

3.5 ZAGOTOVILO PRI OPRAVLJANJU VARNOSTI INFORMACIJ

Zagotovilo za varnost informacij organizacijam omogočajo postopki, kot so načrtovanje, nadzor in popravila, način izvedbe ter stalne izboljšave. Ta postopek je bolj znan pod kratico PDCA (Plan, Do, Check, Act).

Za standard BS 7799/ISO 17799 so glavni postopki upravljanje tveganja, načrti izboljšav ter nadzorstvo, ki je izvedeno iz analize tveganja. Analiza tveganja predstavlja nosilni del standarda.

Kontinuiteto in stalne izboljšave zagotavljamo z obveznimi notranjimi pregledi sistema. Zunanji neodvisni pregled pooblaščene ustanove pa nam omogoča tudi certificiranje skladnosti s standardom.

3.6 VARNOST INFORMACIJSKIH SISTEMOV V EU

Razvoj elektronskega poslovanja močno spodbuja komisija Evropske unije in pripravlja rešitve za zmanjševanje tveganj na tem področju. Ključno pri tem je zagotavljanje zaupnosti v elektronsko poslovanje.

Evropska unija ureja varnosti mrež in informacijskih sistemov z več dokumenti, med katerimi ima posebno vlogo resolucija Sveta Evrope za mrežno in informacijske varnosti znotraj Evrope. V nadaljevanju je predstavljena vsebina te resolucije in nekateri pomembni sprejeti dokumenti, ki jih navedena resolucija upošteva.

3.6.1 RESOLUCIJA SVETA EVROPE

Pomembno vlogo v tej resoluciji igrajo članice, ki morajo promovirati varnost kot občutljiv element na področju upravljanja v javnem in privatnem sektorju, ljudem zagotoviti ustrezno izobraževanje in zavedanje o problemih s področja varnosti. Vpeljati morajo tudi ukrepe za preprečitev in odzivanje na varnostne grožnje z nenehnimi izboljšavami pri odkrivanju varnostnih problemov ter z uporabo primernih kontrol.

Institucije Evropske unije in članice morajo razviti tudi obsežno evropsko strategijo na področju mrež in informacijskih sistemov ter vzspostaviti kulturo na področju varnosti pri mednarodnih povezavah. Pomembna naloga pri razvoju kulture je določitev odgovornosti na področju varnosti mrež in informacijskih sistemov. Državljani in podjetja morajo imeti zaupanje v informacije, ki morajo biti točne, zaupne in zanesljive.

Za dosego ustrezne kulture na področju varnosti pa je pristojen OECD (angl. Organisation for Economic Co-operation and Development) - Organizacija za ekonomsko sodelovanje in razvoj, ki predstavlja navodila za varnost informacijskih sistemov in mrež.

3.6.2 RESOLUCIJA SVETA EVROPE IZ LETA 2002

Resolucija poudarja pomembnost varnosti mrež in informacijskih sistemov. Sem spadajo smernice, ki jih je Evropski parlament sprejel po letu 1995 in se nanašajo na telekomunikacijske povezave, obdelovanje, prenos in zaščito osebnih podatkov ter na elektronski podpis. Varnost transakcij in podatkov postaja občutljiva pri elektronskem poslovanju. Zato se pojavlja potreba, da posamezniki, podjetja in organizacije zaščitijo svoje informacije, podatke in komunikacijske sisteme z učinkovitimi tehnologijami. Varnost mrež in informacij se nanaša na:

- zaščito zaupnosti podatkov;
- zaščito informacijskih sistemov proti nepooblaščenim dostopom;
- zagotavljanje razpoložljivosti servisov in podatkov;
- preprečevanje prekinitev in nepooblaščenega prestrezanja podatkov;
- potrjevanje, da so podatki, ki so bili poslani, prejeti ali arhivirani, kompletni in nespremenjeni;
- zaščito verodostojne overovitve;
- zaščito proti zlonamernim programom.

Navodila OECD za varnost informacijskih sistemov in omrežij so:

- pospeševati večje zaupanje med članicami,
- dvigovati zavest o tveganju na tem področju,
- pospeševati zavedanje o varovanju informacijskih sistemov in mrež med vsemi članicami,
- ustvariti splošna navodila za boljše razumevanje varnostnih ciljev,
- pospeševati večjo pozornost varovanju kot pomemben cilj med vsemi članicami,
- pospeševati sodelovanje in izmenjavo informacij med vsemi članicami pri razvoju in implementaciji varnostnih politik.

Ob tem so sledili načelom:

- zavedanja, da se članice morajo zavedati nujnosti varovanja informacijskih sistemov in mrež ter izboljšanje tega področja;
- odgovornosti za varovanje informacijskih sistemov in mrež;
- reagiranja na varnostne incidente;
- etike o spoštovanju pravic ostalih udeležencev v procesu;
- demokratičnosti z osnovnimi vrednotami demokratične družbe;
- načrtovanja in izspostavitve varovanja;
- vrednotenja tveganja;

- upravljanja varovanja;
- ponovnega ocenjevanja; članice morajo pregledovati in izvajati ponovne ocene varovanja informacijskih sistemov in mrež ter hkrati narediti ustrezne popravke v varnostnih politikah, navadah, merah in postopkih.

3.7 AKCIJSKI NAČRT E-EVROPE DO LETA 2005

Akcijski načrt e-Evrope je izdelan za obdobje od leta 2003 do 2005. Cilj tega načrta je zagotoviti novih delovnih mest, dvig produktivnosti, moderniziranje javnih služb in dajanje možnost vsakomur, da sodeluje v informacijski družbi. Načrt pa je sestavljen iz dveh delov, ki sta medsebojno povezana, in sicer na e- poslovanje in postavitev varne informacijske infrastrukture (Andolšek, Terčelj, 2003, str. 146).

4 ELEKTRONSKO POSLOVANJE IN INTERNET

EP je poljubna oblika poslovne transakcije, v kateri stranke delujejo elektronsko in ki nadomešča pošiljanje sporočil v fizični obliki oz., pri katerem stranke niso v neposrednem stiku. EP je komercialna aktivnost, ki se izvaja prek elektronskih omrežij, pogosto prek interneta, in je povezana s poslovno storitvijo, prodajo ali nakupom.

Razvoj elektronskega poslovanja označujemo z razvojem računalniških omrežij in interneta, z združevanjem informacijske in telekomunikacijske tehnologije ter standardom za računalniško izmenjavo podatkov, katerega začetki segajo v leto 1968. Takrat ni nihče slutil, s kakšno hitrostjo in kako intenzivno bo razvoj informacijske tehnologije in telekomunikacij vplival na spremembo načina življenja in poslovanja (Jerman-Blažič, 2001, str. 13).

Pomembne sestavine elektronskega poslovanja so računanalnik, programska oprema in komunikacije, ki so nek podsistem organizacije poslovanja, ki je ključnega pomena za podporo ciljev poslovnega sistema.

Elektronsko poslovanje lahko opredelimo kot: elektronsko trgovanje (trading), elektronsko bančništvo (banking, telebanking), elektronsko plačevanje (potrošniško: e-čeki, e-gotovina, e-kartice, bankomati), delo na daljavo (teleworking), elektronsko založništvo (e-publishing), elektronska ponudba (katalogi, videotekst), elektronsko zavarovalništvo, elektronsko borzno poslovanje, elektronska prodaja (potrošniška, retailing, avkcije na daljavo) ter notranje elektronsko poslovanje (npr. v organizaciji) (Toplišek, 1998, str. 5).

Pomembni elementi elektronskega poslovanja so:

- Način dela: gre za računalniško izmenjavo podatkov ob uporabi odprtih omrežij, kot je internet;

- Vsebina poslovanja: prodaja blaga in storitev, plačevanje, prodaja informacij, bančne transakcije, izmenjava dokumentov in listin, storitve trženja in medosebnega komuniciranja, nakupovanje v spletnih trgovinah, opravljanje dela na daljavo, omogočanje pomoči na daljavo (npr. zdravniške), izvajanje pouka na daljavo, storitve državne uprave na daljavo ipd;
- Udeleženci poslovanja: posamezniki (podjetniki, raziskovalci, managerji, občani, kulturni delavci, študenti, učitelji, dijaki, upravni delavci), podjetja, bolnišnice, muzeji, galerije, univerze, izobraževalne ustanove in državne ustanove. Gre za poslovanje znotraj posameznih skupin in za poslovanje med skupinami. V zadnjem času je vse več predvsem poslovanja med posamezniki ter med posamezniki in podjetji (Jerman-Blažič, 2001, str. 11-12).

Poznamo več vrst elektronskega poslovanja. V tabeli 1 so prikazane vrste elektronskega poslovanja glede na medsebojno delovanje udeležencev.

Tabela 1: Vrste elektronskega poslovanja glede na medsebojno delovanje udeležencev

	DRŽAVA (ang. Government)	**PODJETJA** (angl. Business)	**POTROŠNIKI** (angl. Customers)
DRŽAVA (ang. Government)	G2G npr.koordinacija	G2B npr.informiranje	G2C npr. informiranje
PODJETJA (angl. Business)	B2G npr. oskrba	B2B npr. e-trgovina, e-banka	B2C npr. e-trgovina, e-banka
POTROŠNIKI (angl. Customers)	C2G npr. davki	C2B npr. primerjava cen	C2C npr. dražbe

Vir: Penger, 2001, str. 65.

Tabela 1 prikazuje možne kombinacije elektronskega poslovanja med različnimi področji poslovanja.

Tako elektronsko poslovanje med podjetji in potrošniki (B2C, angl. Business to Customers) zajema področja, ki večinoma temeljijo na poslovanju z uporabo internetnih spletnih strani. Na ta način lahko potrošnik opravlja raznovrstna opravila (izobraževanje, nakupi, plačevanje položnic) prek domačega računalnika oz. ima neposreden dostop do informacij pri proizvajalcu.

Elektronsko poslovanje med podjetji (B2B, angl. Business to Business) zajema povezavo med prodajalci na drobno in dobavitelji, elektronsko bančništvo, sodelovanje na skupnih projektih itn. Po ocenah raziskav to predstavlja največji del elektronskega poslovanja. Elektronske dražbe na internetu so primeri povezav potrošnik – potrošnik (C2C, angl. Customers to Customers).

Pri poslovanju z državno upravo ločimo njeno poslovanje s podjetji (G2B, angl. Government to Business) in poslovanje s prebivalci (G2C, angl. Government to Customers). Zadnje je eno najzahtevnejših področij, ker zahteva lokalni dostop do teh storitev vseh državljanov in članov skupnosti. Povezava potrošnik – javna uprava (C2G, angl. Customers to Government) omogoča elektronsko povezavo med navedenima skupinama, npr. e - dohodnina in povezava podjetje - javna uprava (B2G, angl. Business to Government) pokriva vse transakcije med podjetji in javno upravo.

4.1 INTERNET

Internet lahko opredelimo kot omrežje računalniških omrežij in samostojnih računalnikov, ki povezuje računalnike po vsem svetu in s tem ljudi, ki delajo z njimi, ter vsebuje ogromno količino podatkov. Kar je pomembno, je to, da nihče ni lastnik interneta. Računalniška omrežja so povezana preko interneta tako, da lahko vsak računalnik po elektronski poti komunicira z vsakim. Internet v najširšem pomenu besede zajema številne strežnike, ki nam ponujajo določene storitve, ter združuje množico uporabnikov interneta. Strežnik je računalnik, ki je povezan v internet, in v katerem so shranjene vse datoteke posamezne spletne strani. Njegova naloga je, da prikaže spletno stran vsakemu uporabniku interneta, ki prek brskalnika sporoči zahtevo za ogled strani. Datoteka je oblika organizacije podatkov v poslovnih sistemih, ki jo sestavlja skupina zapisov, ki opisujejo kakšno stvar, osebo ali dogodek. (Gradišar, Resinovič, 1993,str. 199) .Poleg posredovanja podatkov lahko strežniki opravljajo še številne druge naloge – lahko obdelajo podatke, preden jih pošljejo stranki, medsebojno sodelujejo z zunanjimi aplikacijami itn.

Glavna prednost interneta je v njegovi izjemni razširjenosti po vsem razvitem svetu in nizkih stroških uporabe njegovih storitev, med katere spada:

- Uporaba svetovnega spleta (World Wide Web-a, WWW-ja) za objavljanje, iskanje ter prenašanje podatkov. Svetovni splet je najhitreje rastoči del interneta, sestavlja pa ga množica spletnih strani, ki tvorijo obsežen vir najrazličnejših informacij in podatkov. Spletne strani so običajno napisane v programskem jeziku HTML (Hypertext Markup Language), podatki pa se prenašajo po protokolih HTTP ali HTTPS.

- Prenos datotek iz drugih računalnikov in strežnikov – poteka preko posebnega protokola (FTP – File Transfer Protocol).

- Dostop do drugih računalnikov – Telnet. Uporablja ga malo ljudi, ker ne omogoča veliko povezav. Primer uporabe telneta je katalog elektronske knjižnice.

