

UNIVERZITET SINGIDUNUM
DEPARTMAN POSLEDIPLOMSKIH STUDIJA
STUDIJSKI PROGRAM
POSLOVNI SISTEMI U TURIZMU I HOTELIJERSTVU

MASTER RAD
UTICAJ INFORMACIONIH SISTEMA NA BEZBEDNOST
TURISTA U HOTELIMA

Mentor: prof. dr Radmila Živković

Student: Sanja Jevtić 405258/2012

Beograd, 2014.

Sadržaj

Uvod.....	4
1. Analiza turističkih kretanja.....	9
2. Koncept i uloga bezbednosti u turizmu.....	14
2.1. Sigurnost i bezbednost u doba globalnog turizma.....	14
2.2. Bezbednost kao strategija diferenciranja u turizmu.....	18
3. Vrste putničkih rizika i kriza.....	21
3.1. Prirodne katastrofe.....	24
3.2. Zdravstvene krize.....	28
3.3. Terorizam.....	36
3.4. Kriminal.....	37
4. Percepcija turista o bezbednosnim potrebama.....	41
5. Istraživanje o sigurnosti i bezbednosti na putovanju.....	45
5.1. Istraživanje Udruženja za korporativna putovanja.....	45
5.2. Istraživanje ACTA Elsevier science	45
6. Bezbednost turista u hotelima.....	47
6.1. Sigurnost u hotelskim sobama.....	49
6.1.1. Sigurnost u hotelskim bazenima.....	51
6.1.2. Prevencija krađe.....	51

6.2. Bezbednost od požara.....	51
6.3. Sanitarni i zdravstveni zahtevi.....	54
7. Bezbednost informacionih sistema u hotelima.....	55
7.1. Značaj informacionih sistema u hotelima.....	59
7.2. Propisi i standardi sigurnosti i zaštite gostiju.....	60
7.3. Savremeni sistemi tehničke zaštite u hotelima.....	60
8. Osnovni pojmovi upravljanja rizicima.....	62
8.1. Procena rizika.....	64
8.2. ISO standardi.....	75
8.3. Inventar informacione imovine hotelskih sistema.....	79
9. Studija slučaja: smanjenje rizika hotelskog poslovanja na prihvatljiv nivo na primeru hotela Park.....	83
10. Primeri iz prakse- Sigurnost i bezbednost turista u hotelima u svetu.....	89
10.1. Sigurnost turista u „Hilton worldwide” hotelima.....	89
10.2. Sigurnost turista u „Marriott” hotelima.....	90
10.3. Sigurnost turista u „Hyatt Hotels & Resort” hotelima.....	91
10.4. Sigurnost turista u „Sheraton” hotelima.....	93
Zaključak.....	94
Literatura.....	96

Uvod

Svet u kome živimo je doživeo dramatične promene kroz vekove. Ovo je posebno tačno kada govorimo o bezbednosti i sigurnosti. Uz povećanu učestalost prirodnih kriza i kriza koje je čovek izazvao tokom proteklih decenija, naša sigurnost je ugrožena, odnosno naša bezbednost je na nižem nivou nego pre.

Ljudi koji su željni putovanja, upoznavanja drugih kultura i odmora, prvo proveravaju koliko je sigurno otići na određenu destinaciju. Pitanja koja turisti sebi postavljaju su da li, kada, gde, kako i zašto treba otputovati na neko mesto, ako ta destinacija nije dovoljno bezbedna.

Negativni uticaji i posledice terorističkih napada, lokalnih ratova, prirodnih katastrofa, epidemija i pandemija su učinili turizam ranjivim kako na lokalnom, tako i na globalnom nivou. Zbog toga je potrebno da se ovaj segment turizma istražuje i proučava. Pitanja koja se sama nameću su: Zašto su sigurnost i bezbednost postali toliko važni za turizam? Kako problemi na destinaciji utiču na turiste i kako se opredeljuju za određeno putovanje? Šta je zadatak i odgovornost učesnika u turizmu? Koji su ključni elementi koji dovode do problema turističke destinacije?

Odgovorima na ova pitanja ne samo da može da se zadovolji istraživačka radoznalost, već i da se postave neke smernice za upravljanje, svim učesnicima turizma ili bar da se smanje rizici. Bezbednost i bezbednosna pitanja su uvek bila veoma važan deo turizma. Poznato je da su drevne Olimpijske igre bile toliko važne da su svi ratovi odloženi, u periodu trajanja igara.

Pitanje bezbednosti u turizmu je došlo do izražaja sa razvojem masovnog turizma od 1950. godine. Međutim, ono što je nekad bilo vezano za bezbednost i sigurnost u turizmu, danas je drugačije zbog razvoja tehnologije, povećanih turističkih kretanja, pojave novih oblika narušavanja ljudske slobode i mnogo drugih stvari što je donelo novo doba.

U novom dobu informacija je postala ključna, kada govorimo o uspehu. Informacija može biti u pisanom obliku, elektronski skladištena, prikazana na filmu ili izrečena tokom razgovora. I bez obzira u kom se obliku ona pojavila mora biti zaštićena. Sa pozicije bezbednosti informacije uočavamo 3 dimenzije: bezbednost podataka, bezbednost kanala, distribucije podataka (kuda, kako i na koji način putuju podaci) i bezbednost upotrebe tj. korišćenja informacije (identifikacija prijema, pristupi za korišćenje i ovlašćenja za korišćenje). Svaka kompanija koja želi da zaštiti svoj kapital postavlja pitanje kako se najefikasnije može zaštititi. Tipična pojedinačna rešenja ne mogu biti efikasna, jer svaka organizacija ima svoje segmente, svaki od

tih segmenata komunicira sa okruženjem (klijenti, šira zajednica, konkurencija, zakonodavstvo) kao i međusobno. Svaka od tih interakcija sadrži mnoštvo informacija i podataka, poverljivih i onih sa manjim stepenom poverljivosti, čime izazovi za njihovo diferenciranje i očuvanje nivoa bezbednosti postaju jako veliki i kompleksni. Jasno je da sve izazove i rizike ne možemo potpuno anulirati, ali ih možemo predviđati, planirati naše akcije i preventivno delovati, tj. moramo stvoriti sistem zaštite koji će upravljati njima, kroz aktivan odgovor na pretnje a ne samo preduzimanjem defanzivnih strategija. Informacioni sistem mora da bude fleksibilan, da može brzo da se prilagodi promenama vezanim za promenu delatnosti ili cilja poslovne politike, da se može uvesti za relativno kratko vreme, da se iz baze podataka može dobiti bilo koja željena informacija koja ima smisla za sve nivoe odlučivanja i da omogućava racionalno poslovanje koje je u funkciji dobiti.

Metodologija istraživanja

Predmet istraživanja

Predmet istraživanja ovog naučnog-istraživačkog rada je zasnovan na bezbednosti i sigurnosti u turizmu. Sigurnost i bezbednost su uvek bili neophodni uslov za putovanje i turizam. Poslednje dve decenije ova dva faktora su stekla mnogo veći značaj zbog terorističkih napada, lokalnih ratova, prirodnih katastrofa, epidemije i pandemije. Zbog ovih negativnih uticaja turizam i putovanje ne mogu, a da ne budu ranjivi. Zbog toga ova oblast zahteva istraživanje i proučavanje odnosa bezbednosti i turizma i stvaranja novog pojma „Bezbednost u turizmu“. Sigurnost i bezbednost su postali multidimenzionalni pojam sa širokim spektrom komponenti koje obuhvataju: političku bezbednost, javnu bezbednost, zdravlje, lična bezbednost podataka, pravna zaštita turista, sigurnost u komunikaciji, zaštita od katastrofa, ekološka bezbednost, osiguranje kvaliteta. Bezbednost je prošla kroz značajne promene: od više ili manje pasivnog faktora postala je aktivan element turizma, koji deluje u cilju zaštite turista.

Ciljevi i zadaci istraživanja

Naučni i društveni cilj ovog rada je naučna deskripcija elemenata, analiza i razumevanje bezbednosti u turizmu . Cilj rada se ogleda u utvrđivanju međuzavisnosti i povezanosti turizma sa rizicima koji utiču na dimenziju i smer turističkih kretanja, kao što su nepovoljno stanje okruženja, nepovoljna politička i sigurnosna situacija, ekološke katastrofe, epidemije, upravljanje rizicima i bezbednost informacione imovine.

Društveni cilj se ogleda u pružanju adekvatnih informacija i pojašnjenja pojedincima, grupama i organizacijama o aktuelnim dešavanjima vezanim za bezbednost u turizmu.

Hipoteza istraživanja:

Hipotetički okvir istraživanja sastoji se iz sledećih stavki:

Generalna hipoteza: Negativne promene u okruženju, neminovno dovode do promena u turističkim kretanjima na način da se smanjuje obim turističkih putovanja ili dolazi do njihovog preusmeravanja van uobičajenih tokova. Pored toga, bezbednost turista koji dođu na receptivno područje moraju biti zaštićeni, kao i njihove informacije u hotelima u kojima borave.

Generalna hipoteza se dalje operacionalizuje na posebne hipoteze:

- Sigurni turizam doprinosi dostizanju društvenih i kulturnih ciljeva turizma, učvršćivanju međunarodnog poverenja u domenu ove delatnosti, gde sigurnost turizma treba biti uključena u planiranje i promociju samog turizma.
- Turista bi trebao da poseduje sve informacije vezane za putovanje kako bi se rizici sveli na minimum.
- Svaka destinacija bi trebalo da ima odgovarajuću strategiju od moguće krizne situacije (terorizma, krađe, klimatskih promena), kao i bezbednosne standarde koji će se sprovoditi u pogledu: sigurnosti hrane, prevencije požara, prevencija ilegalnih radnji.
- U savremenom „društvu rizika“ turisti su na svojim putovanjima sve više zabrinuti za vlastitu bezbednost. Ulaganje u bezbednost se više ne posmatra kao trošak već kao investicija. Zagarantovana sigurnost brojčano povećava posete određenoj turističkoj destinaciji.
- U hotelima u kojima turisti borave mora postojati dobar rezervacioni sistem koji će zaštititi sve lične podatke turista od mogućeg hakovanja, virusa, socijalnog inženjeringa.
- Za hotele je bitno da znaju kako da upravljaju rizikom. Upravljanje rizikom je važan proces koji omogućava upravi organizacije da se uravnoteže operativni i ekonomski troškovi zaštitnih mera za očuvanje sigurnosti informacionog sistema organizacije. Upravljanje rizikom podrazumeva identifikaciju rizika, procenu rizika i preduzimanja koraka da se rizik smanji na prihvatljivi nivo.

Metode istraživanja

Uzimajući u obzir specifičnost i složenost proučavanog predmeta istraživanja, u radu su korišćene osnovne metode kako bi bili zadovoljeni osnovni metodološki zahtevi: objektivnost, pouzdanost, opštost i sistematičnost.

Prema metodološkoj i široj naučnoj lektiri pod opštenaučnim metodama se smatraju one metode koje se, kao celine, koriste ili mogu koristiti za sticanje naučnog saznanja u svim naukama i svim naučnim disciplinama. To su:

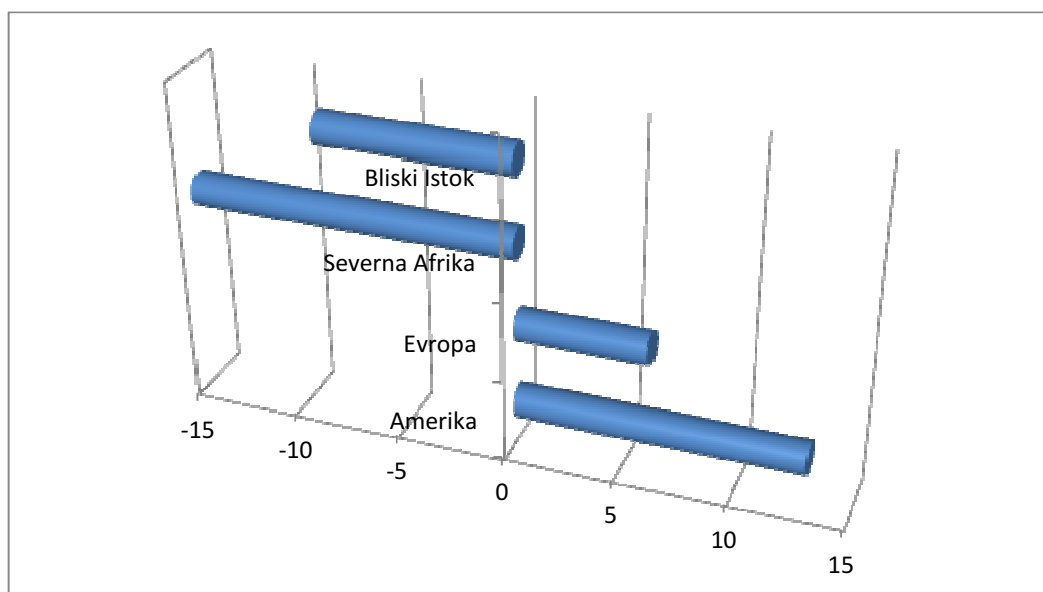
- Hipotetičko–deduktivna metoda,
- Statistička metoda,
- Metoda modelovanja,
- Aksiomska metoda,
- Analitičko–deduktivna i
- Komparativna metoda.

Od opštenaučnih metoda u radu su korišćene hipotetičko-deduktivna, statistička i komparativna metoda. Od metoda prikupljanja podataka korišćen je metod analize sadržaja dokumenata.

1. Analiza turističkih kretanja

Prema Svetskoj turističkoj organizaciji u prvoj polovini 2011. godine zabeležen je porast u međunarodnom turizmu. Rezultati potvrđuju da je uprkos, višestrukim izazovima, međunarodni turizam nastavio rast započet u 2010. godini. Dolasci turista u prvoj polovini 2011.godine su bili 4,5% veći nego 2010. godine. Između januara i juna ove godine, ukupan broj dolazaka turista dostigao je 440 miliona, što je 19 miliona više nego u istom periodu 2010. godine. Svi svetski (pod) regioni pokazali su pozitivne trendove, sa izuzetkom Bliskog Istoka i Severne Afrike. Rezultati su bili bolje nego što se očekivalo: u Evropi (+6%), pojačani oporavak severne Evrope (+7%) i centralne i istočne Evrope (+9%). Zbog dešavanja u Severnoj Africi zabeležen je pad (-15%) i na Bliskom Istoku (-9%). Amerika je bila iznad proseka sa izuzetno jakim rezultatima za Južnu Ameriku (+13%).¹

Diagram br.1: Tabela rasta turističkog prometa ostvarenog u 2011.godini²



U 2011. godini prihodi od međunarodnog turizma, uključujući i međunarodni putnički saobraćaj (izvoz od turizma) iznosili su 1.2 biliona dolara, ili blizu 6% izvoza u svetu robe i usluga.

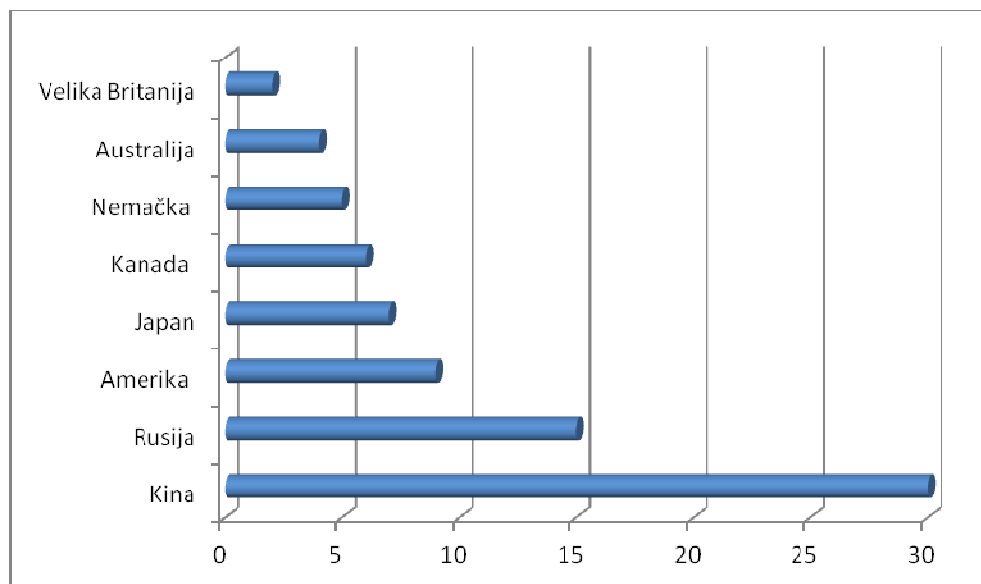
U 2012.godini dolazak turista je za 4% porastao u periodu između januara i avgusta u odnosu na isti period 2011. godine. U 2012. godini je bilo 705 miliona turista do avgusta. Rast je usporio u

¹ www.unwto.org UNWTO World Tourism Barometar November 2011.

² www.unwto.org , UNWTO World Tourism Barometar, Interim Update , April 2010.

junu i u julu, u odnosu na prvih pet meseci ove godine (prosek od 5%), ali u avgustu 4% što je pozitivan rezultat za mesec koji se smatra za period najvećeg obima, međunarodnog turizma u godini. Po regionima rast je bio jači u Aziji, na Pacifiku i Africi, zatim Americi i Evropi. Bliski Istok je pokazivao znake oporavka, sa posebno obećavajućim rezultatima u Egiptu. Među prvih deset međunarodnih tržišta od potrošnje na putovanja u inostranstvo, rast je bio zabeležen u prvih šest meseci u Kini (+30%), Rusiji (+15%), Americi (+9%), Kanadi (+6%), Nemačkoj (+5%) i Australiji (+4%), kao i u Japanu gde 7% povećanja potvrđuje oporavak ovog tržišta. Velika Britanija je beležila skroman rast od 2% u turističkoj potrošnji, dok su Italija i Francuska pokazale pad u potrošnji na putovanje u inostranstvo.

Diagram br.2: Tabela rasta turističkog prometa ostvarenog u 2012. godini³



Druge velike razvijene ekonomije su pokazale značajan rast izdataka: Austrija (+16%), Belgija (+13%), Švajcarska (+11%) i Norveška (+11%). Među ekonomijama u razvoju, pored Kine i Rusije dvocifren rast je postavila Poljska (+22%), Malezija (+18%), Argentina (+16%), Filipini (+14%), Indija (+11%) i Indonezija (+10%).⁴ „Iako je ekonomska kriza bila izražena u 2012. godini, međunarodni turizam je uspeo da ostvari dobre prihode. Turizam je uspeo da se prilagodi promenljivim tržišnim uslovima i očekuje se da će se nastaviti širenje u 2013.godini po nešto

³ www.unwto.org UNWTO World Tourism Barometar November 2012.

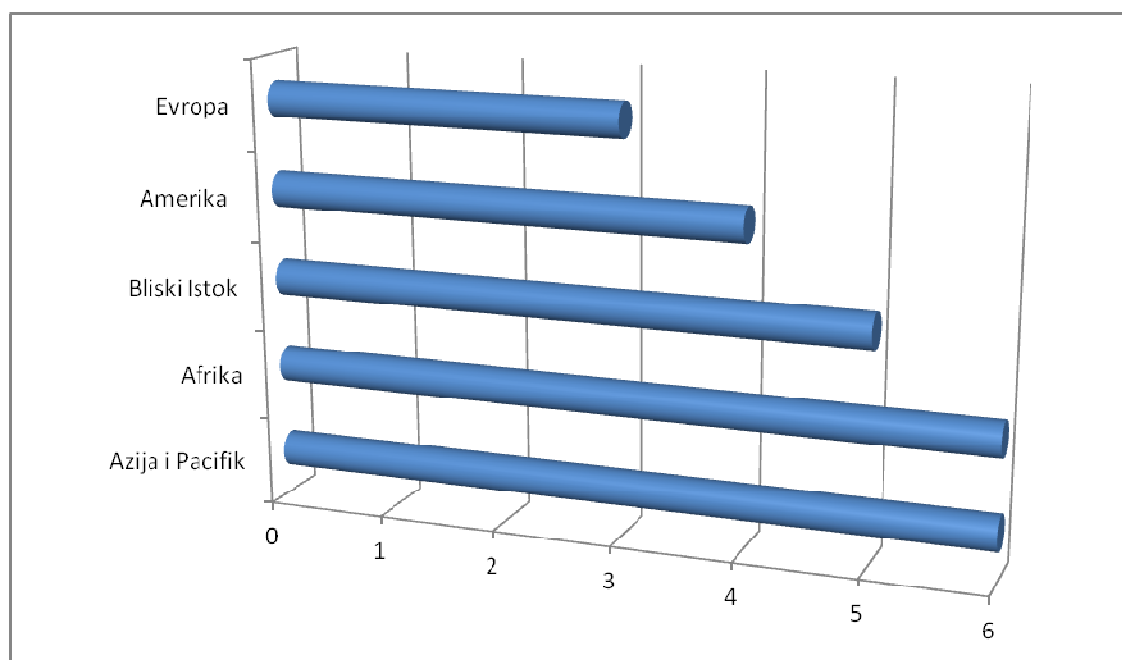
⁴ www.unwto.org, UNWTO World Tourism Barometar November 2012.

skromnijim stopama. Turizam je jedan od stubova koji treba da bude podržan od strane vlade širom sveta kao deo rešenja za stimulisanje ekonomskog rasta.“⁵

U prvih par meseci 2013. godine, međunarodni turizam je doživeo porast od (+5%), odnosno 845 milion turista u Evropi, Aziji i na Pacifiku, sto je 41 milion više nego u istom periodu 2012. godine. U Evropi je 2013. godine broj turističkih dolazaka porastao za (+6%), gde je zabeleženo (+7%) u Centralnoj i Istočnoj Evropi i Južnoj Evropi (+6%). U Aziji i na Pacifiku zabeležen je rast od (+6%) i u jugoistočnoj Aziji porast od (+12 %). U Severnoj Americi je zabeležen porast od (+4%) i u Centralnoj Americi (+3%). U Africi je zabeležen rast od (+5), što je podstaklo razvoju Severne Afrike (+4), dok je Bliski Istok imao samo marginalni rast (+0,3). U 2013. godini je zabeležen pozitivan trend turističkih dolazaka što je uticalo na povećanje turističkih prihoda širom sveta za prvih šest do devet meseci. Među prvih 25 međunarodnih turističkih primanja, najveće prihode su zabeležile: Sjedinjene Američke države (+11), Kina (+10), Velika Britanija (+18), Tajland (+28), Hong Kong (+21), Turska (+13), Indija (+13), Japan (+23), Grčka (+15). Rusija je zabeležila porast turističkih kretanja za 29% u prvih devet meseci 2013.godine. Kina je 2012. godine je imala prihod od 102 milijardi dolara, da bi 2013. godine zabeležila rast od 22%. Zemlje kao što su Kanada (+3), Velika Britanija (+2) i Francuska (+2) je zabeležile su slabiji rast turističkih kretanja.

⁵ Citirane reči Generalnog sekretara UNWTO Taleba Rifai

Diagram br.3: Tabela turističkih dolazaka u 2013. godini⁶



Predviđa se da će 2020. godine biti oko 1,6 milijarde, a 2050. godine oko 2 milijarde turista, koji će ostvariti oko 24 milijarde dolara prometa, pri čemu će Indija, Kina, Indokina i Brazil zasigurno biti najveće turističke destinacije.

⁶ www.unwto.org, UNWTO World Tourism Barometar November 2013.

Tabela 1: Broj turista (u milionima)

Regija	Bazna godina	Procena			Prosečni godišnji rast		
	1995.	2000.	2010.	2020.	1995-2000	2000-2010	2010-2020
Afrika	20	26	46	75	5,4	5,7	5,1
Amerika	110	131	195	284	3,6	4,0	3,8
Istočna Azija/Pacifik	81	105	231	438	5,2	8,2	6,8
Evropa	334	386	526	717	3,0	3,2	3,1
Srednji Istok	14	19	37	69	6,4	7,1	6,5
Južna Azija	4	6	11	19	5,6	6,8	5,8
Svet	563	673	1.046	1.602	3,6	4,5	4,4

Izvor: Avelini – Holjevac I., A vision of tourism and the hotel industry, Zbornik „Hotelska kuća 2000“, Fakultet za turizam i hotelijerski menadžment, Opatija, 2000. godine.

Najveći broj turista 1995. godine je bio zabeležen u Evropi sa 334 miliona turista, a najmanji broj turista je zabeležen u Južnoj Aziji 4 miliona turista. 2000. godine Evropa je imala najveći broj turista 386 miliona u odnosu na Afriku 26 miliona i Južnu Aziju 6 miliona turista. Evropa je i 2010. imala najveći broj turista 526 miliona. Predviđa se da će Evropa do 2020. i dalje imati visok rast i brojaće 717 miliona turista. Na drugom mestu će biti Istočna Azija/Pacifik sa 438 miliona turista i na trećem Amerika sa 284 miliona turista.

2. KONCEPT I ULOGA BEZBEDNOSTI U TURIZMU

Sigurnost i bezbednost su uvek bili neophodni uslov za putovanje i turizam. Poslednje dve decenije ova dva faktora su stekla mnogo veći značaj zbog terorističkih napada, lokalnih ratova, prirodnih katastrofa, epidemije i pandemije. Zbog ovih negativnih uticaja turizam i putovanje ne mogu, a da ne budu ranjivi. Zbog toga ova oblast zahteva istraživanje i proučavanje odnosa bezbednosti i turizma i stvaranja novog pojma „Bezbednost u turizmu“.

