

INFORMACIONA BEZBEDNOST - OSNOVA BEZBEDNOG BIZNISA

Sinkovski Stevan, dipl.ing. VP 1100 Beograd
ssinkovski@yahoo.com
mr Branislav Lučić, dipl.ing, Jugoimport SDPR
b_tempest@EUnet.yu

Apstrakt: U radu je prikazana problematika informacione bezbednosti u oblasti poslovanja. U uslovima savremenog tržišta, poslovni uspeh i ekonomska bezbednost nezamislivi su bez informacione bezbednosti. Informacije i informacioni resursi predstavljaju materijalna dobra i zbog toga je zaštita informacija neodvojivi deo poslovanja. U cilju upoznavanja sa osnovnim postavkama informacione bezbednosti u oblasti poslovanja, u osnovnim crtama, obrađeni su rizici i vidovi napada na informacije, poslovanje i zaštita informacija. Poslovna strana zaštite informacija – gubici usled neadekvatne zaštite i izdaci za njenu organizaciju ilustrovani su kroz podatke iz objavljenih istraživanja.

Ključne reči: informaciona bezbednost, zaštita informacija, poslovanje i zaštite informacija, organizacija zaštite informacija.

INFORMATION SECURITY – BASIS OF SUCCESSFUL BUSINESS

Abstract: In this article are given problems information protection, as methods for successful business. In modern market conditions, there is no business success without information security. Information and information resources are material goods and information security is part of business. In order to understand base rules information security in a business, the risks, the attack forms on information and business security, are elaborated. Business site information security- a deficit in case information security not in full form, are illustrated in research articles announced.

Key words: information security, information protection, business and information protection, organization protection information.

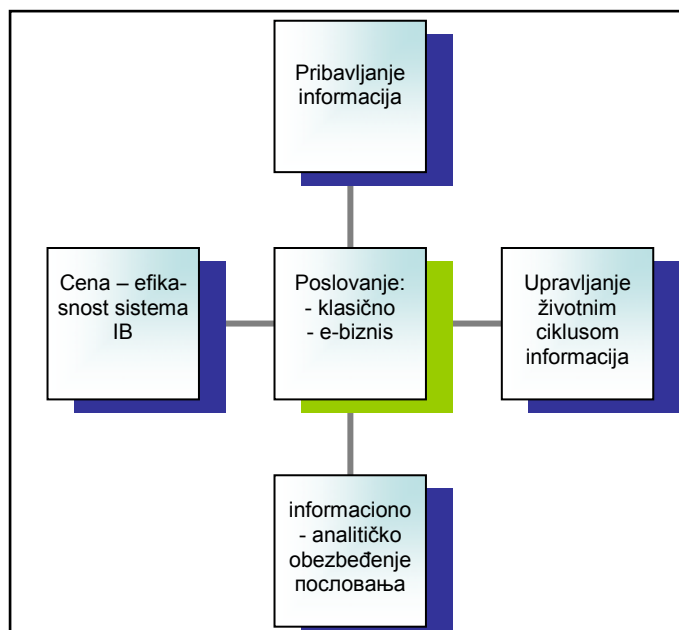
1. UVOD

Odnos između informacione bezbednosti (IB) i poslovanja ima četiri različita aspekta (slika 1). Prvi se odnosi na proces pribavljanja poslovnih informacija o konkurentima a drugi na problem čuvanja poslovnih informacija u bazama podataka. Ekonomska strana IB – cena «koštanja» sistema organizacije zaštite informacija i «cena» gubitaka zbog neadekvatne zaštite informacija, kao deo audita i procene stanja IB, predstavlja treći aspekt tog odnosa. Kao četvrti aspekt, imamo tzv. informaciono-analitičko obezbeđenje poslovanja. Naime, svaka država, u cilju sopstvenog napretka, mora stvoriti optimalne uslove u pogledu transparentnosti odvijanja ekonomskih procesa i sprečavanja birokratskih zloupotreba, nelojalne konkurencije i maksimalne obaveštenosti svih učesnika o stanju na tržištu.

Različite organizacije iz različitih razloga treba da štite informacije. Za banke je od presudnog značaja **integritet** informacija (neizmenljivost novčanih transakcija). Za provajdere Internet-usluga najvažnije su **raspoloživost i pouzdanost** informacija (dostupnost i pouzdan rad ključnih elemenata sistema). Za državne i vojne institucije najvažnija je **poverljivost** (mogućnost da informacija pristupe samo ovlašćena lica) informacija itd.

Kako se odlučiti za izbor sistema zaštite informacija? Univerzalan recept ne postoji. Moguće je dati samo neke opšte preporuke. Kao prvo, troškovi za obezbeđenje zaštite informacija ne smeju da budu veći od veličine gubitaka koji mogu nastati usled napada (princip ekonomičnosti). U literaturi se sreću različiti podaci o tome koliko sredstava treba izdvajati za IB (od 5 do 20% !)¹. Ono što je sigurno, to je činjenica da izdaci za sredstva zaštite informacija rastu sa razvojem informacionih tehnologija i da su u 2003.godini dostigli rast po godišnjoj stopi od 2,8%.

IB, kada je reč o biznis-procesima, nije neka egzotična disciplina, već deo poslovanja. Informaciona tehnologija i IB poslovanje mogu učiniti krajnje efikasnim, ali i dovesti ga do propasti. Kao i sve u poslovanju, i IB mora imati svoju **ekonomsku računicu** o potrebnim finansijskim izdacima za realizaciju zaštite informacija. U skladu sa tim su definisani neko od modela: uprošćeni model procene gubitaka, model vraćanja investicija i model matematičke analize efektivnosti sistema bezbednosti Abalmozova. Za realizaciju funkcije IB pored sredstava potrebni su i kadrovski resursi – služba IB. U datom podnaslovu, pored aspekata ispoljavanja odnosa IB i poslovanja, date su osnovne postavke o organizaciji službe IB kao i rezultati nekih ispitivanja o odnosu IB i poslovanja.



Slika 1: Oblasti preslikavanja odnosa informacione bezbednosti i poslovanja

2. INFORMACIONA BEZBEDNOST U OBLASTI POSLOVANJA

2.1. Poslovno izviđanje i industrijska špijunaža

Kada je reč o **pribavljanju ekonomskih informacija**, sreću se različiti termini: **konkurentsko izviđanje** (*competitive intelligence*), biznis izviđanje, komercijalno izviđanje, poslovno izviđanje i industrijska špijunaža. Osnovna razlika među njima je da li se koriste zakonskim (konkurentsko izviđanje) ili nezakonskim (industrijska špijunaža) sredstvima. Sve vrste izviđanja osnovno uporište imaju u legitimnosti (etičnosti), t.j. pribavljanju informacija samo zakonskim i etičkim metodama (prospekti, objavljeni izveštaji, radovi iz stručne literature, predavanja, organizovane posete, razmena literature, različiti oblici poslovne saradnje itd.). Za razliku od konkurentskog izviđanja, industrijska špijunaža je dobijanje informacija ili podataka (bilo zakonitim ili nezakonitim putem) o konkurentu iz oblasti naučnog istraživanja, proizvodnje sa najnovijim tehnologijama kao i personalnih podataka rukovodećih ljudi (sa ciljem njihove zloupotrebe).

Pored termina izviđanje, odnosno obaveštajna delatnost što je bliže originalnom izrazu – *intelligence*, u upotrebi je i termin kontraizviđanje. Kontraizviđanje služi za zaštitu i obezbeđenje bezbednosti privrednih subjekata od delovanja konkurentskog izviđanja i obično ga izvršavaju pripadnici službe bezbednosti.

Obaveštajna delatnost (izviđanje) je namenjena za pribavljanje strategijske (taktičke ili konkurentske) **prednosti** nad potencijalnim protivnikom (konkurentom), saznavanje mogućih rizika (opasnosti) ili mogućnosti i upravljanje njima. Osnovni zadatak konkurentskog izviđanja je obezbeđenje strategijskog menadžmenta firme i njenog generalnog strategijskog marketinga. Pribavljene informacije omogućavaju donošenje najvažnijih odluka i rešenja u pogledu razvoja i budućnosti firme. Ovako shvaćeno konkurentskog izviđanje obavljaju eksperti biznisa (za marketing, za planiranje, za menadžment itd.)ⁱⁱ. Granica između konkurentskog izviđanja i industrijske špijunaže je veoma tanka.