- “Pogovor” preko računalnika – IRC (Internet Relay Chat). IRC je namenjen sporazumevanju z drugimi uporabniki preko intrnetnetga omrežja. Pogovor poteka v živo z uporabo tipkovnice, s katero se odtipka sporočilo ali vprašanje in skoraj tako dobimo

odgovor. To pomeni, da se vsi lahko pogovarjamo z vsemi. Najpogosteje se za IRC uporablja program mIRC, s katerim se povežemo s strežnikom, ki se nahaja v enem izmed večih omrežij.

- Videokonferenca.

- Skupinske javne novice – Newsgroups. Namen javnih novic je omogočiti diskusijo s puščanjem sporočil in odgovorov na skupni oglasni deski. Potrebujemo dostop do strežnika, ki streže novice, npr. news.uni-lj.si, in program za delo z novicami, npr. Outlook Express.

- Archie, Gopher, Veronica, Wais. Program Archie je bilo kot eno prvih iskalnih orodij na Internetu. FTP omogoča pridobivanje datotek s podatki ali programi, Archie pa je orodje za iskanje teh datotek. Gopher je storitev, ki preko menijev omogoča preprosto iskanje informacij o najrazličnejših temah in uporabniku ni potrebno poznati ukazov. Vse podatke prikazuje kot imenike ali datoteke. WAIS (Wide Area Information Servers) omogoča distribuirano povezavo iskalnikov, ki skrbijo za iskanje po lokalnih podatkovnih zbirkah, pri katerem sodelujejo tudi strežniki, ki so povezani po celem svetu. Uporabnik postavi WAIS-u iskalno zahtevo, WAIS pa sam posreduje zahtevo izbranim informacijskim strežnikom po celem svetu in od njih spet zbere odgovore. Iskanje torej teče globalno. Gopher in WAIS sta neposredna predhodnika WWW-ja. Celoten Gopherjev splet lahko preiščemo s posebnim servisom Veronica. Z odjemalcem za Gopher se moramo povezati s strežnikom Veronica in temu poslati zahtevo za iskanje.

- Elektronska pošta za prenos elektronskih sporočil med lastniki elektronskih naslovov.

Ko govorimo o računalniških komunikacijah oz. o komunikacijskih protokolih, imamo v mislih predvsem komuniciranje računalnika z računalnikom. Če želimo, da sporočilo, ki ga vnesemo v svoj računalnik, sprejme drug računalnik, ki je v povezavi z našim, moramo zagotoviti komunikacijo med računalnikoma. Tako kot ljudje pri komuniciranju uporabljamo besede in slovnična pravila, računalniki pri svojem povezovanju uporabljajo računalniški jezik. Ta je strukturiran v obliki dogovorjenih pravil in postopkov, ki jim pravimo protokoli. Protokol je računalniški jezik, strukturiran v obliki različnih pravil, dogovorov in postopkov, ki vodijo in opravljajo prenos informacij.

Računalniki, ki so povezani v omrežje internet, za medsebojno komuniciranje uporabljajo standard oz. protokol TCP/IP (Transmission Control Protocol/Internet Protocol). V slovenščini bi lahko protokol TCP/IP opredelili kot krmiljenje pošiljanja/internetni protokol, ki je standardno sredstvo za prenos oz. izmenjavo podatkov med subjektoma komuniciranja v omrežju. Po IP standardu, ki se uporablja v največjem svetovnem omrežju, je dobilo omrežje tudi svoje ime - internet omrežje.

Naslednji zelo pomemben protokol predvsem pri komuniciranju preko interneta je protokol HTTP (Hypertext Transfer Protocol). Običajno gre za HTTPS protokol z dodatnim protokolom za varen prenos podatkov (S je oznaka za varnost, ang. *Secure*). Varnost prenosa podatkov ponavadi zagotovimo z uporabo protokola SSL, ki ga bom predstavil v zadnjem delu diplomske naloge.

V slovenščini imenujemo protokol HTTP protokol za prenos hiperteksta. Njegova osnovna naloga je povezati odjemalca (uporabnika) s strežnikom (ang. server). Omogoča nam prenos besedila, slike, zvočnih zapisov in filmov. Standard za kodiranje hiperteksta oz. http-ja je Hypertekst Markup Language ali s kratico HTML. HTML je jezik, ki se uporablja za kreiranje linkovnih povezav. Ti linki so ali tekstovni ali grafični. S klikom na link, nas le ta poveže z drugim HTML dokumentom.

HTTP omogoča iskanje po svetovnem spletu – internetu ter branje in kopiranje vsebine spletnih strani. Omogoča kopiranje tako teksta, zvoka, videa, kot vseh drugih elementov. HTML pa se uporablja predvsem za predstavitev podatkov v spletnih straneh. Njegove oznake določajo, kako prikazati podatke, o podatkih samih pa ne povedo ničesar. HTML je torej odličen za predstavitev podatkov na spletu, vendar ne olajša ali pospeši integracije informacij na spletu z obstoječimi poslovnimi aplikacijami (Dečman, 2000, str. 52).

Konzorcij W3C (World Wide Web Consortium) je zaradi tega predlagal razvoj novega jezika. Leta 1998 so izdali podatkovni standard XML (Extensible Markup Language), ki je pomenil pomemben preobrat na nivoju definiranja same strukture dokumentov. Je univerzalni jezik za opis polstrukturiranih dokumentov ne glede na vsebino. Standardizacijo zapisa dokumenta dosega z opisnimi oznakami podatkov (meta-podatki) (Vavpotič, 2001, str. 71). Pred standardom XML je bila največja težava prebrati podatke v drugem programu, ki ga je izdelal drug razvijalec, saj vsak program po svoje shranjuje podatke v datoteke. Torej XML lahko naredi prenos podatkov med programi bolj učinkovit.

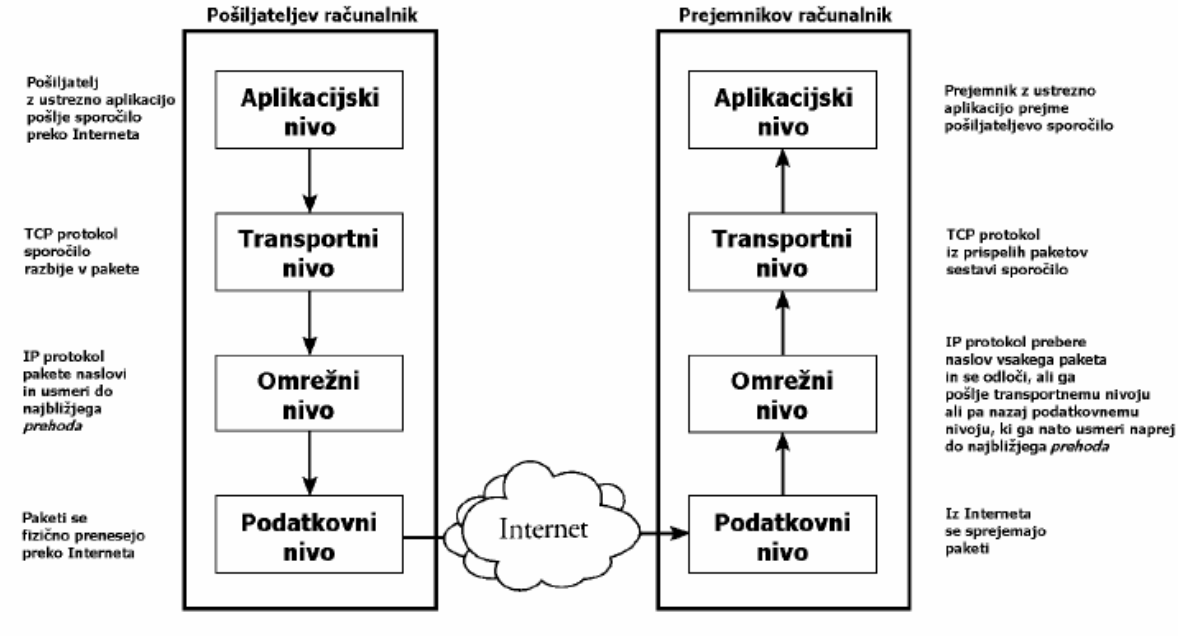
Osnovno načelo prenosa podatkov preko interneta je, da se podatki ne prenašajo celovito (v enem kosu), temveč kot »paketi« (Danda, 2001, str. 18). Tako se sporočilo, ki ga želimo prenesti preko interneta, najprej razbije v več kosov (paketov), nato pa se ti paketi posamično prenesejo do ciljnega računalnika, kjer se spet sestavijo v prvotno sporočilo. Na ta način lahko preko ene povezave (linije) poteka komunikacija med več uporabniki (računalniki), kar je glavna prednost tega protokola. Klasični način povezave med uporabniki (kot je npr. telefonska povezava) takšnega načina dela ne omogoča, saj mora vsak par uporabnikov, ki želita komunicirati med seboj, uporabljati svojo linijo. Ker pa je vedno na voljo le omejeno število povezav, lahko tak sistem hitro postane preobremenjen. Da bi si lahko uporabniki (s svojimi računalniki) preko Interneta izmenjevali podatke, mora biti vsak od njih enolično označen. V ta namen se uporabljajo IP naslovi oz. številke. Vsak računalnik, ki je neposredno priključen v internet, dobi svoj IP naslov, sestavljen iz dvanajstih številk (npr. 193.165.135.121).

Ko se sporočilo, ki ga pošiljamo preko interneta, razbije v več manjših paketov, se vsak od njih opremi tudi s posebno glavo, ki vsebuje IP naslov pošiljatelja in prejemnika paketa (Danda, 2001, str. 21). Ko paket potuje med računalniki po omrežju, vsak računalnik, ki sprejme paket, najprej preveri IP naslov prejemnika in temu primerno paket usmeri naprej do naslednjega računalnika ali omrežja. Takšnim računalnikom, ki skrbijo za usmerjanje paketov preko interneta, pravimo *usmerjevalniki* (routerji). Če pa je usmerjevalnik hkrati povezan tudi z določenim internim omrežjem (in imajo torej računalniki v internem omrežju preko tega usmerjevalnika tudi dostop do interneta), pa takšnemu računalniku pravimo *prehod* (gateway). Usmerjevalniki (ali prehodi) torej sprejemajo pakete, ki se prenašajo preko interneta, in jih usmerjajo naprej do naslednjih usmerjevalnikov (prehodov), ki so bližje ciljnemu računalniku. Ko paket pride do prehoda, ki je najbližje ciljnemu računalniku, ga prehod izvzame iz interneta in ga odvisno od povezave s ciljnim računalnikom po lokalnem omrežju ali modemu pošlje do tega računalnika.

Proces prenosa podatkov razdelimo na štiri nivoje (Danda, 2001, str. 20):

- aplikativni nivo (aplikacije, s katerimi uporabniki dostopajo do internetnih storitev);
- transportni nivo (ustvarjanje in sestavljanje paketov sporočil);
- omrežni nivo (naslavljanje in usmerjanje paketov);
- podatkovni nivo (fizično upravljanje s podatki, ki se prenašajo preko interneta, ter s strojno opremo, ki je potrebna za prenos podatkov).

Slika 5: Prenos podatkov preko interneta



Vir: Danda, 2001, str. 21.

TCP/IP protokol se izvaja na dveh od teh nivojev. Proces prenosa podatkov se začne na aplikativnem nivoju, ko uporabnik želi npr. poslati elektronsko sporočilo. Aplikacija, s katero

uporabnik pošilja sporočilo, le-to pošlje do transportnega nivoja, kjer jo TCP protokol razbije v več paketov in jih pošlje do omrežnega nivoja. Na tem nivoju IP protokol vsakega od paketov pripravi za prenos tako, da jih opremi z glavo, v katero zapiše vse podatke, potrebne za prenos paketa preko interneta (med drugim tudi IP naslov prejemnika in pošiljatelja). Ko so paketi pripravljeni za prenos, podatkovni nivo opravi še ostale korake, potrebne za prenos paketov preko interneta (preveri povezavo z internetom, modem oziroma mrežno kartico, nosilec podatkov računalnika itd). Paketi se nato pošljejo najbližjemu *usmerjevalniku* oz. *prehodu*, nato pa se preko drugih *usmerjevalnikov* in *prehodov* prenesejo do ciljnega računalnika. Sprejem sporočil (oz. paketov sporočil) poteka v obratnem vrstnem redu. Pakete iz interneta sprejema podatkovni nivo, ki skrbi za povezavo z internetom. Podatkovni nivo vsak sprejeti paket pošlje omrežnemu nivoju protokola. Ta preveri IP naslov paketa in ugotovi, ali je ta računalnik končni prejemnik tega paketa ali ne; če je, paket pošlje transportnemu nivoju, če pa ni, pa paket vrne podatkovnemu nivoju, ki ga usmeri do naslednjega računalnika (*usmerjevalnika* oz. *prehoda*).

Na transportnem nivoju TCP protokol sprejema pakete in iz njih sestavlja sporočilo. Paketi lahko prihajajo v drugačnem vrstnem redu, kakor pa so bili poslani, poleg tega pa se kakšen od njih med prenosom lahko tudi poškoduje ali izgubi. TCP protokol mora zato med sestavljanjem sporočila preveriti, ali so paketi prispeli nepoškodovani. Vsak paket se pred pošiljanjem ustrezno označi, tako da transportni nivo prejemnika natančno ve, kateri del sporočila je prispel, hkrati pa transportnemu nivoju pošiljatelja tudi sproti sporoča dolžino vsakega prispelega paketa, tako da se v primeru poškodbe določenega paketa ta pošlje še enkrat.