2.1. Sigurnost i bezbednost u doba globalnog turizma

Sigurnost i bezbednost su postali multidimenzionalni pojam sa širokim spektrom komponenti koje obuhvataju: političku bezbednost, javnu bezbednost, zdravlje, lična bezbednost podataka, pravna zaštita turista, sigurnost u komunikaciji, zaštita od katastrofa, ekološka bezbednost, osiguranje kvaliteta. Bezbednost je prošla kroz značajne promene: od više ili manje pasivnog faktora postala je aktivan element turizma, koji deluje u cilju zaštite turista. Bez obzira na rezultate u proučavanju problema bezbednosti u turizmu, postoji nekoliko izazova za turizam vezana za istraživanja:

- Posledice nedeljivosti bezbednosnih problema u globalnom svetu
- Bezbednosni problemi koje je stvorio Internet
- Bezbednost u turizmu u odnosu na ljudske slobode i prava⁷

Poslednjih par godina teoretski odnos između turizma i bezbednosti se bazirao na tri glavne stavke ili grupe i njihovim varijablama:

- Grupa A koja podrazumeva koncepte koji se odnose na prirodu turizma- bezbednosni incidenti i krize (uključujući vrste, uzroke, način rada, motive, ciljeve itd.),
- Grupa B koja podrazumeva koncepte vezane za uticaje bezbednosnih incidenata i kriza na turizam, turiste i receptivno područje
- Grupa C koja podrazumeva koncepte koji se odnose na kratkoročne, srednjeročne i dugoročne reakcije.

⁷ Harper, D. (2001). *Comparing tourists' crime victimization. Annals of Tourism Research*, 28(4), 1053–1056.

Prvi i možda osnovni koncept, u okviru prve grupe, koji treba spomenuti je vrsta incidenta koja utiče na turizam. Mogu se identifikovati četiri vrste incidenta koji bi mogli negativno da utiču na lokalnu zajednicu, turizam i na same turiste. To su: kriminal, terorizam, rat i nepovoljna politička situacija.⁸

Postoji šest podgrupa, u okviru B grupe, koje prikazuju različite bezbednosne situacije u turizmu. Svaka od tih podgrupa uključuje varijable koje mere uticaje na destinaciji. To su sledeće podgrupe:⁹

- **Uticaj incidenata**

Dokazi širom sveta pokazuju da je uticaj incidenata na turizam, lokalnu zajednicu i turiste višestruk.

- **Uticaj na samoj destinaciji**

Jedna od prvih stvari koje treba preduzeti je procena štete. Ona je potrebna kako bi se formulisali rezervni planovi i politike za rukovanje i da bi se ublažila šteta koja je načinjena domaćoj industriji.

- **Uticaj na ponašanje turista**

Promene koje se dese na turističkoj destinaciji, a vezani su za bezbednost mogu da utiču na odluku turista da ne otputuje. Turista može da otkáže rezervaciju i da se odluči za neku bezbedniju destinaciju.

- **Uticaj na turizam**

U slučaju organizovanih putovanja, ponašanje turista će zavisići od turoperatora koji je organizovao putovanje i turoperatora koji se nalazi na destinaciji. Usled promene bezbednosne zone može doći do štete, koja se može sprečiti ili preduzeti mera da se ublaži ista.

- **Uticaj na vlasti zemlje u koju se putuje**

Turizam služi kao važan faktor koji doprinosi razvoju lokalne, regionalne i nacionalne ekonomiji. Incidenti koje se jave na destinaciji mogu imati veliki negativan uticaj na obim ekonomije, što može biti velika briga vlade. Takva briga može da menja politiku vlade kad je u pitanju turizam; njenu ulogu i nivo uključenosti u turizam. Al takođe, vlada može da pokrene i

⁸Abraham Pizam and Yoel Mansfeld, *The management of hospitality and tourism enterprises series ,Tourism, Security and Safety, from theory to practice, Toward a Theory of Tourism Security, Elsevier, 2006. p.3.*

⁹Abraham Pizam and Yoel Mansfeld, *The management of hospitality and tourism enterprises series ,Tourism, Security and Safety, from theory to practice, Toward a Theory of Tourism Security, Elsevier, 2006. p.3-4.*

poboljša bezbednosne mere koje će sprečiti pojavu novih incidenata, koji se dešavaju na turističkoj destinaciji.

- **Uticaj na proizvodna tržišta**

Ponašanje potencijalnih turista će zavisi i od toga na koji način je zemlja iz koje dolaze dala informacije o nekoj destinaciji. Mnogi turisti cene tačnost informacija. Bitno je da se informacije o pogođenoj destinaciji, odnosno o destinaciji na kojoj je došlo do incidenta, na pravilan način iznesu turistima, da budu objektivne.

- **Uticaj medija**

Incidenti koji se dese na destinaciji se prenose putem medija. Turisti na taj način mogu biti preopterećeni informacijama o incidentima i imati, što je u većini slučajeva, preuveličanu sliku događaja.

Grupa C obuhvata očekivane i stvarne napore od strane raznih učesnika u turizmu koji odgovaraju na razne incidente na destinaciji. Za mnoge destinacije širom sveta pitanje bezbednosti i sigurnosti turista nije prošlost već ciklus krize i oporavka. U vreme krize, turizam ima veliku ulogu kada je u pitanju ekonomsko i socijalno preživljavanje.¹⁰

✚ Prema Asocijaciji helenističkih turističkih preduzeća, broj dolazaka na aerodrome u Grčkoj je pao za 3,3 posto u 2012. godini, a turistički prihodi su se povećali za 400.000 evra. Glavni prioritet za 2013. godinu grčke vlade je stvaranje što povoljnijih uslova za privlačenje stranih turista u Grčku. Ekonomska i politička previranja u Grčkoj bitnije utiču na smanjenje dolazaka standardnih turista iz EU, posebno Nemačke, Italije, Velike Britanije. Istovremeno, raste broj turista sa Balkana i iz Ruske federacije. Za uspešniju turističku sezonu potrebno je da je politička situacija održiva, da se redukuju socijalni i politički protesti i povede računa o bezbednosti stranih ali i domaćih turista.¹¹

Kada se situacija na turističkim destinacijama pogoršava, rezultat ne mora uvek da dovode do dugoročnog štetnog uticaja na lokalni turizam. Međutim, ako je ta situacija praćena jakom medijskom pažnjom, informacije koje se prenose stvaraju jak negativan imidž. Ako bi turista tu sliku, koja je prenešena putem medija, shvatio kao neprihvatljiv nivo rizika, sigurno bi došlo do

¹⁰ Abraham Pizam and Yoel Mansfeld, *The management of hospitality and tourism enterprises series ,Tourism, Security and Safety, from theory to practice, Toward a Theory of Tourism Security, Elsevier, 2006.p. 12.*

¹¹ www.balkanmagazin.net

otkazivanja rezervacije i odluke putovanja u neko sigurnije mesto. Zato je bitno da vlada uspostavi ravnotežu negativne slike, koja se prenosi, i preciznijih, manje pristrasnih poruka. Da bi se takve poruke poslale, mora se otkriti i analizirati koliki su uticaj ostavili mediji na turiste. Bitno je da učesnici u turizmu, pored medija, znaju kako da odgovore na incidente koji su se javili. Da bi moglo da odgovore, moraju da krenu od pitanja: kako je došlo do incidenta i kada se incident dogodio i izazvao turistički krizu. U tom trenutku se prave planovi kako da se izađe iz nje i kako da se upravlja krizom. Bolje destinacije imaju bolje pripremljene planove, ali iako nisu destinacije jake, bitno je da budu efikasne u rešavanju problema, da se spreči i smanji dalje širenje krize i da subjekti u pogođenim zemljama imaju saradnju kako bi izašli iz krize što pre. Kada destinacije shvate zašto je došlo do krize moraju ići ka oporavku. Da bi se oporavili od krize, potrebno je povratiti poverenje turista kroz razne akcije, medije za šta su potrebna velika finansijska sredstva i jaka propaganda.¹²

¹² Abraham Pizam and Yoel Mansfeld, *The management of hospitality and tourism enterprises series ,Tourism, Security and Safety, from theory to practice, Toward a Theory of Tourism Security, Elsevier, 2006.p.14.*

2.2. Bezbednost kao strategija diferenciranja u turizmu

Svaka turistička destinacija ima jedno ili više prioriternih tržišta i nekoliko sekundarnih tržišta na koja privlači najveći broj turista. Sposobnost da se privuku ovi tržišni segmenti zasnovana je na tržišnoj poziciji destinacije- predstavi o destinaciji koja postoji u svesti potrošača u odnosu na konkurenciju. Postojeće i željene pozicije turističke destinacije su važna i složena pitanja u procesu strateškog upravljanja destinacijom i njenim položajem na tržištu. Pozicija turističke destinacije je opšte definisana kao predstava koju u svojoj svesti imaju potrošači o destinaciji i njenom mestu u odnosu na konkurenciju. Odnosno, pozicija destinacije na tržištu je način na koji destinaciju vide potencijalni i sadašnji posetioци u smislu iskustava (i potencijalnih koristi) koje ona pruža u odnosu na konkurentske destinacije. Pojam pozicioniranja su uveli J. Trout i A. Reis. Po njima pozicija proizvoda/usluga određena je skupom tehnoloških i psiholoških vrednosti koje su ugrađene u proizvod/uslugu. Drugim rečima destinacija mora pored stvaranja dobrog proizvoda učiniti i mnogo više- ona mora da pažljivo pozicionira proizvod u svest potrošača. Pozicioniranje turističke destinacije je sistemski proces analiziranja i donošenja odluka koji vode menadžeri ka pronalaženju najpogodnijeg i najprofitabilnijeg položaja destinacije u svesti potrošača u odnosu na konkurenciju. Ovaj proces je zasnovan na postizanju kompatibilnosti između karakteristika destinacije i tražnje sa jednog ili više tržišnih segmenata i odgovarajuće ciljne promocije takve pozicije tj. imidža.¹³ Upravljanje destinacijom mora podrazumevati i analitičke metode i procese koji su neophodni menadžerima destinacija da bi razumeli i efikasno pratili i prilagođavali svoju trenutnu tržišnu poziciju. Efikasno pozicioniranje je zasnovano na upravljačkom znanju i na većim sposobnostima nego što ih imaju upravljači u konkurentskim destinacijama. U procesu pozicioniranja naglašena je potreba za efikasnim kombinovanjem ključnih strateških sposobnosti (anticipiranje budućih kretanja, stvaranje različitih opcija i njihova uspešna implementacija) sa mogućnostima koje pruža okruženje. Suština ovog procesa jeste ponuda potrošačima najbolje proizvode po razumnoj ceni, čime se smanjuje verovatnoća da će potrošači otići kod konkurencije.

¹³ Čerović S., *Menadžment u turizmu*, PMF- department za geografiju, turizam i hotelijerstvo , Novi Sad 2003. godine , str. 8-9

Postoje tri pristupa za uspostavljanje prednosti u odnosu na konkurenciju:¹⁴

- Cenovno vođstvo: kontrolom i sniženjem cena uz povećanju efikasnosti kvaliteta
- Fokusiranje: postati specijalista na specifičnom području aktivnosti
- Diferenciranje: pružiti proizvode, usluge i iskustva različita od konkurencije

Ključ diferencijacije destinacije je u jedinstvenoj prodajnoj ponudi i promociji sopstvenih jedinstvenih predloga i vrednih karakteristika u glavama potencijalnih ili postojećih turista. Ono što turiste vezuje za neku destinaciju je pored dobre slike koja im je stvorena u glavi za neku destinaciju, jedinstveni emocionalni predlozi odnosno mogućnost uživeti se u emocije drugog, sa destinacijom i njenim vrednostima.

Jedinstveni emocionalni predlozi su:

- Nešto što konkurenti nisu u stanju da ponude
- Nešto što prevazilazi očekivanja turista
- Osnova kompetitivne strategije i svih komunikacija¹⁵

Da bi se izgradio brend na bilo kojoj destinaciji potrebno je da postoji osnov, odnosno sigurnost i bezbednost na nekoj destinaciji. Sektor putovanja i turizma mora da ima ovu osnovu i da se od nje krene kako bi destinacija bila uspešna. Ukoliko toga nema turisti mogu da se pitaju da li, gde, kada i kako da putuju, a i da se to loše odrazi na ekonomiju i ostale sektore jedne destinacije.

Evo nekih primera koji su loše uticali na destinaciju:

- **PRIRODNE NEPOGODE:** razorni cunami u Aziji 2004. godine, uragan Katrina u Nju Orleansu i Vilma u Meksiku 2005. godine i zemljotres na Haitiju 2010. godine, su dokaz kolika je sila prirode i da nas može u bilo koje vreme, na bilom kom mestu i bez ikakvog upozorenja iznenaditi. Prirodne nepogode mogu izazvati velike štete i ozbiljna oštećenja u turizmu, na socijalnu i ekonomsku infrastrukturu ali i velika oštećenja na psihi lokalnog stanovništva i turiste.
- **ZDRAVSTVENE KRIZE:** one mogu često biti nevidljive ali napraviti veliku štetu, posebno kad je u pitanju, u početku, neizlečivo oboljenje koje posle preraste u epidemiju ili pandemiju i prenese se na ceo svet putem saobraćaja, odnosno putnika koji su zaraženi.

¹⁴ Čerović S., *Menadžment u turizmu*, PMF- department za geografiju, turizam i hotelijerstvo , Novi Sad 2003. godine, str. 8-9

¹⁵ www.dgt.pmf.uns.ac.rs

- **TERORIZAM:** Nakon 11. septembra smo postali svesni kolika opasnost preti u svakom trenutku i da se nikada ne može sve predvideti i biti potpuno siguran. Globalna vazduhoplovna industrija je nakon ovog datuma uvela rigoroznije mere i ograničenja kako bi bezbednost bila na visokom nivou od trenutka ulaska u avion do izlaska.
- **KRIMINAL:** Na individualnom i kolektivnom nivou, na destinaciji, turisti su izloženi većem kriminalu nego pre. Bilo da je prevara putem kreditnih kartica ili lični napadi, turisti su izloženi riziku. Nažalost, smanjuje se udobnost i nivo poverenja, a sumnja se povećava. Ovo baca tešku senku na globalno putovanje i turističku industriju uopšte.

Terorizam i klimatske promene su glavni faktori koji utiču na otkazivanje turističkog putovanja. Klimatske promene doprinose stvaranju novih epidemija i prema jednom istraživanju većina bolesti su poreklom iz tropskih krajeva: 30% turista je prema istraživanju zatražilo medicinsku pomoć za prehlade, mučnine i bolove u stomaku, dok je 60% turista, iz tropskih krajeva, zatražilo pomoć zbog problema sa respiratornim organima, organa za varenje, problema sa kožom i očima. Međutim, iako nedavna istraživanja pokazuju da zarazna bolest predstavlja glavni uzrok smrti turista, 2,4% njih je zbog nebrige i neznanja dovelo sebe do realne situacije i rizika. Primer tome je bolest SARS koja je imala veliki uticaj na ponašanje turista. Odnosno, brzo širenje ove bolesti i nedostatak znanja o njoj dovelo je do naglog pada turista u 2003. godini. Tada se smatralo da sami turisti prenose ovu bolest putem saobraćaja, pogotovo avio saobraćaja, kada su se u velikom broju otkazivani letovi.¹⁶

¹⁶ www.elsevier.com/locate/tourman

3. Vrste putničkih rizika i kriza

Analizirajući uslove u kojima se turizam danas odvija, UNWTO naglašava da je ovo vreme neizvesnosti i da je neophodno pripremiti se za neočekivane događaje. Odgovor na krizu zahteva solidarnost, fleksibilnost i stručnost. U okviru organizacije formiran je tim stručnjaka za delovanje u kriznim situacijama (Crisis Action Team). Tim se sastoji od 11 vrhunskih svetskih stručnjaka iz područja komunikacija, marketinga, promocije, sigurnosti i zaštite i raspoloživ je zemljama članica koje zadesi kriza. Imenovani tim je izradio vodič koji bi turističkim preduzećima i destinacijama pomogao da brže i efikasnije prebrode krizne situacije i vrate poverenje turista. Ključna stvar u kriznom menadžmentu je pripremljenost unapred. Nekoliko važnih odluka koje treba da se urade pre nego što dođe do krize su: trening kriznog menadžmenta, isplanirana prevencija i trenutni odgovor. Da bi krizni menadžment bio efektivan, mora de se poslužiti proaktivno, sa ciljem da se odbrane i zaštite interesi kompanije/destinacije. U suštini, krizni menadžment je deo strategije planiranja, traženog od organizacije.

Svaka država mora posmatrati delokrug i stepen pretnje životu i zdravlju, vlasništvu i ekonomskim interesima turista i u skladu sa navedenim razviti nacionalnu strategiju o sigurnosti turizma, uključujući i prevenciju rizika. Još jedan pristup podele rizika (koji se koristi u praksi), obuhvata direktne i indirektne opasnosti, sa kratkoročnim, srednjoročnim i dugoročnim posledicama na pojedince, zajednice, regione i zemlju (tabela 2). Značaj ovog pristupa ogleda se u tome da se više pažnje obraća na indirektne šokove, čiji uticaj nije očigledan na turizam. Primeri indirektnih šokova uključuju: nestabilnost valute, zaokret u ekonomiji, bolesti životinja.¹⁷

¹⁷ www.riskmanagement.qld.gov.au -Government in Queensland, Australia (Tourism Queensland), 2003. *International Strategy for Disaster Reduction*, 2002.

Tabela 2: Plan upravljanja krizom¹⁸

POTENCIJALNI TURISTIČKI ŠOKOVI	POTENCIJALNE OPASNOSTI PO TURIZAM	OPŠTI ODGOVORI	SPECIFIČNE TEME ODGOVORA
DIREKTNI: -propusti, -kolapsi industrija povezanih sa turizmom (npr. avio kompanije), -prirodne katastrofe, -povrede i smrt turista.	KRATKOROČNE: -remećenje, -prekid odmora, remećenje budućih planova, -finansijske neugodnosti za turoperatore i posetioce, -negativan publicitet, -smanjenje broja posetilaca, -smanjenje prihoda turoperatora, -višak osoblja.	PRE-ŠOKOVI (prevencija / pripremljenost): -pripreme za pomoć vlade, -portfolio diverzifikacija tržišta, -protok informacija, -promovisati turoperatorima pripremljene koristi, -istraživati uticaj potencijalnih šokova.	KOMUNIKACIJA: -koristiti plansku komunikaciju, -kreirati mrežu pristupačnih Web sajtova, -obaveznu SOS liniju, -uspostaviti komunikaciju sa hitnim službama. ISTRAŽIVANJE: -regionalnih turističkih aktivnosti, -marketing

¹⁸ www.riskmanagement.qld.gov.au -Government in Queensland, Australia (Tourism Queensland), 2003.

INDIREKTNI: -terorističke akcije(npr. 11.septembar), -ekonomska kriza, -nestabilnost valute, -bolesti životinja.	SREDNJOROČNE/ DUGOROČNE: -averzija prema putovanju uopšte ili prema određenoj destinaciji, -dugoročno smanjenje broja posetioca, -dugoročna nezaposlenost, -gubitak obučenosti osoblja (potreba za obukom), ,poslovni neuspeh (bankrotstvo).	POST-ŠOKOVI (odgovori/ oporavak): -koristiti TQ komunikacije, -imenovati ključne menadžmere za: procenu uticaja, definisanje odgovora, saradnja sa vladom, saradnja sa hitnim službama.	obaveštavanje. MARKETING (kratkororočni/ srednjoročni): -prikupiti tržišne informacije, -izložiti predlog odgovora industriji, -implementirati odgovarajuću strategiju. INDUSTRIJA razvoj/ asistencija (srednjoročno/ dugoročno): -praćenje (SOS), -stručna edukacija, -pozajmice.
---	---	--	---

WTO je prepisala preporučene mere za sigurnost u turizmu, čime je obavezala zemlje koje se bave turizmom da identifikuju potencijalne rizike u turističkoj delatnosti i da propišu odgovarajuće standardne mere; sastavni deo ove obaveze je i procena ugroženosti turističke delatnosti i aktivnosti. Davanje sigurnosnih i bezbednosnih turističkih informacija je veoma važno, pošto može da pomogne turistima da: razviju objektivan stav o turističkim rizicima baziranih na stavkama, da shvate sigurnost kao važan aspekt turističkog proizvoda koji kupuju. Takođe, turistički radnici treba da daju informacije putnicima: pre polaska na put, u vreme dolaska i tokom puta, na destinaciji.

3.1. Prirodne katastrofe

Ljudske aktivnosti i kretanja su sada toliko prodorna da utiču na Zemlju u globalnim razmerama na složen, interaktivan i ubrzan način. Kako je broj ljudi na planeti sve veći i sve je veća potreba za kretanjem i putovanjem to može da ugrozi životnu sredinu. Termin klimatske promene se vrlo često, danas, zamenjuju terminom globalno zagrevanje. Do globalnog zagrevanja dolazi usled emisije „gasova staklene bašte“. Sve je više naučnih dokaza o uzrocima i budućim pravcima klimatskih promena. Naučnici su sad u mogućnosti da povežu verovatnoću nastanka i temperaturne ishode i uticaje na prirodno okruženje, povezane sa različitim nivoima stabilizacije gasova staklene bašte u atmosferi. Gomilanje gasova staklene bašte u atmosferi se povećava kao rezultat ljudske aktivnosti.¹⁹

- Prema međuvladinom panelu o promeni klime (the UN Intergovernmental Panel on Climate Change- IPCC, 2001) procenjeno je kako je moguće da ljudske aktivnosti značajno doprinose porastu temperature u prethodnih pola veka i procenjuje tu mogućnost u intervalu od 90 do 99 odsto.²⁰

Mnoge naučne studije ukazuju na činjenicu da bi klimatske promene mogle da ugroze ljudsku bezbednost, utičući na intezitet tropskih oluja, poplava, odronjavanja zemljišta i požara.

- U Francuskoj se 1999. godine desila elementarna nepogoda prilikom naleta oluja, koja je pogodila i Švajcarsku, Dansku i Nemačku.
- U 2005.godini Azijski kontinent je pretrpeo jednu od najvećih katastrofa- cunami u kojoj je nastradao i poginuo veliki broj ljudi
- XX vek ukazao je na dramatičan porast broja nesreća. U 2006. godini poplave su činile 55 odsto svih registrovanih nesreća.
- 2007. godine je Pakistansku obalu pogodio ciklon
- 2008. godine kinesku provinciju Sečuan je pogodio zemljotres u kome je poginulo 90.000 ljudi
- 2011. godine Japan je pogodio zemljotres koji je doveo do razornog cunamija kada je preko 20.000 ljudi izgubilo život²¹

¹⁹ www.emins.org

²⁰ Vladimir N. Cvetković- Rizik, moć, zaštita; Uvođenje u nauke bezbednosti, Službeni glasnik, Beograd 2010., str.687

²¹ www.pressonline.rs

Klimatske promene su pretnja osnovnim elementima života ljudi u svetu- pristupu vode, proizvodnji hrane, zdravlju i korišćenju zemljišta i okruženja. Klimatske promene utiču na ekonomske cene u jednoj zemlji, ali postoji niz metoda ili pristupa koji nam omogućavaju ocenu verovatne veličine rizika i njihovo poređenje sa troškovima. Sledeći pregled razmatra tri ovakva pristupa. Pregled se prvo detaljno bavi fizičkim uticajima na ekonomsku aktivnost, na ljudski život i na okruženje:

🚩 Po trenutnim trendovima, prosečna globalna temperatura će porasti za 2-3 stepena u toku naredni pedesetak godina. Zemlja će biti izložena zagrevanju od nekoliko stepeni više ako se emisije i dalje budu povećavale.

Zagrevanje će imati mnogobrojne ozbiljne uticaje, obično ispoljene kroz vodu:

- Topljenje glečera će najpre povećati rizik od poplava, a zatim u velikoj meri smanjiti zalihe vode i na kraju ugroziti jednu šestinu svetske populacije, prvenstveno na indijskom potkontinentu, u delovima Kine i na Andima u Južnoj Americi
- Opadanje prinosa žitarica, posebno u Africi može da ostavi milione bez mogućnosti da proizvedu ili kupe dovoljno hrane. Na srednjim i velikim geografskim širinama prinosi žitarica mogu da se povećavaju kod umerenog povećavanja temperature, ali sa većim stepenom zagrevanja oni će opadati.
- Na većim geografskim širinama smanjiće se smrtnost zbog hladnoće. Ali klimatske promene će širom sveta uticati na povećanje broja umrlih zbog loše ishrane i toplotnog stresa. Vektorske bolesti, kao što su malarija i tropska groznica mogu postati raširenije ako se ne preduzmu efektivne mere kontrole.
- Podizanje nivoa mora rezultiraće time što će svake godine na desetine do stotine miliona ljudi dodatno doživljavati poplave uz zagrevanje od 3-4 stepena. Postojeće ozbiljni rizici i povećani pritisci da se zaštiti obala Jugoistočne Azije (Bangladeš i Vijetnam), mala karipska i pacifička ostrva i veliki priobalni gradovi, kao što su Tokio, Njujork, Kairo i London. Prema jednoj proceni, sredinom ovog veka 200 miliona ljudi može postati stalno raseljeno zbog povećanja nivoa mora, većitih poplava i intenzivnijih suša.
- Ekosistemi će biti posebno osetljivi na klimatske promene, a oko 15-40% vrsta će se potencijalno suočavati sa izumiranjem nakon otopljenja od samo 2 stepena. Osim toga,

acidifikacija okeana, direktan rezultat povećanja nivoa ugljen-dioksida, imaće ogroman uticaj na morske ekosisteme sa mogućim negativnom posledicama na riblji fond²²

Klimatske promene su ozbiljna pretnja svetu u razvoju i glavna prepreka stalnom smanjenju siromaštva u svim njegovim dimenzijama. Prvo, oblasti u razvoju imaju jedan geografski nedostatak, one su već u proseku toplije od razvijenih regiona, a uz to imaju problem velike promenljivosti padavina. Kao rezultat toga, dalje otopljanje će doneti siromašnim zemljama visoke troškove i malo koristi. Drugo, zemlje u razvoju, a posebno najsiromašnije, u velikoj meri zavise od poljoprivrede koja je od svih ekonomskih sektora najosetljivija na klimu i imaju problem nedovoljne zdravstvene zaštite i nekvalitetnih javnih usluga. Treće, zbog niskih prihoda i osetljivosti njihovo prilagođavanje klimatskim promenama je posebno teško.²³

Kad je u pitanju naša zemlja problem ekološke vrednosti je veći nego ikad. Stepenn industrijskog razvoja je prilično nizak, a zastarele tehnologije su potencijalna opasnost i baza za industrijske akcidente. Ali Srbija ima pravni sistem gde je oblikovana sadržina pojma ekološka bezbednost i koji je otvoren za izmene i preoblikovanje koje će ići u susret novim ekološkim bezbednosnim izazovima.²⁴

Postoji pet katalizatora koji mogu dovesti do nestabilnosti na nekom području.