Industrijska špijunaža se organizuje na državnom nivou. Kao jedna od najugruženijih zemalja, kada je reč o industrijskoj špijunaži, SAD su 1996.god. donele zakon o industrijskoj špijunaži. Neposredan povod je bio izveštaj načelnika federalnog biroa za istraživanje (FBI), po kome je u 1995.god. podignuto 700 optužnica za

industrijsku špijunažu (poređenja radi u celoj 1944.god. iz sličnih razloga podignuto je samo 400 optužnica) ! Industrijska špijunaža je proglašena za jednu od pretnji (rizika) za američku ekonomiju. Prema izveštaju Edvina Fridmana (objavljenom u Public Administration Review, 1995.god.), agenata FBI i asistenta na fakultetu kriminalnog prava pri ministarstvu za društveno upravljanje (Njujork), industrijska špijunaža je nanela štetu američkoj ekonomiji od 25 do 100 milijardi USDⁱⁱⁱ.

2.2. Poslovanje i upravljanje životnim vekom informacija

Vođenje poslovanja pretrpelo je korenite promene poslednjih godina. Njegova stabilnost i dinamičnost u mnogome zavisi od tehničke opremljenosti. Posebno mesto u okviru tzv. tehničke opremljenosti pripada infrastrukturi čuvanja podataka. Naime, rast biznis-transakcija doveo je do enormnog porasta obima podataka koji se čuvaju na različitim medijumima. U skladu sa tim nastao je **problem čuvanja podataka** (baza podataka) jer gubitak opreme nemora da znači gubitak biznisa, ali gubitak podataka – obično to jeste (npr. bankarski podaci o izvršenim transakcijama, podaci o isporučenim robama u kompanijama itd.). Zapostavljenost ove problematike, iziskuje da joj posvetimo dužnu pažnju.

Termin «čuvanje podataka», sa svojom terminološkom naznakom nekakve stabilnosti, postao je preuzak za *on-line* biznis-procese i prerastao je u novi – upravljanje informacijama, odnosno upravljanje životnim ciklusom informacija. Inače, poslovni informacioni sistemi (PIS) i upravljanje informacijama predstavljaju okosnicu budućih trendova razvoja. U skladu sa tim, značaj i uloga upravljanja informacijama (čuvanje podataka), dobija na značaju i u infrastrukturi informacionih tehnologija. Zašto? Sistemi obrade podataka menjaju se svakih 5 godina, sa promenom tehnologije, a sistemi čuvanja podataka treba da obezbede kompatibilnost i funkcionisanje od 25 do 250 godina^{iv} ! Poznat je «efekat NASA» kada je američka kosmička agencija izgubila 1,2 miliona magnetnih traka sa informacijama o kosmičkim letovima (u proteklih 30 godina) zbog neodgovarajućih standarda zapisa sa novim tehnologijama! Vrednost čuvanih informacija se, poslednjih godina, mnogostruko puta uvećala. Prema podacima firme Imation (specijalizovane firme u oblasti čuvanja podataka) jedna kaseta sa magnetnom trakom može sadržati informacije – u zavisnosti od oblasti – čija je vrednost i do 2, 8 miliona dolara^v ! S druge strane, elektronsko poslovanje je bazirano na *on-line* operacijama tako da vreme pristupa podacima i 24-četvoročasovna spremnost baza podataka za operativni rad postaju osnova savremenog poslovanja [21].

Moćan katalizator procesa nagomilavanja podataka je i Internet. Mogućnost razmene velike količine podataka različitih formata (muzičke, grafičke i druge vrste informacija), koji su se ranije čuvali na trakama, papiru ili drugim medijumima, dovela je do rasta potrebe za fiksiranim računarskim memorijama. Procenjuje se da je povećanje kapaciteta diskova 50 do 125 % godišnje (prema oblastima i metodologiji procene). To za sobom povlači niz problema. Kao prvo, u velikim kompanijama se koriste mnogobrojni sistemi čuvanja podataka različitih proizvođača što donosi probleme u upravljanju. Kao drugo, administrator je u stanju, po nekim procenama, da opsluži oko 1 TB podataka, a već danas imamo slučajeve opterećenja i do 3 TB ! Kako se broj osoblja ne povećava potrebna je «inteligentija» aparatura koja će stajati na raspolaganju administratoru. Kao treće, velike kompanije poslednje u dve godine operišu, prema procenama analitičara, sa obimom podataka i od 150 TB. Iako su memorijski resursi već organizovani kao mreže (SAN – *Storage Area Network* ili NAS – *Network Attached Storage*), problem upravljanja različitim vrstama podataka nije rešen. Mreže čuvanja podataka ne samo da koncentrišu memorijske resurse, već i same zahtevaju efikasno upravljanje [21].

Sa rastom obima informacija, rastu i izdaci. Njih čine infrastrukturne komponente i softver za upravljanje sa njima. Na sisteme čuvanja podataka otpada 55 % od ukupno prodate IT opreme. Bez reorganizacije sistema čuvanja podataka, može se

desiti da u trenutku zapisa važnog biznis-procesa disk prijavi nedostatak slobodnog prostora, a da pri tome na ostalim kumpjuterima bude više od 50 % memorijskog prostora slobodno! Efikasnost savremenih sistema čuvanja informacija varira od 25 % (kod servera koji su direktno priključeni, DAS – *Direct Attached Storage*) pa do 50-60 % (mreža SAN i NAS). Prema istim analitičarima 62 % postojećih organizacija je već danas u situaciji da treba da vrši reorganizaciju svojih sistema čuvanja podataka [21].

Upravljanje informacijama (čuvanjem podataka) opterećeno je sa dva principijelna problema – visokom cenom i neefikasnim korišćenjem. Čak i kada cena memorija na diskovima pada 30 %, potreba za njima raste 100 %. Rešenje je u uvođenju **sistema upravljanja resursima** čuvanja podataka – SRM (*Storage Resource Menagement*).

Sredstva za upravljanje čuvanjem podataka delima na tri kategorije (slika 14):

- sredstva arhiviranja, kopiranja i restauracije podataka,
- sredstva upravljanja tehnologijama mrežnog čuvanja (interfejsi i komutatori^{vi}) i
- sredstva upravljanja resursima SRM.

Sredstva SRM su (prema «Narandžastoj knjizi»^{vii}) aktivna, intelektualna, centralizovana **rešenja** za vođenje biznisa na nivou preduzeća **sa stanovišta resursa čuvanja podataka**. Ona su, za administratora, **sredstva vizuelizacije mreže**^{viii} koja definišu pravila (politiku) upravljanja i vode računa o upotrebi resursa čuvanja podataka. Sredstva SRM imaju mogućnost podržavanja heterogene sredine, predstavljaju sredstva integracije sa savremenim i budućim tehnologijama a samo administriranje, pomoću njihovih pravila, je relativno jednostavno. Sredstva SRM su namenjena da sniže izdatke za resurse čuvanja podataka, da poboljšaju povratak uložених investicija i da spreče zastoje u funkcionisanju.

Po definiciji Gartner Group, sredstva SRM su **komponenta cele infrastrukture upravljanja**, koja poboljšava pristup podacima (putem analize tendencija ponašanja kapaciteta i operativnosti memorije, konfiguracije uređaja u mreži i u podsistemu daljinskog upravljanja medijumima). Sredstva SRM predstavljaju sredstvo za merenje resursa mreže i upravljanje njima [21].

Funkcije koje obavljaju sredstva SRM su mnogobrojne: detekcija, registracija i definisanje tipove objekata u mreži (*discovery*), prikupljanje podataka (*data collection*), prikazivanje (*mapping/ visualization*), formiranje operativnih i retrospektivnih izveštaja (*real-time and histolical reporting*), upravljanje događajima uključujući i ažuriranje žurnala i upozorenje (*event logging i alerting*), monitoring i analiza kapaciteta (*performance monitoring and analyzer*), upravljanje sadržajem (*content management*), migracija podataka (*data migration*), monitoring resursa pojedinačnog korisnika (*quota monitoring*), upravljanje kapacitetom (*capacity management*), vizuelizacija, planiranje potreba za resursima čuvanja podataka (*provisioning*), upravljanje magnetnim trakama (*media management*), upravljanje promenam i konfiguracijom sistema (*configuration/ change management*), upravljanje pravilima ili politikama (*policy management*), upravljanje aktivima ili sredstvima inventarisanja (*asset management*) itd. [21].