Ko transportni nivo prejemnika prejme vse pakete, je datoteka pripravljena za uporabo, zato jo TCP protokol pošlje aplikativnemu nivoju, s čimer je prenos podatkov zaključen (Danda, 2001, str. 21).

4.2 VARNOST ELEKTRONSKEGA POSLOVANJA

Zaščiteni oziroma zaupni podatki, ki so shranjeni na računalniških sistemih in potekajo preko omrežij, je za posameznike, podjetja in ostale ustanove kot npr. finančne organizacije, katerih dejavnost so denarni in kreditni posli, nevarnost razkritja podatkov, kar lahko pripelje do hudih posledic, kot je lahko finančni primankljaj. Zaupni podatki so lahko številke kreditnih kartic, poslovne skrivnosti, elektronsko-zdravstvene kartice, programske opreme sistemov, torej razne aplikacije, ki služijo za način izvedbe določene naloge.

Napadi, pred katerimi se podjetja želijo zavarovati, ne prihajajo zgolj samo zunaj lokalnega omrežja podjetij, ampak tudi znotraj lokalnega omrežja, zato je potrebno sisteme zavarovati tako zunaj kot znotraj

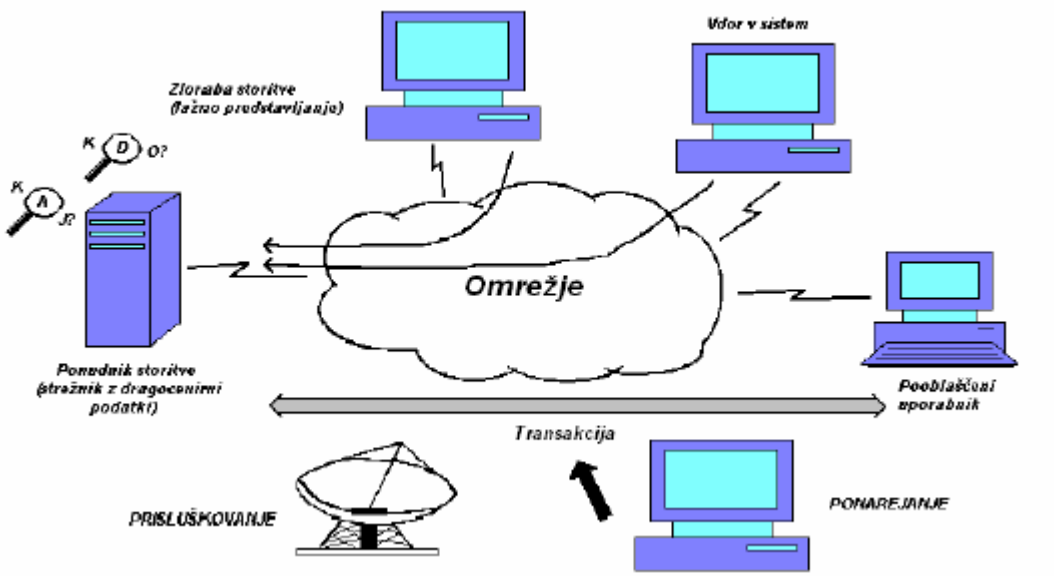
4.2.1 VRSTE NAPADOV

V računalniškem sistemu varujemo shranjene podatke, ki so ponavadi končni cilj potencialnega napadalca. Zaradi tega moramo zagotoviti (Pepelnjak, Bradeško, 1997, str. 157):

- varnost dostopa, kjer so predmet zaščite viri in storitve v sistemu;
- varnost uporabe, kjer je potrebno zagotoviti, da za dostop pooblaščeni uporabniki v sistemu počno le tisto, kar jim glede na njihov položaj pripada; zaščito potrebujejo tudi uporabniki sami – v banki ne pustijo, da bi uporabnik storitve (npr. pri vpogledu v bančni račun) pri tem doživel zlorabo s strani tretje osebe;
- varnost transakcij - vsi pomembni podatki, ki se izmenjujejo preko komunikacijskih poti, morajo preko teh potovati varno, brez možnosti, da bi jih kdo prestregel ali celo poneveril;
- vdori v sistem - ti imajo lahko za posledico le nepooblaščen dostop do podatkov in njihovo krajo, lahko pa tudi spremembo ali še huje, uničenje podatkov (med te napade lahko uvrstimo večino današnjih računalniških virusov, ki se prikradejo do sistema in povzročijo določeno škodo);
- prestrezanje sporočil - tu napadalec ne vdre v sam sistem, pač pa za dostop do podatkov (in tudi morebitno spremembo le-teh) uporabi prenosne poti, kjer z ustrezno strojno in programsko opremo prisluškuje ali spreminja podatke, ki potujejo po napadeni poti;
- onemogočanje storitev (denial-of-service) - kjer napadalec poskuša poslabšati kakovost storitve ali jo povsem onemogočiti (npr. z izjemno povečanim številom zahtev po določeni storitvi na sistemu, ki pod tako obremenitvijo ne deluje več optimalno, ali pa z umetnim ustvarjanjem nepotrebnega omrežnega prometa, ki zasiti prenosne poti);
- povzročanje stroškov - tu napadalec izkoristi določene varnostne pomanjkljivosti in uporabi storitev, do katere sicer ni upravičen – to napadenemu povzroča nepotrebne stroške, druge škode ponavadi nima; ti napadi so danes zelo popularni, saj napadalec pride do informacijskih virov zastonj ali mnogo ceneje kot sicer.

Omenjene napade srečujemo tudi v kombinirani obliki. Z nedolžnim prisluškovanjem se napadalec lahko prikoplje do podatkov (npr. gesel), s katerimi lahko povzroči veliko škode.

Slika 6: Vrste napadov v omrežjih



Vir: Pepelnjak, Bradeško, 1997, str. 159.

V današnjem času so najbolj pogosti vdori v sistem, ki imajo lahko za posledico ogromno škodo, kar še posebej velja za banke, ki se varujejo pred nepooblaščenimi dostopi do podatkov in njihovo krajo. Zato obstajajo določeni programi, ki zaščitijo računalnik oziroma strežnike pred potencialno nevarnimi vsebinami, ki prihajajo iz interneta. Eden izmed teh je požarni zid. S pomočjo tega imajo večji nadzor nad tem, kateri podatki prihajajo v računalnik in kateri gredo iz njega.

Internetni hekerji uporabljajo škodljive programe, kot so virusi, črvi in trojanski konji, in poskušajo najti odklenjena vrata – nezaščiten računalnik. Požarni zid varuje računalnik pred temi in drugimi zlonamernimi napadi.

Kaj lahko heker stori? Odvisno od narave napada. Nekateri napadi so zgolj nadležne potegavščine, drugi pa so ustvarjeni s škodljivim namenom. Ti škodljivi programi poskušajo zbrisati podatke v računalniku, ga zrušiti ali celo ukrasti osebne podatke, kot so gesla in številke kreditnih kartic. Nekateri hekerji z največjim veseljem vdirajo v nezaščitene računalnike. Virusi, črvi in trojanski konji so grozljivi. Na srečo lahko s požarnim zidom zmanjšate tveganje okužbe. Požarni zid preiskuje podatke, ki potujejo v splet in iz njega, ter zazna in prestreže tiste, ki prihajajo z nevarnih lokacij ali se zdijo sumljivi. Če požarni zid nastavite primerno, hekerji, ki iščejo ranljive računalnike, vašega ne bodo mogli zaznati.

Končno se uveljavlja tudi spoznanje, da končni rezultat povezave v internet ni samo požarni zid, ampak tudi posamezni računalniki, ki so za njim skriti. V večjih podjetjih hitro naraste možnost vdora in kraje informacij, saj je priključkov za dostop do omrežja velika. Zato obstajajo npr. omejitve omrežnega priključka na strojni naslov omrežne kartice, ki pa vseeno ni dovolj, saj je mogoče strojni naslov omrežne kartice dokaj enostavno ponarediti. Zaradi

tega so spisali standard (802.1x), ki omogoča dinamični vklop in izklop omrežnega priključka. Še večjo nevarnost za varnost omrežja predstavlja brezžična dostopna točka, saj je medij prenosa podatkov tu zrak in lahko vsak, ki ima prenosnik prisluškuje pogovoru med posameznimi brezžičnimi napravami, kar še posebej oteži zagotavljanje varnosti omrežja.

4.2.2 ELEKTRONSKO PODPISOVANJE KOT ZAŠČITA TRANSAKCIJ

Elektronski podpis je kot nadomestek lastnoročnega podpisa v elektronskem poslovanju. Razvitih je več metod elektronskega podpisovanja, med katere uvrščamo predvsem digitalni podpis, podpis z digitalnim peresom in biometrične metode. Podpis z digitalnim peresom je sistem, ki zajema sistem za zajemanje podpisa, sestavljen iz strojne in programske opreme ter sistem za preverjanje podpisa. Pod biometrične metode spada kar nekaj metod, kot so npr. uporabnikovo glasovno sporočilo, test oči oz. dela očesa (šarenice), ki enolično določa vsakega človeka itn. Sistema sta zelo varna za identifikacijo uporabnika, vendar med uporabniki interneta zaradi prevelikih stroškov strojne opreme, potrebne za njegovo uporabo, ni doživel večjega uspeha. V praksi pa se danes največ uporablja digitalni podpis, ki je zelo varen v elektronskem podpisovanju.

Digitalni podpis

Za digitalni podpis štejemo kodiran oziroma šifriran zapis podpisa v elektronskem sporočilu. Šifriranje spremeni podatke in informacije po nekem računskem postopku oz. algoritmu tako, da jih brez veljavnega kodnega ključa ne moremo dešifrirati oziroma povrniti v prvotno obliko. Na primer besedo "**Ključ**" s postopkom šifriranja spremenimo v "**xyzwq**". Dešifriramo pa jo lahko samo z ustreznim kodnim ključem, ki ga pozna le ustvarjalec oziroma tiste osebe, katerim ta posreduje ustrezni ključ. Lahko se ustvari poljubno število kodnih ključev za poljubno število oseb. Pomen šifriranja je zagotavljanje zasebnosti sporočila, medtem ko digitalni podpis kot lastnoročni podpis v elektronski obloki omogoča večjo verodostojnost oziroma pristnost sporočila in nam pove identiteto osebe, ko digitalno podpiše. Imamo dve vrsti digitalnega podpisovanja: enojni - simetrični in dvojni - asimetrični ključ.

Enojni ključ je geslo za shranjevanje besedila na računalniku ali pa geslo (PIN številka) bančne kartice. Ker imamo en ključ, pomeni da pošiljatelj in prejemnik uporabljata isti ključ oz. simetrični ključ. Pošiljatelj uporabi dogovorjeni ključ, prejemnik pa podpiše oz. preveri z istim ključem.

Pri podpisovanju dvojnih ključev gre za zasebni ključ (tajni) in javni ključ. Zasebni ključ je znan le enemu pošiljatelju in ga lahko dodatno zavaruje še z geslom. Da bi prejemnik lahko sporočilo dešifriral, mu mora biti znan drugi pošiljateljev ključ, ki se imenuje javni ključ. Javni ključ lahko pozna vsak. To pomeni, da javni in zasebni ključ nista ista. Zasebna ključa poznata le onadva (vsak le svojega), oba javna ključa pa sta vsem znana. Pošiljatelj sporočilo šifrira s svojim zasebnim ključem in prejemnikovim javnim ključem. Ta nato sporočilo dešifrira s svojim zasebnim ključem in pošiljateljevim javnim ključem

Podpis z identifikacijsko kartico

Elektronska kartica (chipcard, smart card), lahko se ji reče tudi pametna kartica, je naprava, ki je podobna kreditni kartici. Na njej imamo običajno shranjen zapis o istovetnosti pooblaščenega imetnika (certifikat oz. digitalno potrdilo), lahko pa vsebuje tudi množico drugih podatkov. Kot preprosto pomnilniško sredstvo se kartica uporablja tudi za elektronsko podpisovanje. Imetnik ima tako na elektronski kartici shranjen svoj zasebni ključ, ki ga naprava pri podpisovanju dokumentov avtomatično prebere s kartice.

Največjo možno varnost podatkov pa si zagotovimo, če uporabimo kartico, na kateri imamo shranjen svoj zasebni ključ v sistemu podpisovanja s ključi uporabnikov.

4.3 ELEKTRONSKO BANČNIŠTVO

Z reformo plačilnih sistemov so slovenske poslovne banke začele opravljati storitve plačilnega prometa tako za fizične kot za pravne osebe, s čimer so poleg novih poslovnih priložnosti naletele tudi na organizacijske in tehnične probleme. Banke so se pri ponudbi svojih storitev namreč soočile z množico novih komitentov, katerim dotedanje tržne poti, preko katerih so banke v začetkih devetdesetih let omogočale dostop do svojih storitev (bančno okence, bančni avtomat, telefaksno sporočanje in telefonski klicni center – teledom), zaradi obsežnosti njihovega poslovanja niso več zadoščale (Sistem elektronskega bančništva, 2004).