- Prvi katalizator je ekonomska nestabilnost i stagnacija. Prehrambena kriza, gubitak uslova za život i nezaposlenost su posledice negativnih klimatskih promena u mnogim delovima sveta.
- Drugi katalizator je smanjenje državnog prihoda usled nepovoljnih klimatskih promena.
- Treći katalizator je povećanje konkurentnosti resursa što može izazvati društveni rascep, čineći stanovništvo ranjivijim i ugroženijim.
- Pogoršanje ekoloških prilika može uticati na masovnu migraciju ljudi i izazvati ekološki stres u zemljama koje im pružaju utočište.
- Peti faktor je prilagođavanje ili ublažavanje klimatskih promena koje mogu dovesti do porasta tenzije i konflikata. Zbog takve osetljivosti, klimatske promene u zemljama u razvoju bi verovatno dodatno smanjile njihove već niske prihode i povećale stopu oboljevanja i smrtnosti.

²² www.emins.org

²³ www.emins.org

²⁴ Želimir Kešetović, *Bezbednost, Teorijsko stručni časopis Ministarstva unutrašnjih poslova Republike Srbije, Kosmos, Zemun, 2006., str. 572*

Na nacionalnom nivou, klimatske promene će smanjiti prihode i povećati potrebu za potrošnjom, čime će ugroziti javne finansije.²⁵

Primer kako klimatske promene mogu pozitivno da uticu na neke zemlje:

- ✚ Zemlje kao što su Kanada, Rusija i Skandinavija, klimatske promene mogu da dovedu do koristi kod povećanja temperature od 2-3 stepena koje bi se ogledale u višim poljoprivrednim prinosima, manjoj smrtnosti u zimskom periodu, nižim temperaturama zagrevanja i u mogućem porastu turizma. Ali i ovi regioni će biti izloženi najvećim stopama zagrevanja do tada koje će izazvati oštećenja infrastrukture, pogoršanje ljudskog zdravlja, smanjenje lokalnih prihoda i biodiverziteta.²⁶

Povećani troškovi štete prouzrokovane ekstremnim vremenskim uslovima (oluje, uragani, tajfuni, poplave, suše i toplotni talasi) poništiće neke početne koristi od klimatskih promena i rapidno će se povećavati sa višim temperaturama. Na osnovu jednostavnih ekstrapolacija, samo troškovi nastali zbog ekstremnih vremenskih uslova mogu do sredine ovog veka dostići 0,5-1% svetskog BDP na godišnjem nivou i nastaviti da rastu ako se svet i dalje bude zagrevao.

- ✚ Predviđa se da će povećanje brzine uraganskog vetra od 5 ili 10% povezano sa povećanjem temperature mora, otprilike udvostručiti godišnje troškove zbog šteta u SAD.
- ✚ U Velikoj Britaniji godišnji gubici zbog poplava mogu se povećati sa 0,1% BDP danas na 0,2-0,4% BDP kada povećanje prosečne globalne temperature dostigne 3 ili 4 stepena
- ✚ Toplotni talasi kao oni u Evropi 2003. godine, kada je 35 000 ljudi stradalo, a poljoprivredni gubici dostigli 15 milijardi američkih dolara, biće uobičajeni sredinom veka.

Promena istorijskog trenda u rastu emisija i ostvarenje smanjenja od 25% ili više u odnosu na današnje nivoe je najveći izazov. Troškovi će rasti dok se svet bude prebacivao sa viokarbonskog pravca na niskokarbonski. Ali, sa širenjem tržišta niskokarbonske, visokoefikasne robe i usluga takođe će se javljati i poslovne mogućnosti. Emisije gasova staklene bašte mogu da se smanje na četiri načina. Troškovi će u velikoj meri varirati u zavisnosti od toga koja se kombinacija ovih metoda koristi i kojem sektoru:

- Smanjenje tražnje za robom i uslugama sa intenzivnom emisijama

²⁵ Vladimir N. Cvetković- Rizik, moć, zaštita; Uvođenje u nauke bezbednosti, Službeni glasnik, Beograd 2010., str.692

²⁶ www.emins.org

- Povećana efikasnost koja može i da uštedi novac i da smanji emisije
- Aktivnosti na neenergetskim emisijama, kao što je izbegavanje seče šuma
- Prelazak na niskokarbonske tehnologije za proizvodnju električne energije, zagrevanje i saobraćaj²⁷

3.2. Zdravstvene krize

Zdravlje na putovanju

Turizam i medicina su usko povezani. Osnovni motivi u turizmu su zdravlje, odmor i rekreacija. Nova grana javnog zdravstva je zdravlje turista, koja se bavi zaštitom i unapređenjem zdravlja turista. Svako ko putuje bi trebalo pre putovanja da poseduje osnovne informacije o zemlji u koju putuje i koji su to faktori koji bi mogli da možda ugroze njihovo zdravlje (nadmorska visina i zagađenost, dostupnost lekara i apoteka, vakcine pre puta...). Zdravlje na putovanju može biti ugroženo, jer pred organizam postavljamo psihofizičke zahteve kakvim je retko izložen kod kuće, a pored toga navike u spavanju i ishrani se menjaju. Zbog toga je izuzetno važno obratiti pažnju na preventivne mere i informisati se, šta treba uraditi, u slučaju onih najčešćih bolesti koje vas mogu zahvatiti tokom putovanja. A najčešće bolesti na putovanju su: rizici od ujeda insekata i životinja, hepatitis B, meningitis, evropski encephalitis i dr.

Pored navedenih bolesti, veliki rizik mogu predstavljati i ekstremne temperature, bilo da je toplo ili hladno. Jake temperature utiču na ljudski organizam. Danas se dosta govori o ozonskim rupama koje prekomerno propuštaju sunčeve zrake, što je naročito izraženo u letnjim mesecima. Efekti Sunca mogu da izazovu jake bolesti, privremeno slepilo i smrt. Sunčevo zračenje je sada veće, zbog oštećenog Zemljinog omotača što izaziva crvenilo na koži i pogoršanje imunog sistema. Međutim, postoji i dobra strana Sunca. Sunčevi zraci proizvode vitamin D koji je potreban našem organizmu, tako da je preporučljiva izloženost Suncu 10-30 minuta.²⁸

- ✚ Po statistici većina saobraćajnih nezgoda se desi tokom letnjih meseci kada je umanjena koncentracija vozača zbog visokih temperatura u kolima; uslovi koji su podnošljivi za čovekov organizam su od 23 stepena.²⁹

²⁷ www.emins.org

²⁸ www.politika.rs/magazin

²⁹ www.travelmedicine.com

Rizici od ujeda insekata i životinja

Veliki broj turista kada putuje na odabranu turističku destinaciju nije upućeno u sve detalje određenog mesta. U nekim od njih insekti prenose veliki broj bolesti, tako da postoji rizik kojeg turisti nisu svesni. Osim što prenose bolesti, ujedi od insekata uzrokuju neprijatne i burne reakcije na koži:

- ✚ Komarci prenose malariju i druge bolesti. Ujed nije bolan, ali izaziva neprijatan svrab i reakcije na koži
- ✚ Malarija je najstrašnija bolest Afrike, koja ubija više od milion ljudi svake godine, ili oko 3.000 dnevno. Devedeset procenata slučajeva desi se u podsaharskoj Africi, slično kao i u slučaju side.
- ✚ Barem 300 miliona ljudi pati od slučajeva akutne malarije svake godine, što često dovodi do smrtonosnih efekata. Malariju prenosi malarični komarac- od malarije se najbolje može zaštititi tako što kada se nađemo na egzotičnom putovanju, u zemlji u kojoj se može sresti malarični komarac, obavezno tražiti da se u hotelskoj sobi, kreveti sa svih strana prekriju mrežom protiv komaraca, koja je prethodno, po mogućstvu, tretirana insekticidom.

Teška bolest tropskih i suptropskih zemalja, može biti fatalna, ali se može sprečiti na sledeće načine:

- Nošenjem odgovarajuće odeće,
- Korišćenjem sredstava protiv insekata
- Upotrebom tableta protiv malarije, sa kojima se počinje tri nedelje pre puta uz nadzor lekara i nastavlja na putu, uz ili posle obroka.³⁰

Pored malarije, komarci su prenosioci i žute groznice:

- ✚ Žuta groznica je virusna bolest koju prenose komarci. Bolest varira, tako da može da ima lagane simptome, ne teže od običnog gripa, do teškog hepatitisa i hemoragične groznice.
- ✚ Žutu groznicu prenosi "stanovnik" surle komarca - virus. Žuta groznica se isključivo može dobiti u podsaharskoj Africi i tropskoj Južnoj Americi, gde se javlja u prirodnom,

³⁰ www.travelmagazin.rs

okruženju i gde se začinju i epidemije. Iz Afrike stiže i najveći broj prijavljenih slučajeva, a stopa smrtnosti je viša od 20 odsto.

- ✚ U Južnoj Americi, bolest se najčešće javlja kod mladih muškaraca koji su zbog posla izloženi komarcima, u područjima Bolivije, Brazila, Kolumbije, Ekvadora, Venecuele i Perua, gde se ova bolest najčešće i pojavljuje.
- ✚ Lokalna populacija je često prilično imuna na žutu groznicu, a epidemije veoma često izbijaju u zabitim krajevima džungli uz reke, tako da je u velikoj većini slučajeva "mir" i "bezbednost" u nekom području samo puki privid.³¹

Uzročnik bolesti koja se javlja u endemičnim delovima Afrike i ugrožava, kako domaće stanovništvo tako i turiste, je muva Ce-Ce:

- ✚ Prvi simptomi se javljaju od prve do četvrte nedelje nakon infekcije. Na mestu ujeda muve javlja se bol i razvija se rana. Ovu lokalnu promenu prate povišena telesna temperatura, glavobolja, bolovi u mišićima i zglobovima.
- ✚ Kada prođe početna faza ove bolesti, parazit prelazi u nervni sistem i dolazi do poremećaja u vidu konfuzije, promene ponašanja, nerazgovetnog govora i otežane koordinacije pokreta.
- ✚ Poremećaj ciklusa spavanja je glavno obeležje ove bolesti, gde oboleli spavaju preko dana, a uveče imaju nesanicu. Zato je i zovu spavajuća bolest. Ukoliko se blagovremeno ne leči, bolest se može fatalno završiti za nekoliko nedelja ili meseci.³²

Da bi bismo bili bezbedni na putovanju, trebali bi da koristimo sredstva protiv ujeda insekata:

- Sredstva za zaštitu koristiti samo na nepokrivene delove kože
- Nije potrebno nanositi debeo sloj zaštite
- Ne nanositi sredstva za zaštitu na posekotine, rane, iziritiranu kožu, oči i usne
- Sprej ne treba prskati direktno na lice. Naprskajte ga na dlanove, pa dlanovima razmazati po licu
- Sredstva držati podalje od male dece- da im ne dospe u oči. Kod dece glavna zaštita treba da bude odeća, a sredstva samo ako su neophodna
- Pre upotrebe sredstva za zaštitu proučiti upustvo

³¹ www.travelmagazin.rs

³² www.stetoskop.info

Pored insekata, prilikom boravka na nekoj turističkoj destinaciji, treba se paziti i od ujeda životinja:

- ✚ Da ne bi došlo do ovoga, ne treba imati kontakt sa životinjama koje su agresivne i koje bi mogle da napadnu. Ukoliko dođe do ujeda ili ogrebotine, treba odmah oprati vodom to mesto.
- ✚ Turisti koji mogu da budu izloženi ujedu životinje, trebalo bi da prime vakcinu pre puta i da se informišu o mogućim rizicima u predelima koje posećuju.
- ✚ Poznato je da bi Australija bila savršeni raj, da nema otrovnih meduza; najgorih ubica u Pacifiku kojih ima svuda u toplim vodama Kvinslenda, a najgora je morska osa od čijih pipaka godišnje 1,25% ljudi nastrada.³³

Vakcinacija

Zarazne bolesti mogu biti fatalne. Pre polaska na put, obavezno treba proveriti kakvo je stanje u zemljama u koje nameravate da putujete. Za neke afričke i azijske zemlje preventivna vakcinacija je apsolutno neophodna. Vakcinacija predstavlja zaštitu od mogućih zaraznih bolesti. Svaki turista treba da primi vakcinu, koja će ga zaštititi od bolesti. Vakcina bi trebala da se primi četiri do osam nedelja pre polaska na put, koliko je potrebno da se stvori odbrambeni sistem u organizmu.³⁴

U zavisnosti gde se putuje i od lokalne situacije, putnici treba da se vakcinišu za sledeće:

- Hepatitis B (Vakcina protiv Hepatitisa A treba onima koji neće biti u mogućnosti da nadziru higijenu hrane i vode koju će konzumirati.)
- Evropski encephalitis
- Meningitis
- Besnilo
- Tetanus (Vakcine protiv tetanusa su za one koji će tokom službenog puta biti izloženi povredama ili u stalnom kontaktu sa lokalnim stanovništvom.)
- Grip (Vakcinu protiv gripa treba da prime hronični bolesnici.)

³³ www.travelmagazin.rs

³⁴ www.who.int

Povrede na putovanju

Mogućnost povrede, pa i nesreće, nije beznačajna kada spomenemo putovanje, a pogotovo avanturistički turizam. Postoji niz faktora koji mogu izazvati probleme:

- Problemi klijenata koji učestvuju (nesporazumi oko nivoa rizika i iskustva pojedinaca)
- Environmentalni činioci (nepredvidivost terena, prirodni ambijent, slučajnost)
- Problemi u vezi opremom (kvar zaštitne opreme)
- Uticaj faktora izvan kontrole organizatora (vremenski uslovi, nepogode, pogrešna vremenska prognoza i sl.)
- Greške u menadžmentu i organizaciji (nedostatak iskustava zaposlenih, propust u informisanju klijenata, pokušaj uštede na troškovima i sl.)³⁵

Turisti bi trebali da budu što pažljiviji i da poseduju informacije kako ne bi došlo do povreda. Ukoliko dođe do povrede trebali bi da imaju pri ruci prvu medicinsku pomoć. Opšta pravila postupanja u slučaju da je neko povređen ili da smo mi povređeni, treba postupati po sledećim pravilima: plikove od opekotina ne trljati i ne bušiti, rana se ne treba ispirati nikakvim sredstvima, strana tela iz rane ne treba vaditi nego ih fiksirati i prekriti u zatečenom položaju, kod povreda prilikom kojih dolazi do oteklina (opekotine, smrzotine), ne stezati zavoj i povređenom ne navlačiti obuću i odeću, kod težih povreda imobilizacija je obavezna i treba je izvesti bez nameštanja.³⁶

Bezbednost hrane

Sa porastom kupovne moći potrošača, vrednost potrošnje proizvoda hrane raste u celokupnoj strukturi turističkih proizvoda, to istovremeno znači da će potrošači neprekidno zahtevati kvantitativno i kvalitativno povećanje standarda bezbednosti hrane.

HACCP (Hazard analysis and Critical control poin) omogućava navedene standarde kroz bezbednost potrošača, povećanje zadovoljstva, smanjenje troškova, zaštitu reputacije proizvođača i osiguranje profita. HACCP obezbeđuje proizvodnju i promet zdravstveno ispravne hrane, tako da je ona bezbedna od hemijskih, bioloških i fizičkih rizika. Proizvođači i distributeri prehrambenih proizvoda i gotove hrane treba da se u svojim aktivnostima definišu svaki korak koji je kritičan u pogledu bezbednosti hrane i da adekvatnim postupcima identifikuju, sprovode,

³⁵ Branislav Rabotić, *Selektivni oblici turizma, Visoka turistička škola strukovnih studija, 2012.*

³⁶ www.travelmagazin.rs

održavaju i preispituju definisan sistem.³⁷ HACCP sistem je veoma bitan za proizvođače hrane zato što se njime obezbeđuje proizvodnja i promet zdravstveno bezbedne hrane. Krajnji cilj HACCP sistema je proizvodnja što je moguće bezbednijeg postupka, što znači da ovaj sistem ne obezbeđuje uvek 100% sigurnost za korisnike, ali za preduzeće je to najbezbedniji i najbolji način proizvodnje hrane.

U skladu sa odlukama Ministarstva poljoprivrede pri izradi Strategije o bezbednosti hrane i Zakona o hrani, HACCP je od 01.01.2009. godine postao zakonska obaveza svih subjekata koji posluju sa hranom. Uvođenjem zakonske obaveze, Ministarstvo je krenulo u pripremu domaće industrije za plasiranje proizvoda na evropsko tržište u skladu sa zahtevima Evropske Unije.

HACCP sistem ima sedam principa kojih bi se, svi koji se bave hranom, trebalo pridržavati:

1. Sprovođenje analize opasnosti- identifikovanje opasnosti/rizika koji mogu da se pojave u procesu proizvodnje, prerade, pakovanja, skladištenja, distribucije i ponude u cilju prodaje, prodaju i služenje hrane. Opasnost može biti fizička, hemijska ili biološka i mora da se odnosi isključivo na bezbednost hrane.
2. Određivanje Kritičnih Kontrolnih Tačaka (CCP)- CCP su tačke u procesu gde je moguća pojava opasnosti/rizika. Za svaki identifikovani rizik, mora da postoji bar jedna kritična kontrolna tačka za kontrolu tog rizika. Kritične kontrolne tačke se odnose na fazu u kojoj je hrana najosetljivija na kontaminaciju. Sve kritične kontrolne tačke moraju biti u okviru definisanog HACCP plana.
3. Određivanje kritičnih granica – kritične granice su max ili min vrednosti pomoću koje se biološke, hemijske i fizičke opasnosti kontrolišu. To su one vrednosti kje se moraju postići kako bi se eliminisala opasnost od trovanja hranom. Kritična granica je kriterijum koji mora da se ispuni u svakoj CCP. Ako postoje, kritične granice se usklađuju sa zahtevima propisa ili zakona.
4. Određivanje procedura/postupaka za praćenje CCP- su postupci kojima se osigurava da CCP ostane u kritičnim granicama. Postupci nadzora mogu da zahtevaju instrumente i opremu za merenje ili drugi način ocene procesa u CCP. Način merenja mora biti jasno definisan sa tačnim zaduženjima za njihovo sprovođenje. Praćenje Kritičnih granica podrazumeva odgovore na pitanja šta, kako, koliko često i ko.
5. Određivanje korektivnih mera – korektivna mera u slučaju da nadzor pokaže da CCP nije u okviru kritičnih granica. Kada se problem pojavi, moraju da postoje korektivne mere da spreče

³⁷ Živković Radmila- „Ponašanje i zaštita potrošača u turizmu“ ; Fakultet za turistički i hotelijerski menadžment; Univerzitet Singidunum; Beograd, 2006., str. 192.

pojavu zdravstvenog rizika za potrošače. Korektivne mere osiguravaju da: uzrok problema bude identifikovan i eliminisan,

CCP budu pod kontrolom i nakon preduzetih korektivnih mera, ni jedan proizvod ne ugrozi zdravlje ljudi ili bude distribuiran na tržište.

HACCP plan mora da ima definisane korektivne mere za svaku od identifikovanih CCP. Mera mora da bude definisana tako da nedvosmisleno informiše zaposlenog koje aktivnosti mora da preduzme u slučaju odstupanja izmerenih vrednosti od definisanih kritičnih granica.

6. Uspostavljanje procedura/postupaka za verifikaciju – postupci i potvrđivanja da je HACCP sistem efektivan i da funkcioniše dobro. Postupci verifikacije mogu da uključe preispitivanje HACCP planova, zapisa u CCP, kritičnih granica kao i uzorkovanja za laboratorijska ispitivanja. U verifikacione aktivnosti treba da budu uključena ovlašćena lica zaposlena u proizvodnji, HACCP tim i predstavnici inspekcije u pogonu.
7. Uspostavljanje i vođenje efektivne evidencije i dokumentacije – dokumentovanje da HACCP sistem dobro funkcioniše. Zapisi treba da dokumentuju podatke dobijene praćenjem – nadzorom CCP uključujući i odstupanja i postupke verifikacije. Precizno vođenje zapisa je izuzetno važno i zbog mogućih kontrola od strane nadzornih organa koji mogu tražiti na uvid zapise kojima se svedoči dosledna primena HACCP sistema. Treba imati u vidu da HACCP nije samo preventivna mera za bezbednost hrane, već i zakonska obaveza prema Zakonu o bezbednosti hrane.³⁸

Zaraze vode i hrane su primarni uzroci bolesti kod turista. Treba voditi računa da su voda i hrana bezbedni. Bolesti koje se mogu javiti su hepatitis A i E, tifus, kolera i druge koje se prenose putem vode i hrane. Na putu, treba koristiti flaširanu vodu i treba prati ruke pre svakog obroka. Takođe, treba znati kakav je kvalitet određene namirnice i gde ih treba kupovati.

Indija i Tajland su zemlje gde se najčešće javlja problem sa dijarejom:

-  Najopasnija zemlja na svetu za one koji imaju „osetljiv stomak“ je Tajland. Iza nje je Indija. U ovim zemljama se može javiti dijareja i ostali slični simptomi, zbog mnogo začinjene ili masne hrane. Ukoliko dođe do toga, treba nadoknaditi tečnost i soli iz organizma.

³⁸ <http://www.nacor.co.rs/#!haccp-sistem-bezbednosti-hrane/c1r7r>

Prednosti sistema HACCP-a u odnosu na klasičan način proizvodnje hrane i proizvoda za ishrane su:

- Primenjivo u kompletnom lancu hrane, od poljoprivredne proizvodnje do krajnjeg korisnika
- Efikasna i ekonomična kontrola rizika hrane
- Premeštanje tržišta sa provere kvaliteta krajnjeg proizvoda na preventivno upravljanje procesom
- Smanjuje troškove
- Povećava zadovoljstvo korisnika
- Omogućava projektni pristup i timski rad
- Povećava konkurentnost na tržištu i institucionalan imidž
- Može se verifikovati i proveravati
- U slučaju spora obezbeđuje objektivne dokaze

HACCP je primeljiv u svim sistemima koji se bave proizvodnjom i prometom hrane, ambalaže, opreme, uključujući:

- Proizvođače primarnih poljoprivrednih proizvoda
- Prehrambenu industriju
- Distributere proizvoda
- Proizvođače ambalaže
- Trgovine
- Organizacije koje se bave pripremom i distribucijom hrane
- Hotele i restorane

Strateško opredeljenje da se proces proizvodnje hrane usaglasi sa sistemom HACCP značio bi prelazak na jedan potpuno nov i savremen koncept poslovanja i potpuno zadovoljnog potrošača. Suština HACCP koncepta je sadržana u stalnom nastojanju da se pozicioniraju, definišu i na vreme otklone sve opasne faze ili situacije u celokupnom ciklusu proizvodnje, odnosno u preventivnom delovanju kako bi se na vreme otklonili, umanjili ili doveli na prihvatljiv nivo realno potencijalni rizici u pogledu bezbednosti hrane. Uspeh HACCP sistema će zavisi najviše od obrazovanja i obuke zaposlenih koji moraju da budu upoznati sa odgovarajućim procedurama i radnim upistvima.³⁹

³⁹ <http://www.nacor.co.rs/#!haccp-sistem-bezbednosti-hrane/c1r7r>

3.3. Terorizam

Poslednjih godina turistička industrija se suočava sa posebnim problemima kao što su: terorizam, ekološke katastrofe, pojava raznih bolesti. Svet se promenio posle napada na London, Madrid, Njujork. Većina nas ne zna šta da radi kada dođe do terorističkog napada koji se mogu desiti bilo kad i bilo gde. Zbog toga je potrebno istraživati turističku destinaciju u koju se putuje i skupiti što više informacija kako bi povećali bezbednost. Takođe, veoma je važno da se unapređuju sistemi bezbednosti, da se preduzmu mere predostrožnosti i da se informacije pravilno prenesu turistima kako se ne bi stvarala nervoza.:

- Ako turista smatra da će na destinaciji verovatno doći do terorističkog napada i da će on biti moguća meta, turista neće otputovati. Putem medija se mogu ponavljati izveštaji o terorističkim napadima što može izazvati strah kod turista i njihovog otkazivanja rezervacija. Međutim ima i turista koji bez obzira na rizik putuju, jer im to predstavlja dozu adrenalina.⁴⁰

Primeri kako je terorizam uticao na turizam:

- Terorizam je na velika vrata ušao 11. septembra napadom na SAD i terorističkim napadom na London 2005. godine što se odrazilo na razvoj turizma
- Izraelska avijacija je 2009. godine ubila dva Palestinca, u centralnoj Gazi. Očevidci kažu da su ubijena dva vojnika koja su pokušala da postave granatu
- U Japanu je 2011. godine došlo do zemljotresa u kojem je poginulo ili nestalo oko 1.700 ljudi. Objavljen je podatak da je oko 100 osoba lakše ozračeno. Ovo je jedna od više sličnih havarija u svetu na nuklearnim elektranama u poslednjih 25 godina;⁴¹
- Tokom sukoba od strane Iraka u Persijski zaliv je ispušteno 1,1 milijarde litara sirove nafte što je izazvalo velike posledice na ukupnu životnu sredinu
- Zabeležen je i individualni teroristički napad koji je ugrozio uži region 2000. godine je zabeleženo da su radnici hemijske industrije u severnoj Francuskoj ispustili oko 3.000 litara sumporne kiseline u reku Meus, kada im je uskraćena finansijska nadoknada za rad.⁴²

⁴⁰ www.elsevier.com/locate/tourman

⁴¹ www.today.reuters.com

⁴² Vladimir N. Cvetković- Rizik, moć, zaštita; Uvođenje u nauke bezbednosti, Službeni glasnik, Beograd 2010., str.673

Terorizam zauzima najvažnije mesto u sferi negativnih događaja, kada postaje oružje u borbi ekstremista čije delovanje vodi ka ugoržavanju bezbednosti turista. Terorističke aktivnosti u kojima se turistička kretanja uzimaju u situaciju taoca mogu biti usmerene u dva pravca :

1. Aktivnosti usmerene ka samoj turističkoj destinaciji
2. Aktivnosti u kojima se turisti koriste kao ucena za postizanje ciljeva domicilne zemlje terorista

Značaj turizma kao privredne grane koja ostvaruje značajne prilive od turističkog prometa čini ovu sferu izuzetno osetljivom na ovaj tip pretnji. Terorizam može poprimiti oblik: domaćeg terorizma, međunarodnog i prekograničnog terorizma. Odnos između terorizma i turizma se može manifestovati kroz tri moguće situacije: terorizam koji je usmeren na civilne mete, gde su ponekad turisti te mete; terorizam usmeren ka ekonomskim ciljevima koji su u vezi sa turizmom i terorizam koji je usmeren na turizam i turiste sa velikom medijskom pokrivenošću.⁴³ Ukoliko su mete turisti i ukoliko dođe do otmice, jedini cilj koji turisti treba da vodi je preživljavanje. Takođe, ne treba pomišljati na bežanje, jer ishod može biti tragičan. Odeljenja koja su zadužena za vandredne situacije preduzimaju u takvim situacijama sve kako bi vas spasili.⁴⁴

3.4. Kriminal

Turizam može doneti razne vrste beneficija svojoj zemlji, posebno ekonomske koristi od dolazaka turista. Međutim, brz rast turizma može izazvati mnoge negativne uticaje, kao što su društvene promene i kriminal. Postoji niz faktora koji dovode do krivičnog rizika:

- Prvi faktor je veliki broj turista u određenoj oblasti što otežava policiji da obavlja svoj zadatak.
- Drugo ukoliko je turistička regija blizu granice, to će posao policije biti teži. To je zato što, geografska lokacija omogućava lakše bekstvo kriminalca. Kao treći faktor mi bio ekonomski jaz koji postoji između turista i lokalnih ljudi što može dovesti do povećanja

⁴³ Abraham Pizam and Yoel Mansfeld, *The management of hospitality and tourism enterprises series*, Tourism, Security and Safety, from theory to practice, Toward a Theory of Tourism Security, Elsevier, 2006.p. 23.