Iako tržište sredstvima SRM ne raste tako brzo kao za prve dve kategorije sredstava čuvanja podataka, Gartner predviđa da će već 2007.god. svetsko tržište sredstava SRM dostići 24 % ukupnog tržišta sredstvima čuvanja podataka [21].

U savremenom poslovnom svetu, gde informacija i načini njene obrade i čuvanja imaju odlučujući značaj za realizaciju biznis-zadataka, **centri obrade i čuvanja podataka** postaju ključni faktor svih poslovnih zbivanja. Njih karakterišu četiri važne osobine: **pouzdanost** (otpornost na otkaze), efekasan **pristup podacima** (dostupnost), uspešna realizacija svih **uslužnih servise** i **fleksibilno** i srazmerno (poslovnim potrebama) konfigurisanje sistema čuvanja podataka.

Pre nego što se upoznamo detaljnije sa navedenim osobinama centara za obradu i čuvanje podataka, definišimo pojam sistema čuvanja podataka. **Sistem čuvanja podataka** je kompleks koji obuhvata ne samo masive za čuvanje podataka, već i transport ulaz/izlaz, metode razmeštanja podataka kao i softver za obezbeđenje optimizacije transporta, garantovanog dostavljanja, razmeštanja i čuvanja podataka.

Dobro projektovan sistem čuvanja podataka podrazumeva optimalan odnos između kapaciteta, mogućnosti pristupa podacima i ukupne cene koštanja TCO^x [22].

Spektar metoda povećanja **pouzdanosti sistema čuvanja podataka** je širok: dubliranje komponenata opreme, izbor nivoa RAID^x, razmeštaj podataka u odnosu na sistem fajlova, obezbeđenje pouzdanosti transporta za prenos podataka i ugrađena sredstva kontrole. Po pravilu, otkazi tehničkog karaktera su posledica narušenog funkcionisanje neke od komponenti sistema. Otkazi logičkog karaktera su posledice narušenog integriteta informacija zbog greške sistemskog softvera ili zbog nepravilnih postupaka personala.

Pouzdanost masiva diskova na račun dubliranja je opštepoznata stvar. Treba napomenuti da, prvo, dubliranje ne povećava kapacitet sistema čuvanja podataka i, drugo, da u novim tehnološkim rešenjima nemamo uzdvojene module^{xi} pojedinih sastavnih komponenti. Dubliranje, kao metod, je veoma skup. Masivi diskova imaju neke «unutrašnje» mogućnosti koje se mogu klasifikovati na sledeći način: trenutna kopija (*cloning*), trenutni snimak (*snapshot*) i daljinska sinhronizacija podataka (*remote mirror*).

Transport predstavlja prenos podataka između servera i masiva diskova. U zavisnosti od tipa sistema čuvanja podataka razlikujemo sledeće vrste transporta: direktno priključenje (DAS), pomoću mreže IP (NAS), mreža SAN, pomoću protokola Fiber Channel, protokol za proširenja SCSI na IP iSCSI i protokol Fiber Channel u IP - FCIP [22].

Porast računarskih resursa zahteva povećanje prostora na diskovima kao i garanciju integriteta i dostupnosti podataka. Jedna od važnih osobina centra obrade i čuvanja podataka je **pristup informacijama**. Tradicionalni model pristupa podacima «jedan na jedan» (server – disk) je krajnje neefikasan. Rešenje je **virtuelizacija**. U osnovi virtuelizacije leži princip razdvajanja i predstavljanja. Umesto više fizičkih diskova postoji jedan virtuelni disk. Na taj način korisnik nije vezan za određeni fizički disk, već za virtuelno prostranstvo. Virtuelizacija se realizuje softverski ili softversko-hardverski (npr. pomoću *HP StorageWorks Enterprise Virtual Array 5000*, *Sun StorEdge 9970*, *IBM Tivoli SANergy*, *Magnitude* itd.). Osim pouzdanosti i univerzalnosti, virtuelizacija omogućava jednostavno i efikasno upravljanje podsistemom diskova. Kapacitet operacija ulaz/izlaz se kreće od desetak do nekoliko hiljada operacija u sekundi što znatno premašuje vrednosti u tradicionalnim mrežama čuvanja podataka. Virtuelizacija se izvodi na različitim delovima infrastrukture pa razlikujemo virtuelizaciju na bazi hosta, na bazi sakupljača (sistemi sa intelektualnim kontrolerima) i na bazi mreže (simetrična i asimetrična integracija). Vreme dostupa i obrade podataka, smeštenih na mnogobrojnim i raznovrsnim medijumima, organizovano je preko komutatora. Virtuelizacija nije rešenje svih problema. Za sveobuhvatno upravljanje čuvanjem podataka neophodno su i dopunski servisi: rezervno kopiranje podataka, visok stepen operativnosti i upravljanje resursima čuvanja podataka [23].

IB u sistemima čuvanja podataka organizovana na krajnje ozbiljan način. U slučaju sistema DAS zaštita informacija je organizovana na mogućnostima operativnih sistema na principu razgraničenja prava pristupa i mogućnostima specijalnog softvera (antivirusni programi i kriptografski mehanizmi). Instrumenti zaštite u mrežama SAN su: autentifikacija hostova putem procedura *Fabric Login* i *Process Login*, upravljanje pristupom hostova ciljevima pomoću razbijanja na zone (*zoning*) i spiskovima pristupa i tehnologija VSAN – fizička mreža SAN se «reže» na mnoštvo (i do 1000) virtuelnih komutirajućih struktura.

Opasnosti za informacije, koje se čuvaju na hard disku, posmatramo u dva različita konteksta. Prvi je kada je hard disk elemenat komputera ili neke računarske mreže, pa u tom slučaju imamo klasičan tzv. kompjuterski kanal oticanja informacija (softverski ili hardverski načini «skidanja» informacija sa hard diska sa varijantom pristupa iz lokalne ili javne mreže), a drugi kada se hard disk posmatra kao samostalan elemenat koji je ili neispravan ili imitira neispravnost zbog koje je potrebno njegovo servisiranje. U prvom slučaju je moguća i direktna predaja informacija (putem radiopre-

dajnika, hardverskih «umetaka» - npr. kliper čip i nedokumentovanih mogućnosti^{xii}). U drugom slučaju neispravan disk (koji ne podleže dijagnostici standardnim programima) sa svim informacijama dospeva (kao deo ugovorom predviđenih garancija) u firmu koja ga je proizvela ili u servisni centar.

Otvorena literatura se ne bavi problematikom rekonstrukcije ranije zapisanih informacija. To ne znači da nije moguće pretpostaviti da postoje različite metode rekonstrukcije uništenih informacija (po nekim autorima i do 5 slojeva zapisa^{xiii}) koje su zasnovane na različitim fizičkim prilazima u restauraciji tanke strukture polja magnećenja nosioca informacija. Npr. moguća je upotreba, za kontrolu radnih površina hard diska, uređaja koji rade na osnovu efekta Barhauzena koji registruje skokovit karakter krive magnećenja na mikrostrukturnom nivou.

Nije isključena ni mogućnost upotrebe modifikovane tehnologije PRML (*partial response maximum likelihood* – maksimalna verodostojnost pri nepotpunom odzivu) koja se koristi kod savremenih hard diskova. Navedena tehnologija je razrađena zbog toga što pri postojećim gustinama zapisa više nije moguće jasno i jednoznačno očitavanje signala sa površine diska jer je nivo smetnje i izobličenja veoma velik. Umesto direktne transformacije signala koristi se njegovo upoređenje sa skupom etalona (obrazaca) i na osnovu maksimalne sličnosti (verodostojnosti) donosi se zaključak o prijemu ove ili one mašinske reči. Primena tehnologije PRML zajedno sa korelacionom obradom povećava mogućnost rekonstrukcije uništenih informacija standardnim brisanjem pomoću magnetnog polja.

Kao pouzdana i tehničko-tehnološki prihvatljiva (disk ostaje neoštećen), upotrebljava se **tehnika delovanjem jakog spoljašnjeg magnetnog polja** (200 do 320 KA/m). U slučaju zahteva da disk ne dospe u neovlašćene ruke (posebno osetljive informacije), koristi se termohemijska metoda uništavanja medijuma pomoću procesa samogoruće visokotemperaturne sinteze SVS^{xiv}.