Že manjše podjetje namreč v povprečju opravi vsaj desetkrat več transakcij kot fizična oseba, vrednost teh transakcij pa je lahko tudi do stokrat višja, zato je zanj zelo pomemben sprotni vpogled v stanje in takojšnja možnost prenosa sredstev med svojimi računi ter na račune drugih pravnih oseb. Vsak dan, ko podjetje svojih sredstev ne investira, temveč ostanejo neizkoriščena na njegovem transakcijskem računu, pomeni zanj določeno izgubo v višini oportunitetnih stroškov. Banka sredstva na računih komitentov obrestuje po minimalni obrestni meri, zato je na računu najbolje hraniti le toliko sredstev, kolikor jih podjetje potrebuje za zagotavljanje tekoče likvidnosti, vsa ostala sredstva pa takoj vložiti v bolj donosne investicije.

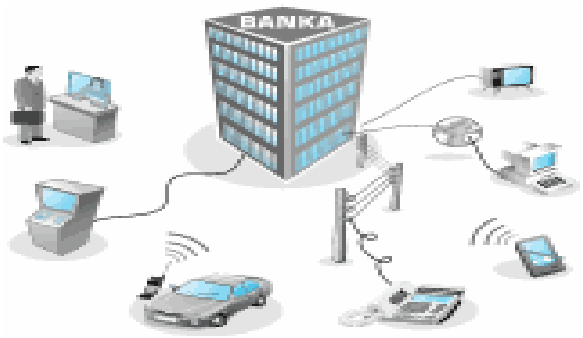
Po drugi strani je sprememba družbenoekonomskega sistema prinesla konkurenco tudi na področje bančnih storitev. Poslovne banke so tako že pred reformo plačilnega prometa začele iskati nove načine za čim večjo racionalizacijo poslovanja, hkrati pa so povečale borbo za ohranitev obstoječih in pridobitev novih komitentov. Zaradi vseh teh dejavnikov so banke zato kljub siceršnji konzervativnosti relativno hitro razvile nove tržne poti, ki jih je omogočil silovit razvoj informacijskih in komunikacijskih tehnologij v devetdesetih letih. Vse nove tržne poti temeljijo na takšni ali drugačni obliki elektronskega poslovanja oz. elektronskega bančništva.

4.3.1 SODOBNE E-BANČNE TRŽNE POTI

Sodobne tržne poti uporabljajo številne komunikacijske kanale, internet in telefon. Z uporabo skupnega sistema za povezavo produkcijskega okolja banke in tržnih poti lahko banka zagotovi učinkovito in cenovno ugodno podporo vsem tržnim potem. Večina poslovnih bank v Sloveniji se je odločila, da svojim komitentom ponudi storitve elektronskega bančništva, pri čemer se za prenos podatkov uporablja predvsem Internet. Banke ponujajo naslednje nove tržne poti (slika 7):

- spletno bančništvo;
- neposredno računalniško izmenjavo podatkov;
- klicne centre in klicne odzivnike;
- »off-line« bančništvo na podlagi arhitekture odjemalec strežnik;
- prenosne telefone, SMS sporočanje in WAP;
- telefaksno sporočanje;
- informacijske terminale.

Slika 7: Sodobne e- bančne poti



Vir: Sistem elektronskega bančništva, 2004.

Slika 7 predstavlja ključne tržne poti elektronskega bančništva oziroma osrednji bančni sistem elektronskega bančništva, ki temelji na enotnem strežniku sistema elektronskega bančništva in omogoča skrbništvo ter nadzor nad tržnimi potmi z enega mesta, obenem pa zagotavlja sprotno prenašanje zahtevkov, poslanih s katerekoli tržne poti. Bistvo sistema elektronskega bančništva se nahaja na banki in je skrito uporabnikovim očem. Poleg strojne in programske opreme, ki zagotavlja varno, neprekinjeno in stabilno delovanje sistema, je potrebno sistem upravljati in spremljati njegovo delovanje, za kar pa skrbijo usposobljeni bančni delavci.

Spletno bančništvo pravzaprav pomeni tretji korak t.i. samopostrežnega bančništva, ki se je začelo z bančnimi avtomati v sedemdesetih in nadaljevalo s telefonskim bančništvom v osemdesetih letih prejšnjega stoletja. Po nekaterih izračunih je opravljanje transakcij preko interneta za banke veliko cenejše od klasične transakcije, opravljene na bančnem okencu, in

dosti cenejše od opravljanja transakcij preko telefonskega bančništva (Sistem elektronskega bančništva, 2004).

Po drugi strani je internet v zadnjih letih postal izredno popularen in vsesplošno dostopen, tako da se njegovo število uporabnikov strmo povečuje. Priljubljenost novega medija in možnost za občutno racionalizacijo poslovanja sta tako večino bank po svetu in v Sloveniji vodila k ponudbi te nove tržne poti. Ker banke v Sloveniji sredi devetdesetih let še niso izvajale plačilnega prometa za pravne osebe, so spletno bančništvo najprej ponudile fizičnim osebam, pozneje pa so razvile tudi različne rešitve za potrebe podjetij.

Komitenti se iz različnih razlogov lahko odločijo tudi za neposredno računalniško izmenjavo podatkov z banko. Ta tržna pot je namenjena predvsem velikim podjetjem v podporo izmenjavi podatkov med velikimi podjetji. Njena prednost je v izmenjanih podatkov, saj omogoča enostavno povezavo z obstoječim informacijskim sistemom banke.

Vloga klicnega centra je v telefonskem svetovanju in trženju, telefonskemu bančništvu in posredovanju informacij prek samodejnega odzivnika. Poglavitno vlogo v klicnem centru imajo telefonski svetovalci in operaterji, ki si pri delu pomagajo s sodobnim skrbniško nadzornim sistemom. Klicni center je pomemben člen tudi zaradi podpore ostalim tržnim potem. Prihodnost klicnih centrov bo namreč temeljila na prenosu govora prek internetnih protokolov, ki poleg cenejših povezav omogočajo tudi sočasen prenos podatkov, slike in posnetkov ter tako postavljajo temelje video komunikaciji.

Arhitektura odjemalec strežnik odpravlja temeljno pomanjkljivost spletnega bančništva, ki onemogoča delo v načinu, ko uporabniki niso v živo povezani z bančnim strežnikom (Sistem elektronskega bančništva, 2004). Namenjena je predvsem manjšim in srednjim podjetjem, saj omogoča večbančno poslovanje (pregled računov podjetja pri različnih bankah) ter pripravo plačilnih nalogov v »off-line« načinu (brez povezave z bančnim strežnikom), poleg tega pa se lahko vse podatke avtomatično prenese v informacijski sistem podjetja, tako da ni potrebe po dvojnem vnosu podatkov in s tem povezanih napak pri vnosu ter izgube časa.

Razmah mobilne telefonije prinaša nove možnosti elektronskega poslovanja tudi preko teh naprav. Banke že sedaj ponujajo sporočanje v obliki kratkih sporočil (SMS), ki pa je zaradi varnostnih omejitev omejeno na pošiljanje podatkov v smeri iz banke proti komitentom. Vsebina sporočil zajema vse najpomembnejše informacije za komitente – spremembe na računih (prilivi, odlivi), stanje itn.

Nekatere banke in mobilni operaterji so pričakovali večji razmah mobilnega bančništva z uveljavitvijo protokola WAP, ki omogoča povezavo mobilnega telefona z internetom. Vendar pa trenutno obstoječa komunikacijska tehnologija še ne omogoča dovolj hitrega prenosa podatkov, tako da ta način poslovanja ni nikoli prav zaživel. Zato je glavni slovenski mobilni operater postavil mobilni sistem tretje generacije (UMTS), ki omogoča mnogo hitrejše

povezave z internetom, kar prav gotovo pripomore k večji popularizaciji mobilnega elektronskega poslovanja vseh vrst.

Prenos dokumentov v obliki telefaksnih sporočil sicer izginja iz širše uporabe, vendar v nekaterih okoljih ostaja trdno zakoreninjen. Zato je sporočanje v obliki telefaksnih sporočil zanimiva tržna pot za številne uporabnike, predvsem v poslovnih okoljih, tehnično pa je oblikovan kot sestavni del klicnega centra. Tehnične omejitve z vidika varnosti omogočajo sporočanje podatkov le v smeri iz banke proti bančnim strankam.

Informacijski bančni terminali so pravzaprav posodobljeni bančni avtomati, ki v večjem in sodobno oblikovanem ohišju združujejo računalnik in različne vhodno-izhodne naprave (poleg zaslona, občutljivega na dotik, je možno uporabljati tudi prirejeno tipkovnico in miško), kot sestavni del funkcionalnosti pa vsebujejo spletni vmesnik za elektronsko bančništvo. Takšni informacijski terminali bodo verjetno v nekaj letih zamenjali obstoječe bančne avtomate, ki so po obliki in funkcionalnosti že nekoliko zastareli. Internet prinaša tako nove priložnosti kot tudi nevarnosti za poslovne banke. Za njihovo razumevanje moramo najprej spoznati osnovne značilnosti novega medija ter način prenosa podatkov preko njega.

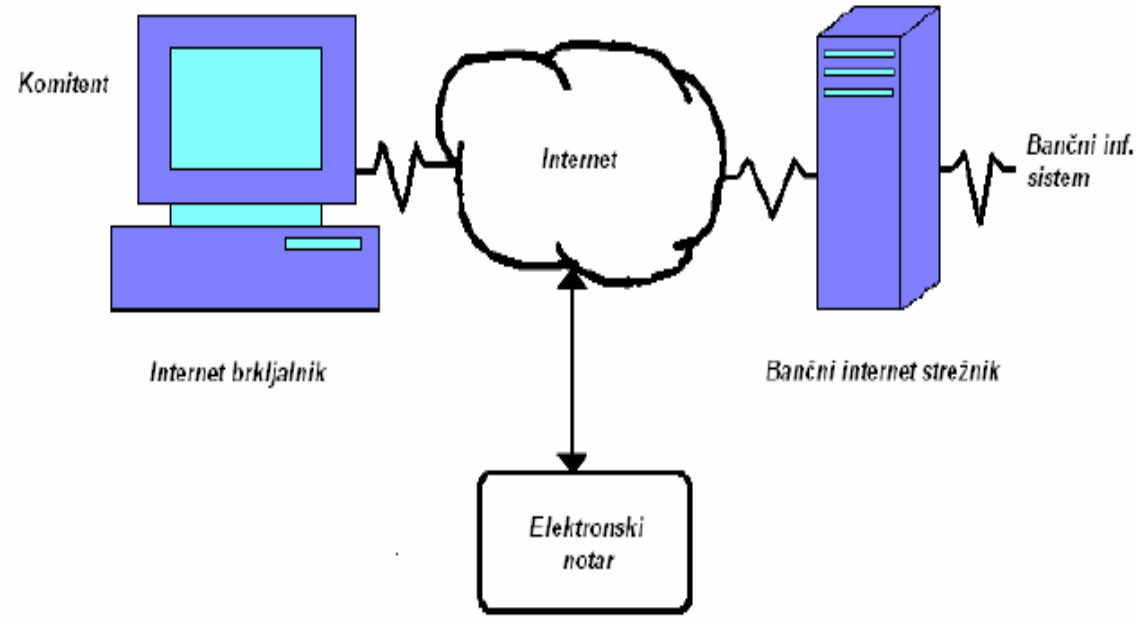
4.3.2 ELEKTRONSKO BANČNIŠTVO PREKO INTERNETA

Ponujene storitve preko elektronskega bančništva delimo na informacijske in transakcijske. V okviru informacijskih storitev banka nudi informacije o stanjih in transakcijah na računih, o dogajanju na kapitalskih trgih itd.. Med transakcijske storitve, ki jih opravljamo s sistemi elektronskega bančništva, štejemo vse storitve, ki vključujejo plačilne instrumente.

Delovanje elektronskega bančništva preko interneta ima nekaj pomembnih prednosti (Kovačič, 1997, str. 132):

- temelji na javnem standardnem načinu prenosa po komunikacijskem omrežju,
- vmesniki so standardizirani,
- za uporabo komitenti potrebujejo le osebni računalnik z modemom, telefon in standarden vmesnik,
- vmesniki nekaterih najbolj uveljavljenih proizvajalcev so brezplačni,
- vmesniki podpirajo varen prenos podatkov preko javnih telefonskih omrežij,
- komitent in banka se lahko prepričata o medsebojni identiteti na standardiziran način.

Slika 8 : Princip delovanja sistemov elektronskega bančništva preko interneta



Vir: Kovačič, 1997, str. 133.

Stranke oz. komitente elektronskega bančništva razdelimo na fizične osebe, pravne osebe in samostojne podjetnike.