⁴⁴ Robert Macpherson, Bennett Pafford, *CARE International SAFETY & SECURITY HANDBOOK*

krivičnih dela. Pored krivičnog rizika, postoje i turistički rizici: psihološki, finansijski, fizički i socijalni.⁴⁵

Kada se putuje u neku zemlju treba imati na umu da li je ta zemlja bezbedna i koliko i da li postoji i u kojoj meri rizik, da se bezbednost ugrozi.

- Zemlje koje imaju nizak rizik su zemlje, regioni ili gradovi koji su u suštini stabilni i bez političkih, ekonomskih i socijalnih nemira. Zločin u ovakvim zemljama je na niskom nivou. Važno je spomenuti da iako postoji niska stopa kriminala na ovim područjima i dalje može postojati pretnja, kao što su neke prirodne katastrofe, vulkani ili poplave. I ovde su potrebne mere preostrožnosti.
- Zemlje koje imaju umeren rizik su zemlje, gde postoji nizak nivo političkih, ekonomskih i društvenih nemira, a sigurnosna infrastruktura je slabo razvijena. Ovakve zemlje pokazuju visoku stopu kriminala i mogućnost elementarnih nepogoda ili bolesti epidemije. I u ovim zemljama su potrebne povećane mere predostrožnosti.
- Zemlje sa visokim rizikom su zemlje ili regioni u kojima su anti-vladine ili terorističke grupe veoma aktivne i predstavljaju ozbiljnu pretnju zemlji. Ovakve zemlje mogu biti i blizu vojnog puča ili da izlažu slom socijalne infrastrukture. Ovde bi turisti bili izloženi velikom riziku i morale bi da postoje velike mere bezbednosti u toj zemlji.
- Postoji još jedna grupa rizika koja podrazumeva četvrti ili najrizičniji vid ugrožavanja bezbednosti. Ovde spadaju zemlje gde nivo nasilja predstavlja direktnu pretnju za bezbednost i dobrobit humanitarnih radnika, pre svega lekara. Njihovo prisustvo je neophodno na ugroženim područjima i na mestima gde je nizak nivo higijene, gde postoje uslovi za stvaranje epidemije. Humanitarni radnici u takve zemlje idu uz vojnu podršku.⁴⁶

Primer najnestabilnijih i najstabilnijih zemalja na svetu:

🚩 Afrika i arapske zemlje politički su najnestabilniji regioni na svetu, pa samim tim predstavljaju i najrizičnije destinacije. Analiza koja je urađena marta 2013. godine obuhvata dinamičke političke rizike koje se odnose na konflikte, terorizam, vladavinu prava i okvirne uslove po pitanju sigurnosti resursa i infrastrukture. Od zemalja u regionu, bolje rangirane su

⁴⁵ Pimmada Wichasin , Nuntiya Dounghummes, *A Comparative Study of International Tourists' Safety Needs and Thai Tourist Polices' Perception towards International Tourists' Safety Needs*, *World Academy of Science, Engineering and Technology* 67, 2012.

⁴⁶ Robert Macpherson, Bennett Pafford, *CARE International SAFETY & SECURITY HANDBOOK*

Hrvatska (6,85), Crna Gora (6,78) i Makedonija (6,40), dok su iza Albanija (5,89) i Bosna i Hercegovina (5,53).

Najopasnija zemlja na svetu i dalje je Somalija sa ocenom 0,82, a slede DR Kongo, Sudan, Avganistan, Mjanmar i Irak.

🚩 Na prvom mestu po bezbednosti je Luksemburg sa 9,04, zatim Novi Zeland, San Marino i Norveška. Među državama u okruženju Italiji ima ocenu 6,83, Rumuniji 6,62, Bugarska 6,31, Grčka 6,06, Turska 5,10, a najlošije rangirana evropska zemlja je Rusija sa 3,18. U odnosu na prošlu godinu, broj zemalja u kojima svakodnevicu karakteriše politički motivisano nasilje porastao je na 38, odnosno za 36 odsto, što se objašnjava činjenicom da su se nasilje i terorizam iz Libije i Sirije proširili na Mali, Liban, Alžir i druge zemlje zapadne i severne Afrike, kao i Bliskog istoka.⁴⁷

Civilni ili politički nemiri mogu biti u obliku prevrata, demonstracija, pobuna i nereda. Navedeni incidenti su izazvali velike padove turističke tražnje u različitim delovima sveta; bilo da je puč na ostrvu Fidži, nasline demonstracije protiv grupe sedam zemalja (G7), pobuna od strane Palestinaca na Zapadnoj obali Gaze ili neredi u Čiapas regionu u Meksiku; koji su imali ozbiljan uticaj na lokalnu turističku industriju, a kao rezultat su dobili otkazivanje rezervacija i odlaženje na bezbednije destinacije. Pokazatelji učestalosti incidenata obično se mere putem sledećih varijabli: broj incidenata u datom vremenskom periodu i frekvenicija tih incidenata.

Motivi i ciljevi incidenata, mogu da se predvide, al tek pošto se shvate koji su motivi. Proučavanje motiva može da pruži dragocene informacije o potencijalnim metama. Veće razumevanje ove uzročno-posledične veze može dovesti do efikasnog sprečavanja ili ublažavanja situacije koja je nastala na određenoj destinaciji.

Ciljevi zbog kojih dolazi do incidenata mogu biti:

- Politički
- Verski
- Socijalni
- Ekonomski
- Turisti koji idu na destinaciju ili se vraćaju sa destinacije
- Instalacije i postrojenja u turizmu i ugostiteljstvu

⁴⁷ www.maplecroft.com

- Javni i privatni servisi koji služe turistima⁴⁸

Izvori rizika koji se mogu javiti na destinaciji su:

- Ljudsko i institucionalno okruženje van sektora turizma
- Sektor turizma i povezani komercijalni izvori
- Individualni putnici (lični rizik) i
- Fizički rizici iz okruženja (prirodni, klimatski, epidemije)

Kriminal u turističkoj sezoni je u porastu u odnosu na celu godinu. Najizraženije su krađe i teške krađe, razbojništva i prevare.

Krađe prema mestu i vremenu se mogu podeliti u dve grupe:

- Krađe koje se počine tokom sezone- krađe na kupalištima, plažama i kampovima; krađe po hotelima, motelima, apartmanima i drugim objektima koji pružaju usluge u turizmu
- Krađe koje se javljaju tokom cele godine, a nastupanjem turističke sezone njihov broj se povećava- krađe putničkih prtljaga u sredstvima pomorskog, železničkog prometa, kao i autobuskim, železničkim stanicama i brodskim pristaništima; džepne krađe i krađe sa i iz motornih vozila

Teške krađe su složeniji i teži oblik krađe i tu spadaju:

- Provala u objekte uslužnog, ugostiteljskog i smeštajnog karaktera
- Provale u garderobne kabine i druge objekte na kupalištima
- Provale u kamp kućice i šatore
- Provale u vozila

Primeri krađa i prevara u svetu:

🚩 U Južnoj Africi, ima najviše oružanih pljački turista. SAD na ovoj listi zauzima drugo mesto. Južna Afrika i Tajland, dele prvo mesto po broju izgubljenog prtljaga i stvari. Najmanje neprijatnosti turisti su doživljavali u Irskoj, Belgiji, Holandiji, Nemačkoj i Francuskoj.

⁴⁸ Abraham Pizam and Yoel Mansfeld, *The management of hospitality and tourism enterprises series ,Tourism, Security and Safety, from theory to practice, Toward a Theory of Tourism Security, Elsevier, 2006., str. 56*

- ✚ Motorizovani turisti su lak plen za organizovane bande u Evropi. Treba biti izuzetno oprezan kada se staje na pumpama jer oni imaju načine da prevare turiste. Najopasnije je u Italiji.
- ✚ Popularna letovališta su "raj za lopove", Nica, Mikonos, Hurgada do Rija i Punte del Este.
- ✚ Kad vidite slatkog malog majmuna na ulici, čvrsto držite svoje lične predmete. Ako ste nepažljivi, i ne držite svoje torbe ili fotoaparate čvrsto, možete lako da ostanete bez njih. Egipat, Tajland, Iran, Indija, Kenija zemlje gde možete imati bliski susret sa majmunima lopovima. U Nju Delhiju hiljade majmuna krade sve što stigne od ljudi.⁴⁹

4. Percepcija turista o bezbednosnim potrebama

Prilikom kupovine turističkog aranžmana, turista na prvo mesto stavlja bezbednost samog putovanja, a potom cenu, lokalitet, atraktivnost područja i ostale komponente. Današnji turista želi da se odmori od svakodnevnog stresa i da ode na destinaciju koja je sigurna i koja ne predstavlja krizno područje. Svakodnevno slušamo na vestima o terorističkim napadima i elementarnim nepogodama koje pogađaju poznate turističke destinacije, što izaziva osećaj nesigurnosti. Informisanje potrošača možemo podeliti u tri faze: izloženost uticajima, pažnja i razumevanje, što se jednim imenom može nazvati, percepcija. Percepcija je process kojim ljudi biraju, organizuju i interpretiraju informacije kako bi stvorili razumljiviju sliku sveta. Percepcija, ustvari, predstavlja, prevođenje spoljnog sveta u interni (mentalni) svet osobe, tj. potrošača i u velikoj meri zavisi od kvaliteta stimulansa. Takvi stimulansi ostvaruju određeni efekat i kada nisu opaženi od strane potrošača.⁵⁰ Poseban stimulans ostavlja intezitet boje, kod potrošača ili turista, a da ga oni nisu ni svesni. Tako na primer crvena boja u restoranima ima snažan uticaj na apetit potrošača, oslobađa ih „pritiska vremena”, zbog čega se često koristi za enterijere u restoranima, kazinima. Sa druge strane žuta boja stimuliše intelektualne aktivnosti, a njene asocijacije su radost i veselje.⁵¹ Percepcija je glavna kada je u pitanju odluka turista, da li će da otputuje na neku destinaciju i ona utiče na odluku, a ne činjenice ili okolnosti. U suštini, odluka turista je bazirana na percepciji, a ne na stvarnosti što nekada može biti rizično i dovesti do

⁴⁹ www.travelmagazine.rs

⁵⁰ Živković R.- „Ponašanje i zaštita potrošača u turizmu“ ; Fakultet za turistički i hotelijerski menadžment; Univerzitet Singidunum; Beograd, 2010., str. 117.

⁵¹ Maričić B., Ponašanje potrošača, Beograd, str. 351

posledica. Kada kažem rizično mislim na prirodne nepogode, terorizam, političke nemire, ratove, koji se mogu desiti na destinaciji. Percepcija turista se može promeniti, ako se podigne njihovo posmatranje na viši nivo, u smislu, da turista bude svestan rizika. Druga stvar je kada turista nema informacije o nekoj destinaciji, mediji igraju ključnu ulogu u stvaranju slike o toj destinaciji i o mogućem riziku. Kada dobiju takve informacije i oseću koliko bi bili izloženi nekom incidentu, menjaju svoju percepciju, menjaju planove, otkazuju rezervacije.⁵²

Vodeći faktori koji utiču na turistička kretanja su :

- Nepovoljno stanje okruženja,
- Nepovoljna politička i sigurnosna situacija, ekološke katastrofe, epidemije i drugi zdravstveni problemi,
- Nepovoljna ekonomska kretanja,
- Nepovoljno stanje saobraćaja, posebno avio saobraćaja, vodeći su faktori koji utiču na uobičajena turistička kretanja⁵³

Turista može da ima informacije koje će ga odvući od putovanja i sprečiti ga da ode u neku zemlju zbog faktora koje sam navela. Ali ako turista ima informacije da je neka destinacija bezbedna i on otputuje, opet se mogu javiti problemi.

Problemi koji mogu da se jave na turističkoj destinaciji, nastaju zbog:

- Kulturoloških razlika koje izazivaju krive interpretacije ponašanja i dobrih namera osoba u novoj sredini,
- Ulaska u novu situaciju u kojoj ne postoji sistem sigurnosti uobičajen u svakodnevnom životu kao i nemogućnosti primene reakcije na novo nepoznato stanje sigurnosti u određenom vremenu-nepoznavanje jezika, običaja, hrane i slično,
- Prelaza iz redovnog stanja u stanje turista (turisti je svojstveno opuštanje od svakodnevne rutine, odmor, rekreacija, razonoda, istraživanje nepoznatog ili opasnog i sl.), što spušta lični nivo sposobnosti predviđanja potencijalnih rizika, prepoznavanje opasnosti i samozaštite.
- Želje i shvatanje pojedinaca kako biti turista znači pravo i na nedolično ponašanje,

⁵² www.elsevier.com/locate/tourman

⁵³ Živković R.- „Ponašanje i zaštita potrošača u turizmu“ ; Fakultet za turistički i hotelijerski menadžment; Univerzitet Singidunum; Beograd, 2010., str. 187

- Poimanje kako je turista lak plen za pljačku, te da uvek postoje kriminogeni pojedinci koji planiraju svoju kriminalnu delatnost nad turistima,
- Povećanje rizika nastanka i tragičnih posledica prirodnih i tehnoloških nesreća i katastrofa kao posledica velikog broja ljudi na malom prostoru, bez odgovarajućih znanja o postupcima zaštite u slučaju opasnosti,
- Neprofesionalnog ponašanja pojedinca u turističkoj delatnosti, koji turistima uskraćuju elementarna potrošačka prava.⁵⁴

Po rečima turista, najveću pretnju na destinaciji predstavljaju sledeće stavke:

- Najveću zabrinutost turisti pokazuju za ličnu fizičku sigurnost, što je veoma naglašeno u vreme političkih i ratnih kriza.
- U današnje vreme terorizam predstavlja najveću pretnju fizičkoj sigurnosti.
- Paniku i nesigurnost među posetiocima izazivaju i požari, posebno u hotelijerstvu.
- Zdravlje turista ugrožava i neodržavanje higijene što može uzrokovati razvoj mnogih bolesti.⁵⁵

Ljudsko i institucionalno okruženje van sektora turizma podrazumeva vrstu rizika kada je turista žrtva i ovde spada: delikvencija, organizovani kriminal, trgovina belim robljem, ratni sukobi, socijalni sukobi i terorizam. U okviru sektora turizma i povezanih komercijalnih izvora se podrazumeva ugrožavanje lične sigurnosti, fizičke bezbednosti i ekonomske sigurnosti posetioca u oblasti turizma, transporta, sporta, trgovine, kroz:

- Nepostojanje standarda za zaštitu od požara, građevinskih grešaka, zemljotresa;
- Nedovoljnog nivoa higijensko-sanitarne zaštite;
- Nepoštovanja ugovora;
- Obmane u komercijalnim transakcijama;
- Štrajkove zaposlenih.

Putnici i posetioci mogu ugroziti ličnu i bezbednost domaćina kroz:

- Primenu opasnih sportova, nebezbedne vožnje, konzumiranje nebezbedne hrane i pića;
- Narušeno zdravlje;

⁵⁴ Dobranović Ž., *Opći pristup sigurnosti u turizmu, Sigurnost i samozaštita u turizmu, Defimi, Zagreb.2003. str.6-8*

⁵⁵ Živković R., *Ponašanje i zaštita potrošača u turizmu*; Fakultet za turistički i hotelijerski menadžment; Univerzitet Singidunum; Beograd, 2010., str.188

- Izazivanje konflikta sa lokalnim stanovništvom, kršenjem zakona;
- Kriminalne radnje;
- Posete opasnim mestima;
- Gubitak dokumenata, novca itd.

Fizički rizici iz okruženja nastaju kao posledica:

- Ukoliko turisti nisu svesni rizika prirodnih karakteristika destinacije, npr. flore i faune;
- Ukoliko nisu preduzeli profilaktičke mere, npr. vakcinisanje;
- Poseta zabranjenim i opasnim područjima;
- Izlaganja opasnostima prilikom prirodnih katastrofa i epidemija.⁵⁶

Opasnu pretnju predstavlja po turiste ekološka katastrofa i epidemija. Savremene države su pristupile proširenju koncepta bezbednosti kako bi se moglo odgovoriti na nove izazove. Spektar savremenih društvenih vrednosti koje su zaštićene pravnim poretkom, pored osnovnih: zaštita života, političkih sloboda i prava, u evropskim državama su istaknute ekološke vrednosti kao osnov za očuvanje zdrave socijalne i ekonomske baze.

⁵⁶ Živković R.- „Ponašanje i zaštita potrošača u turizmu“ ; Fakultet za turistički i hotelijerski menadžment; Univerzitet Singidunum; Beograd, 2006. god., str.188

5. Istraživanja o sigurnosti i bezbednosti na putovanju

5.1. Istraživanje Udruženja za korporativna putovanja-ACTA

Istraživanje sprovedeno putem Interneta o sigurnosti i bezbednosti na putovanju, sprovedeno februara 2009. godine od strane ACTE (Udruženje za korporativna putovanja) je pokazalo da je preko milion putovanja u proteklih godinu dana bilo realizovano ka razvijenim zemljama. Dvanaest vrsta rizika je bilo obuhvaćeno i spomenuto u upitnicima. Incident se definiše kao pojava koja ometa završetak ili ispunjenje svrhe putovanja, osim redovnih putovanja koji su zbog nekih razloga pomereni. Upitnici su bili podeljeni u tri dela. Prvi deo se odnosio na pitanja vezana za tipična putovanja: broj putovanja u 20 top destinacija, procenat putovanja u razvijene zemlje, prosečna dužina putovanja i rang hotela. Drugi deo se odnosio na tri pitanja vezana za putne rizike, kolika je sigurnost na putovanju i kolika je bezbednost na destinaciji. Rezultati su pokazali da većina kompanija putuje u razvijene zemlje, a na pitanje kolika je bezbednost na destinaciji, kompanije sa najveći brojem putovanja nisu htele da odgovore na ovo pitanje. Rezultati upitnika su bili rangirani prema 12 incidenata, gde je na milion putovanja išlo za zločine i saobraćajne nezgode i prema 13 incidenata na milion putovanja za vremenske nepogode. Dok 61% obuhvata terorizam kao faktor koji ometa putovanje. Ovo su bili rezultati kompanija koje su dale odgovor o sigurnosti na destinaciji.⁵⁷

5.2. Istraživanje Elsevier science na Tajlandu

Druga vrsta istraživanja, koju je sprovedla Elsevier⁵⁸, bila je sprovedena da bi se proučio uticaj rizika od bolesti i terorizma na Tajlandu i kako to utiče na turizam. Odnosno: identifikovati probleme sa kojima su turisti suočeni kada putuju u inostranstvo, da se istraži da li subjektivni rizici utiču na odluku turista tokom krize, da istraži da li prethodna loša iskustva utiču na turiste i u kojoj meri i da se utvrdi uticaj SARSa, ptičijeg gripa i terorizma na ugostiteljstvo i na turističko putovanje. Za tu studiju je korišćeno kvantitativno i kvalitativno istraživanje u tri faze:

⁵⁷ <http://mtrc.asu.edu/publications/files/safety-and-security-of-corporate-travel-executives.pdf>

⁵⁸ www.elsevier.com/locate/tourman

- U prvoj fazi (kvalitativni pristup) je rađen intervju sa turistima koji su se vratili sa Tajlanda. Oni su trebali da navedu tri razloga zbog kojih ne treba ići na Tajland, gde su skoro svi naveli SARS, ptičiji grip i terorizam. Bilo je i onih turista koji nisu znali razliku između ptičijeg gripa i SARSA i kojima to nije poremetilo odmor, jer nisu imali znanje o tome i nisu pravili razliku. Drugi turisti koji su radili intervju nisu znali da su bili izloženi terorizmu jer nisu imali informacije, odakle bi saznali o problemima na destinaciji. Nakon ove faze, koja je bila pilot test, došlo se do bitnih informacija za projektovanje upitnika o tome koliko je rizično putovati na Tajland.
- U drugoj fazi (kvantitativni pristup) su korišćene informacije iz prve za pravljenje upitnika koji je sadržao četiri dela, o riziku na putovanju, o ponašanju turista, o namerama turista prilikom kupovine internacionalnih putovanja i o izabrane demografije. Rezultati nakon ove druge faze su pokazali, da je većina ispitanika bilo ženskog roda, menadžeri i studenti. Više od polovine je odgovorilo da ne bi brinuli o sopstvenoj bezbednosti ako bi putovanje platili skupo. Takođe, više od pola ih je odgovorilo da bi radije oputovali u menje rizičnu destinaciju nego da prestanu skroz da putuju. A mali broj ispitanika je odgovorilo da bi prestalo skroz da putuje da postoji opasnost od terorizma.
- U trećoj fazi (kvalitativni pristup) su bili intervjuisani zaposleni u ugostiteljstvu na Tajlandu. Ova faza je bila završena tokom trećeg napada ptičijeg gripa i treće godine terorizma od januara do maja 2006. godine. Rezultati treće faze su doveli do dubljeg uvida u temu koja se razmatrala i uslugama koje su pružane.

Na osnovu ovog istraživanja došlo se do informacija da je SARS imao negativan uticaj na poslovanje turističke idustrije. Iako su se tokom te krize prodavali aranžmani po nižim cenama, turističke agencije su i dalje bile na gubitku. Kada je u pitanju ptičiji grip, nije se osetila velika kriza i putovanja se nisu toliko smanjila, jer su tursisti bili putem medija obavešteni o merama preventive. A kada je u pitanju terorizam, on nije imao nikakav uticaj na turističke odluke da oputuju na Tajland. Osim, u rizortima koji su bili smešteni na 500 km od terorističkih napada, osetilo se neznatno smanjenje turista.⁵⁹

⁵⁹ www.elsevier.com/locate/tourman

6. Bezbednost turista u hotelima

Sve češći razlog zbog kojeg se turista opredeljuju za neku destinaciju pored atraktivnosti, cene, povezanosti i kvaliteta usluge je i bezbednost i sigurnost te destinacije. Pored sigurnosti određene destinacije, sigurnost u hotelima je još jedan od elemenata, koji u velikoj meri može da utiče na odluku gde će gost boraviti.⁶⁰

Zato da bi turista bio sigurniji u svoju odluku o putovanju definisana su neka prava klijenata vezana za rezervaciju, eventualan otkaz rezervacije i boravak u hotelima:

- Svako putovanje je povezano sa određenim zdravstvenim rizicima. Većina ovih rizika se može izbeći ili znatno redukovati odgovarajućom edukacijom, promocijom zdravlja, prevencijom bolesti i zaštitom okoline. Te aktivnosti zahtevaju odgovornost svih pojedinaca uključenih u turizam, kako posetioca i domicilnog stanovništva s jedne strane i turističkih radnika, zdravstvenih profesionalaca i lokalnih vlasti s druge strane. Za vreme boravka u hotelu, hotelijer je dužan da vodi računa o bezbednosti i zdravlju gostiju. Ako se gost, na primer, povredi zbog lošeg osvetljenja, vlažnog poda za to odgovornost snosi hotelijer.
- Rezervacija se može obaviti na dva načina: obična rezervacija-telefonom se usmeno dogovore uslovi, klijent ostavi ime i prezime i u tom slučaju postoji obaveza hotelijera da ispuni dogovoreno, dok se potrošač u bilo kom trenutku može predomisli. Poželjno bi bilo potvrditi rezervaciju faksom kako bi ostao pisani trag potvrđene rezervacije gde se preciziraju svi uslovi. Ugovor rezervacija- sve je češća praksa da se prilikom rezervacije uplati određena suma novca kao kapara, ili ostavi broj kreditne karte kao garancija. U tom slučaju i potrošač se obavezuje da će koristiti uslugu smeštaja, a hotelijer da će mu tu uslugu pružiti.
- Ukoliko hotelijer nije u mogućnosti da klijentu sa potvrđenom rezervacijom obezbedi smeštaj, u obavezi je da mu obezbedi smeštaj u drugom hotelu iste ili više kategorije, što je ujedno i najbolje rešenje, ili da mu da nadoknadu štete.
- Obaveza klijenta je da se prijavi u hotel, a ukoliko to ne ispuni, najčešća je praksa da se naplati prva noć, odnosno cena jednog noćenja, tako da se time izbegne i šteta za hotelijera za slučaj da „zaboravni“ turista ne otkaže na vreme rezervaciju.