Obezbeđenje neprekidnosti poslovanja (biznisa) zahteva odgovoran prilaz pri izboru strategije čuvanja i pristupa informacijama. Klasično rešenje tog zadatka je organizacija sistema čuvanja podataka na bazi mreže SAN, organizacija rezervnog kopiranja po principu obilaska servera i formiranje rezervnog centra obrade i čuvanja podataka za zaštitu od katastrofa. Naprednija rešenja podrazumevaju i sredstva za upravljanje resursima SRM.

2.3. Informaciono-analitičko obezbeđenje poslovanja

Svi aspekti značaja IB u sferi ekonomskog poslovanja često nisu vidljivi na prvi pogled^{xv}. Naime, u skladu sa nekadašnjim shvatanjima pod IB se obično tretira samo zaštita informacija prenebregavajući činjenicu da je pojam IB širi pojam koji podrazumeva i drugu stranu medalje, a to je **dostupnost** ili otvoenost informacija za subjekte kojima je ona namenjena. Uspešno poslovanje, kao i bilo koja druga delatnost, je nezamisliv bez informaciono-analitičkog obezbeđenja. Pod pojmom **informaciono-analitičko obezbeđenje** podrazumeva se dostupnost informacija^{xvi} svim privrednim subjektima pod jednakim uslovima čime se sprečava nelojalna konkurencija i, finansijskim dobitkom motivisano, dogovaranje učesnika, pre svega, u nabavkama. Informaciono-analitičko obezbeđenje shvaćeno kao sigurnost u dostupnosti svim relevantnim informacijama potrebnim za uspešno poslovanje nije samo u interesu biznisa, već i države jer je uspešno polovanje privrednih subjekata garant nepretka celog društva pa samim tim i pojedinca.

Problematiku informaciono – analitičkog obezbeđenja biznisa reguliše država bilo preko svojih organa bilo pravnom regulativom rada nedržavnih sistema zaštite pravnog poretka i sistema bezbednosti (detektivske, analitičarske i druge agencije) kao i regulativom pristupa «otvorenim» informacijama. Ovoj problematici pripada i regulisa-

nje rada profesionalnih udruženja (npr. advokatska komora) koja, između ostalog, kontrolišu profesionalnu etiku svojih članova^{xvii}.

Problematika informacionog-analičkog obezbeđenja proističe iz shvatanja da je **dostupnost** (*открытость* – otvorenost) **informacija** sastavni deo pojma informacione bezbednosti^{xviii}, odnosno sigurnosti društva i pojedinaca da niukom pogledu nisu «uskraćei» za informacije koje im «pripadaju»^{xix}. Posmatrano u ekonomskoj sferi, informaciona otvorenost doprinosi efikasnosti ekonomije na taj način što informaciono – analitička podrška doprinosi da preduzetništvo raspolaže sa adekvatnim procenama rizika i da može donositi pravilne odluke o poslovnim potezima. Npr. informaciona otvorenost u oblasti investicionih projekata, povećava interes stranog ulaganja na račun smanjenih sistemskih i specifičnih investicionih rizika.

Pitanje informacione otvorenosti je regulisano i međunarodnim normama – dokument o globalnom informacionom društvu (sporazum iz Okinave) i Preporuka broj R(81) 19 Komiteta ministara država članica Saveta Evrope - «O dostupnosti informacija koje se nalaze na raspolaganju u državnim ustanovama»^{xx}.

Drugi aspekt problema informacionog-analičkog obezbeđenja je inkorporacija sveobuhvatnih **poslovnih informacionih sistema** (PIS) u proces upravljanja poslovanjem. PIS-i treba da zadovolje potrebe top-menadžmenta za analitičkim, prognozirajućim i faktičkim informacijama na osnovu kojih je moguće doneti pravilne odluke u strategijskoj orijentaciji razvoja firme, a da pri tome zadovolje i potrebe nižih nivoa upravljanja u delokrugu njihovih nadležnosti^{xxi}. Problematika informatizacije i automatizacije putem PIS oličena je u tzv. sistemima planiranja korporacijskih resursa ERP (*Enterprise Resource planning*).

2.4. Elektronsko poslovanje i infrastruktura zaštite

Elektronsko poslovanje (*e-business*) obuhvata elektronsko bankarstvo (*e-banking*) i elektronsku trgovinu (*e-commerce*)^{xxii}. Elektronsko bankarstvo i elektronska trgovina se međusobno tesno prepliću i predstavljaju deo savremenog koncepta ekonomske sfere društva i sveta u celini^{xxiii}. Kao posebna grana elektronske trgovine, sve se više razvija mobilna trgovina (*m-kommerce*) – trgovina pomoću mobilnih telefona.

Elektronsko bankarstvo predstavlja novi način realizacije bankarskih biznis-procesa čija je suština u realizaciji bankarskih transakcija pomoću računarskih mreža. U tom smislu elektronsko bankarstvo je važna komponenta elektronskog poslovanja. Ono podrazumeva *on-line* informacionu podršku (pre svega elektronske trgovine), emisiju digitalnog novca, elektronska plaćanja, depozitne kredite, valutne i investicione operacije. Na tržištu se sreće nekoliko modela *on-line* bankarskog biznisa: Internet odelenja tradicionalnih banaka, Internet – banke, virtuelne banke i elektronski finansijski supermarketi^{xxiv}.

Elektronska trgovina predstavlja najekonomičnije okruženje za prezentaciju i plasman roba i usluga. Tipične e-commerce šeme su B2B, B2C (*business-to-business, business-to-customer*) i B2E (*business-to-ethernet*). Reč je o elektronskom poslovanju između preduzeća, između preduzeća i korisnika (klijenata) i integraciji internog segmenta poslovanja kako sa drugim preduzećima tako i sa klijentima (B2B i B2C e-commerce šemama).

B2B predstavlja poslovanje između preduzeća, tj. razmenu proizvoda, usluga i informacija sa drugim firmama iz okruženja. B2B poslovanje je zasnovano na Internetu i obuhvata tri faze razvoja: EDI (*electronic data interchange*) – elektronsku razmenu podataka, osnovni B2B e-commerce (prodaja proizvoda kompanija distributerima) i elektronski marketing (*eMarkets*). Elektronski marketing (*e-marketplaces*) je novi oblik *on-line* posrednika koji na jednom mestu efikasno postavlja ponudu i tražnju, pružajući kupcima niže troškove nabavke uz mogućnost kontakta sa dobavljačima, a isto tako i dobavljačima niže troškove prodaje uz mogućnost kontakta sa novim kupcima.

B2C predstavlja poslovanje između preduzeća i neposrednih korisnika (klijenata). Kao oblici poslovanja (prema nekim autorima u razvoju B2C sistema zabeleženo je 5 modela) susreću se virtuelni trgovinski centar (VTC) i Internet *on-line* aukcija. Virtuelni (elektronski) trgovinski centar predstavlja skup dve ili više elektronskih prodavnica, u kojima se kupcima nude neki proizvodi ili usluge, uz koje može biti uključen i program pratećih usluga ili sadržaja. *On-line* aukcije omogućavaju kupcima nadmetanje, a trgovcima postizanje maksimalne cene. Osim toga svako može da ponudi bilo kakvu robu i da na globalnom svetkom tržištu nađe kupca.

Pojave B2B i B2C oblika poslovanja, donele su sa sobom nove pojmove (elektronsko plaćanje, elektronski novac, digitalni novčanik, digitalni ček, platne kartice itd.) i neke nove delatnosti kao što su internet marketing^{xxv}, upravljanje odnosima sa korisnicima CRM (*customer relationship management*) i rad coll centara. Upravljanje odnosima sa korisnicima u elektronskoj trgovini (e-commerce CRM - eCCRM) predstavlja složen skup poslovnih procesa i tehnologija upravljanja relacijama sa postojećim i potencijalnim korisnicima i poslovnim partnerima, u marketingu, prodaji i podršci (preko i uz pomoć svih raspoloživih komunikacija). Iako je Web tehnologija sve više prihvaćena kao kanal tehničke podrške, i dalje se preko 70 % kontakata realizuje preko coll centara. I u našoj zemlji je u planu razvoj nekoliko coll centara.