5 ELEKTRONSKO BANČNIŠTVO SKB BANKE

Elektronsko bančništvo SKB banke je sodoben in varčen način poslovanja, ki omogoča varen dostop do banke, poslovnih partnerjev in do sveta nasploh. Da lahko uporabljamo elektronsko bančništvo potrebujemo samo transakcijski račun, ki omogoča tolarsko in devizno poslovanje v plačilnem prometu, in seveda računalnik, da omogoča delo z internetom. Skb banka nudi kar nekaj elektronskih produktov, in sicer: Skb net, poslovni Skb net, multi Skb net, Sogecash in multi Skb net B2B. Poleg teh produktov je še na voljo zbirni center Skb net in telefonsko bančništvo kot je zeleni telefon, bankotel, avtomatski odzivnik za devizne tečaje in mobilno bančništvo – Wap Skb net. Te sodobne bančne poti lahko uporabljajo pravne osebe, samostojni podjetniki, obrtniki in ostalo prebivalstvo. SKB Banka d.d. spada med tri največje banke v Sloveniji, v določenih segmentih poslovanja (elektronsko bančništvo) pa so že leta med vodilnimi. Izbral sem Poslovni Skb net, ki ga bom predstavil v nadaljevanju.

SKB banka d.d. je začela poslovati kot samostojna banka, delniška družba po odcepitvi od Ljubljanske banke v januarju 1990, čeprav je poslovala že pred tem, in sicer kot specializirana stanovanjsko-komunalna banka. Danes ima SKB banka d.d. vse značilnosti splošne komercialne banke, s sposobnim vodstvom, dobro razvitim mednarodnim poslovanjem in ponudbo, ki jo dopolnjujejo podjetja bančne skupine. Konec leta 2003 se po velikosti bilančne vsote uvršča na četrto mesto, njena poslovna mreža pa šteje 56 poslovalnic in 9 poslovnih enot po vsej Sloveniji. Poslovalnice opravljajo bančne storitve za podjetja, samostojne

podjetnike in prebivalstvo, poslovne enote pa upravljajo poslovalnice na svojem geografskem območju in opravljajo zahtevnejše posle za podjetja. V banki je zaposlenih 1200 ljudi. Sedež banke je v Ljubljani, Ajdovščina 4.

Leto 2000 je za SKB banko pomenilo pravo prelomnico v razvojnem smislu, saj je začela razvijati strategijo o povezavi s tujo banko. Leta 2001 se je banka povezala s strateškim partnerjem in sicer z francosko banko Société Générale in prešla v last strateškega partnerja iz EU, francoske banke Société Générale S.A., Pariz. V letu 2003 je imela francoska banka že 99.58 odstotkov vseh delnic SKB banke.

5.1 INFORMACIJSKI SISTEM SKB BANKE

V SKB banki so kot prva banka v Sloveniji ponudili storitve elektronskega bančništva Skb net. Uvedli so informacijski sistem Symbols, ki se že uporablja v slovenskem jeziku. Informacijski sistem Symbols je aplikacija tipa odjemalec/strežnik, ki je narejena z razvojnim orodjem Oracle Developer/2000 in teče na podatkovni zbirki Oracle. Izpeljali so tudi prenos informacijskega sistema Symbols na višjo verzijo podatkovne zbirke. Poleg samega prenosa na višjo verzijo podatkovne zbirke (Oracle 8i), so uporabili tudi nov program za zaščito podatkov Fine-Grained Access Control.

Arhitektura Symbolsov je zasnovana na treh podsistemih. To so: osebna obravnava komitenta, podporni podsistem in distribucijski kanali. Najpomembnejši je podsistem osebne obravnave komitenta, ki predstavlja osebno komuniciranje s komitentom, kot sta svetovanje in prodaja, kar preko interneta. Podsistem je zasnovan na skladišču podatkov o komitentu, storitvah banke, tržišču, konkurenci, in sicer vse z namenom celovite obravnave komitenta. Drugi podsistem je podporni in vključuje kredite, depozite, akreditive... Tretji podsistem je namenjen različnim distribucijskim kanalom, od bančnih okenc, interneta do telefona. Ukvarja se tudi z raznimi programskimi rešitvami za podporo posameznim distribucijskim kanalom.

Z uvedbo informacijskega sistema Symbols so pričeli izvajati prenovo informacijskega sistema. Sistem zajema poslovne module in module skupnega okolja, ki so med seboj integrirani. Banke uporabljajo module kot njihove bančne pripomočke za dosego določenega cilja. Primer modula v banki je lahko elektronski plačilni nalog oziroma servis za spremljanje evidenc o neplačanih obveznosti od komitentov ali pa do komitentov.

V prvi fazi prenove so uvedli module Kernel - skupni šifranti, financiranje izvoznih poslov, prenosi sredstev med različne bančne račune, glavna knjiga, računi bank, zapiranje nostro računov, denarni trg in devizni tečaj. V drugi fazi so uvedli module, ki zagotavljajo opravljanje domačega plačilnega prometa ter vodenje deviznih in tolarskih računov in depozitov komitentov banke. Dopolnili so še modul za denarni trg za tolarsko poslovanje. Poleg tega so intenzivno uvedli projekta, in sicer prenova kreditov in prenova poslovanja s prebivalstvom. Ta projekt pa so zaključili s posodobljeno informacijsko podporo poslovanju z

občani, in sicer preko bančnih okenc. V modulu potrošniški krediti so bili na začetku zajeti le devizni krediti za tuje pravne osebe, kasneje pa so ga razširili še z ostalimi krediti, in sicer krediti domačih pravnih oseb in občanov. Uporabljati so začeli še dva nova modula skupnega okolja. To sta limiti poslovanja in zavarovanja.

Rezultat prenove informacijskega sistema je v tem, da bodo zaposleni imeli mnogo več kakovostnih in pravočasnih informacij, ki jih potrebujejo za svoje dnevno delo s komitenti. Vzporedno z uvedbo Symbols-ov je potekalo še elektronsko bančništvo, ki je v celoti integriran z informacijskim sistemom banke. Osnovo storitvam elektronskega bančništva za celovito podporo poslovanja s transakcijskimi računi predstavlja osrednji informacijski sistem Symbols.

V primeru nedelovanja informacijske podpore je bil ustanovljen krizni štab, ki skrbi nad delovanjem sistema in rešuje nastale težave ter obvešča komitente o tem, kako, kje in kdaj so posamezne bančne storitve omogočene

5.2 POSLOVNI SKB NET

Poslovni Skb net je elektronsko bančništvo Skb banke in je namenjen za srednja in velika podjetja. Omogoča opravljanje bančnih storitev preko interneta. Dostopen je vedno in povsod, kjer je omogočena povezava z internetom ter ustrezen računalnik. Deluje 24 ur na dan, vse dni v letu. Poslovni Skb net podjetju omogoča, da z SKB banko posluje po elektronski poti, kar mu prinaša številne prednosti:

- takojšnjo obdelavo naročenih transakcij (on-line),
- preglednost finančnega poslovanja,
- informacije o transakcijah, stanju in prometu v realnem času,
- 24-urno dostopnost,
- boljši nadzor nad tolarskimi in deviznimi sredstvi,
- nižje provizije,
- dosegljivost s kateregakoli konca sveta,
- varno in enostavno uporabo.

Pri uporabi Poslovnega Skb net potrebujemo tudi osebni računalnik z naslednjimi minimalnimi tehničnimi zahtevami:

- močan procesor, npr Celeron , pomnilnik 64MB RAMa ali več,
- grafična kartica z ločljivostjo 800 x 600 ali več,
- prosta serijska vrata (COM port ali USB priključek),
- monitor,
- 20 MB prostora na trdem disku (ob nameščeni potrebni programski opremi),
- Windows 98, WIN ME, Windows 2000 ali Windows NT 4.0 (Service pack 6),

- internet brskalnik Internet Explorer 5.0 ali novejši,
- pametno kartico s čitalcem kartice in programski paket za Poslovni Skb net, ki se prejme od banke.

Poslovni Skb net je hiter in pregleden in nam omogoča:

- pregled prometa na računu,
- pregled izpiskov,
- pregled stanja za tolarski in devizni del transakcijskega računa, odprtega pri SKB banki,
- prejemanje podatkov za domače plačilne naloge,
- pregled prejetih prilivov iz naslova plačilnega prometa s tujino,
- izvoz podatkov oziroma izpiska v formatu APP,
- vnos, urejanje in potrditev paketov za domače in tuje plačilne naloge,
- shranjevanje in urejanje predlog za domače in tuje plačilne naloge,
- izpolnjevanje in pošiljanje obvestil o prilivu za plačilni promet s tujino,
- varno pošiljanje sporočil v banko.

Poslovni Skb net omogoča številne prednosti. Vedno lahko pogledamo trenutno stanje na transakcijskih računih; pregled prometa omogoča popolno preglednost finančnega poslovanja; v arhivih so zbrani vsi podatki o plačilih preko Poslovnega Skb net-a. Ker nam ni treba hoditi v banko plačevati računov, lahko tako pridobljeni čas porabimo za kaj drugega. Kar se tiče same uporabe, pa ne potrebujemo nobenega računalniškega predznanja. Zelo pomembna pa je varnost poslovanja, da uporabniki lahko zaupajo v Poslovni Skb net.

5.2.1 VARNOST POSLOVANJA POSLOVNEGA SKB NET

V SKB banki uporabljajo najsodobnejšo tehnologijo za zaščito zaupnih podatkov in transakcij, ki potekajo preko interneta. Med pomembnimi so:

- usmerjevalniki,
- požarni zidovi,
- interne kontrole,
- identifikacijske kartice,
- avtorizacija.

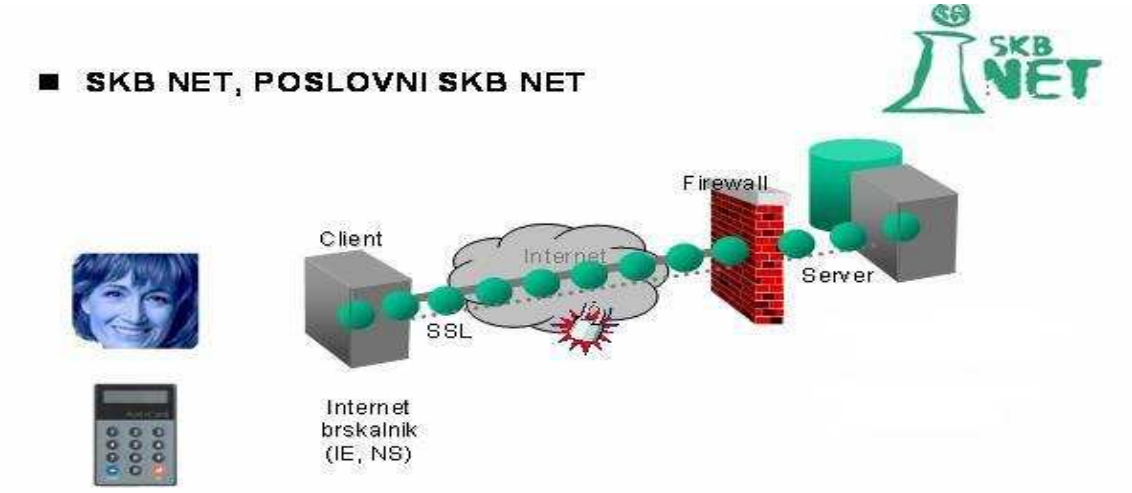
Požarni zid se uporablja za zaščito bančne računalniške mreže pred nepooblaščenimi dostopi. Ves promet je naslovljen na požarni zid, ki preverja vir in cilj za vsak podatkovni paket. Proxy strežnik oz. usmerjevalnik spremeni naslov paketa in ga spusti naprej v omrežje. Na ta način so vsi notranji naslovi zaščiteni pred zunanjimi vdori. Proxy strežnik je program narejen z namenom:

- povečanja hitrosti dostopov,

- zmanjšanja zasedenosti povezav,
- izboljšanja varnosti pri komunikacijah prek TCP/IP mreže.

Hitrost dostopov se poveča, ker uporabnik dobi dokumente iz proxy strežnika in to na najhitrejši možen način. Zasedenost povezav se zmanjša, ker uporabniki dostopajo večinoma samo do proxy strežnika. Varnost pa je zagotovljena, ker strežnik omogoča komunikacijo prek požarnega zidu do interneta. Na sliki 9 je prikazano, kako poteka obdelava transakcij v realnem času.

Slika 9: Obdelava transakcij v realnem času



Vir: Elektronsko bančništvo v Skb banki, 2003.

Slika 9 prikazuje, kako poteka bančno elektronsko poslovanje preko poslovnega Skb net. Ko se komitent (client) poveže z SKB banko preko interneta z internetnim brskalnikom, ponavadi je to Internet Explorer (IE) ali Netscape (NS), se banka med stranko in svojim strežnikom (server), ki skrbi za delovanje sistema za elektronsko poslovanje, vmes še zaščiti s programom požarni zid (Firewall), ki onemogoča vdor v bančni elektronski sistem oz. vstop drugim, nepooblaščenim osebam. S tem ima SKB banka večji nadzor nad tem, kateri podatki prihajajo in odhajajo iz računalnika, ter prepozna tiste, ki prihajajo z nevarnih lokacij. Za dodatno varno izmenjavo podatkov, ki so ustrezno šifrirani in dopolnjeni z digitalnim podpisom, pa preko poslovnega Skb net skrbi še protokol SSL (Secure Socket Layer), ki omogoča varno pot med odjemalcem (komitent SKB banke) in bančnim strežnikom.