⁶⁰ <http://www.turizaminfo.hr/hoteli-moraju-biti-sigurni-za-goste-i-za-zaposlenike>

- Za vreme boravka u hotelu, hotelijer je dužan da vodi računa o bezbednosti i zdravlju gostiju. Ako se gost npr. povredi zbog lošeg osvetljenja, vlažnog poda, i sl. odgovornost za to snosi hotelijer, ali on neće snositi odgovornost ako je do povrede došlo zbog neprimerenog ponašanja gosta.
- Što se tiče predmeta i ličnih stvari gostiju, hotelijer se ne može ograditi od odgovornosti koju ima u za slučaj oštećenja ili nestanka. Hotelijer snosi odgovornost za stvari koje nisu predate na čuvanje i ona je ograničena (odšteta ne može biti veća od vrednosti sto puta od cene noćenja).
- Neograničena odgovornost je za stvari koje su predate na čuvanje i iz tog razloga hotelijer može da prihvati na čuvanje predmete od prevelike vrednosti. Preporučuje se korišćenje sefova.
- Što se tiče vozila, nije dovoljno samo da se nalazi na parkingu ili u garaži hotela, već je potrebno napraviti poseban dogovor o čuvanju vozila koji podrazumeva ostavljanje ključa hotelijeru i naknadu za čuvanje.⁶¹

Primer napada na hotel :

- 🚩 U Pakistanu je 2008. godine ubijeno 53 ljudi tokom bombaškog napada na Hotel Marriot u Islamabadu.⁶²

Da bi se turisti osećali bezbedno na nekoj destinaciji, moraju da steknu utisak kao da su kod svoje kuće, da osete udobnost i kvalitet dobrodošlice. To omogućava turistima da se nasele u nepoznato okruženje i da uživaju bez straha. A sa druge strane zaposleni u hotelu mora da uzmu tu odgovornost ozbiljno, ali da ispoštuju lokalne i nacionalne propise. Bezbednost u hotelima se zasniva na posedovanju:

- Znaka za izlaz u slučaju opasnosti
- Osvetljenje izlaza iz hotelski zgrade
- Alarm sistem i sistem za dojavu požara
- Sistem za suzbijanje požara
- Genaratora u slučaju nestanka električne energije⁶³

⁶¹ Živković R.- „Ponašanje i zaštita potrošača u turizmu“ ; Fakultet za turistički i hotelijerski menadžment; Univerzitet Singidunum; Beograd, 2006., str. 189

⁶² www.today.reuters.com

⁶³ <http://www.4hoteliers.com/features/article/7612>

Značajni elementi programa sigurnosti u svakom hotelu su sledeći:

- Stalna kontrola
- Odgovarajuća i adekvatna obuka osoblja
- Odgovarajuće osvetljenje i održavanje
- Eksterna kontrola
- Edukacija zaposlenih
- Efikasan sistem za zaključavanje soba za goste
- Pisane i sigurnosne politike i procedure
- Uspostavljanje brzih odgovora na incident i sprovođenje korektivnih akcija⁶⁴

6.1. Sigurnost u hotelskim sobama

Kada se odredi turistička destinacija, turista određuje hotelski smeštaj u kojem će boraviti. Treba da izabere hotel poznatog hotelskog lanca u centru grada u koji putuje. Pravila hotela treba da budu unapred poznata:

- Kada se turista smesti u hotelsku sobu važno je da vodi računa da hotelska vrata budu zaključana
- Svi uređaji treba da budu isključeni pre izlaska iz sobe, jer se na taj način sprečavaju eventualne neželjene posledice
- Vredne stvari treba ostaviti u sefu
- Gosti treba da se upoznaju sa požarnim izlazima i mestima na kojima se nalaze protivpožarni aparati⁶⁵

Kvalitet hotelskih usluga podrazumeva: besprekoran rad uređaja i opreme, besprekorne ljude, besprekorne proizvode i usluge, uklanjanje svih nevolja i problema gostiju čim se pojave, uljudno ponašanje, poverenje u hotelsko osoblje, sigurnost gostiju, poštovanje termina, pravi odnos cene i nivoa kvaliteta hotelskih usluga, sprečavanje grešaka osoblja, dobro informisanje gostiju i dr. U tom smislu proizvode i usluge možemo posmatrati kao skup opipljivih i neopipljivih atributa (materijalnih i nematerijalnih) koji zadovoljavaju neku potrebu gosta. Marketinški definisan hotelski proizvod zamenjuje masovni turizam i jednoličnost u hotelskoj

⁶⁴ <http://hotelmule.com/forum>

⁶⁵ <http://hotelmule.com/forum>

ponudi i to na način da zadovoljava specifične potrebe unapred određenih tržišnih segmenata. Jasno definisanje proizvoda je važno jer osigurava prepoznatljivost na tržištu i prednost u odnosu na konkurenciju, omogućuje strukturirane i efikasne prodajne i promotivne aktivnosti što rezultira većim zadovoljstvom gostiju i njihovom lojalnošću. Proizvod definiše hotel prvo u marketinškom (stil, image, ciljna grupa, kanali distribucije, cenovna strategija, brand i sl.), a potom i u fizičkom smislu (veličina, kategorija, stil, sadržaji i usluge i sl.), a često služi i kao tehnički zadatak odnosno podloga za izradu arhitektonskih rešenja.⁶⁶

Podizanje kvaliteta smeštaja, profilisanje ponude i sl., za posledicu ima da se na tržištu sve manje nude hoteli opšteg tipa, već hoteli čije razvrstavanje uključuje i specijalizaciju na niz podvrsta, kao što je:

- Poslovni (Business). Hotelski smeštaj specijalizovan je za poslovne ljude.
- Konferencijski. Hotel specijalizovan za održavanje sastanaka. Važnije ponudene usluge čine: sale za sastanke, odgovarajuća tehnička oprema i usluge, poslovni centar, centar za komunikaciju, usluge hrane i pića.
- Klub hotel. Hotel specijalizovan za rekreativne i sportske aktivnosti koji nudi najmanje 5 različitih sportskih sadržaja: sportski treneri, celodnevni rekreativni programi za decu i odrasle, sa animatorima, bazenima, fitness centrima, vrtovima i zelenim površinama, restoran sa uslugom ručka i večere koji uključuje sportski dijetetski jelovnik.
- Porodični hotel. Smeštaj usmeren ka porodicama sa decom. Standardi podrazumevaju međusobno povezane sobe, sa mogućnošću dodavanja dečjeg ili dodatnog kreveta, usluga čuvanja dece i dečji klub sa licima za nadzor, igraonicama za bebe i decu, restoran s jelovnicima za decu i dr.
- Hotel za osobe trećeg doba. Smeštaj je prilagođen za pružanje specijalnih sadržaja i usluga osobama trećeg doba. Boravak mora da osigura zdravlje i bezbednost, kao i zabavni program posebno prilagođen ovoj vrsti korisnika.
- Mali i prijateljski. Ograničen broj soba i određeni ambijetalni detalji.
- Zdravlje i fitness. Smeštaj prilagođen pružanju kombinovane opreme i usluga za brigu o zdravlju i kondiciji. Smeštaj za zdravlje i kondiciju usmeren je isključivo na rekreaciju (nije usko namenjen pitanjima zdravlja).

⁶⁶ Živković R.- „Zaštita potrošača u hotelijerstvu“ ; Fakultet za turistički i hotelijerski menadžment; Univerzitet Singidunum; Beograd, 2007. god., str. 8

Kako današnji korisnici raspolažu sa dosta informacija i imaju dosta iskustva, oni traže nove doživljaje i žele da stiču nova iskustva. Zato da bi hotel odgovorio na njihove zahteve neophodno je da svoj sadržaj prilagodima gostima, kao što su specifične ponude u sobama, usluge hrane i pića i dr.⁶⁷

6.1.1. Sigurnost u hotelskim bazenima

Veoma je važna sigurnost bazena, s obzirom na to da se mnoge nesreće događaju u istom. Jako je važno da se gosti hotela informišu o čestim rizicima u bazenima, i kako da do njih ne dođe. Važno je da na bazenu bude spasilac, da se pazi na klizavim delovima bazena (kod ulaza), da deca uvek budu nadgledana od strane odraslog, da se i deci saopšte svi mogući rizici, da se ne skače u vodu i ne roni i da voda bude čista.⁶⁸

6.1.2. Prevencija krađe

Prevencija od krađe počinje temeljnom i učestalom kontrolom ključeva od strane osoblja sa recepcije. Ključeve gostiju držati na sigurnom mestu, van dometa neovlašćenih osoba. Ukoliko recepcija nije uvek pod nečijim nadzorom, ključevi ne bi trebalo da se izdaju bez identifikacione provere. Ulaz bi trebalo obezbediti sa video nadzorom. Sistem kartica, sigurnosne brave, sefovi u sobama i na recepciji, fizičko obezbeđenje, dobro osvetljenje u hotelu, ulazima-izlazima, parkingu, omogućava kontrolu i svodi moguće krađe na minimum.⁶⁹

6.2. Bezbednost od požara

Svi objekti za pružanje usluga smeštaja i ishrane i pića moraju da ispunjavaju propisane uslove utvrđene posebnim propisima za zaštitu od požara. Svi hoteli moraju da imaju:

- Protivpožarnu zaštitu u skladu sa propisima, u svim sobama, javnim prostorijama, kuhinji i hodnicima
- Odgovarajuće izlaze da bi se obezbedio izlazak iz zgrade svim licima u slučaju požara

⁶⁷ Živković R.- „Zaštita potrošača u hotelijerstvu“ ; Fakultet za turistički i hotelijerski menadžment; Univerzitet Singidunum; Beograd, 2007. god., str.12-13

⁶⁸ www.beuc.org (BEUC- The European Consumers Organization)

⁶⁹ Živković Radmila- „Zaštita potrošača u hotelijerstvu“, Fakultet za turistički i hotelijerski menadžment; Univerzitet Singidunum; Beograd, 2007., str. 182-198

- Signalizaciju koja se redovno proverava i koja mora da bude osvetljena sa sopstvenim izvorom energije
- Creva za vodu visokog pritiska, detektore dima i hidrante koji se moraju redovno proveravati ⁷⁰

Međutim, većina hotela nije otporna na vatru kao neki moderni hoteli. Unutrašnji materijali su uglavnom ekstremno zapaljivi. Putevi za bekstvo u slučajevima požara možda nisu obeleženi u hodnicima, a izlaza je uglavnom malo. Takođe, takvi hoteli verovatno oskudevaju i u opremi za gašenje požara, zalihama vode, detektorima dima, automatskim vodenim topovima. Gosti hotela moraju da prihvate odgovornost za svoju bezbednost, kao i za bezbednost svoje porodice. Treba planirati unapred.

Preporučene mere opreza su sledeće:

- Boraviti u najmodernijim hotelima
- Tražiti niže spratove
- Raspitati se da li hotel ima detektore dima i automatske vodene tuševe, kao i alarme za požare (upoznati se sa lokacijama ove opreme)
- Uvek nositi bakterijsku lampu sa sobom
- Pročitati plan za evakuaciju u slučaju požara
- Locirati dva izlaza u blizini sobe u kojoj se odseda
- Locirati alarme za požare u okolini sobe
- Nikada ne konzumirati cigarete u krevetu kada dođe do požara, treba preduzeti sledeće:
- Ukoliko požar izbiye u sobi, brzo izaći, zatvoriti vrata, uključiti alarm i obavestiti recepciju
- Uvek koristiti stepenice, nikada lift
- Ukoliko požar nije u sobi, brzo izaći ukoliko je to bezbedno
- Kada se izlazi iz sobe, prvo proveriti sa zadnjim delom šake temperaturu vrata; ukoliko su topla to znači da je požar ispred sobe u hodniku; u tom slučaju ne otvarati vrata, već zapečatiti vrata mokrim peškirom ili pokrivačima, zatim isključiti sve električne elemente u sobi (fen, klima), pozvati recepciju i dati svoju lokaciju; ako su vrata hladna onda brzo izaći iz sobe i krenuti ka najbližem izlazu.

⁷⁰ Živković Radmila- „Zaštita potrošača u hotelijerstvu“ ; Fakultet za turistički i hotelijerski menadžment; Univerzitet Singidunum; Beograd, 2007., str.9

Prema statističkim podacima iz Velike Britanije, požar izbija u:

- Kuhinji 23%
- Sobi 18%
- Skladištima 12%
- Hodnicima, holovima, liftovima 9%
- Barovima 4%
- Foajeima, salonima 4%

Najčešći uzroci požara su:

- Oprema za kuvanje 17,8 %
- Materijal za pušenje 17,4%
- Električni uređaji i kablovi 11,2%⁷¹

Protivpožarna zaštita obuhvata tri osnovna aspekta:

- Strukturalna zaštita, uključujući otpornost elemenata i komponenti uz ograničenje upotrebe zapaljivih materijala sa visokim stepenom površinskog širenja vatre
- Aktivna zaštita obuhvata uređaje za automatsku detekciju dima/vatre, uređaje za upozorenje i gašenje pri pojavi u bilo kom delu zgrade
- Putevi evakuacije su u vezi sa razdaljinom i vremenom neophodnim za siguran izlaz iz objekta uz identifikaciju i zaštitu puteva evakuacije⁷²

🚒 Na Kopaoniku je 2012. godine izbio požar u hotelu „Grand“ gde je bilo oko sedamdeset gostiju. Vatra je oštetila veliki broj soba, jedan deo krova i aperitiv salu. Do požara je došlo zbog ljudske nemarnosti, a velika šteta nije mogla da se spreči zbog malog broja vatrogasaca i nedovoljne tehničke opreme.⁷³

⁷¹ Živković Radmila- „Ponašanje i zaštita potrošača u turizmu“ ; Fakultet za turistički i hotelijerski menadžment; Univerzitet Singidunum; Beograd, 2006., str.191

⁷² www.safety.com

⁷³ www.smedia.rs

6.3. Sanitarni i zdravstveni zahtevi

Ovaj aspekt podrazumeva odgovarajuće osvetljenje i ventilaciju, održavanje pribora i opreme, svakodnevno čišćenje i dezinfekciju, dispoziciju otpadnih materija i ličnu higijenu osoblja, opremljenost i funkcionalnost objekta. Razlog za brigu u hotelu su kvalitet vode, temperatura i higijensko sanitarni nadzor u kuhinji. Objekti koji imaju sopstveni vešeraj i hemijsko čišćenje moraju poštovati sve zdravstvene i sanitarne propise. Zahtevi predstavljaju mere prevencije od zaraznih bolesti tokom zajedničkog boravka gostiju u hotelu.

Ostali zahtevi:

- Prilaz

Pešački, saobraćajni i prilaz za personal, treba da budu jasno odvojeni, označeni i kontrolisani. U hotelima u gradskim centrima trebalo bi obezbediti nekoliko parking mesta, udaljenih od saobraćajnih linija, kako bi se obezbedili što je moguće bolji uslovi za dolazak i odlazak gostiju;

- Staze i turistički objekti moraju biti prilagođeni hendikepiranim posetiocima

- Parking:

Svi objekti treba da imaju adekvatne parking prostore u skladu sa svojim načinom i stilom poslovanja. Otvoreni parking prostori treba da budu uređeni, dobro osvetljeni, čuvani i zaštićeni od sunca. Poželjne su kamere za nadzor parkinga;

- Uklanjanje otpada:

Otpad je problem savremene civilizacije i središnji problem zaštite okoline. Počeo je nastajati nastankom čoveka, a recipročno raste sa razvojem čovečanstva, posebno industrije. Otpad nije samo rezultat razvoja već i jasan otisak materijalnog društva, koje još ne zna veliku većinu ekoloških, klimatskih i zdravstvenih problema koje otpad nosi sa sobom.

- Turistička signalizacija

- Zaštita od buke⁷⁴

⁷⁴ Živković Radmila- „Zaštita potrošača u hotelijerstvu”, Fakultet za turistički i hotelijerski menadžment; Univerzitet Singidunum; Beograd, 2007., str. 182-198

7. Bezbednost informacionog sistema u hotelima

Da bi turista bio bezbedan u hotelu, pored navedenih mera bezbednosti, mora da postoji dobar informacioni sistem koji će sve informacije o gostima u hotelu, imati na jednom mestu i koji će zaštititi hotel od bilo kakvog spoljnog uticaja, koji bi mogao ugroziti bezbednost.

Priroda hotelskog poslovanja je takva da se svakodnevno dobijaju informacije o gostima za potrebe rezervisanja ili podrške lojalnosti. Najveću pretnju za hotel predstavlja krađa identiteta što predstavlja zloupotrebu ličnih podataka od strane trećeg lica u cilju sticanja lične koristi ili činjenja krivičnog dela. Da do ovog problema ne bi došlo razvijeni su PCI DSS (Payment Card Industry Data Security Standard) standardi od strane kompanija: Visa, MasterCard, American Express, Discover i JCB (Japan Credit Bureau), gde su postavljeni 12 ključnih zahteva pred organizaciju u cilju zaštite poslovnih informacionih sistema koji skladište, obrađuju i prenose podatke vlasnika kartice. I pored ovih standarda nije potpuna zaštita od narušavanja bezbednosti jer postoji prostor da hakeri ukradu poverljive informacije. Bezbednost informacione imovine se može postići implementacijom, uspostavljanjem, održavanjem i poboljšanjem sistema za upravljanje bezbednošću informacija (ISMS, ISO/IEC 27001 i 27002 standard). Prema standardima ISO/IEC 27001, ISMS (Information Security Management System) je namenjen za tretman rizika za bezbednost informacione imovine i utvrđivanje ciljeva i programa menadžment sistema bezbednosti informacija. Procesni pristup ISMS-a podrazumeva izradu ISMS politike zaštite, procenu rizika, definisanje obima ISMS, razvoj svesti o potrebi zaštite, obuke, edukacije i primenu tehnologije zaštite za umanjenje rizika na prihvatljiv nivo. Informaciona imovina se može definisati kao fizička imovina (sve što je opipljivo), informaciona imovina (informacije u štampanoj i elektronskoj formi, softver i podaci) i humana imovina (zaposleni, partneri...). Kada govorimo o bezbednosti informacione imovine odnosi se na sve resurse i imovinu organizacije, a može se definisati kao preduzimanje čitavog niza mera, kontrola zaštita i akcija u cilju zaštite informacija i njenih kritičnih tačaka, uključujući ljude, hardver i softver koji obrađuje, skladište i prenose te informacije.⁷⁵ Rizik je verovatnoća da će pretnja iskoristiti neku manu sistema i time ugroziti vrednost imovine. Glavne pretnje bezbednosti hotelskog informacionog sistema su hakovanje, virusi, socijalni inženjering i ovlašćeni korisnici hotelskog IS.

⁷⁵ Njeguš A. „Bezbednost informacione imovine u hotelskom poslovanju“, Seminar o zaštiti podataka o ličnosti u hotelskoj industriji, JPM & HORES, Beograd 2013. godine, str. 20

Najveći procenat napada na informacije se dešavaju u oblasti trgovine (15%) i turizma (23%), finansija (33%). Hotelijersko poslovanje je veoma atraktivno za napade hakera i prema postojećim istraživanjima više od 55% prevara sa kreditnim karticama se dešava upravo u ugostiteljstvu. Hakeri najčešće napadaju menadžere hotela koji imaju pristup osetljivim podacima hotela, a to su podaci o gostima i zaposlenima u hotelu. Finansijski rizici se nalaze, takođe, među prioritenim rizicima kao i pretnje od nezadovoljnih zaposlenih.

U sledećoj tabeli su prikazani rizici u hotelskom poslovanju.

Tabela 3: Rizici u hotelijerstvu⁷⁶

Spoljni rizici			Unutrašnji rizici
Strategijski rizici	Pravni i finansijski rizici	Ostali rizici	Operativni rizici
Rizik reputacije hotela (tzv. spaljivanje brenda, negativni publicitet, npr. širenjem neistina na društvenim mrežama)	Regulativna usklađivanja (promene vladinih zakona i propisa, fiskalna politika, pripremanje hrane, prodaja hrane i pića, higijena, licence ...)	Teroristički napadi (hoteli su meke mete jer im se može lako pristupiti)	Zdravlje i bezbednost gosta (poštovanje higijenskih standarda u pripremi hrane, bezbednost u bazenima, saunama, salonima ...)
Procena održivosti novog projekta (rizik izbora lokacije, poslovnog modela, kašnjenja u izgradnji, dobijanja dozvola ...)	Pravni rizici (odredbe, pravni postupci, tužbe i dr. što može negativno da utiče na poslovanje)	Politički rizici (promene u političkoj strukturi, nestabilnost vlade, valute, nacionalizacija ...)	Zdravlje i bezbednost zaposlenih (povrede na radu, bolesti, ...)

⁷⁶ Njeguš, A., „Bezbednost informacione imovine u hotelskom poslovanju“, Seminar o zaštiti podataka o ličnosti u hotelskoj industriji, JPM & HORES, Beograd 2013., str.20-22

Konkurencija (napredovanje konkurencije u pogledu poboljšavanja usluga, postojećih kapaciteta, snižavanja cena, boljim distribucionim kanalima i sl.)	Kreditni rizik (rizik davanja ili uzimanja kredita i njihovo kasno isplaćivanje)	Prirodne nepogode (požari, cunami, zemljotresi, građ. rat, kontaminacija...)	Regrutovanje i zadržavanje zaposlenih (zaposleni igraju stratešku ulogu)
Poslovni portfolio (npr. preterana zavisnost od određenog tržišnog segmenta ili geografske lokacije ...)	Devizni rizik (česte promene kursa, poslovanje na drugim međunarodnim tržištima ...)	Namerne pretnje čoveka (lažno predstavljanje, presretanje i ometanje)	Odnosi među zaposlenima (rešavanje konflikta, štrajkovi, ...)
Sezonalitet (hotelijerstvo je po prirodi sezonskog karaktera, te postoje rizici od različitih nivoa prihoda po sezonama)	Kamate i troškovi finansiranja (troškovi harmonizacije, promene u kamatnim stopama, uslovi finansiranja, cene...)	Pandemija (epidemija npr. ptičji, svinjski grip i dr. mogu dovesti do pada prometa)	Prevara (krađa, zloupotreba sredstava, pronevera, manipulacija finansijskih izveštaja, nezakonite radnje ...)
Promene ponašanja potrošača (sposobnost predviđanja i	Poštovanje zakona o zaštiti životne sredine (rizik od nepridržavanja	Ekonomski ciklusi (ekonomska kriza, niska aktivnost, ...)	Informacione tehnologije (zastarelost, neuspeh rada hardvera, softvera,

reagovanja na promene u preferencijama i potražnji potrošača)	ekoloških zakona i propisa ...)		interneta ...)
Ugovaranje i zajednička ulaganja (<i>joint venture</i>)	Porezi (promene poreza, boravišnih taksi, PDV-a ...)		Kontinuitet lanca snabdevanja
Kanali prodaje i rezervacioni sistemi (rizik povećane zavisnosti, visoke provizije ...)	Nelikvidnost nekretnine i imovine (rizik investicija u nekretnine ...)		Troškovi (operativni troškovi, održavanje vozila, popravke ...)
			Bezbednost infrastrukture (klimatizacija, vatrogasna služba, lift, vodovod, osvetljenje, pranje vešta ...)

Izvor: Njeguš, A. (2013) „Bezbednost informacione imovine u hotelskom poslovanju“, Seminar o zaštiti podataka o ličnosti u hotelskoj industriji, JPM & HORES, Beograd

Rukovodeći menadžment kompanije najčešće koristi informacione tehnologije za obezbeđenje podataka o nabavci ulaznih materijala i sirovina, stanju zaliha, plasmanu i prodaji, naplati potraživanja, naručiocima roba i usluga, budžetu i drugim podacima neophodnim za brzo i kvalitetno odlučivanje. Svedoci smo da je danas gotovo uobičajna praksa za brzo i kvalitetno odlučivanje i gotovo uobičajna praksa da se mobilni telefoni, elektronska pošta, video konferencije široko primenjuju u poslovnoj komunikaciji. U proteklih deset godina, čak i u našoj sredini, koja važi za nerazvijeno informatičko evropsko društvo, povećanjem broja profesionalnih računara po glavi stanovnika, upotrebom i širenjem javne mreže Interneta, kao

posledica da je u praksi je zaživelo elektronsko trgovanje kao termin za sve transakcije ostvarene „elektronskim putem“, odnosno putem računara.⁷⁷

Ovakav prodor informacionih tehnologija i elektronske trgovine prividno je umanjio ne ne mali jaz između visoko razvijenih i nerazvijenih društava. To je omogućilo šansu za ravnopravno poslovanje i velikim i malim zemljama odnosno kompanijama velikih i malih kapaciteta. Državne uprave prikupljaju i analiziraju ogromne količine podataka koristeći informacione tehnologije što dovodi do pružanja kvalitetnije usluge građanima. Elektronska vlada omogućava suštinsku transformaciju ogromog državnog aparata, organizovanog i ustoličenog tako da prvenstveno zadovolji zahteve i potrebe birokratskog aparata u jednu modernu, efikasnu i jeftinu vladu informatičkog doba, po funkcijama usaglašenu sa potrebama građana. Elektronska vlada koristi računarske i telekomunikacione tehnologije sa ciljem radikalnih izmena u pružanju servisa građanima i javnosti, poslonim subjektima, zaposlenima u upravi i drugim vladinim organizacijama i resorima.