Osvrnimo se na **infrastrukturu zaštite u elektronskom poslovanju**. Razvoj elektronskog poslovanja zasnovan je na razvoju Internet tehnologije i primeni kriptografskih mehanizama. Na njihovim osnovama razvijaju se finansijske i korporacijske računarske mreže bazirane na TCP/IP protokolima. Informaciona i svaka druga bezbednost elektronskog poslovanja zasnovana je na tri kamena temeljca:

- **autentikaciji** (identifikaciji - predstavljanju korisnika),
- **autorizaciji** (korisnik dobija ovlašćenje da realizuje određene zadatke) i
- **zaštiti tajnosti** (šifrovanju podataka).

Autentikacija se bavi problemom neovlašćenog pristupa informacionim sistemima. Autentikacija korisnika u distribuiranim mrežama realizuje se kroz dva modela: model predstavljanja (delegiranja) i model servera. U prvom modelu korisnik se predstavlja serveru sa bazom podataka i na osnovu akreditiva mu je odobren pristup. U drugom modelu, neposredan pristup serveru nema korisnik, već aplikacija. Kao instrumenti koriste se parole, lozinke i sredstva biometrijske identifikacije.

Autorizacijom se reguliše nivo ovlašćenja korisnika mreže. Autorizacija omogućava određenim korisnicima ili servisima kontrolisani pristup resursima. Sa stanovišta sigurnosti je veoma važno da su novi pristupi ograničeni na samo autorizovane korisnike.

Zaštita tajnosti podataka podrazumeva šifrovanje podataka u cilju sprečavanja neovlašćenog pristupa osetljivim informacijama. Zaštita tajnosti se implementira na nivou međuserverske komunikacije i realizuje se preko privatnih virtuelnih kanala (VPN – *virtual private network*) ili SSL (*security socket layer*) protokola^{xxvi}.

Osnovni kriptografski aspekti savremenih računarskih TCP/IP mreža, odnosno elektronskog poslovanja su:

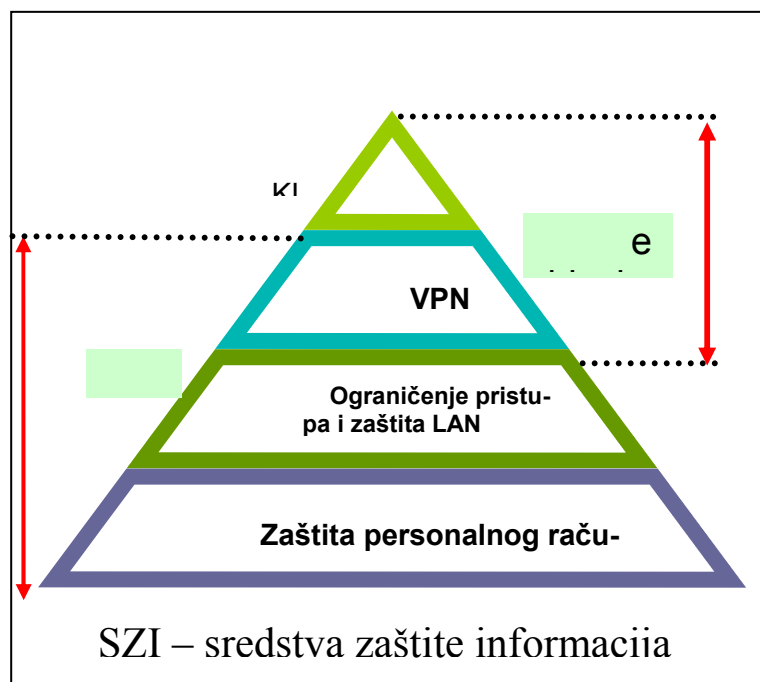
- infrastruktura sistema sa javnim ključevima (PKI – *public key infrastructure*),
- tehnologija digitalnog potpisa bazirana na asimetričnim šifarskim sistemima i
- zaštita tajnosti podataka primenom simetričnih šifarskih sistema.

PKI sistem predstavlja najvažniji aspekt sistema elektronskog poslovanja, kao i savremenih finansijskih i korporacijskih računarskih mreža. PKI sistem obezbeđuje pouzdano okruženje za realizaciju četiri osnovne funkcije zaštite komercijalnih i poslovnih transakcija - autentičnost strana u komunikaciji, integritet podataka, nemogućnost naknadnog poricanja sadržaja poslatih podataka i zaštitu tajnosti podataka. Prve tri funkcije realizuju se na bazi tehnologije digitalnog potpisa primenom asimetričnih kriptografskih sistema, dok se funkcija zaštite tajnosti realizuje primenom simetričnih kriptografskih sistema. Srce PKI sistema predstavlja Certifikaciono telo (CA – *certification authority*) čija je osnovna funkcija pouzdano uspostavljanje zaštićenog digitalnog identiteta ovlašćenih učesnika u datoj računarskoj mreži. Pomenuta funkcija se postiže pri-

menom digitalnog sertifikata koji jednoznačno povezuje identitet ovlašćenog učesnika sa javnim ključem asimetričnog šifarskog sistema. Autentičnost i jednoznačnost svakog digitalnog sertifikata dokazuje se digitalnim potpisom svakog digitalnog sertifikata od strane Certifikacionog tela. Na taj način certifikaciono telo postaje treća strana od poverenja za bezbednu komunikaciju bilo koja dva ovlašćena učesnika u datoj računarskoj mreži.

Istorijski postoji više različitih načina za primenu tehnologije digitalnog potpisa. U poslednje vreme skoro isključivo se koristi tehnologija sa standardom PKSC# 1 (*public key cryptographic standards*)^{xxvii}. Prema tom standardu, tehnologija digitalnog potpisa se sastoji od dve operacije: **digitalnog potpisa i provere digitalnog potpisa**. Sadržaj koji treba potpisati se prvo redukuje (algoritmi tipa MD5 ili SHA-1), da bi se zatim šifrovao asimetričnim algoritmom (npr. algoritmom RSA) i to operacijom tajnog ključa korisnika. Operacija provere digitalnog potpisa se sastoji od razdvajanja poruke na podatke koji se prenose i na sam digitalni potpis. Digitalni potpis se dešifruje pomoću javnog ključa pošiljaoca. Ovim postupkom dobijaju se dve *hach* funkcije na osnovu kojih se zaključuje o autentičnosti pošiljaoca, integritetu prenetih podataka i o neporecivosti poslate poruke.

Uspostavljanjem PKI sistema u računarskoj mreži, moguće je realizovati bezbedno okruženje za realizaciju različitih aplikacija (zaštićeni Web servisi, zaštićeni E-mail, zaštićeni FTP, bezbedno upravljanje dokumentacijom, bezbedna funkcija kontrole pristupa, bezbedno plaćanje i formiranje zaštićenih sesija – virtuelnih privatnih kanala VPN).



Slika 2: Infrastruktura zaštite informacija u elektronskom poslovanju

U elektronskom poslovanju kriptografske funkcije se realizuju i pomoću kriptografskog hardvera – *smart* kartica. Reč je o mikroprocesorski baziranom medijumu koji poseduje javni i, PIN-kodom (*personal identification number*), zaštićeni deo memorije. Na njima se mogu čuvati i generisati kriptografski ključevi i svi lični podaci što ih čini pogodnim za bezbedno poslovanje.

2.5. Organizacija službe informacione bezbednosti

Projektovanje i realizacija mera zaštite informacija u cilju obezbeđenja informacione bezbednosti povlači za sobom postojanje **organa zaštite informacija**. Često je izbor strukture ovih organa od presudnog značaja za sistem zaštite. Istraživanja pokazuju da je mnogo propusta u ovoj oblasti i svaka druga poruka, na osnovu provedenih istraživanja je, da se zaštita informacija prepusti stručnjacima u toj oblasti.

Sve je veći broj firmi u kojima pored direktora bezbednosti (CSO – *Chief Security Officer*) postoji, kao zasebna funkcija, **direktor informacione bezbednosti** (CISO – *Chief Information Security Officer*)^{xxviii}. Pored direktora IB, koji se bavi razradom i realizacijom politike bezbednosti, sve je češća i funkcija menadžera službe IB (BISO – *Business Information Security Officer*) koji se bavi praktičnom realizacijom politike bezbednosti na nivou odeljenja (npr. plansko-ekonomskog, marketinga ili odeljenja IT)^{xxix}.