Interne kontrole varujejo uporabnika pred nepooblaščenimi transakcijami s strani banke.

Avtorizacija pomeni, da vsak uporabnik Poslovnega Skb net-a lahko uporablja le tiste račune in transakcije, za katere ima vpisano dovoljenje v bančni skrbniški aplikaciji.

Identifikacijska kartica je varnostni pripomoček, ki zagotavlja identifikacijo oz. pristnost uporabnika elektronskega bančništva. Za ugotovitev identitete uporabnika sistem uporablja

njegov digitalno potrdilo in zasebni ključ. Digitalno potrdilo zato, da strežniku pove, kdo je, zasebni ključ pa zato, da mu s posebnimi matematičnimi postopki to tudi dokaže.

Digitalno potrdilo izdajajo pooblaščene agencije (lahko tudi banke), ki s svojim digitalnim podpisom na certifikatu jamčijo, da javni ključ, ki je v njem shranjen, res pripada uporabniku, na katerega se certifikat glasi. Digitalni certifikat oziroma potrdilo je digitalni dokument, ki se uporablja za identifikacijo uporabnika, podjetja, organizacije oz. kakšnega drugega subjekta. Lahko ga primerjamo s potnim listom ali drugim dokumentom in je priznan kot dokaz o identiteti njegovega lastnika.

Banka Skb d.d. sama izdaja digitalno potrdilo. Poleg bank, kot overitelja digitalnega potrdila, so še drugi kot npr. Center vlade za informatiko oz. CVI , Pošta Slovenija ter ostale fizične ali pravne osebe, ki izdajajo potrdila ali opravljajo druge storitve v zvezi z overjanjem ali elektronskimi podpisi.To so overitelji kvalificiranih digitalnih potrdil, za katere velja najvišja stopnja varovanja in načela t.i. močne enkripcije in deluje v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP) in objavljenimi politikami delovanja. Overitelji izdajajo digitalna potrdila za javno upravo, pravne in fizične osebe. Poleg tega so izdajatelji mednarodno registrirani, medsebojno priznani, ter tehnološko in zakonsko enakovredni in enako veljavni. Certifikat dopolnjuje še zasebni ključ (osebno geslo), ki je ključen pri identifikaciji uporabnika, saj programska oprema na računalniku uporabnika najprej prebere digitalni certifikat ter ga pošlje na strežnik, na katerega uporabnik vstopa, nato pa s pomočjo zasebnega ključa izvede še nekaj kriptografskih operacij, ki strežniku dokažejo, da uporabnik res poseduje pravi zasebni ključ. Šele po takšnem preverjanju se uporabniku dovoli opravljanje storitev.

Digitalni certifikat skupaj z zasebnim in javnim ključem uporabnika tvori identiteto uporabnika. V njem so zapisani podatki o lastniku zasebnega in javnega ključa, tako da jih banka lahko preveri vsakič, ko jih zanima identiteta lastnika določenega javnega ključa. SKB banka računa na zaupnost uporabnikov storitev elektronskega bančništva, saj je v skupnem interesu, da ne bi prišlo do zlorab identifikacijskih sredstev. Zato gesel in drugih identifikacijskih elementov se ne posreduje tretjim osebam.

Za ustrezno stopnjo varnosti in zaupnosti na internetu pa so v banki Skb poskrbeli z uporabo posebnega protokola, imenovanega SSL – Secure Sockets Layer Protocol. Protokol je množica pravil, ki jih računalniki upoštevajo pri medsebojni izmenjavi podatkov. Računalnika, ki za sporazumevanje uporabljata SSL protokol, imata med seboj zagotovljen varen kanal za prenos digitalnih podatkov; med prenosom so podatki ustrezno šifrirani in opremljeni z digitalnim podpisom.

SSL protokol je eden od najbolj razširjenih šifrirnih sistemov za prenos podatkov preko interneta. Razvilo ga je podjetje Netscape že leta 1995, danes pa ga podpirajo uporabljani spletni brskalniki, zato se ga uporablja kot standardno rešitev tudi pri zagotavljanju varnega elektronskega bančništva. Tehnično gledano je SSL varnostni nivo, ki deluje med

aplikativnim nivojem procesa prenosa podatkov in TCP/IP protokolom. Ker SSL protokol deluje pod aplikativnim nivojem procesa prenosa podatkov, lahko vse aplikacije, ki znajo uporabljati internet, za vzpostavitev varne povezave brez težav uporabijo tudi SSL protokol. Prednost SSL protokola je tudi ta, da ne temelji na vnaprej določenem šifrirnem algoritmu, tako da bi lahko določen algoritem v primeru, če bi zastarel ali pa bi v njem našli kakšno napako, enostavno zamenjali z drugim. Osnova za SSL protokol so digitalni certifikati, s katerimi se subjekti, ki si želijo izmenjati podatke, predstavijo drug drugemu. Ponavadi gre za povezavo med spletnim strežnikom in spletnim odjemalcem. Spletni strežnik je npr. strežnik Skb banke, ki svojim uporabnikom omogoča storitve elektronskega bančništva, spletni odjemalec pa je uporabnik Skb.net oziroma spletni brskalnik uporabnika interneta.

Za vzpostavitev SSL povezave je potreben vsaj en digitalni certifikat, saj se mora spletni strežnik vedno predstaviti spletnemu odjemalcu. Digitalni certifikat, s katerim se spletni strežnik predstavi spletnemu odjemalcu, mora podpisati (izdati) eden od uradov, ki izdaja certifikat, ki jim spletni odjemalec zaupa. Če tudi spletni strežnik od spletnega odjemalca zahteva predstavitev, pa tudi spletni odjemalec potrebuje digitalni certifikat. Digitalni certifikat, s katerim se predstavi spletni odjemalec, mora podpisati eden od uradov, ki izdaja certifikat, ki jim zaupa spletni strežnik. V primeru, da spletni odjemalec ne zaupa spletnemu strežniku (torej ne zaupa njegovemu digitalnemu certifikatu, kar pomeni, da nima javnega ključa od urada, ki je spletnemu strežniku izdala digitalni certifikat), ali pa da spletni strežnik ne zaupa spletnemu odjemalcu, do izmenjave podatkov preko SSL protokola ne bo prišlo

Kaj je šifriranje sporočil?

S šifriranjem zaščitimo vsebino sporočila pred vpogledi s strani neavtoriziranih oseb. Kako varna so zaščitena sporočila, je odvisno od vrste uporabljenega šifrirnega postopka, predvsem pa od velikosti šifrirnega ključa (merjeno v bitih). Daljši je ključ, težje je zaščito zlomiti in prebrati vsebino sporočila

Včasih so uporabljali 40-bitno zaščita, sedaj pa je 128 bitna ali več. Bistvena razlika med 40- in 128-bitno zaščito je v številu možnih ključev, s katerimi je zaklenjeno sporočilo:

- pri 40-bitni zaščiti je možno 2^{40} različnih možnih ključev, le eden ključ je pravi,
- pri 128-bitni zaščiti pa je možno 2^{128} različnih ključev, sporočilo je kodirano le z enim od njih.

Pri 128-bitni zaščiti je pravi ključ praktično nemogoče odkriti, zato je sporočilo med prenosom bistveno bolj varno pred nepooblaščenimi vpogledi.

Po navedbah Netscape-a bi z današnjo tehnologijo 128-bitno šifrirano sporočilo razbili kar 309.485.009.821.345.068.724.781.056-krat težje od tistega, ki je kodiran s 40-bitnim ključem.

Brskalniki vsak na svoj način pokažejo, ali se nahajamo v varnem načinu delovanja, kjer se podatki pred prenosom po internetu šifrirajo. V tabeli 2 so prikazane oznake, ki jih uporabljajo posamezne različice brskalnikov:

Tabela 2: Varnostne oznake posameznih brskalnikov

Vrsta brskalnika	Zaščiten	Nezaščiten
Netscape Navigator 1.1X ali kasnejši		
Netscape Communicator 4.0		
Microsoft Internet Explorer (katerakoli verzija)		**Ni ikone**

Vir: Skrt, 2002, str. 72.

Microsoft Internet Explorer prikaže ikono v spodnjem desnem kotu, pri programih podjetja Netscape pa je oznaka v spodnjem levem kotu ekrana.

5.3 KRIPTOGRAFIJA SKB BANKE

Kriptografija je veda o šifriranju oz. zakrivanju sporočil. Osnovni namen kriptografije je zaščititi zaupne podatke pred nepooblaščenimi dostopi in ponarejanjem. Sporočilo se po nekem postopku oz. algoritmu spremeni v kodirano sporočilo, pri tem pa se za parametre algoritma uporabi določena vrednost, ki ji pravimo ključ. Osebi, ki si želita izmenjati šifrirana sporočila, se morata zato najprej dogovoriti o algoritmu in ključu. Algoritem je nekako zaporedje definiranih pravil in ukazov, ki zagotavlja rešitev problema v končnem številu korakov. Med najbolj pomembnini algoritmi so DES, RSA, AES, PGP, DSS, DH, RC4, RC5, RC6 itd. Ponavadi gre za kratice priimkov avtorjev teh algoritmov.

5.3.1 SIMETRIČNA KRIPTOGRAFIJA

Simetrična kriptografija temelji na tem, da se pošiljatelj in naslovnik sporočila dogovorita za algoritem in en skupen ključ, s katerim se sporočila šifrirajo oz. dešifrirajo. Vsak par naslovnikov in pošiljateljev ima svoj tajen ključ; če se sporočila izmenjujejo z več osebami, je torej potrebno varno hraniti več različnih tajnih ključev, kar seveda predstavlja problem. Poleg tega sta običajno v uporabi dva komunikacijskega kanala; prvi, preko katerega se izmenjavajo šifrirana sporočila, in drugi, ki mora biti veliko bolj varen, za določitev tajnega ključa.

Običajna dolžina ključev je 40, 64, 128, ali 256 bitov, pri čemer je treba upoštevati, da so dovolj varne šele dolžine od 128 bitov dalje. V Skb banki so zaščiteni s 128 bitnim ključem.

5.3.2 ASIMETRIČNA KRIPTOGRAFIJA

Asimetrična kriptografija ali kriptografija z javnimi ključi temelji na takšni kombinaciji ključev, da bo sporočilo, ki je bilo šifrirano s prvim, mogoče dešifrirati samo z drugim, in obratno. Zato se vsakemu uporabniku dodeli en tak par ključev in določi, da je eden od njiju javen (znan vsem), drugi pa zaseben (znan samo uporabniku). Vsak, ki pozna javni ključ neke osebe, lahko tej osebi pošlje sporočilo, ki ga bo mogla odšifrirati samo ona s svojim drugim, zasebnim ključem. In obratno: ta oseba lahko vsem drugim pošlje sporočilo, ki ga je zašifrirala s svojim zasebnim ključem. Takšno sporočilo lahko vsi ostali odšifrirajo in preberejo, vendar vedo, da ga ni mogel zašifrirati nihče drug, kakor ta oseba, saj ima le ona dostop do svojega zasebnega ključa. Izključno ona je torej mogla zašifrirati neko sporočilo na tak način, da ga je možno odšifrirati z njenim javnim ključem. Temu postopku se sicer pravi elektronsko podpisovanje; sporočilo je lahko samo šifrirano, samo podpisano ali tako šifrirano kot podpisano.

Kriptografija z javnimi ključi ima več prednosti pred klasično kriptografijo:

- Delo s ključi je poenostavljeno, saj mora uporabnik paziti le na svoj lastni zasebni ključ, javni ključi pa so lahko shranjeni v splošno dostopni bazi.
- Poenostavljen je tudi problem izmenjave (distribucije) javnih ključev. Uporabniku ni potrebno pošiljati javnega ključa vsakemu uporabniku, temveč ga lahko objavi na javnem strežniku. Za distribucijo javnih ključev je možno uporabiti več načinov. Pri prvem načinu uporabimo zaupanja vreden strežnik, da hrani javne ključe. Ob vsakem zaupnem sporočilu nekemu drugemu uporabniku se pošiljatelj obrne na ta strežnik in povpraša za prejemnikov javni ključ.

Drugi način pa je uporaba **digitalnega potrdila z digitalnim podpisom**.