7.1. Značaj informacionih sistema u hotelima

Efikasan sigurnosni i bezbednosni sistem u hotelima podrazumeva integrisani sistemski pristup, koji obezbeđuje zaštitu za goste hotela, zaposlene i javnost, stejkholdere i zaštitu turističke destinacije. Odeljenje za bezbednost u hotelima se sastoji od menadžera za bezbednost, službenika za bezbednost, obezbeđenja i vratara. Struktura, veličina i nivo izveštavanja obezbeđenja varira od hotela do hotela. Upravljački sistem treba da uspostavi procedure koja će voditi ka bezbednosm funkcionisanju hotela, a svi zaposleni treba da budu obučeni i da poznaju odgovarajuće bezbednosne strukture koje će pomoći u zaštiti gostiju.

Drugi nivo sigurnog i bezbednog menadžmenta treba da bude odžavan na nivou industrije. Lokalne hotelske asocijacije i policijske snage treba da sarađuju sa hotelima u cilju osiguranja sigurnosti i bezbednosti. Treći nivo menadžmenta je nacionalni nivo, što uključuje poštovanje pravnih akata i pomoć civilnih odbrambenih snaga kada je reč o požaru i drugim opasnostima. Sistem zasnovan na tri nivoa menadžmenta treba da obezbedi okvir za bezbednost i upravljanje bezbednošću u hotelu.⁷⁸

⁷⁷ <http://www.cqm.rs/2011/2/pdf/28.pdf>

⁷⁸ Leong Choon Chiang, *Strategies for Safety and Security in Tourism, The Journal of Tourism Studies*, Vol. 11, No. 2, (Singapore: Nanyang Business School, 2000.), *cmp.* 43-46

7.2. Propisi i standardi sigurnosti i zaštite gostiju

Propisivanje standarda u hotelima neophodno je kako bi se osiguralo potpuno upravljenje kvalitetom. Date standarde su dužni da poštuju i sprovode svi zaposleni, ali i svi gosti hotela. Sigurnost i zaštita gosta obuhvata sve aktivnosti koje su usmerene ka tome da spreče sve što može da ugrozi život, zdravlje i imovinu gosta. To znači da se treba pridržavati svih mera da se gost u hotelu oseća udobno.

Standarde sigurnosti i zaštite turista u hotelima treba stalno unapređivati i proveravati, kao i izvršiti njegovu redovnu kontrolu i merenje. Svaki hotel je u obavezi da poseduje pravila i postupke za sve moguće sličajeve rizika koji ugrožavaju sigurnost posla. Potrebno je da se osigura da svi zaposleni, kao i gosti hotela dobiju pisana pravila i postupke koje je neophodno poštovati. Potrebno je napomenuti da se pisana pravila hotela zasnivaju na postojećim eksternim zakonima i internim pravilima hotela.

Postoje eksterni i interni standardi i propisi u hotelima koji imaju za cilj obezbeđenje sigurnosti turista u hotelima. Eksterne standarde je propisala Međunarodna organizacija za standardizaciju, a oni se odnose na zaštitu okoline i zdravlja (kvalitet vazduha, vode i zemlje, zaštita od buke, vibracije, požara, kriminala itd.). Interne standarde osigurava menadžment hotela, a za njihovo sprovođenje je potrebno da se osiguraju i ulože novčana sredstva u odgovarajuću opremu (kartica za vrata, TV kamere, mikrosenzori, alarmi za požar i dim itd.).⁷⁹

7.3. Savremeni sistemi tehničke zaštite u hotelima

Na razvijenim tržištima, na kojima su svi propisani sistemi zaštite već implementirani, hotelijeri povećavaju nivo sigurnosti za turiste, ulaganjem u nove tehnologije. Investicija hotelijera u sisteme tehničke zaštite se isplate jer dolazi do uštede energije, smanjivanja svih mogućih troškova i jednostavnosti upravljanja, a istovremeno su turisti zadovoljniji jer je njihova sigurnost u hotelu veća.

Sistemi „safety“ odnose se na zaštitu ljudi i imovine od nesrećnog slučaja ili elementarne nepogode u smeštajnim objektima su uglavnom obavezni, a podrazumevaju niz uobičajnih načina zaštite gostiju i osoblja. To su SOS sistemi za poziv u nuždi koji mora imati svako

⁷⁹ Holjevac Avelini I., „Upravljanje potpunim kvalitetom u turizmu I hotelskoj industriji“, Fakultet za turistički i hotelijerski menadžment, Opatija, 2002., str. 131-133

hotelsko kupatilo, evakuacijska i panik rasveta kojom se označavaju evakuacijski putevi, sistem koji omogućava nesmetanu evakuaciju u slučaju požara, sistem gašenja požara itd.

Sa druge strane „security“ se primenjuju zbog zaštite ljudi i imovine od zlonamernog delovanja trećih ljudi. Za prevenciju većine rizika moraju da se angažuju hotelijeri, koji to čine ugradnjom različitih sistema tehničke zaštite u svoje objekte prvenstveno sa ciljem veće sigurnosti gostiju i osoblja. To su sistemi protiv provala s centralnom dojavom, videonadzori koje efikasno nadgleda krađe u prostorijama s većom fluktuacijom ljudi, sistemi za kontrolu gostiju i osoblja.

Hoteli koji imaju veći broj soba imaju centralizovan sistem kontrole pristupa u sobe. Ovaj sistem obuhvata i pristup parking, garaži i drugim objektima u sklopu hotela, a može imati ulogu evidencije potrošnje gostiju. Koristi se i za evidenciju radnog vremena osoblja i pristupa prostorijama u kojima nije dozvoljen ulaz. Uz pomoć ovog sistema uspešno se rešava i problem neovlašćenog ulaska ljudi i vozila u turističkim naseljima i kampovima.⁸⁰

⁸⁰ Dončević R., „Suvremeni sustavi tehničke zaštite u hotelima“, str.1-4
preuzeto sa http://www.alarmautomatika.com/documents/files/clipping/2013/2013-09_alarm-automatika-sigtur.pdf

8. Osnovni pojmovi upravljanja rizicima

Upravljanje rizikom je proces koji omogućava upravi organizacije da se uravnoteže operativni i ekonomski troškovi zaštitnih mera za očuvanje sigurnosti informacionog sistema organizacije. Upravljanje rizikom je proces identifikacije rizika, procene rizika i preduzimanja koraka da se rizik smanji na prihvatljivi nivo. Upravljanje rizikom zahteva analizu rizika u odnosu na potencijalne koristi, uzimanje u obzir alternative i primenu onoga što se utvrdi kao najbolji tok akcije.

Proces upravljanja rizikom se zasniva na sledećim principima:

- Procena rizika i određivanje bezbednosnih zahteva
- Uspostavljanje sistema za centralno uparavljane rizikom
- Implementacija rentabilnih politika i kontrola zaštite
- Promovisanje svesti o potrebi i obuka
- Nadzor i kontrola sistema zaštite i evaluacija efektivnosti i usklađenosti

Važan faktor za efektivnu imlementaciju ovih principa je princip njihovog cikličnog povezivanja koji obuhvata tekuće faktore rizika u realnom vremenu. Razvojni životni ciklus sistema (System development life cycle – SDLC) ima pet faza:

- Uvođenje
- Razvoj ili nabavka
- Primena
- Rad ili održavanje
- Odbacivanje⁸¹

⁸¹ Doc.dr Lidija Barjaktarovic, *Upravljanje rizikom*, Univerzitet Singidunum, Beograd 2009., str.36

Tabela 4: Razvojni životni ciklus sistema ⁸²

SDLC faze	Karakteristike faze	Podrška putem upravljanja rizikom
Faza 1- Uvođenje	Izražava se potreba za informacionog sistema i dokumentuju se njegova svrha i cilj	Identifikovani rizici se koriste da podrže razvoj zahteva na sistem, uključujući i sigurnosne zahteve i sigurnosni koncept rada(strategiju)
Faza 2- Razvoj ili nabavka	Informacioni sistem je dizajniran, naručen, programiran, razvijen ili drugačije konstruisan	Rizici koji su identifikovani tokom ove faze mogu da se koriste da podrže sigurnosne analize informacionom sistema koji mogu dovesti do kompromisa u arhitekturi ili dizajnu za vreme razvoja sistema
Faza 3- Primena	Sigurnosne karakteristike sistema bi trebale biti konfigurisane, testirane i potvrđene	Proces upravljanja rizikom podržava procenu primene sistema u odnosu na zahteve i unutar radnog okruženja. Odluke donesene u pogledu identifikovanog rizika se mora primeniti pre rada sistema.
Faza 4- Rad ili održavanje	Sistem izvršava svoje funkcije. Tipično, sistem je modifikovan u procesu kroz dodavanje hardvera i softvera i kroz promene organizacionih procesa, politika i procedura	Aktivnosti upravljanja rizikom se izvode za periodičke aktivnosti, ponovne autorizacije sistema ili kad god su veće promene učinjene u informacionom sistemu u njegovom radnom, produktivnom okruženju
Faza 5- Odbacivanje	Ova faza podrazumeva odbacivanje informacija, hardvera ili softvera. Aktivnosti mogu podrazumevati, u ovoj fazi, premeštanje, arhiviranje, odbacivanje ili uništavanje informacija i odlaganje	Aktivnosti upravljanja rizikom se izvode za komponente sistema koje će biti odbačene ili zamenjene da bi se osiguralo da u hardver i softver pravilno odloženi, da su preostali podaci pravilno održavani i da je premeštaj sistema urađen na siguran

⁸² http://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf

	hardvera i softvera	način.
--	---------------------	--------

Izvor: http://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf

8.1. Procena rizika

Opšti model za analizu i procenu rizika

Odnosi sistema i okruženja i stepen kontrole koju neka organizacija može izvršiti na faktore okruženja sistema, u najvećoj meri zavisi od obima i inteziteta skupljanja informacija potrebnih za analizu i procenu faktora rizika.

Opšti model za analizu i procenu rizika sadrži tri konceptualne oblasti:

Upravljanje rizikom, procena rizika i neodređenost koja interaktivno deluje na procenu rizika. Procena rizika je prvi proces u metodologiji upravljanja rizikom. Organizacije koriste procenu rizika da bi odredile opseg potencijalnih pretnji i rizika koji prate jedan informacioni sistem kroz SDLC. Ova aktivnost pomaže da se identifikuju odgovarajuće kontrole za smanjenje ili eliminaciju rizika za vreme procesa ublažavanja rizika. Da bi se odredila verovatnoća budućih štetnih događaja, pretnje informacionom sistemu, moraju da se analiziraju zajedno sa potencijalnim ranjivostima i postojećim kontrolama. Uticaj se odnosi na veličinu štete koja može biti uzrokovana iskorišćavanjem ranjivosti od strane pretnje.

Metodologija procene rizika se sastoji od devet koraka:

- Karakterizacija sistema
- Identifikacija pretnji
- Identifikacija ranjivosti
- Analiza kontrola
- Određivanje verovatnoće
- Analiza uticaja
- Određivanje rizika
- Preporuka kontrola
- Dokumentovanje rezultata⁸³

⁸³ www.crnarupa.singidunum.ac.rs

U proceni rizika IT sistema, prvi korak je da se definiše obim napora. U ovom koraku, granice informacionog sistema se identifikovane, zajedno sa resursima i informacijama koje čine sistem. On karakteriše IT sistem i uspostavlja obim rizika, ocrtava operativne dozvole (akreditacije), granice i pruža informacije (na primer hardver, softver, sistem veze i pomoćno osoblje) od suštinskog značaja za definisanje rizika. U drugom koraku identifikacije, definiše se izvor pretnji za uspešno vršenje određene ugroženosti. Ranjivost je slabost koja se može slučajno ili namerno aktivirati ili eksploatisati. Cilj je da se identifikuju potencijalne pretnje- izvori i sastaviti spisak potencijalnih pretnji koji se mogu primeniti na IT sistema koji se ocenjuju.

Tabela 5: Ljudske pretnje- izvori, motivacije, opasnosti

Pretnje- izvori	Motivacija	Opasnosti
Haker	Izazov, ego, pobuna	Upad u sistem, neovlašćen pristup sistemu
Računarski kriminal	Uništavanje informacija, neovlašćeno menjanje podataka	Lažna dokumenta, presretanje
Terorisanje	Ucena, iznuda, osveta	Bomba, informaciono ratovanje
Industrijska špijunaža	Konkurentska, ekonomska špijunaža	Krađa informacija
Insajderi (slabo, obučeni, nezadovoljni, bivši zaposleni)	Radoznalost, monetarni dobitak, slučajna greška, osveta	Ucenjivanje, zloupotreba i krađe, sabotaza sistema

Izvor: <http://www.cqm.rs/2011/2/pdf/28.pdf>

Treći korak predstavlja analizu opasnosti, informacioni sistem mora da sadrži analizu ranjivosti u vezi sa sistemom životne sredine. Cilj ovog koraka je da se razvije lista ranjivosti sistema (nedostatke ili slabosti) koji mogu da budu iskorišćeni od strane potencijalnih pretnji- izvora.

Cilj sledećeg koraka je da se analiziraju kontrole koje su sprovedene, ili su u planu za implementaciju, od strane organizacije kako bi se smanjile ili eliminisale mogućnosti od opasnosti. U petom koraku određujemo ocenu verovatnoće po utvrđenom kriterijumu i usvojenoj gradaciji, najčešće treći nivo, peti ili deseti nivo. Sledeći korak u merenju nivoa rizika je da se utvrdi uticaj negativnih posledica uspešnog ostvarivanja ugroženosti (pretnje). Pre početka analize uticaja, neophodno je dobiti sledeće potrebne informacije:

- Sistem misije- (na primer, procese obavljaju informacioni sistemi)
- Sistema i podataka kritičnosti (na primer, sistema vrednosti)
- Sistema i podataka osetljivosti

Svrha sedmog koraka je da proceni stepen rizika u IT sistemima. Određivanje rizika za određenu opasnost:

Tabela 6: Razmera rizika- Visoka (>50 do 100), srednja (>10 do 50), niska od (1 do 10)

Verovatnoća pretnje	Niski	Srednji	Visoki
Visoka	Niska $10 \times 1.0 = 10$	Srednja $50 \times 1.0 = 50$	Visoka $100 \times 1.0 = 100$
Srednja	Niska $10 \times 0.5 = 5$	Srednja $50 \times 0.5 = 25$	Srednja $100 \times 0.5 = 50$
Niska	Niska $10 \times 0.1 = 1$	Niska $50 \times 0.1 = 5$	Niska $100 \times 0.1 = 10$

Izvor: <http://www.cqm.rs/2011/2/pdf/28.pdf>

Osmi korak je kontrola koja bi mogla ublažiti ili eliminisati identifikovane rizike, na odgovarajući način poslovanja organizacije. Cilj kontrole je da se smanji nivo rizika u informacionim sistemima i podacima na prihvatljiv nivo. Sledeće faktore treba uzeti u obzir:

- Efektivnost
- Zakonodavstvo i regulativa
- Organizaciona politika
- Operativni uticaj

- Sigurnost i pouzdanost ⁸⁴

Kada je procena rizika završena, rezultati treba da budu dokumentovani u službenom izveštaju. Izveštaj procene rizika je izveštaj koji pomaže menadžmentu, misiji vlasnika, donose odluke o politici, budžetu i izmeni u operativnom sistemima upravljanja. Za razliku od revizije ili istrage izveštaja, izveštaj procene rizika ne bi trebalo da bude predstavljen na optužujući način, već kao sistemski i analitički pristup procene rizika, tako da će više rukovodstvo razumeti rizike i rasporediti sredstva da se umanje i ispravi potencijal gubitak. Za sve kompanije je neophodno da imaju osnovnu liniju sigurnosti koja će im pružiti minimalni nivo zaštite. Na primer, napadi kompjuterskih virusa mogu zapretiti bilo kojoj lokalnoj mreži kao i pojedinim računarima. Oni treba da imaju backup sisteme koji će ih zaštititi od gubitka ili uništavanja informacija i koji će osigurati fizičku zaštitu ličnih podataka i opreme.⁸⁵

→ **Karakterizacija sistema**

U proceni rizika za neki informacioni sistem, prvi korak je definisati cilj poduhvata. U ovom koraku identifikuju se granice informacionog sistema, zajedno sa uređajima i informacijama koji čine sistem. Karakterizacijom informacionog sistema se ustanovljava cilj procene rizika, daju se osnovne informacije za definisanje rizika. Najpre je potrebno prikupiti informacije o samom sistemu: hardveru, softveru, podaci i informacije, osoblje koje odžava i koristi informacioni sistem, kritičnost sistema i podataka, osetljivost sistema i podataka. Mogu se koristiti sledeće tehnike prikupljanja informacija: upitnik, intervjui odgovornog osoblja, upotreba automatskih skenirajućih aparata. Očekivani izlaz iz ovog koraka je karakterizacija procenjivanog informacionog sistema, dobra slika okruženja informacionog sistema i nacrt granica sistema.

→ **Identifikacija pretnji**

Pretnja je potencijalno štetna za imovinu, poput informacija, procesa i sistema, prema tome i po organizaciju. Poreklo pretnje može biti prirodne ili ljudskog porekla, a mogu biti slučajne ili namerne. Bilo da je izvor pretnje slučajan ili nameran, on mora biti identifikovan. Pretnja može nastati unutar ili van organizacije. Pretnje treba identifikovati generički i po tipu (npr. neovlašćen pristup, fizičko oštećenje, tehnički otkazi), pa ih generički klasifikovati. Tako se izbegava da se

⁸⁴ <http://www.cqm.rs/2011/2/pdf/28.pdf>

⁸⁵ <http://www.cqm.rs/2011/2/pdf/28.pdf>

pretnja izgubi iz vida, čak i slučajno, zbog ograničenja zahtevane količine posla. Neke pretnje pogađaju više od jedne imovine. U ovakvim slučajevima, one mogu izazvati različite uticaje, u zavisnosti od vrste imovine. Ulazi za identifikovanje pretnji i procenu verovatnoće pojavljivanja mogu se prikupiti od vlasnika imovine ili korisnika, osoblja, održavaocima objekta, specijalista informacione bezbednosti, eksperata za fizičku zaštitu, pravnih službi i drugih organizacija, uključujući sudske organe, organe za vremenske prilike, osiguravajuće kompanije i državne vlasti. Takođe, prilikom identifikovanja pretnji, treba uzeti u obzir životnu sredinu i kulturološke aspekte. U trenutnu procenu treba uključiti interna iskustva o incidentima, kao i prethodne rezultate procene pretnji. Može biti od koristi uvid u druge kataloge pretnji (nešto što je specifično za organizaciju ili posao kojim se bavi), kako bi se kompletirala lista generičkih pretnji, gde god je to relevantno. Katalogi pretnji i statistike dostupni su u industrijskim organima, državnim organima, pravnim organima, osiguravajućim društvima, itd. Kada se koriste katalogi pretnji, ili rezultati prethodnih procena, treba imati na umu da su promene relevantnih pretnji kontinuirane, naročito kada se radi o poslovnom okruženju ili izmenjenim informacionim sistemima. Sama pretnja ne predstavlja rizik kada nema ranjivosti koja se može iskoristiti. U određivanju verovatne pretnje potrebno je razmotriti potencijalne pretnje i postojeće kontrole. U proceni pretnje važno je razmotriti sve potencijalne izvore pretnji koje mogu prouzrokovati štetu u informacionom sistemu i u njegovoj okolini. Postoji više izvora pretnji:

- Prirodni izvori pretnji- prirodne nepogode
- Tehnički izvori pretnji- tehnički kvarovi opreme
- Ljudski izvori pretnji su: Unutrašnji (nestručni projektanti informacionog sistema, neodgovorni vlasnici celokupnog i delova informacionog sistema, ovlašćeni korisnici koji zloupotrebljavaju svoju vlast, službenici koji imaju fizički pristup informacionoj opremi itd.) i spoljašnji (zlonamerni pojedinci van, kriminalističke organizacije, strane obaveštajne službe, komercijalne organizacije, terorističke organizacije itd.)

Prikaz pretnji ili lista potencijalnih izvora pretnji bi morala da bude prilagođena pojedinoj organizaciji i njenom radnom okruženju i informacije o prirodnim pretnjama (npr. poplavama, zemljotresima, olujama) bi takođe trebala da bude lako dostupne.

→ **Identifikacija ranjivosti**

Analiza pretnji tokom informacionog sistema mora uključiti i analizu ranjivosti u okolini sistema. Cilj ovog koraka je da se razvije lista ranjivosti sistema (slabosti) koje bi se mogle iskoristiti od strane određene pretnje.

Ranjivosti se mogu identifikovati u sledećim oblastima:

- Organizacija
- Procesi i procedure
- Navike rukovodstva
- Osoblje
- Fizičko okruženje
- Konfiguracija informacionog sistema
- Hardver, softver ili komunikacioni uređaji
- Zavisnost od eksternih strana

Prisustvo ranjivosti samo po sebi nije štetno, potrebno je prisustvo pretnji koja je može iskoristiti. Za ranjivost koja nema odgovarajuću pretnju možda i ne mora da se implementira kontrola, ali njene promene moraju se nadgledati i prepoznati. Treba napomenuti da je pogrešno implementirana ili neispravna kontrola, sama po sebi ranjivost. U zavisnosti od okruženja, kontrola može biti efektivna ili neefektivna. Nasuprot tome, pretnja koja nema odgovarajuću ranjivost ne mora izazvati rizik. Ranjivosti mogu da se odnose na osobine imovine koja se ne koristi na pravi način, ili prema njenoj nameni za koju je kupljena ili napravljena. Treba imati u vidu da ranjivosti dolaze iz različitih izvora, na primer, one koje su na unutrašnjoj ili spoljašnjoj strani imovine.⁸⁶

⁸⁶Prof. dr Slobodan R. Petrović , *Strani pravni život- dilema (Kiber ili sajber)*, Institut za uporedno pravo, Beograd 2012. godine, str.25-30

Tabela 7: Ranjivost, pretnja i akcije pretnje

Ranjivost	Pretnja	Akcija pretnje
Iz sistema nisu uklonjeni korisnički računi otpuštenih radnika	Otpušteni radnici	Spajanje na mrežu organizacije i pristup poverljivim podacima organizacije
Rfačunarski centar koristi aparate za gašenje vatre, ali nema nema vodootpornih prekrivača za hardver i ostalu opremu	Vatra, neodgovorno osoblje	Uključivanje aparata za gašenje vatre u računarskom centru

Izvor: http://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf

Preporučene metode za identifikaciju ranjivosti sistema su upotreba izvora informacija o ranjivostima, sigurnosno testiranje sistema i razvoj liste sigurnosnih provera. Potrebno je naglasiti da će se pojaviti, kao i metodologija potrebna da se utvrdi da li ranjivosti postoje, obično zavisi od prirode informacionog sistema i od faze životnog ciklusa (SDLC) u kojoj se sistem nalazi:

- Ako informacioni sistem još nije dizajniran, potraga za ranjivostima bi se trebala usmeriti na sigurnosne politike organizacije, planirane sigurnosne procedure, definicije zahteva na sistem, sigurnosne analize produkata od strane dobavljača ili osobe koja je napravila sistem.
- Ako je informacioni sistem u fazi primene, identifikacija ranjivosti treba da se proširi kako bi se uključilo više informacija, kao što su planirana sigurnosna svojstva sistema, opisana u dokumentaciji sigurnosnog dizajna i proceni sistema.
- Ako je informacioni sistem u radnoj fazi, proces identifikacije ranjivosti bi trebao da uključi analizu sigurnosna svojstva sistema i sigurnosne kontrole, tehničke i proceduralne, koje se koriste za zaštitu sistema.
- Izvori informacija o ranjivostima može biti: dokumentacija od prethodnih rizika procenjivanog informacionog sistema, izveštaji kontrolnih pregleda sistema, izveštaji o anomalijama sistema, izveštaji sigurnosnih pregleda, izveštaji testiranja i procene sistema, liste ranjivosti, sigurnosna

upozorenja, upozorenja dobavljača, specijalizovane mailing liste, sigurnosne analize softver sistema.⁸⁷

→ Analiza kontrola

Cilj ovog koraka je da se analiziraju kontrole koje su primenjene ili su planirane za primenu u organizaciji da bi smanjile ili uklonile verovatnoću da pretnja iskoristi ranjivost sistema. Sigurnosne kontrole obuhvataju upotrebu tehničkih i netehničkih metoda.

Tehničke kontrole su zaštitni alati koji su ugrađeni u računarski hardver, softver (npr. mehanizmi za kontrolu pristupa, mehanizmi za identifikaciju, softver za otkrivanje upada). Netehničke kontrole su kontrole upravljanja i radne kontrole, kao što su sigurnosne politike, radne procedure, sigurnost osoblja, fizička sigurnost i sigurnost okoliša.