Ovakvom organizacijskom strukturom izmenjen je status službe IB. Direktor IB (CISO) pripada top-menadžmentu firme! Isto tako izmenjen je i profil njegove kompetentnosti - za razliku od direktora IT, on mora posedovati ne samo tehnička, već i upravljačka (menadžment, ekonomija, privredno pravo) i specijalistička znanja (organizacija sistema IB, zaštita poslovnih tajni, specijalna psihologija, osnovi kriminalistike i industrijska špijunaža)^{xxx}. Ovakvo definisano radno mesto podrazumeva koordinaciju i konsultaciju sa nizom različitih sektora međusobno prilično udaljenih (finansijski, komercijalni, sektor proizvodnje, sektor informacionih tehnologija itd.). Očigledno je da stručnjaka ovakvog profila nema ili ih je malo i da firme moraju da rade na njihovom stvaranju.

Interesantno je napomenuti da je u firmama koje se bave elektronskim poslovanjem, **odgovornost za informacionu bezbednost poverena komercijalnom menadžeru**, a ne menadžeru za informacione tehnologije! Očigledno je da je reč o nastojanjima da se IB - zaštita informacija tretira sa stanovišta tržišta i što veće ekonomske dobiti, a ne aspekta tehnike i tehnologije.

U budućim organizacijskim rešenjima nazire se objedinjavanje službe IB i službe bezbednosti na čijem čelu bi bio direktor CPO (*chief privacy officer*)^{xxxi}. U ovom slučaju je reč o konceptu integralne bezbednosti.

U kontekstu mera za očuvanje informacione bezbednosti, kao stanja koje omogućava nenarušeni rad sa informacijama i informacionim resursima, zaštita informacija prerasta u zasebnu delatnost sa široko razgranatom lepezom profesija^{xxxii}. Prema predviđanjima analitičara u SAD, kao vodećoj zemlji u oblasti informacionih tehnologija, do 2007.god. u oblasti zaštite informacija će profesionalno raditi oko 100 000 ljudi [19].

Istaknimo još jednom - informaciona bezbednost nije samo problem informacionih tehnologija. Ona je u suštini mnogo više.

Nizak nivo IB može dovesti do gubitka reputacije, tržišta, povećanja izdataka i smanjenja profita. U ozbiljnim firmama politika IB obuhvata sve segmente delovanja, a ne samo informacione tehnologije (IT). Pravila upravljanja IB data su u standardu ISO 17799. Interesantno je pomenuti da su samo velike firme ugradile ovaj standard u svoje poslovanje. Osim finansijskih izdataka reč je i o drugim faktorima. Zvuči nestvarno, ali istraživanje iz 2002.^{xxxiii} je ustanovilo da 73% personala u službi IB nema nikakve formalne kvalifikacije u oblasti IB^{xxxiv}!

3. STANJE INFORMACIONE BEZBEDNOSTI U OBLASTI BIZNISA

O stvarnom stanju IB u oblasti biznisa moguće je suditi samo po rezultatima istraživanja. Nažalost, takva istraživanja za našu zemlju autoru nisu poznata. U okviru istraživanja koja se provode mahom u zapadnim zemljama, na čije se rezultate pozivamo, primenjuje se metod anketnog ispitivanja struktura koje se bave informacionom bezbednošću. Ograničenje rezultata ovakvih istraživanja je činjenica da su odgovori na neka pitanja, kao što su veličina finansijskih gubitaka, iz mnoštva razloga subjektivni i obično umanjeni. Pored subjektivnosti, rezultate ovakvih istraživanja karakteriše, na opšte zaprepašćenje, nedovoljan stepen edukovanosti ispitanika i pomanjkanje tačnih i ažurnih podataka o problemu o kome je reč. S druge strane, ovim ispitivanjima obuhvaćeni je samo kompjuterska bezbednost^{xxxv}.

U iznošenju rezultata istraživanje polazimo od istraživanja Global information security survey^{xxxvi} jer je vršeno u različitim sektorima i širom svih kontinenata za razliku od istraživanja Secure Enterprise koje je izvršeno na manjem uzorku (431) i samo u SAD^{xxxvii}.

Zabrinjavajuća je činjenica da je broj neregistrovanih, neprocenjenih (sa stanovišta veličine materijalnih gubitaka) ili nedovoljno tačno procenjenih **napada** velik (npr. 19% organizacija ne zna koliko je vremena potrošeno za obnovu sistema posle napada virusom, dok 42% ne zna veličinu finansijskih gubitaka). Direktni gubici (srednja vrednost) iznose 108 000 USD. Ako se dodaju indirektni gubici (zastoj u radu personala, izdaci za usavršavanje sistema zaštite) i gubitak reputacije firme, posledice napada mogu poprimiti velike razmere. S druge strane, publikovane rezultate treba prihvatiti sa rezervom.

Uspešno upravljanje rizikom podrazumeva **učešće najvišeg rukovodstva** kompanija i angažovanje finansijskih sredstava. Ustanovljeno je da je u 47% kompanija za IB odgovoran savet direktora i da je, kao srednja vrednost, za bezbednost IT potrošeno 2,6 miliona USD, odnosno 10,1% IT budžeta.

Prema istraživanju u SAD u 80% kompanija izdaci za sredstva IB se nalaze u okviru budžeta za IT. Gartnerova predviđanja^{xxxviii} su da će izdaci za IT u narednom periodu rasti po stopi od 6%, pri čemu izdaci za IB rastu po godišnjoj stopi od 28%. Interesantno je napomenuti **da ¾ kompanija zahteva da rashodi za IB budu «opravdani» sa tačke gledišta ukupnog biznisa** ! Na američkom tržištu najviše se prodaju zaštitni zidovi^{xxxix} (81%), antivirusni programi (79%), virtuelni privatni kanali VPN (71%) i sistemi za otkrivanje napada IDS (43%). Posledica toga je da je u SAD 2003.god., po prvi put od 1999.god., registrovano smanjenje gubitaka zbog napada na informacione sisteme tako da su gubici (202 milona USD) za 56% manji nego 2002.god. (455 milona USD).

Posmatrano u svetskim razmerama, i pored učestalih slučajeva «rušenja» IS, mnoge kompanije još uvek **IB posmatraju kao tehničko pitanje** koje se odnosi na kompetencije specijalista IT. Po stepenu uključenosti najvišeg rukovodstva prednjači finansijski sektor koji se tradicionalno najozbiljnije odnosi prema pitanjima zaštite informacija u finansijskim transakcijama koje inače zahtevaju viši stepen zaštite.

Problem praćenja stanja i efikasnosti zaštite informacija je najdoslednije tretiran na američkom kontinentu. To se objašnjava činjenicom da organizacije iz tog regiona tradicionalno koriste **formalizovane metode** (oličene u standardima) u svim sferama upravljanja u kompanijama. Neočekivano je što su najlošiji rezultati (60% se ne koristi formalizovanim kriterijumima) u sektoru industrije i trgovine. Među malobrojnim kompanijama koje koriste formalizovane kriterijume, neznatan je broj koji primenjuju kompleksnu metodologiju koja objedinjava različite prilaze u oceni efikasnosti sistema IB. Samo 34% kompanija vode formalnu registraciju incidenata u oblasti IB. Ostale kompanije nemaju informacije o broju napada na IS i, razumljivo, ne mogu suditi o veličini nanete štete !

Rezultati ispitivanja pokazuju da kompanije lakše i brže preduzimaju mere protiv saradnika, nego spoljnjih napadača. Pored čuvanja reputacije, reč je i o pravnim problemima – identifikaciji i dokaznom materijalu protiv napadača.

Postojanje posebnih službi za IB je u porastu. Broj posebnih odeljenja za IB je od 2001. do 2003.god. porastao za 10%. Broj personala je proporcionalan veličini kompanije (broju zaposlenih i obrtnom kapitalu) i kreće se oko 5 na 100 zaposlenih i obrtni kapital do 100 miliona USD. U finansijskom sektoru **služba IB** je odvojena od službe IT (45%) prema 29% u industrijskom sektoru. Zanimljivo je da je kvalifikaciona struktura zaposlenih u službi IB (formalno posedovanje zvaničnih sertifikata) na nivou od 5 do 8% !!! Broj onih koji rade u službi IB od 1 do 5 godina je 66%.