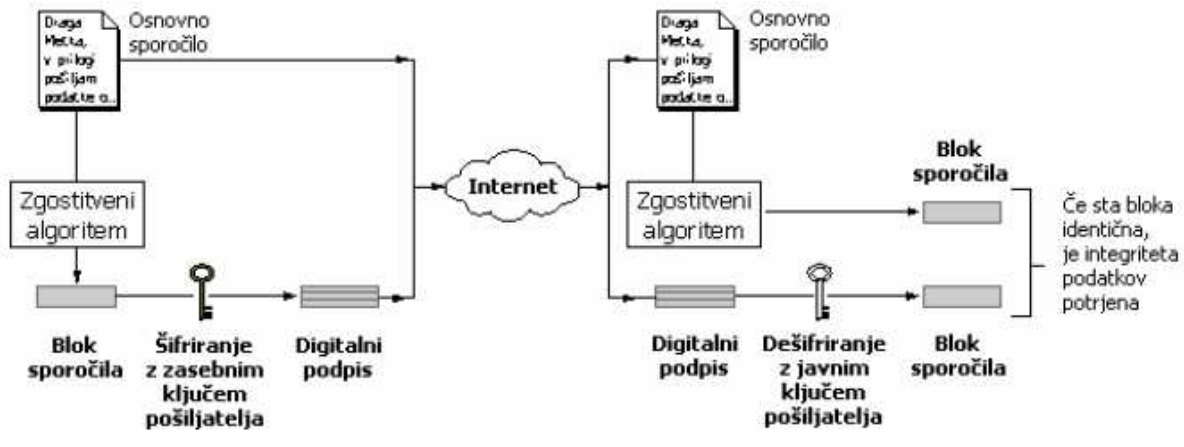
5.3.3 DIGITALNI PODPIS SKB BANKE

Digitalni podpis preprečuje spreminjanje in zlorabljanje sporočil in zagotavlja, da tok podatkov med banko in uporabnikom ostane nedotaknjen.

Ob začetku transakcije pošljemo preko brskalnika v banko varno sporočilo. Banka vrne certifikat oziroma digitalno potrdilo, ki vsebuje njen javni ključ. Bančni strežnik, ki podpiše javni ključ, s svojim strežniškim zasebnim ključem potrdi, da javni ključ spada k temu in temu uporabniku. Za resničnost vsebine digitalnega potrdila jamči elektronski podpis strežnika, ki je potrdilo izdal. Ko želi pošiljatelj prejemniku poslati zaupno sporočilo, se mu zato, da bi dobil njegov javni ključ, ni več treba obračati na strežnik, pač pa naslovnika samega povpraša za njegovo digitalno potrdilo. Ko potrdilo dobi v roke, najprej preveri, kateri strežnik ga je izdal in ali je ta strežnik vreden zaupanja. Če je odgovor pozitiven, pošiljatelj preveri, ali je strežnikov podpis na digitalnem potrdilu veljaven. Če je tudi tu rezultat

pozitiven, potem javni ključ v potrdilu resnično pripada želenemu naslovniku. Pošiljatelj nato sporočilo šifrira s tem javnim ključem in ga odpošlje.

Slika 10 prikazuje uporabo digitalnega podpisa v praksi med dvema uporabnikoma



Vir: Danda, 2001, str 49.

Ko pošiljatelj želi prejemniku digitalno podpisati, svoje sporočilo stisne v blok sporočila, ki ga še zašifrira s svojim zasebnim ključem. Blok sporočila je posebna šifra, ki je krajša od osnovnega sporočila. Rezultat šifriranja je digitalni podpis in ga aplikacija pred pošiljanjem pripne osnovnemu sporočilu. Seveda se proces šifriranja oziroma dešifriranja ne izvaja ročno, saj za to poskrbi aplikacija, s katero pošiljatelj (prejemnik) pošilja (prejema) sporočilo preko interneta.

5.4 VARNOST NA INTERNETU

Seveda pa mora Skb banka poskrbeti tudi za varnost na internetu, ko gre za opravljanje transakcij med banko in komitenti. Osnovna zahteva je, da je prenos podatkov po omrežju šifriran in da so podatki digitalno podpisani. Varnostna aplikacija mora zagotoviti, da sporočilo ne bo spremenjeno in da je poskrbljeno za overitev strežnika, s čimer bosta obe strani, tako banka kot uporabnik, prepričani, s kom komunicirata. Varnostna aplikacija mora torej zagotoviti (Tonejc, 2001, str. 2):

- verodostojnost,
- kontrolo dostopa,
- zaupnost,
- celovitost,
- preprečevanje tajenja oziroma zanikanje.

Pri zanikanju oz. preprečevanju tajenja komitent pozneje ne more trditi, da ni poslal sporočila, prav tako pa tudi banka pozneje ne more trditi, da ni prejela sporočila. Celovitost je pomembna zato, da banka ve, da sporočila od komitenta ni mogel nihče spreminjati. Pod

zaupnost podatkov in sistema je mišljenja zaščita podatkov pred nepooblaščenim branjem ali kopiranjem. V poštev pridejo tudi posamezne informacije, ki so same zase lahko nepomembne, vendar bi z njihovo pomočjo lahko prišlo do zlorabe drugih, zaupnih informacij. Kontrola dostopa zagotavlja podatke in storitve uporabnikom, kadar je potrebno, in da bi bila njena uporaba onemogočena, mora biti verjetnost realizacije minimalna. Danes pa se v Skb banki pri transakcijah zelo gleda na verodostojnost transakcije. To pomeni, da gre za overjanje oziroma, da bančni strežnik Skb banke ve, da je lahko le originalna oseba oz. komitent v pravem oziroma veljavnem času (natančen datum) plačal plačani račun oziroma, da komiten, ko dobi priliv od Skb banke, banka ve, da je potrdilo še veljavno.

V sodobnem svetu poslovnih komunikacij se vedno pogosteje srečujemo s težavami pri zagotavljanju varnosti in verodostojnosti prenešenih podatkov. Načinov, kako zagovotoviti verodostojnost podatkov je več, poleg zaščitenih podatkovnih poti in šifriranja podatkov, je zato tudi uporaba digitalnega podpisa. V ta namen se je razvilo podpisovanje sporočil in potrjevanje ključev. Digitalno potrdilo vsebuje poleg podatkov o ključu še čas nastanka, podatke o lastniku, rok veljavnosti in podobno.

5.5 PREVERJANJE DIGITALNIH POTRDIL

Kar nekaj podjetij in ljudi že ima spletno digitalno potrdilo, ki je temeljni pogoj za uporabo nekaterih e- storitev, kot je elektronsko bančništvo. Za njihovo identifikacijo sta na voljo dve označbi: matična in davčna številka podjetja oziroma občana. Najbolj uveljavljena je davčna številka, vendar standard (X.509), ki ga upoštevajo overitelji digitalnih potrdil, polja za vnos te ne predvideva. Nekateri overitelji so se odločili, da davčno številko pravne ali fizične osebe vključijo v serijsko številko ali organizacijsko enoto razločevalnega imena v potrdilu, nekateri jo vključijo v posebno polje, nekateri pa je v potrdilo sploh ne zapišejo in vodijo lastno evidenco za istovetnost potrdil z davčnimi številkami. Vprašanje pa je, kako preveriti potrdilo in pridobiti tudi podatke, ki so na njem zapisani. Lahko jih imenujemo spletni servisi posameznih podjetij.

Servis za preverjanje veljavnosti digitalnega potrdila preveri digitalni podpis, njegovo časovno veljavnost in preveri, ali je potrdilo morebiti preklicano. Bistvena pri tej zadevi je povezava z najnovejšim seznamom preklicanih potrdil. Z drugim imenom lahko temu rečemo tudi časovni žig.

Spletni servis za preverjanje davčnih številk preveri njihovo pravilnost. Pri nekaterih storitvah moramo vnesti tudi svojo davčno številko, in servis to na podlagi podatkov iz potrdila potrdi ali pa sporoči, da ni bila vnesena davčna številka. Servis deluje zgolj za potrdila, ki tako ali drugače vsebuje zapis davčne številke.

Tretji servis pa poskrbi za vračanje podatkov uporabniku storitev, a le tistih, ki so tako ali drugače že vsebovani v potrdilu in to ni v nasprotju z zakonom o varovanju osebnih podatkov.

V Skb banki je avtomatsko preverjeno proti neveljavnosti certifikata tako, da te strežnik ne spusti v sam sistem delovanja oziroma ve, da je potrdilo neveljavno in se tako ne da elektronsko poslovati.

V praksi vse to pomeni storitev, ki jo ponudniki e-storitev uporabijo ali pa tudi ne. Načeloma lahko vsak napiše svojo programsko opremo, ki počne podobno, vendar je to zamudno in dražje.

Skb banka, d.d. za varno izmenjevanje podatkov preko Poslovnega Skb net zahteva odprti protokol SSL (Secure Socket Layer), ki temelji na kombinaciji asimetričnih in simetričnih algoritmov. Na začetku izmenjave podatkov, bančni strežnik in uporabnikov programski paket tvorita simetrični ključ, ki si ga izmenjata z uporabo svojih javnih ključev. Problem avtentikacije obeh strani, ki se pojavi pri uporabi asimetričnih algoritmov, se rešuje z uporabo digitalnega potrdila. Obema stranema javne ključe overi Skb banka, ki ji oba zaupata.

Postopek preverjanja podpisa na digitalnem potrdilu poteka takole: oseba, ki podpis preverja, mora poznati javni ključ strežnika, ki naj bi bil to potrdilo izdal. Nato ta oseba s strežnikovim javnim ključem poskusi dekodirati digitalno potrdilo. Če poskus uspe, je digitalno potrdilo veljavno, sicer ne.

5.6 VARNOST PRI UPORABNIKU

Pri prijavi na Poslovni Skb net, programski paket samodejno poskrbi za vzpostavitev varne povezave s strežnikom. Od Skb banke dobiš pametno oziroma identifikacijsko kartico s čitalcem kartice in programski paket na CD-u, ki se imenuje BAP 2000+ oziroma bančni asistent za podjetje. Pametna kartica je trenutno najvarnejši način hranjenja in varovanja zasebnega ključa. Uporaba (dostop do ključa) je možna le s pravilnim geslom, ki je znano le uporabniku. Za varovanje in podpisovanjem z geslom je odgovorno podjetje. Pri tem za pravilno predstavitev vaše identitete uporabi vaš digitalno potrdilo in vaš zasebni ključ; digitalno potrdilo zato, da strežniku pove, kdo ste, zasebni ključ pa zato, da mu s posebnimi matematičnimi postopki to tudi dokaže. Tretjim osebam preprečuje dostop do vašega zasebnega ključa trenutno najvarnejši način varovanja – pametna kartica, ki jo lahko uporabljate le s pravilnim geslom.

5.7 STRATEGIJA VAROVANJA E-SISTEMA SKB BANKE

Celovita varnostna politika za varovanje informacijskega sistema mora definirati načela in postopke varovanja tako za zbiranje, hranjenje in obdelavo podatkov. Varnostna politika mora obravnavati varovanje informacijskega sistema in informacij samih, prav tako pa tudi varovanje vseh medijeh in naprav, ki so nosilci podatkov, ter pravila in postopke o delu osebja v zvezi z varovanjem podatkov in informacij. Končni rezultat je postavitev varnostnih pravil, seznanjanje in šolanje uporabnikov, postavitev naprav in uvedba nadzora nad izvajanjem varnostnih pravil (Prepadnik, 2001, str. 56).

Kontrole in postopki za zagotavljanje varnosti računalniško podprtega informacijskega sistema v Skb banki zajemajo:

- fizično varovanje,
- varovanje informacijskega sistema (pravila, naloge, pristojnosti in odgovornosti notranjega in zunanjega osebja,
- organiziranje varovanja,
- obvladovanje dostopa do sistema,
- načrtovanje neprekinjenega poslovanja,
- varovanju nosilcev podatkov pred okvarami in uničenjem,
- varovanje podatkov in informacij pri uporabi interneta in elektronskega poslovanja,
- varovanje podatkov in informacij pri računalniških storitvah zunanjih organizacij in osebja,
- razvrstitev in kontrola sredstev,
- varnostni razvoj in vzdrževanje sistemov,
- nadzor računalniškega omrežja,
- usklajenost sistema,
- varovanje pred računalniškimi virusi,
- varovanje proti vdoru v sistem elektronskega bančništa,
- naložbe v varnost.

Zanesljivo so vsi postopki za varovanje elektonskega bančništva enakovredni, vendar pa vsi najprej pomislimo, kaj če kdo vdre v elektronski sistem Skb banke oziroma, če pride do nepooblaščenega dostopa do našega računa v banki. V vsakem primeru je to tveganje banke, ki ni povezano z računi strank. Stvar pa je seveda drugačna, če bi komitent SKB banke zaradi nevestnega ravnanja s svojimi osebnimi elementi prepoznave ali gesli, bil za zlorabo dostopa do svojega računa preko Poslovnega Skb.net-a odgovoren sam.

V javnosti je zadnje čase veliko govora o varnosti sistema elektronskega bančništva. Zmeda, ki so jo povzročile različne interpretacije, je v zvezi s "trojanskim konjem" oziroma lažnim podpisom, lahko zaradi nepoznavanja in napačnih informacij povzroči nepotrebno škodo elektronskemu bančništvu.

Trojanski konji so zlonamerni računalniški programi, z namenom škodovati končnim uporabnikom. Trojanski konj v osnovi izrablja možnost nadgradnje Microsoftovega spletnega brskalnika Internet Explorer, ki opravlja transakcije po uspešni prijavi na storitev in ki na ta način lahko postane tudi pomanjkljivost omenjenega spletnega brskalnika. S tem je banka tudi zaščitena pred računalniškimi virusi z najsodobnejšimi računalniškimi programi.