I tehničke i netehničke kontrole mogu se dalje klasifikovati na preventivne i aktivne:

- Preventivne kontrole sprečavaju pokušaje prekršaja sigurnosne politike i uključuju takve kontrole kao što su kontrola pristupa, enkripcija i autentikacija.
- Aktivne kontrole upozoravaju na prekršaje sigurnosne politike i sadrže takve kontrole kao što su nadzorna praćenja (audit trails), metode otkrivanja upada i kontrolne sume (checksums).⁸⁸

→ Određivanje verovatnoće

Da bi se izvela klasifikacija verovatnoće, koja označava mogućnost da se iskoristi ranjivost od strane pretnje, moraju se razmotriti sledeći faktori:

- Motivacija i mogućnosti pretnje
- Priroda ranjivosti
- Postojanje i učinkovitost tekućih kontrola

Tabela 8: Nivoi verovatnoće

Nivo verovatnoće	Definicija verovatnoće
Visoki	Pretnja je visoko motivisana i ima dovoljno mogućnosti za realizaciju, a kontrole koje bi trebale da spreče iskorišćavanje ranjivosti su neefektivne
Srednji	Pretnja je motivisana i ima mogućnosti da se realizuju, ali postoji kontrola koje mogu

⁸⁷ http://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf

⁸⁸ http://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf

	sprečiti uspešno izvođenje pretnje.
Nizak	Pretnja nije motivisana ili nema dovoljno mogućnosti za realizaciju, ili postoje kontrole koje mogu sprečiti iskorišćavanje ranjivosti

Izvor: <http://www.cqm.rs/2011/2/pdf/28.pdf>

→ Analiza uticaja

Sledeći korak u merenju nivoa rizika je da se odredi štetni uticaj koji je rezultat uspešnog iskorišćavanja ranjivosti od strane pretnje. Pre početka analize uticaja, potrebno je dobiti sledeće informacije:

- Svrha sistema (npr. proces koji treba izvršiti)
- Kritičnost sistema i podataka (npr. vrednost sistema ili njegova važnost za organizaciju)
- Osetljivost sistema i podataka

Ove se informacije mogu dobiti iz postojeće dokumentacije organizacije, kao što su izveštaj o analizi uticaja na poslovanje ili izveštaj o proceni kritične opreme. Analiza uticaja na poslovanje klasifikuje nivoe uticaja koji bi mogli ugroziti informatička sredstva organizacije zasnovana na kvalitativnoj ili kvantitativnoj proceni osetljivosti i kritičnosti tih sredstava. Procena kritične opreme identifikuje i klasifikuje osetljivu i kritičnu informacionu opremu organizacije (npr. hardver, softver, sistem, servise i propratna tehnološka sredstva) koja podržava kritične poslovne procese organizacije.⁸⁹

Neki uticaji se mogu meriti kvantitativno, kao npr. gubitak u prihodu, troškovi prepravke sistema ili nivo napora koji zahteva da se poprave problemi uzrokovani uspešnom akcijom pretnji. Drugi uticaji (npr. gubitak poverenja javnosti, gubitak verodostojnosti) se ne mogu meriti određenim jedinicama, ali se mogu opisati pojmovima visokog, srednjeg ili niskog nivoa uticaja.

Neki uticaji se mogu meriti kvalitativno. Glavna prednost kvalitativne analize uticaja je da ona klasifikuje rizik i identifikuje područje za neposredno poboljšanje i meri veličinu uticaja koja se može iskoristiti u proceni troškova za preporučene kontrole. Mana kvalitativne analize je da ne daje specifične kvantitativne mere veličine uticaja, tako da se ne može sprovesti analiza troškova.

⁸⁹ <http://www.cqm.rs/2011/2/pdf/28.pdf>

→ **Određivanje rizika**

Svrha ovog koraka je procena nivoa rizika za informacijski sistem. Određivanje rizika za određeni par pretnja/ranjivosti se može prikazivati kao funkcija od:

- Verovatnoće određene pretnje da iskoristi određenu ranjivost
- Veličine uticaja, ako je pretnja uspešno iskoristila ranjivost
- Prikladnosti planiranih ili postojećih sigurnosnih kontrola za smanjenje ili eliminisanje rizika⁹⁰

Tabela 9: Nivoi rizika

Nivo rizika	Opis rizika i potrebne akcije
Visoki	Ako je neka pojava procenjena kao visoki rizik, postoji jaka potreba za korektivnim merama. Postojeći sistem može nastaviti sa radom, ali plan korektivnih akcija mora da se ostvari što je pre moguće.
Srednji	Ako je neka pojava procenjena kao srednji rizik, potrebne su korektivne akcije i mora se razviti plan da se te akcije ostvare u razumnom vremenu.
Nizak	Ako je neka pojava procenjena kao nizak rizik, mora se odlučiti da li su potrebne korektivne akcije ili se rizik može prihvatiti.

Izvor: http://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf

→ **Preporuke za kontrolu**

Za vreme ovog koraka u procesu upravljanja rizikom, prepoučuju se kontrole koje mogu da ublaže ili eliminisati rizik, na način koji odgovara radnim operacijama organizacije. Cilj preporuke kontrola je smanjiti nivo rizika za sistem i njegove podatke na prihvatljiviji nivo. Kod preporuke kontrola treba da se razmotre sledeći faktori:

- Efektivnost preporučenih kontrola
- Zakoni i uredbe
- Organizaciona politika

⁹⁰ http://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf

- Uticaj na rad
- Sigurnost i pouzdanost

Preporuka kontrola je rezultat procesa procena rizika i daje smernice za process ublažavanja rizika, za vreme koje se preporučene proceduralne i tehničke sigurnosne kontrole procenjuju, klasifikuju i primenjuju. Identifikacijom postojećih kontrola izbegava se nepotreban posao ili troškovi, npr. dupliciranje kontrola. Pored toga, prilikom identifikovanja postojećih kontrola, treba proveriti da li rade kako treba – referenciranje na postojeće izveštaje ISMS audita štedi vreme. Ako kontrola ne radi kako treba, onda je moguće da može otvoriti ranjivosti. Treba razmotriti situaciju kada odabrana kontrola (ili strategija) propusti u radu, zbog čega su potrebne komplementarne kontrole za efektivno rešavanje identifikovanog rizika. U ISMS-u, prema ISO/IEC 27001, ovo je podržano merenjem efektivnosti kontrola. Način procene efekta kontrole je da se vidi kako ona redukuje verovatnoću pojave pretnje i iskoristivost ranjivosti, ili uticaj incidenta. Menadžerska preispitivanja i izveštaji audita takođe nude informacije o efektivnosti postojećih kontrola. Kontrole koje se planiraju mogu se implementirati prema planovima implementacije tretmana rizika, treba razmotriti na isti način kao one koje su već implementirane. Postojeće ili planirane kontrole mogu biti ocenjene kao neefektivne, nedovoljne, ili neopravdane. Ukoliko nisu dovoljne ili opravdane, treba ih proveriti i utvrditi da li ih treba ukloniti, zameniti drugom stabilnijom kontrolom, ili ih ostaviti, npr. zbog cene.

Za identifikovanje postojećih ili planiranih kontrola mogu biti od koristi sledeće aktivnosti:

- Preispitivanje dokumentacije o kontrolama (na primer, planovi implementacije tretmana rizika). Ako su procesi upravljanja zaštitom informacija dobro dokumentovani, onda je dostupan i status implementacije svih postojećih i planiranih kontrola
- Sa odgovornima za zaštitu informacija (službenici za zaštitu ili upravljanje sistemom zaštite informacija, upravnik objekta ili izvršni direktor) i korisnicima koji sprovode kontrolu, proveriti kontrole koje su implementirane u posmatranom informacionom sistemu
- Provera fizičkih kontrola na licu mesta, poredeći implementirane sa onim koji tek treba tu da budu, kao i provera da li su postojeće kontrole ispravne i efektivne⁹¹

⁹¹ http://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf

→ Dokumentovanje rezultata

Rezultati procene rizika (identifikovanje pretnje i ranjivosti, procenjeni rizik i preporučene kontrole) trebaju da se dokumentuju u obliku izveštaja. Izveštaj o proceni rizika opisuje pretnje i ranjivosti, meri rizika i preporučuje kontrole koje se trebaju primeniti.

8.2. ISO standardi: ISO/IEC 27001/2

ISMS(Sistem menadžmenta bezbednosti informacija- Information Security Menagement System) je deo ukupnog sistema organizacije projektovan po zahtevima standard ISO 27001 koji ima za cilj da primenom principa PDCA (Plan-Do-Check-Act) kroz procese stalnih unapređenja, uspostavi, implementira, deluje, nadgleda, pregleda, održava i unapređuje bezbednost informacija, uzimajući u obzir sve bezbednosne rizike po poslovanje organizacije. ISMS pokriva sledeća područja:

- Analiza i upravljanje rizikom
- Politika bezbednosti
- Bezbednost organizacije
- Klasifikacija i upravljanje imovinom
- Politika bezbednosti u upravljanju ljudskim resursima
- Fizička i informatička bezbednost imovine i okruženja organizacije
- Upravljanje komunikacijama i operativom
- Kontrola pristupa
- Razvoj i održavanje ISMS-a
- Upravljanje incidentima
- Upravljanje kontinuitetom poslovanja
- Usaglašenost sa zakonskim propisima

Ovakvim pristupom, posmatranja celine kao jednog uvezanog sistema informacija u kome se generisanje, distribucija i čuvanje istih, u svim segmenatima organizacije (nabavka, dizajn, projektovanje, prodaja, montaža, marketing itd.), stavlja u funkciju pravilnog rada celog sistema. Na ovaj način se dobija efikasna i efektivna organizacija gde ISMS, na osnovu jasno identifikovanih međuprocenih veza, filtrira informacije sa pozicije zajedničkih imenitelja (pravo pristupa, pravo korišćenja i pravo administriranja) i tako omogućava njihovo korišćenje od strane

više korisnika, održavajući pri tom njihovu pravovremenost, konzistentnost i poverljivost. Sve ovo rezultuje odličnom komunikacijom između segmenata, izbegavajući pri tom ponavljanje informacija ili pak distribuciju istih do učesnika kojima one nisu neophodne. Ovakvim pristupom štitimo informacije od namerne ili nenamerne zloupotrebe, smanjujemo vreme komunikacije i time direktno utičemo na povećanje efikasnosti tj. produktivnosti. Uvezivanjem svih zaposlenih dokumentacijom i informacijama, unapređujemo procesnu kontrolu kojom smanjujemo rizike na minimum i proizvodimo sinergetski efekat timskog rada. Procesom Integracije ISMS-a i postojećih sistema upravljanja kvalitetom, pitanje bezbednosti informacija postaje pitanje kvaliteta i to je ključna informacija koju kompanija šalje svojim sadašnjim i potencijalnim klijentima i partnerima. Ovakav pristup realizaciji projekta, omogućiće organizaciji da zajedno sa konsultantima razvije i implementira ISMS adekvatan organizacionoj strukturi, raspoloživim resursima (ljudskim i materijalnim) i zahtevima korisnika (klijenti, dobavljači, zaposleni, šira zajednica, međunarodno tržište itd.), široko prihvaćen i promovisan od strane svih zaposlenih, što je osnovni preduslov za njegovo kontinuirano unapređenje.⁹² ISO 27001 je nastao kao rezultat potrebe definisanja međunarodno prihvaćenih normi, koji će svojim zahtevima definisati okvir formiranja sveobuhvatnog sistema zaštite i ciljeve njegovog delovanja kako bi se na efektivan i efikasan način upravljalo bezbednošću informacija. Ovaj standard svojim zahtevima definiše četiri glavna područja sistema zaštite informacija:

- Sistem menadžmenta bezbednosti informacija (ISMS)
- Odgovornost rukovodstva
- Ocena rukovodstva
- Unapređenje ISMS-a

ISO 27001 je sveobuhvatan, jer tretira bezbednosti informacija sa tri aspekta:

- Informatičkog – analizirajući i definišući performanse IT opreme, prava pristupa, kriptovanja, lozinke, protokoli, politike sa aspekta pojave rizika po bezbednost podataka i informacija
- Administrativnog – definišući jasna uputstva, politike i procedure za generisanje informacija, njihovu distribuciju, čuvanje (skladištenje)
- Fizičku – fizička kontrola pristupa, evidencija zaposlenih, video nadzor, zaštita radnih prostorija⁹³

⁹² www.tqmkonsalting.com

⁹³ www.tqmkonsalting.com

ISO/IEC 27001 precizira da se na bazi rizika, kontrole implementiraju u okviru, granicama i kontekstu ISMS-a. Ovaj zahtev može da se ispuni primenom procesa upravljanja informaciono-bezbednosnim rizikom. Razni su pristupi za uspešnu implementaciju ovog procesa u organizaciji. Organizacija treba da koristi pristup koji najviše odgovara okolnostima za svaku konkretnu primenu procesa. Prema ISMS-u, formiranje konteksta, procena rizika, izrada plana tretmana i prihvatanje rizika deo su faze planiranja “plan”. ISMS faza primene “do”, radnje i kontrole za redukovanje rizika na prihvatljiv nivo primenjuju se u prema planu tretiranja rizika. U ISMS fazi provere “check”, rukovodioci na osnovu incidenata i promena u okolnostima utvrđuju potrebu za preispitivanjem procene i tretmana rizika. U fazi delovanja “act”, izvršavaju se sve potrebne akcije, uključujući i dodatne primene procesa upravljanja informaciono-bezbednosnim rizikom. Na sledećoj tabeli dat je pregled aktivnosti upravljanja informaciono-bezbednosnim rizikom, u odnosu na faze ISMS procesa:

Tabela 10: Usklađivanje ISMS i procesa upravljanja informaciono-bezbednosnim rizikom

ISMS Proces	Proces upravljanja informaciono-bezbednosnim rizikom
	Formiranje konteksta Procena rizika
Do	Primena plana tretmana rizika
Chek	Neprekidan nadzor i preispitivanje rizika
Act	Održavanje i poboljšavanje procesa upravljanja informaciono-bezbednosnim rizikom

Izvor: www.tqmkonsalting.com

ISO/IEC 27001 je bezbednosno informativni sistem usvojen oktobra 2005. godine od strane Međunarodne organizacije za standarde. Ovaj sistem obuhvata sledeće stavke:

- Bezbednosnu politiku- smer menadžment
- Organizaciju bezbednosti informacija- upravljanje sigurnosti informacija
- Upravljanje aktivom- popis i klasifikaciju informacija imovine
- Bezbednost ljudskih resursa- bezbednosni aspekti za zaposlene i organizaciju

- Fizičku i životnu sigurnost- zaštita od kompjuterskih objekata
- Komunikacije i operacije- menadžment tehničkih bezbednosnih kontrola u sistemima i mrežama
- Kontrolu pristupa- ograničenje prava pristupa mreži, sistemu, aplikacijama, funkcijama i podacima
- Informacione sisteme sticanja, razvoja i održavanja- izgradnja bezbednosti u aplikacijama
- Bezbednost upravljanja informacijama- predviđa i reaguje na odgovarajući način za kršenje informacione bezbednosti
- Upravljanje kontinuitetom poslovanja- štite i oporavljaju od poslovno kritičnih procesa i sistema
- Usklađenost- usklađenost sa politikama i obezbeđuje sigurnost podataka, standarda, zakona i propisa.

Ovaj međunarodni standard nudi osnove upravljanja informaciono-bezbednosnim rizicima, podržava opšte koncepte date u ISO/IEC 27001 i izrađen je da doprinese zadovoljavajućoj implementaciji zaštite informacija, na bazi pristupa upravljanja rizikom.

Za potpuno razumevanje ovog međunarodnog standarda, potrebno je poznavati koncepte, modele, procese i terminologiju međunarodnih standarda ISO/IEC 27001 i ISO/IEC 27002.

Ovaj međunarodni standard je primenljiv na sve tipove organizacija (npr. komercijalna preduzeća, vladine agencije i neprofitne organizacije) koje nameravaju da upravljaju rizicima koji bi mogli kompromitovati bezbednost informacija organizacije.

Većina organizacija ima veliki broj informacionih sistema koji se bave sa bezbednošću sistema. ISO/IEC 27002 daje kodeks dobre prakse koji opisuje neophodne elemente za osnovnu zaštitu, uključujući i:

- Politiku za upravljenje sigurnošću informacija visokog nivoa
- Značaj korisnika
- Antivirusni softver
- Backup
- Kontrolu pristupa
- Fizičku zaštitu objekata i komercijalno osetljivih akata i dokumenata u papirnoj formi⁹⁴

⁹⁴ www.tqmkonsalting.com

8.3. Inventar informacione imovine hotelskog sistema

Imovina je svaka vrednost organizacije koja zahteva zaštitu. Za identifikovanje imovine treba imati na umu da se informacioni sistem ne sastoji samo od hardvera i softvera.

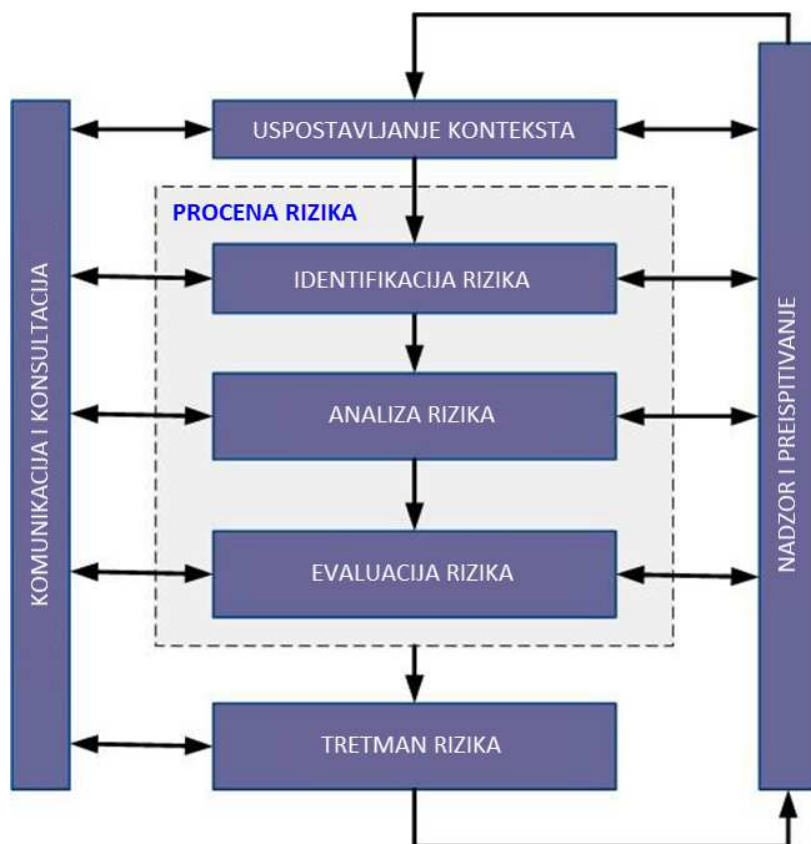
Identifikaciju imovine treba obaviti na prihvatljivom nivou detalja, dovoljnom za procenu rizika. Nivo identifikovanih detalja o imovini, uticaće na celokupnu količinu informacija prikupljenih u toku procene rizika. Za svaku imovinu treba identifikovati vlasnika, kako bi se obezbedila opšta i kontrolisana odgovornost za imovinu. Vlasnik imovine ne mora imati pravo svojine na imovinu, ali ima odgovornost za njenu proizvodnju, razvoj, održavanje, upotrebu i odgovarajuću zaštitu. Vlasnik imovine je uglavnom najprikladnija osoba za određivanje njene vrednosti za organizaciju. Preispitivanje granica je parametar imovine organizacije, definisan da se održava procesom upravljanja informaciono-bezbednosnim rizikom. Zavisno od obima i ciljeva upravljanja rizikom, mogu se primeniti i različiti pristupi. Za pogodan pristup upravljanju rizikom mogu se odabrati ili razviti oni koji se zasnivaju na osnovnim kriterijumima, kao što su: kriterijum evaluacije rizika, kriterijum uticaja, kriterijum prihvatanja rizika.

Pored toga, organizacija treba da proceni da li ima dostupne resurse neophodne za:

- Sprovođenje procene rizika i izradu plana tretmana rizika
- Definisanje i primenu politika i procedura, uključujući implementaciju odabranih kontrola
- Nadzor kontrola
- Nadzor procesa upravljanja informaciono-bezbednosnim rizikom⁹⁵

⁹⁵ Grubor G. „Projektovanje menadžment sistema zaštite informacija“, Univerzitet Singidunum, Beograd 2011., str. 11-13

Diagram 1: ilustruje primenu procesa upravljanja informaciono-bezbednonim rizikom



Proces upravljanja informaciono-bezbednosnim rizikom sadrži kontekst, procenu rizika, tretman rizika, prihvatanje rizika, konsultaciju i razmena informacija o rizicima i nadzor i preispitivanje rizika. Takođe, ilustruje proces upravljanja informaciono-bezbednosnim rizikom, procenu rizika i/ili aktivnosti tretiranja rizika. Prilikom svake procene rizika otkriva se više detalja. Iterativnom procenom rizika obezbeđuje se dobar balans između uštede vremena i truda za identifikovanje kontrola, kao i garancija da su visoki rizici procenjeni na odgovarajući način.

Prvo se formira kontekst, potom se vrši procena rizika. Ukoliko se dobije dovoljno informacija za efektivno utvrđivanje radnji neophodnih za modifikovanje rizika na prihvatljiv nivo, tada se pristupa tretiranju rizika. Ako nema dovoljno informacija, vrši se sledeća iteracija u revidiranom kontekstu (npr. kriterijumi procene rizika, kriterijumi prihvatanja rizika, ili kriterijumi uticaja), eventualno na određenim delovima ukupnog obima procene rizika.

Efektivnost tretmana rizika zavisi od rezultata procene rizika. Tretman rizika podrazumeva kritičan proces:

- procene rizika i određivanje bezbednosnih zahteva;
- donošenja odluke o prihvatljivosti preostalog rizika;
- izrade novog plana tretmana rizika ako su nivoi rizika neprihvatljivi
- procenu efektivnosti tretmana
- promovisanje svesti o potrebi i obuka
- nadzor i kontrola sistema zaštite i evaluacija efektivnosti i usklađenosti

Moguće je da tretman rizika ne dovede odmah do prihvatljivog preostalog rizika. U ovakvoj situaciji potrebno je izvršiti drugu iteraciju procene rizika, sa promenjenim parametrima konteksta (npr. kriterijumi procene rizika, kriterijumi prihvatanja rizika, ili kriterijumi uticaja), uz eventualni dodatni tretman rizika.

U toku procene rizika mora da se obezbedi eksplicitno prihvatanje preostalih rizika od strane rukovodioca organizacije. Ovo je naročito bitno u situacijama gde je implementacija kontrola izostavljena ili odložena, npr. zbog cene.

Tokom celog procesa upravljanja informaciono-bezbednosnim rizikom, važno je sa rukovodiocima i operativcima razmenjivati informacije o rizicima. Čak i pre tretmana rizika, informacije o identifikovanim rizicima mogu biti od velike koristi za upravljanje incidentima i smanjenje potencijalne štete. Svest rukovodioca i osoblja o rizicima, vrsta implementiranih kontrola za ublažavanje rizika i oblasti od interesa za organizaciju, na mnogo efektivniji način doprinose u rešavanju incidenata i neočekivanih događaja. Treba detaljno dokumentovati sve rezultate procesa upravljanja informacion bezbednosnim rizikom, kao i obe tačke donošenja odluka.⁹⁶ Informacioni sistem je uređeni i integrisani skup podataka, procesa, interfejsa, mreža i tehnologija koja su u međusobnoj korelaciji u cilju podrške i poboljšanja svakodnevnih poslovnih operacija, a takođe i u cilju podrške menadžmentu u rešavanju poslovnih problema i donošenja odluka. Informacioni sistemi treba da budu strateški, odnosno da ispunjavaju ciljeve i strategiju poslovanja. Strateški informacioni sistemi (*Strategic Information Systems, SISs*) su sistemi koji pomažu organizaciji da stekne konkurentnu prednost kroz doprinos strateškim ciljevima organizacije i/ili njenoj sposobnosti da znatno poveća svoje performanse i

⁹⁶ http://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf

produktivnost.⁹⁷ Informacionu tehnologiju čini kombinacija računarske tehnologije (hardware i software), telekomunikacione tehnologije, netware, groupware i humanware.

- *Hardware* – fizička oprema kao što su mehanički, magnetski, elektronski ili optički uređaji.
- *Software* – predefinisane instrukcije koje kontrolišu rad računarskih sistema ili elektronskih uređaja. Softver koordinira rad hardverskih komponenata u jednom informacionom sistemu. Softver inkorporira standardne softvere kao što su operativni sistemi ili aplikacije, softverski procesi, veštačka inteligencija i inteligentni agenti i korisnički interfejs.
- Telekomunikacije – prenos signala duž različitih distanci koji uključuju i prenos podataka, slika, glasova koristeći radio, televiziju, telefoniju i druge komunikacione tehnologije.
- *Netware* – oprema i softver neophodni za razvoj i podršku mreže računara, terminala i komunikacionih kanala i uređaja.
- *Groupware* – komunikacioni alati kao što su e-mail, videokonferencije i dr., koji podržavaju elektronsku komunikaciju i kolaboraciju između grupa.
- *Humanware* – intelektualni kapaciteti neophodni za razvoj, programiranje, održavanje i rukovanje tehnologijom. *Humanware* inkorporira znanje i ekspertizu.