Politika IB, odgovarajući standardi i pravila bezbednosti definišu listu ciljeva i zahteva koje je potrebno približiti saradnicima. IB nije problem samo informacionih tehnologija. Ona obuhvata sve segmente delovanja i zbog toga je neophodno angažovanje najvišeg rukovodstva za njeno definisanje, promovisanje i uvođenje. Prema Global information security survey 47% kompanija i firmi ima politiku bezbednosti definisanu na nivou saveta direktora. Pravila upravljanja IB su definisana standardom ISO 17799. Istim ispitivanjem je ustanovljeno da u korišćenju tog standarda prednjači Evropa, ali i da su samo 49% kompanija, koje ga koriste, provele proceduru nezavisnih sertifikacija. Standarde koriste većinom velike firme.

Upravljanje IB obuhvata pitanja svakodnevnih operacija i tekuće kontrole bezbednosti. Istraživanjem je ustanovljeno da 31% kompanija ne koristi nikakvu stranu pomoć, a da je 16% kompanija delegiralo funkcije podrške IB spoljnim saradnicima. Delegiranje funkcija je karakteristično za zemlje Evrope i manje firme, a vezano je za nove tehnologije. Važno je uočiti da delegiranja rizika nema, ali i da neke aktivnosti ne mogu da se delegiraju drugim firmama.

Testiranje pouzdanosti sistema IB se provodi u 77% kompanija i firmi.

Zaštita informacija primenom **moderne tehnološke infrastrukture** (tzv. «bit-bajtni» elementi sistema IB koji počinju sa međumrežnim ekranima - *firewall* i sistemima za otkrivanje napada a završavaju sa infrastrukturom zaštite podataka), prema Global information security survey], na svetlo dana je iznela porazne rezultate. Konstatovano je da je primena savremenih tehnologija slabo zastupljena. Od anketiranih firmi samo 10% ima implementiranu tehnologiju javnog ključa PKI (*public key identification*), od 13% firmi sa bežičnom mrežom^{xl} samo 62% koristi virtuelne privatne mreže VPN (*virtual privacy network*), samo 7% firmi koje koriste portabl uređaje PDA-klase je uvelo bilo kakvu zaštitu u odnosu na informacione sadržaje koji se na njima nalaze, u većini firmi (82%) identifikacija se izvodi klasičnim putem pomoću lozinki koje se menjaju na mesec dana i ređe, biometrijska identifikacija je zastupljena samo u 2% firmi, u 76% firmi udaljeni pristup korporativnoj mreži ostvaruje se putem registracije i lozinke (samo 14% firmi koristi pouzdaniju dvofaktorsku identifikaciju pomoću smart kartica i 1% biometrijska sredstva!). Sistem za otkrivanje napada IDS (*intrusion detection system*) koristi samo 14% firmi dok drugih 15% koristi sistem zaštite pojedinačnih čvorova mreže analizirajući registrovane zapise (log-fajlovi).

4. ZAKLJUČAK

U uslovima savremenog tržišta, poslovni uspeh i ekonomska bezbednost neza-mislivi su bez informacione bezbednosti. Informacije i informacioni resursi predstavljaju materijalna dobra i zbog toga je **zaštita informacija neodvojivi deo poslovanja**. U poslovnom svetu nepisano pravilo je da je informacija jedan od najvažnijih izvora napretka bilo koje firme. Različite organizacije iz različitih razloga treba da štite informacije.

Informaciona bezbednost se reflektuje na poslovanje u četiri različita vida: kao pribavljanje poslovnih informacija putem konkurentskog izviđanja i industrijske špi-

junaže, kroz upravljanje životnim ciklusom informacija – čuvanje baza podataka, kroz različite oblike elektronskog poslovanja i kroz informaciono-analitičko obezbeđenje poslovanja.

Problem zaštite informacija nije pitanje tehničkih, već upravljačkih (poslovnih) struktura i raspoloživih finansijskih sredstava. **Troškovi za obezbeđenje zaštite informacija** ne smeju da budu veći od veličine gubitaka koji mogu nastati usled napada. Savremeni pristup organizaciji zaštite informacija zasnovan je na konceptu upravljanja rizikom.

Lociranje saradnika ili bivših radnika kao potencijalnog žarišta problema zaštite informacija, ukazuje na važnost pravilnog **definisanja politike IB** i ozbiljnog tretmana pojava **konkurentskog izviđanja** i **industrijske špijunaže**. U tom kontekstu pored tehničkih, važno mesto pripada i tzv. psihološkim metodama zaštite informacija (socijalna psihologija).

Sve velike kompanije smatraju da je **informaciona bezbednost jedan od najvažnijih prioriteta u vođenju biznisa**. U skladu sa tim evidentne su radikalne promene u organizaciji službe informacione bezbednosti – ona ne samo da se odvajava od službe za IT, već dobija i direktora i menadžera za IB (CISI i BISO). Pitanja informacione bezbednosti i problem zaštite poslovnih informacija su sa, sve donedavno, krajnjih margina dospela u situaciju da budu delokrug interesovanja samog top-menadžmenta.

Moto savremenog društva je - zaštitite svoj biznis, ali pri tome nikada ne treba smetnuti sa uma činjenicu da zaštita informacija nije konačan cilj, već samo jedno od sredstava uspešnog vođenja biznisa.

LITERATURA

1. Леваков А., Анатомия информационной безопасности США, Jet info online # 6 (109), 2002
2. Леваков А., Новые приоритеты в информационной безопасности США, Jet info, № 10, 2001 г.
3. Панарин И., Н., Проблемы обеспечения информационной безопасности в современных условиях, <http://www.kiev-security.org.ua>, 1997
4. Решение Коллегии Гостехкомиссии России № 7.2/02.03.01г., Специальные требования и рекомендации по технической защите конфиденциальной информации, Москва, 2001
5. Беляев А., В., Методы и средства защиты информации (курс лекций), ЧФ СПбГТУ, 2001
6. Зенковский А.К., Защита информации в компьютерных системах – слагаемые успеха, <http://www.infosec.ru>
7. ИТ-специалисты выигрывают сражение за безопасность, учебные курсы, 2003, www.CNews.ru
8. Барсуков Д., Интегральная защита информации, "Электроника. Наука, технология, бизнес" №3-4, 1998г.
9. Лукацкий А.В., Новые грани обнаружения и отражения угроз, PCWeek/RE, №5, 2000
10. Г Кисиленко, А Хорев, Угрозы безопасности системам электросвязи, <http://kiev-security.org.ua>
11. Лукацкий А.В., Новые подходы к обеспечению информационной безопасности, Компьютер-Пресс. №7, 2000
12. Лукацкий А.В., Информационная безопасность. Как обосновать? Компьютер-Пресс. № 11, 2000
13. Симоньян Т. А, Средства вычислительной техники в защищенном варианте, как часть решения задачи информационной безопасности, Специальная техника, № 2, 2000
14. D. K. Hsiao, D.S. Kerr, S.E. Madnik, Computer security, Academic Press, New York, san Francisko, 1979
15. Лукацкий А.В., Вопросы информационной безопасности, связанные с применением Internet в кредитно-финансовых учреждениях, Тематический выпуск № 1, НИП Инфорзащита, Москва, 1997

16. ИТ-специалисты выиграют сражение за безопасность ?, CNews.ru, 17.10.2003.
17. Ирина Муравьева, Новый взгляд на службу информационной безопасности компании, infosecutivity.ru
18. Барсуков В., С., Интегральная защита информации, Специальная техника, № 12, 2003
19. Global Information Security Survey, Истраживање је публикувано у Обзору РосБизнес-Консалтинг 2002. god.
20. Лукацкий А.В., Возврат инвестиций в информационную безопасность, Компьютер-Пресс. № 3, 2002
21. Абалмазов Э., И., Концепция безопасности – математический анализ эффективности, <http://kiev-security.org.ua>, 2000
22. Ананский Е., В., Защита информации – основа безопасности бизнеса, журнал «Служба безопасности», № 10, 11-12 1999. год. и № 1-2 2000.год.
23. Benesko G., С электронным бизнесом – в третье тысячелетие, глава из кнѣге Das e-business Prinzip, Herausgegeben von IBM Consulting Group. F.A.Z. – Insitut, Frankfurt-am-Main, 1999, журнал «eCommerce World», № 01, 2001 изд. «Открытые сисемы», <http://www.osp.ru>
24. Жилкина Н., Данные в порядке ?, Журнал «LAN», № 4/2004., издательство «Открытие системы» (<http://www.osp.ru>)
25. узварик А., Отказоустойчивые системы хранения, Журнал «LAN», № 4/2004., издательство «Открытие системы» (<http://www.osp.ru>)
26. Bunn F., К цели ведет множество дорог (превод на руски), Журнал «LAN», № 4/2004., издательство «Открытие системы» (<http://www.osp.ru>)
27. Синковски С., Неки аспекти и проблеми заштите информација, Безбедност, 04/2004, стр. 586 – 602
28. Медведовский И., Современные методы и средства анализа и контроля рисков информационных систем компаний, Учебный центр «Информсащита», 12.01. 2004