5.7.1 PRIPOROČILA ZA UPORABNIKE POSLOVNEGA SKB NET

Za zagotavljanje varnosti elektronskega poslovanja z banko, je nujno potrebno ravnati pazljivo in previdno, tako kot z gotovino v denarnici, osebno številko in kartico za bankomatsko poslovanje ali s plačilno kartico pri brezgotovinskem poslovanju. Navodila za zaščito:

1. Skrbno varovati varnostnih elementov (PIN, zasebni ključ ...).
2. Uporaba najnovejših protivirusnih programov.
3. Uporaba najnovejših varnostnih popravkov ter nadgradenj operacijskih sistemov in spletnih brskalnikov,.
4. Omejevanje fizičnega oziroma mrežnega dostopa do računalnika.
5. Ignoriranje elektronskih sporočil (predvsem priponk), ki jih prejmemo od nepoznanih oseb.
6. Ne nameščanje datotek, če ni poznan njihov namen oz. delovanje.

Ostala zaščita:

7. Uporabljajo naj se vsa sredstva, ki jih za preverjanje avtentičnosti programske opreme priporoča dobavitelj (npr. preverjanje digitalnega podpisa, preverjanje digitalnega potrdila mesta, od koder prenašate programsko opremo ipd).
8. Varovanje računalnika – onemogoči naj se samodejno zaganjanje programov s CD-ja, takoj ko je ta vstavljena v enoto.

Če računalnik npr. uporabljamo na poti oz. v službi ali doma, ga ne smemo puščati vklopljenega brez nadzora. V naši odsotnosti vedno zaklepajmo ekran. Nastavimo si samodejno zaklepanje ekrana po določenem času neaktivnosti.

Če otroci ali druge osebe, ki niso varnostno ozaveščene, uporabljajo računalnik brez nadzora, obstaja večje tveganje, da so na računalnik nameščeni trojanski konji. Poskusimo ločiti računalnik za resno uporabo od tistega za zabavo.

5.7.2 NOTRANJI VARNOSTNI MEHAMIZMI V SKB BANKI

Konkretnih internih postopkov mi zaradi varnosti niso izdali, zajemajo pa:

1. Postavitev raznih kontrolnih postopkov in procedur v skladu z bančnimi standardi in protokoli.
2. Redno in občasno izvajanje teh kontrolnih postopkov.
3. Prijavljanje v razne bančne aplikacije samo z osebnimi gesli.
4. Postavitev avtorizacijske sheme za dostope do raznih okolij informacijskega sistema in baz podatkov po poslih.

5. Izvajanje izjemno varnostno tveganih poslov izkjlučno z "super user" karticami, po odobritvi nadrejenega.
6. Opravljanje varnostno tveganih masovnih poslov po metodi "štirih oči" (vedno dva referenta).
7. Varovanje občutljivih materialov, kartic in dokumentacije v varovanih blagajnah.
8. Izvajanje vseh internih in s strani Banke Slovenije predpisanih varnostnih postopkov, vezanih na informacijski sistem banke.

6 SKLEP

Varnost elektronskega bančnega sistema oz. celotnega bančnega sistema Skb banke je nujna, pa ne samo zaradi vedno večje konkurence na področju opravljanja bančnih storitev, temveč tudi zaradi zaupanja v njene produkte, ki jih banka ponuja. V diplomskem delu je ta produkt Poslovni Skb net. Na splošno sem opredelil definicijo informacijskega sistema, standard BS 7799 in informacijski sistem Skb banke, opisal poslovni Skb net, njegove prednosti in namen uporabe. Najbolj sem se osredotočil na varnost elektronskega bančništva, tako s stališča banke kot samega uporabnika.

V zadnjem desetletju banke omogočajo ponudbo novih tržnih poti, ki temeljijo na elektronskem bančništvu, pri čemer se za prenos podatkov uporablja internet. Glede varnega prenosa podatkov preko interneta je banka poskrbela z varnostnim protokolom SSL in požarnim zidom, ki nepooblaščenim osebam onemogoča vpogled v podatke, ki se prenašajo preko interneta. Za dodatno preprečitev vmešavanja v prenos podatkov pa uporabljamo še digitalni podpis, ki je zašifriran z uporabnikovim zasebnim ključem. Za istovetnost digitalnega podpisa pa Skb banka izda istemu uporabniku še certifikat, kot zagotovilo, da je podpisnik res tisti, za kogar se izdaja. Certifikat in zasebni ključ oz. PIN koda so shranjeni na kartici, ki je podobna kreditni kartici. Naloga uporabnika je, da skrbno hrani to kartico oz., da ne izda PIN kode.

Za identifikacijo in overjanje uporabnikov je dobro poskrbljeno. Tehnologija, ki se pri tem uporabljaja, se izvaja zelo dobro. Kot sem ga opisal, je način šifriranja standarden. Kolikor so mi v Skb banki povedali, do zdaj še ni bilo zlorab s strani nepooblaščenih oseb oz. znotraj banke. Določena transakcija je šifrirana z 128 bitno dolžino ključa, kar bi zahtevalo veliko denarja in časa za njegovo odkritje.

Lahko pa se pojavijo tudi določene težave z nepazljivim ravnanjem uporabnikov in neupoštevanja varnostne politike. Najlažja tarča sta uporabnik in njegov osebni računalnik, ki je najmanj varovan. Za to pa mora poskrbeti sam uporabnik z ustrezno varnostno politiko, ki je o tem tudi obveščen.

Seveda pa ne gre brez nadzora nad izvajanjem varnostne politike. Pomembni so periodični varnostni pregledi. Lahko nam pomagajo razne računalniške aplikacije oz. rešitve za nadzor

računalniškega sistema, o stanju sistema oz. kršitvah varnostne politike. Če pride do kršitev, jih je treba nemudoma preprečiti. Poleg nadzora je potrebno še dodatno izobraževanje zaposlenih o varnostni politiki in obveščanje uporabnikov o dodatni varnostni ponudbi ali varnostnih popravkih.

V drugem poglavju sem pisal o standardu BS 7799 oz. PSIST BS7799. Varnostna politika banke temelji na standardu BS 7799 in je tudi prilagojena banki. Glavni del standarda pa predstavlja analiza tveganja. V Skb banki so zelo pozorni na analizo tveganja in sicer na razne grožnje, če heker vdre v računalnik, razna prisluškovanja, nepooblaščene dostope do transakcijskih računov itn. Samo tveganje pa predstavlja verjetnost, da se posamezna grožnja tudi uresniči, problem pa je v tem, da se ga v celoti nihče ne more izogniti. Ta analiza je temelj za sprotno in poznejše ukrepanje, saj nam pove, kje so največje varnostne luknje v informacijskem sistemu. Na njeni osnovi izdelamo varovalne ukrepe. S tem je banka vedno izspostavljena ranljivosti, zato so glavni cilj vedno večje investicije oz. vlaganja v informacijsko varnost.

Za banke je v sedanjem, hitro se spreminjajočem okolju bistveno poznavanje stranke; kaj potrebuje, kako razmišlja in kako se obnaša. Ker je konkurenca močna, je za banko izrednega pomena, da si pridobi uporabnika in še bolj, da ga zna obdržati. Zvest uporabnik je dandanes temelj poslovnega uspeha. Bančna zvestoba pomeni zaupanje stranke banki in predstavlja neko zagotovilo za nadaljevanje odnosa med banko in njim. Zvestobo lahko banka doseže le v primeru, če izboljšuje in upošteva tiste bančne dejavnike, ki so za stranko pomembni in spremlja ter povečuje zadovoljstvo stranke tako s storitvami kot tudi z bančnimi dejavniki.

Ponovno želim povdariti močno zaščito celotnega informacijskega sistema, saj so e-storitve del celotnega sistema, in če nudijo uporabnikom oz. komitentom banke optimalne koristi, je to zelo pomemben dejavnik v smislu zadovoljstva strank in rastočega konkurenčnega položaja za banke, kot tudi samega zaupanja v zaščito in delovanje informacijskega sistema. V Sloveniji je v povprečju več kot dve tretjini vseh podjetij, ki uporabljajo elektronsko bančništvo. Glede dobro zavarovanega varnostnega področja, so banke v Sloveniji med vodilnimi.

Za konec lahko potrdim, da je računalniški sistem varen in skupina v Skb banki, ki sledi novejšim trendom varnostne politike, skuša v največji meri minimizirati varnostne incidente brez hujših posledic. Varnost lahko povečamo oz. ohranimo na veliko načinov, vendar se na njih ne moremo zanesti v celoti. Ker se v današnjih časih tehnologija vedno bolj razvija in s tem tudi računalništvo, to od nas zahteva ogromno odgovornosti in truda, da lahko dosežemo maksimalno vrednost varnosti, tako s strani nas uporabnikov kot bank. Potrebno se je zavedati, da še tako dobra varnost nima učinka, če je nihče ne uresničuje.

LITERATURA

1. Alter Steven: Information System – A Management Perspective. Reading : Addison - Wesley, 1992. 848 str.
2. Alter Steven: Information System – A Management Perspective. 2nd ed. Menlo Park : Benjamin/Cummings, 1995. 728 str.
3. Andolšek Irena, Terčelj Mladen: Evropske smernice varnosti informacijskih sistemov. Zbornik referatov. 11. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov. Ljubljana : Slovenski inštitut za revizijo, 2003, str. 143 - 147.
4. Avison D.E., Fitzgerald G.: Information Systems Development: Methodologies, Tecniques and Tools. 2nd ed. London : McGraw-Hill, 1996. 505 str.
5. Danda Matthew: Protect Yourself Online. Redmond : Microsoft Press, 2001. 368 str.
6. Dečman Mitja: Elektronsko poslovanje in XML. Uporabna informatika, Kranj, 8(2000), 1, str. 51-56.
7. Gradišar Miro, Resinovič Gortan: Informatika v poslovnem okolju. Ljubljana : Ekonomska fakulteta, 2001. 508 str.
8. Gradišar Miro, Resinovič Gortan: Osnove informatike. Ljubljana : Ekonomska fakulteta, 1993. 334 str.
9. Groznik Aleš, Kovačič Andrej: Skladnost poslovnega strateškega načrta s strateškim načrtom informatike. Uporabna informatika, Ljubljana, 9(2001), 1, str. 12-15.
10. Jerman-Blažič Borka et al.: Elektronsko poslovanje na internetu. Ljubljana : Gospodarski vestnik, 2001. 206 str.
11. Kovačič Andrej, Vintar Mirko: Načrtovanje in gradnja informacijskih sistemov. Ljubljana: DZS, 1994. 316 str.
12. Kovačič Matevž: Storitve elektronskega bančništva. Zbornik, Banke in tveganja. Portorož : Zveza ekonomistov Slovenije, 1997, str. 131-141.
13. Pepelnjak Ivan, Bradeško Marjan: Varnost računalniških sistemov in elektronskih transakcij. Zbornik, Banke in tveganja. Portorož : Zveza ekonomistov Slovenije,1997, str.155-165.
14. Penger Sandra: Vpliv nove ekonomije na temeljne funkcije managementa v organizaciji 21. stoletja. Magistrsko delo. Ljubljana : Ekonomska fakulteta, 2001. 143 str.
15. Prepadnik Sebastijan: Načrtovanje varnostne strategije sodobnega računalniško podprtega informacijskega sistema. Magistrsko delo. Ljubljana : Ekonomska fakulteta, 2001. 109 str.
16. Pučko Daniel: Strateško upravljanje. Ljubljana : Ekonomska fakulteta, 1999. 399 str.
17. Razvojno življenjski cikel IS. (2004). [URL:http://www.pti.fgg.uni-lj.si/edu/ispi/seminarji/razvojnozivljenskiciklus.doc], citirano 2.10.2004.
18. Sistem elektronskega bančništva. (2004). [URL:http://www.hermes-softlab.com/SLO/industries/ebanking/ebanking.html], citirano 15.10.2004.
19. Skrt Radoš: Varno internetno nakupovanje v spletnih trgovinah. Ljubljana : Moj mikro, 2002. 96 str.

20. Standard varovanja informacij po standardu BS 7799. (2004).
[URL: http://www.bs-7799.org/ostandardu.asp], citirano 5.10.2004.
21. Šušteršič Darja: Smiselnost oglaševanja čistilnih sredstev na Internetu v Sloveniji.
Diplomsko delo. Ljubljana : Ekonomska fakulteta, 2001. 45 str.
22. Toplišek Janez: Elektronsko poslovanje. Ljubljana : Založba Atlantis, 1998. 336 str.
23. Tonejc Jernej: Osnove kriptografije, 2001. Ljubljana : Monitor, 2001. 124 str.
24. Vavpotič Damjan: Poslovni portali. Uporabna informatika, Kranj, 9(2001), 2, str. 67-74.

VIRI

1. Bančni asistent 2000+.
[URL: http://poslovni.skb.net], citirano 2001.
2. Bančnik Skb banke.
[URL:http://www.skb.si/info/ban/info-ban-1999/info-ban1999-113.html], 1999.
3. Interna gradiva Skb banke, december 2004.
4. Kodeks varovanja informacij (PSIST BS 7799, 2003).
5. Elektronsko bančništvo v Skb banki. (2003).
[URL:http://www.sioug.si/sioug2003/presentation.jsp?id=21], 2003.
6. Slovenski inštitut za standardizacijo (Uradni list RS, št. 124/03).
7. Varnost v Skb banki.
[URL:http: http://poslovni.skb.net/], 2001.