ENDNOTE:

- i Prema istraživanju iz 2002.g. srednja vrednost izdataka na IB je 10,1% od budžeta za informacione tehnologije.
- ii Zanimljivo je napomenuti da svake godine 10 000 japanskih biznismena ode na službeni put u inostranstvo !
- iii М. Расчётов, Идеология и методология промышленного шпионажа, Lan, № 3, 2002
- iv Чиняков Р., Сети хранения в ретроспективе и перспективе, Журнал «LAN» №7 2004.,Издательство «Открытые системы»
- v Keller М., Правильное обращение (prevod na ruski), Журнал «LAN» №7 2004., Издательство «Открытые системы»
- vi Prve mreže čuvanja podataka realizovane su sa interfejsima FC-AL. Diskovi (do 10) su se priključivali u prsten (*private loop*). Potreba za većim kapacitetima memorija (i do nekoliko stotina MB/s) dovela je do pojave komutatora sa funkcijama prenosa kadrova, dufuznih servisa, registracije, kontrolera, službe kataloga, upravljanja, preimenovanja, mnogoadresne distribucije virtuelizacije.
- vii «Narandžasta knjiga» predstavlja standard 5200.28-SRD DoD Trusted Computer Evaluation Criteria (TCSEC), 1985.
- viii Trenutno najmoćnija tehnologija kada je u pitanju regulisanje pristupa podacima koje zadovoljava *on-line* biznis-procese.
- ix TCO (*Total Cost of Ownership*) – ukupna cena koštanja vladanja informacionim sistemom.
- x Kontroleri za upravljanje diskom.
- xi Masivi diskova obuhvataju: diskove, sistem ulaz/izlaz (portovi – SCSI, SSA, FC, FCIP, iSCSI, intelektualne komponente – npr. komutacija Fibre Channel), kontrolere diskova i unutrašnje komutacione komponente.
- xii Kapacitet neformatiranog hard diska se razlikuje od kapaciteta diska formatiranog standardnim programima za 16 do 19%.
- xiii Боборыкин С., Оценка эффективности средств уничтожения информации, хранящейся в накопителях на жестких магнетных дисках, Специальная техника № 1, 2001.год.

-
- xiv SVS sredstva omogućavaju lokalno oslobađanje visoke temperature u vrlo kratkom vremenskom intervalu. Hemijski su vrlo stabilna, ne izazivaju detonaciju i ne oslobađaju gasove. Većina reaktanata je jeftina. Nekoliko grama SVS uništava mikrošemu. SVS sredstva su otkrivena 70-ih godina prošlog veka.
- xv Prema rečima A. A. Streljčova, zamenika načelnika stručnog tela Saveta bezbednosti RF, prilikom pisanja doktrine IB RF propušteno je da se reguliše informaciono obezbeđenje biznisa (Međunarodni forum «Tehnologije bezbednosti», Moskva 2002.god.).
- xvi Rešenje problema državnih nabavki i privilegovanog položaja administracije i birokratije, SAD vide u elektronskoj trgovini koja je zasnovana na elektronskom plaćanju, upotrebi SMART kartica za identifikaciju (naručioca nabavki) i upotrebi elektronskog digitalnog potpisa (kao sredstva neporicijivosti porudžbine i identifikacije naručioca).
- xvii Пилюгин Л., Роль системы негосударственной првоохраны и информационно-аналитической поддержки бизнеса в обеспечении безопасности предпринимательства в России, электронный журнал Факт № 3 1999
- xviii Минаев Ю., Информационная открытость – составная часть национальных интересов России в информационной сфере, Међународни форум «Технологije безбедности», Москва 2002.год.
- xix U uvodnom delu je napomenuto da je pojam informacione bezbednosti sveobuhvatan i da prožima sve sfere ljudskog bitisanja. Filozofski, socijalni i psihološki aspekti informacione bezbednosti su predmet razmatranja ne samo samo ruskih, već i zapadnih istraživača.
- xx Problematika informacione otvorenosti se u Ruskoj federaciji ozbiljno tretira od 1991.god. o čemu svedoče međunarodni forumi i okrugli stolovi .
- xxi Белоусова О., Информационное обеспечение модели стратегической ориентации корпорации, Међународни форум «Технологije безбедности», Moskva 2002.god.
- xxii Prema sajtu www.e-trgovina.co.yu
- xxiii Elektronska razmena podataka EDI (*Electronic data interchange*) pojavila se 1968.god., prvi elektronski prodajni punkt EPoS (*Electronic Point of Sale*) – 1979., prve on-line bankarske usluge preko telefona – 1987.god. i prve kupovine preko Interneta – 1994.god.
- xxiv М. Грачева, Управление рисками в сфере электронных банковских услуг, Журнал «ecommerce World», № 04, 2001.год.
- xxv Elektronsko poslovanje je mnogo više nego puka elektronska trgovina. Izlazak na Internet podrazumeva izradu Internet biznis plana. Razlukujemo nekoliko oblika internet marketinga: marketing u okviru sopstvenog sajta (*Inner site marketing*), marketing u sklopu vizuelne celine (*Inner Web site design marketing*) i promocija u sklopu vizuelnih celina SSM (*Site structure menagment*). Sistem upravljanja sadržajem sajta je CMS (*content menagment system*).
- xxvi Protokol SSL ver. 3.0 predložen je za standard na Internetu. Za plaćanje pomoću platnih kartica predložen je protokol SET (*Secure Electronic Transaction*). Činjenica da ga forsiraju Visa i MasterCard daje za osnovu da se pretpostavi da postoji mogućnost njegovog usvajanja za standard.
- xxvii Marković M., Infrastruktura sistema sa tajnim i javnim ključevima, Naučno tehnički pregled, 1/1999.god.
- xxviii Prema podacima ispitivanja u 431 državnoj i privrednoj organizaciji u SAD (Secure Enterprise Survey, juni 2003.god.) čak 6% organizacija ima obe funkcije.
- xxix Ирина Муравьева, Новый взгляд на службу информационной безопасности компании, infosecutity.ru
- xxx Prema Gartner Reseach 40% najtraženi sertifikati su: CISSP (40% kompanija), SANS (15 % kompanija) i ostali sertifikati (MCSE, CISA, ABCP ...) – 25 % kompanija.
- xxxi Za sada je teško pronaći adekvatan prevod naziva ovako zamišljenog radnog mesta.
- xxxii Prema podacima iz literature u SAD već ima 170 specijalnosti. Poređenja radi u RF ih, za sada, ima 60.
- xxxiii Ирина Муравьева, Новый взгляд на службу информационной безопасности компании, infosecutity.ru
- xxxiv Posmatrane su sledeće vrste sertifikata: sertifikovani specijalista bezbednosti IS (CISSP), univerzitetska diploma specijalnosti IB i sertifikati proizvođača sredstava za zaštitu.

-
- ^{xxxv} Prema podacima sa sajta www.Kiev.security (Экранирование электромагнетных волн) samo za EM ekraniranje (oklapanje) u SAD se troši 1% ukupne industrijske proizvodnje, a ukupni troškovi za zaštitu poverljivih informacija firmi su od 10 do 15 milijardi USD godišnje.
- ^{xxxvi} Istraživanje je publikovano u Obzoru RosBiznesKonsalting 2002. god.
- ^{xxxvii} Cnaws.ru, 17.10.2003.god.
- ^{xxxviii} Anketa sa 815 IT specijalista.
- ^{xxxix} Engl. – *firewall*, ruski – межсетевые экраны
- ^{xl} «Ekvivalent žične poverljivosti» WEP (*wired equivalent privacy*) je daleko od proklamovane poverljivosti.