U hotelijerstvu u informacionu tehnologiju spada:

- Hardware- Računari, terminali u restoranima, interaktivna digitalna televizija, mobilni uređaji, videotekst terminali, CD-ROM, ulazni uređaji (skeneri, tastature, miševi) izlazni uređaji (štampanici, ekrani)
- Software- *Micros-Fidelio* – Sistem za upravljanje imovinom (*Property Management System*) omogućava hotelima da kontrolišu svoju imovinu, dugovanja, kredite i račune gostiju. DBMS, *spreadsheets* programi, web browseri, aplikacije koje pokrivaju računovodstvo, planiranje, kadrove, nabavku, kontrolu zaliha, bezbednost, kontrolu energije, hrane i pića i MIS.
- Telekomunikacije- Telefonske centrale, modemi, LAN, WAN, telekonferencije, satelitska i mobilna komunikaciona tehnologija
- Netware- Mreža hardvera i softvera između odeljenja u hotelima. EDI, bežični i satelitski sistemi
- Groupware- Aplikacije koje dozvoljavaju zaposlenima da dele fajlove, dosije klijenta i operativne informacije kao što su cene⁹⁸

⁹⁷ www.tqmkonsalting.com

9. Studija slučaja: smanjenje rizika hotelskog poslovanja na prihvatljiv nivo na primeru hotela Park

Hotel Park se nalazi u samom centru grada na uglu Njegoševe ulice i ulice Svetozara Markovića. Potpuno je renoviran 2012. godine. Posедуje 122 sobe i 3 apartmana, fitness, wellness, spa zonu, restoran i banket sale. Svaka soba ima besplatan internet, telefonsku liniju, radijski, kablovski i satelitski tv program. Hotel koristi kartični ključ za goste kome je rezervacija napravljena. Sa tim ključem se može proveriti da li je soba pospremljena, da se uključi klimatizacija ili grejanje, da se kontroliše svaki poziv koji je gost napravio, da obavesti gosta o sortimanu filmova koje može da gleda na maternjem jeziku, da alarmira obezbeđenje u slučaju hitnih situacija itd. Banket sale može da ugosti 220 zvanica i prilikom organizacije događaja se koristi audio-vizuelne i tehnička oprema- printer/fax, projektori, ekrani, 35 mm slide projektor, flip čartovi, osvetljnje i ozvučenje. Hotel Park je odabrao savremeno tehničko rešenje koje omogućava jednostavno korišćenje i opsluživanje klijanata. Reč je o informacionom sistemu Bellevue i sve informacije vezane za hotel se nalaze u ovom sistemu, koji ih obrađuje, prezentuje ili donosi neku odluku na osnovu njih.⁹⁹

Da bi sistem bio u stanju da dobije sve informacije u svakom trenutku, mora da ima posebne komunikacione module ili hotelske interfejsе preko kojih Bellevue uspostavlja komunikaciju sa svim aspektima hotelskog poslovanja. Tih interfejsа ima mnogo i ima ih svuda u hotelu koji se kontrolišu. Kontrola se uspostavlja zbog sigurnosnih razloga (SOS poziv, protivpožarna kontrola, protivprovalna kontrola...), zbog tarifiranja određenih usluga (korišćenje Interneta, tarifiranje telefonskih razgovora...), zbog razloga kontrole ovlašćenja gosta (kontrola potrošnje gosta, kontrola pristupa gosta u različite hotelske sadržaje...) itd.

Cilj ugradnje sistema je da se maksimalno izađe u susret gostima i da zna šta gost želi. Gost retko kad pamti raspored stolova, ali zato će sigurno zapamtiti kakva je usluga bila i da li je osoblje bilo ljubazno. I da bi sve u hotelu bilo na nivo, elektronika koja je postavljena u hotelu dosta pomaže da ne dodje do nekog propusta.¹⁰⁰

⁹⁸ Grubor G., „Projektovanje menadžment sistema zaštite informacija“, Univerzitet Singidunum, Beograd 2011., str. 8-15

⁹⁹ www.hotelparkbeograd.rs

¹⁰⁰ <http://www.prointer.rs/sr/bellevue-hotel-software>

Tehničke karakteristike Bellevu sistema:

- Modularnost sistema sa mogućnošću postojanja više terminala recepcije i više back office terminal
- Građeni podsistem za tarifiranje telefonske centrale, komunikaciju sa restoranskim podsistemom sistema Bellevue, komunikaciju sa hotelskim multimedijalnim sistemom, komunikaciju sa restoranskim rezervacijama
- Vođenje rezervacija i najava dolazaka gostiju
- Obrada grupnih najava, prijave, odjave i najave
- Dnevnik rezervacija koji prikazuje formirane rezervacije za izabrani dan sa imenom i prezimenom, datumom formiranja, brojem rezervacije, datumom dolaska gostiju, osoba koja je formirala rezervaciju itd.
- Formiranje ugovora sa pripadajućim cenovnicima po agencijama ili firmama sa mogućnošću formiranja cenovnika u više različitih valuta
- Formiranje alotmana po agencijama i analiza
- Mogućnost uplate cele sobe ili jednog ili više gostiju do ubeleženog dana odlaska ili do željenog dana, sa obračunom svih usluga pansionskih i vanpansionskih. Sa opcijama uplate samo pansionskih usluga sa ili bez takse i osiguranja, uplate samo takse i osiguranja ili uplate samo jedne usluge ili više van pansionskih usluga kao i obračuna popusta na procenat ili konkretan iznos
- Pošto sistem može da radi sa više sezona sa različitim cenama, a ukoliko se dogodi da boravak gosta preklapa sa pomenutom sezonom tj. cene boravka, uplata unapred će na odgovarajući način obračunati promenu cene koja sledi u budućnosti i takvu izmenu prikazati u računu uplate unapred gosta ili gostiju
- Vođenje kartice i praćenje plaćanja firmi
- Vođenje plaćanja VIP gostiju
- Kontrola prava pristupa sistema po šiframa
- Mogućnost rada recepcije po recepcijama, recepcionerima
- Vođenje spiskova stranih i domaćih gostiju sa formiranje knjiga gostiju i modul za eksport podataka u MUP¹⁰¹

¹⁰¹ <http://www.prointer.rs/sr/bellevue-hotel-software>

Na osnovu istraživanja koje sam sproveda u hotelu Parka došla sam do sledećih podataka:

- Hotel Park ima visok nivo zaštite rezervacionog sistema. Kao što sam već navela hotel koristi informacioni sistem Bellevu s tim što recepcija ima poseban modul od restorana i odvojeno funkcionišu.
- Na osnovu istraživanja, koje sam sproveda došla sam do nekih informacija koliko je i da li je hotel imao ikakve pretnje, kao i koje su ranjivosti IKT sistema u hotelu

Tabela 11: Pretnje (ISO/IEC 27001)

001	Otkaz klimatizacije
005	Slučajan propust (greška)
014	Elektronske interferentne smetnje
019	Otkaz opreme/servisa
021	Požar
025	Otkaz hardvera
026	Ljudska greška
044	Greške podrške
046	Maliciozni kod-virus
058	Napajanje poremećaj/varijacije
060	Greške u obradi podataka
068	Otkaz sofvera
069	Neželjena pošta (spam)
072	Tehnički/mehanički otkaz
076	Greške u prenosu

Izvor: Grubor G., „Projektovanje menadžment sistema zaštite informacija“, Univerzitet Singidunum, Beograd 2011.

U tabeli je navedeno koje su sve pretnje javile u hotelu i koje se povremeno dešavaju. Sve navedene pretnje se uspešno rešavaju jer hotel efikasno posluje i ima dobar tim zaposlenih koji se suočava sa istim. Na osnovu istraživanja saznala sam da se u hotelu nije ništa kardinalno desilo osim nekih slučajnih propusta karakterističnih za svako poslovno okruženje. Pored toga, došla sam do informacija koje su vezane za ranjivost IKT sistema.

Tabela 12: Ranjivosti IKT sistema (ISO/IEC 27001)

002	Prisustvo lako zapaljivih materija	Postoje lako zapaljive materije ali se nalaze na sigurnom mestu, tako da postoji mala verovatnoća da se iste zapale
010	Nezadovoljni ili revoltirani zaposleni	Dešavalo se da su zaposleni u hotelu bili nezadovoljni položajem.
021	Posedovanje intelektualne svojine visoke vrednosti	Razvojna rešenja atraktivna za konkurenciju
022	Visoke vrednosti imovine	Visoka vrednost inventara u hotelu
203	Softverske greške	Dešavalo se da sofver ima neku grešku, ali je to vrlo brzo rešavano.
214	Neautorizovano priključena mrežna oprema	Desilo se da je modem bio nepravilno priključen.

Izvor: Grubor G. „Projektovanje menadžment sistema zaštite informacija“, Univerzitet Singidunum, Beograd 2011.

U tabeli sam navela par primera koji predstavljaju ranjivosti IKT sistemau hotelu. Dakle možemo reći da je hotel imao par propusta kada je u pitanju softver ili priključivanje modema.

Takođe, se dešavalo da su zaposlene nezadovoljni položajem, kao i da hotel poseduje lako zapaljive materijale, ali da se nikada nije desio požar ili da su zaposleni bili ugroženi. Možemo reći, na osnovu tabele, da hotel poseduje inventar visoke vrednosti i da ima razvojna rešenja atraktivna za konkurenciju.

Pored informacija vezanih za moguće pretnje i ranjivosti hotela u sledećem delu će biti reči o poverljivosti, integritetu i dostupnosti, kao i o vrednovanju imovine i analizi rizika.

Matrica za vrednost imovine- Vrednost nivoa za poverljivost, integritet i dostupnost. Vrednost imovine je određena kao zbir svega.

Tabela 13: Nivoi

Nizak nivo	1
Srednji nivo	2
Visok nivo	3

Izvor: Grubor G. „Projektovanje menadžment sistema zaštite informacija“, Univerzitet Singidunum, Beograd 2011.

Tabela 14: Vrednost imovine

Poverljivost	Integritet	Dostupnost	Vrednost imovine
Visok	Visok	Visok	3+3+3=9

Izvor: Grubor G. „Projektovanje menadžment sistema zaštite informacija“, Univerzitet Singidunum, Beograd 2011.

Na osnovu istraživanja hotel poseduje visok nivo poverljivosti, integriteta i dostupnosti.

Ozbiljnost i pretnja ranjivosti

Tabela 15: Vrednosti imovine pomnožena sa nivoom opasnosti i ranjivosti daje zbir vrednosti matrice

Vredost imovine	Opasnost	Ranjivost	Vrednost matrice (zbir)
9	Nizak= 1	Ranjivost= 2	9*1*2= 18

Izvor: Grubor G. „Projektovanje menadžment sistema zaštite informacija“, Univerzitet Singidunum, Beograd 2011.

Hotel nije izložena opasnošću, dok je ranjivost na srednjem nivou.

Uticaj rizika

Tabela 16: Verovatnoća rizika

Verovatnoća		
Ocena	Objašnjenje	Primer
3	Retko	Jednom u pola godine

Izvor: Grubor G. „Projektovanje menadžment sistema zaštite informacija“, Univerzitet Singidunum, Beograd 2011.

Hotel je retko izložen riziku, jednom u pola godine, jer je dobro organizovan i ima dobro zaštićen rezervacioni sistem.

Na osnovu celog istraživanja mogu da kažem da hotel poseduje visoku zaštitu informaciono rezervacionog sistema i nije se dešavalo da su neki spoljni faktori ugrozili podatke ili dobili informacije o gostima hotela, kao ni to da su zaposleni odavali informacije vezane za posao. Hotel je imao nekih manjih problema sa softverom, ali je to brzo rešavano. Prema rečima anketirane osobe u hotelu, svakodnevno se dese neki sitni propusti koji su normalni za svako poslovno okruženje, ali ti propusti su toliko minimalni da nikako ne mogu da ugroze poslovanje hotela.

10. Primeri iz prakse-sigurnost i bezbednost turista u hotelima u svetu

10.1. Sigurnost turista u „Hilton worldwide” hotelima



Hotel Hilton je osnovan 1919. godine. u Teksasu. Hilton je postao prvi hotel sa instaliranim televizorima u sobama i prvi hotel koji je dobio LEED i Green Seal sertifikate za očuvanje životne sredine. Hoteli Hilton i odmarališta (Hilton Hotels & Resort) je međunarodni hotelski lanac koji uključuje mnogo luksuznih hotela i odmarališta i danas je u vlasništvu Hilton Worldwide. Danas broji preko 550 Hilton brendiranih hotela u 78 zemalja na šest kontinenata. U okviru korporacije Hilton Worldwide razvijeni su sledeći brendovi:

- Waldorf Astoria Hoteli i Odmarališta (Waldorf Astoria Hotels & Resorts);
- Konrad Hoteli i Odmarališta (Conrad Hotels & Resorts);
- Hilton Hoteli i Odmarališta (Hilton Hotels & Resorts);
- DablTri (DoubleTree);
- Embasi Apartmani (Embassy Suites Hotels);
- Hilton Garden In (Hilton Garden Inn);
- Hempton (Hampton);
- Houmvue Apartmani (Homewood Suites);
- Houm2 Apartmani (Home2 Suites);
- Hilton Grand Vekejšns (Hilton Grand Vacations).¹⁰²

Kada je u pitanju bezbednost u hotelima Hilton, informacije koje se dobiju od gostiju su zaštićene i mogu da se koriste i otkriju samo u slučaju, ako država to zahteva, ako su podaci bitni za otkrivanje nekog zločinca. Ali svi podaci su zaštićeni od gubitka, zloupotrebe, otkrivanja, menjanja i uništavanja. Svaki hotel Hilton je dobro opremljeni kamerama i alarmnim sistemom, postoje i sefovi koji čuvaju sve dragocenosti gostiju, a svako kretanje zaposlenih, gostiju i dobavljača se prate, skeniraju, a elektronski podaci o navedenim aktivnostima se čuvaju u arhivi hotela.¹⁰³

¹⁰² <http://www.hiltonworldwide.com/portfolio>

¹⁰³ <http://www.hiltonworldwide.com/portfolio>

10.2. Sigurnost turista u „Marriott” hotelima



Hotelski lanac Marriott je počeo sa poslovanjem otvaranjem dva motela 1950. godine. Prvi je otvoren blizu aerodroma u Vašingtonu, a drugi u centru grada. Danas broji veliki broj hotela u 74 zemlje, sa više od 3800 smeštajnih objekata. Bezbednosne procedure i procene rizika u hotelima Marriott su česte. Osoblje je obučeno da proceni i na odgovarajući način reaguje na preteće situacije i svi hoteli sarađuju sa lokalnim, državnim, federalnim i međunarodnim organima. Svaki gost hotela Marriott prilikom ulaska u sobu dobija listu saveta kojih bi trebalo da se pridržavaju kako bi bili sigurni u hotelu:

1. Ako neko zakuca na vrata hotelske sobe treba pitati ko je pre otvaranja. Ako se predstavi kao zaposleni hotela proveriti sa recepcijom da li je poslala nekog i zašto, ako niste vi pozvali room service.
2. Nosite sa sobom ključ od sobe i ne ostavljajte ga na vidno mesto dok ste van hotela. Ako ga slučajno izgubite, javite recepciji odmah.
3. Pre izlaska iz sobe proverite da li su svi prozori zatvoreni.
4. Ne pozivajte strance u sobu.
5. Ostavite sve bitne stvari u sef hotela.
6. Ako se vraćate kasno uveče u hotel idite osvetljenim ulicama.
7. Ako vidite neku sumnjivu radnju u hotelu, prijavite recepciji.
8. Proverite sve izlaze u hotelu u slučaju da se desi nešto, kako bi na vreme mogli da reagujete.¹⁰⁴

¹⁰⁴ www.marriott.com

10.3. Sigurnost turista u „Hyatt Hotels & Resort” hotelima



Hotel „Hyatt” je osnovan 1957. godine u Los Angelesu. Širenjem poslovanja ovog hotela osnovani su novi hoteli širom sveta, pa je nastao lanac hotela pod nazivom „Hyatt Hotels & Resort”. Cilj lanca hotela je da pruži komfor i sigurnost gostima, a bezbednosne tehnologije omogućavaju da se očuva bezbednost turista:

- Integrisani sistemi za nadzor
- Napredne brave
- Sistemi za kontrolu ulaska¹⁰⁵

Prilikom dolaska u hotel uzimaju se lični podaci koji se koristi u skladu sa Globalnim pravilima za goste. Ovim pravilima se ostvaruje Hyatt-ova posvećenost zaštite ličnih podataka, a ista su usvojena za sva zasebna i izdvojena pravna lica koja upravljaju, posluju, rukovode, izdaju licence. Vrsta ličnih podataka koje hotel obrađuje su:

- Ime i prezime, pol, kućne i poslovne kontakt informacije, poslovno zvanje, datum i mesto rođenja, nacionalnost i informacije o vizi;
- Informacije o boravku, uključujući hotele u kojima su gosti odsedali, datum dolaska i odlaska, dobra i usluge koje su korišćeni
- Podaci o kreditnim karticama, podaci o članstvu u programu za redovne goste Hyatt Gold Passport®, podaci o korisničkom nalogu na mreži, profilu ili lozinci i svi podaci o članstvu u programima redovnih korisnika avionskih ili putničkih usluga;
- Bilo koje informacije neophodne da bi se ispunili posebni zahtevi (na primer, zdravstveno stanje koje zahteva specifičan smeštaj, nabavku robe i usluga)
- Podaci koje gosti pruže u vezi marketinškim preferencijama ili tokom učešća u anketama, konkursima ili promotivnim ponudama;

¹⁰⁵ <http://www.hyatt.com/hyatt/about/security-safety>

- Podaci dobijeni na osnovu korišćenja nadzornih kamera, sistema ključ-kartica i drugih sigurnosnih sistema;
- Kontakt i drugi relevantni podaci u vezi sa zaposlenima, korporativnih klijenata i dobavljača i drugih pojedince sa kojima poslujemo (na primer, turističkim agentima ili organizatorima sastanaka i događaja); i
- U ograničenim slučajevima, podaci u vezi sa kreditnim stanjem klijenata.

S obzirom da je hotelu veoma važna bezbednost hotela, koristi se SSL softver (engl. Secured Socket Layer) („SSL”) za šifrovanje ličnih podataka. Ako gostov pregledač podržava SSL (a većina podržava), svi lični podaci koji se predaju putem Interneta biće šifrovani. Može da se proveriti da li se lični podaci prenose pomoću SSL šifrovanja tako što se potraži simbol zaključanog katanca ili ispunjenog ključa na donjoj traci prozora pregledača. Takođe može se da proveriti da li će lični podaci biti šifrovani SSL šifrovanjem tako što se pogleda da li se prefiks Internet adrese te strane promenio sa „http“ na „https“. Ako se ne vidi odgovarajući simbol i prefiks „https“, ne bi trebalo da pretpostavljate da će lični podaci koje treba da unesete biti šifrovani pre prenošenja. Lične podatke koje si prikupe putem Interneta se čuvaju u bazama podataka koje su zaštićene kombinacijom fizičkih i elektronskih mera pristupa, tehnologijom zaštitnog zida (engl. „firewall“) i drugim opravdanim zaštitnim merama. Bez obzira na to, takve zaštitne mere ne mogu da spreče sve gubitke, zloupotrebe ili promene ličnih podataka, a hotel nije odgovoran za štete ili gubitke nastale u slučaju takvih incidenata u najvećoj meri koju dozvoljava zakon. Ako to zakon zahteva, gosti se obaveštavaju u slučaju bilo kog takvog gubitka, zloupotrebe ili promene ličnih podataka, kako bi se preduzele odgovarajuće radnje radi zaštite prava gosta.¹⁰⁶

¹⁰⁶ http://www.hyatt.com/hyatt/www/privacy-policy_sb.jsp

10.4. Sigurnost turista u „Sheraton hotels & resorts” hotelima



Hotel Sheraton je osnovan 1937. godine u Springfieldu od strane Ernesta Hendersona i Roberta Mura. U roku od dve godine oni su kupili još tri hotela u Bostonu. 1947. godine Sheraton postaje prvi lanac hotela na Njujorškoj berzi. Danas ovaj lanac hotela ima 400 hotela u 70 zemalja. Sheraton korporacija poseduje najsavremeniji rezervacioni sistem pod nazivom Reservation IV. On sadrži šest setova, plus pakete i programe posebnih usluga i cena, kao sto su Sheraton Executive Traveler. Namenjen je odabranoj poslovnoj klijenteli i određenim kompanijama. Ovaj rezervacioni sistem ima sledeće pogodnosti:

1. Blagovremena informisanost o svim poslovnim promenama u funkcionisanju hotelskog preduzeća. Svaka poslovna promena definisana je kroz standarde i optimume ponašanja. Cilj je postizanje maksimalnih rezultata. Kontinuirani proces promena i prilagođavanja zahtevima korisnika omogućuje brze promene i primenu sistema.
2. Maksimalnu iskorišćenost svih raspoloživih kapaciteta, u zavisnosti od uslova privređivanja na nivou svih tehnoloških celina i poslovnih aktivnosti.
3. Kontinuitet u praćenju troškova i utrošaka i njihova kontrola, koja ima za cilj poboljšanje finansijskih efekata prodaje.¹⁰⁷

¹⁰⁷ <http://www.starwoodhotels.com>

Zaključak

Kada turista započinje proces planiranja putovanja on ulaže svoje vreme, novac i energiju sa ciljem da bude jači i bolji kada se vrati u mesto stalnog boravka. Međutim ono što može poremetiti planove i taj cilj, su rizici ili incidenti na putovanju. Incidenti kao što su pokradenost, teroristički napadi, zemljotresi, epidemije, pandemije, lokalni ratovi, mogu biti uzrok neodlaženja na tu destinaciju.

Ako znamo da je tako, a to vidimo na osnovu mnogih činjenica izloženih u ovom radu, možemo reći da bezbednost predstavlja temelj svake destinacije i veoma važan deo kapitala turističke destinacije. Svaka destinacija bi trebala da ima visok nivo bezbednosti da u slučaju opasnosti ima planove koji će sprečiti moguć napad bilo koje vrste. Odnos između turizma i bezbednosti treba dublje gledati i razumeti. Da bi to shvatili potrebno je proučavanje odnosa, koji podrazumeva dva pravca istraživanja. Prvi pravac istraživanja je pristup gde se kreće od specifičnih zapažanja i mera, formulisanje obrazaca i hipoteza koje treba testirati i potvrditi, koji na kraju dovodi do opštih zaključaka. Drugi pravac istraživanja podrazumeva vođenje studije kako bi se proverila i predložila teorija bezbednosti u turizmu. Postizanje ovog cilja je imperativ, ukoliko turistički subjekti žele da razviju i usvoje efikasne strategije i metode za sprečavanje, ublažavanje i smanjenje incidenata na turističkim destinacijama.

Ono što je bitno, kad su u pitanju strategije, jeste da treba da se izabere optimalna kombinacija strategija za svaku situaciju posebno. Prilikom odabira strategija koje treba primeniti, možda će se jedna strategija od druge više isticati ili izgledati kao pojedinačno rešenje, al bi trebalo više njih kombinovati u cilju jače bezbednosti i sigurnosti.

Pored toga, bitno je da nacionalna odeljenja za turizam rade na sigurnosti i bezbednosti destinacije, a to pre svega mislim na:

- Odeljenje za bezbednost
- Ministarstvo zdravlja
- Odeljenje unutrašnjih poslove
- Hotelska udruženja
- Privredne komore

Osoblje zaposleno u turističkim objektima mora biti obučeno za suočavanje sa kriznim situacijama, kako bi turistima pružili sve potrebne informacije i odgovarajuću pomoć.

Turistička mesta i objekti moraju imati odgovarajuću zaštitu, a javni i privatni sektor moraju definistati i preuzeti odgovornost u svom području. Postojanje službi za hitne slučajeve koji stoje na raspolaganju turistima, ima takođe veliku ulogu i one obuhvataju:

- Intervenciju na licu mesta (telefonske linije za pomoć, prva pomoć, hitna služba, policija)
- Službe za strance (pristup konzulatima i diplomatskim predstavnicima),
- Pomoć na putovanju,
- Službe za osiguranje,
- Udruženja za zaštitu potrošača,
- Državne mere za nadoknadu štete (posebno u slučaju terorizma),
- Službe koje osiguravaju turistima povratak u zemlju

Još jedan od prioriteta u hotelu treba da je bezbednost podataka, privatnost gostiju i analitička arhitektura sistema bezbednosti informacija, kako bi mogli da reaguju i upravljaju znatno većim obimom podataka kao i alati za ublažavanje kritičnih faktora rizika, na prihvatljiv nivo.

Ceo koncept sigurnosti informacija se bazira na konceptu upravljanja rizicima koji podrazumeva proces identifikacije, kontrole, eliminacije sigurnosnih rizika koji mogu da utiču na informacije i informacione sisteme, a koji mora da bude finansijski pravedan.

U vremenu kada postoji izrazit rast količine informacija i znanja u organizacijama i njihovoj komunikaciji sa korisnicima, za potrebe bezbednosti informacija i za potrebe sticanja korisničkog poverenja, neophodno je koristiti zahteve modela ISO 27001, čime se stvara sistem koji je fokusiran na poboljšanje i smanjenje troškova i eliminisanje grešaka iz sistema.

Literatura

1. Barjaktarović L., *Upravljanje rizikom*, Univerzitet Singidunum, Beograd 2009.
2. Breakwell, G. M., *The psychology of risk*, Cambridge, Cambridge University Press. 2007.
3. Beirmann, D., 2003. *Restoring tourism destinations in crisis: A strategic marketing approach*, United Kingdom, CABI Publishing.
4. Branislav Rabotić, *Selektivni oblici turizma*, Visoka turistička škola strukovnih studija, 2012.
5. Blake, A. and Sinclair, M. T., 2003. *TOURISM CRISIS MANAGEMENT: US Response to September 11*. *Annals of Tourism Research*, 30 (4), 813-832.
6. Breakwell, G. M., 2007. *The psychology of risk*, Cambridge, Cambridge University Press.
7. Cavlek, N., 2002. *Tour operators and destination safety*. *Journals of Tourism Research*, 29 (2), 478-496.
8. Creswell, J., 2009. *Research design: qualitative, quantitative, and mixed methods approaches*, Thousand Oaks: CA, Sage.
9. Dobranović Ž., *Opći pristup sigurnosti u turizmu, Sigurnost i samozaštita u turizmu*, Defimi, Zagreb.2003.
10. Vladimir N. Cvetković- *Rizik, moć, zaštita; Uvođenje u nauke bezbednosti*, Službeni glasnik, Beograd 2010.
11. Živković Radmila- „Ponašanje i zaštita potrošača u turizmu“ ; Fakultet za turistički i hotelijerski menadžment; Univerzitet Singidunum; Beograd, 2010.
12. Friedrich Ebert Stiftung-Klimatske promene, studije i analize, Univerzitet u Beogradu, Arhitektonski fakultet, Beograd, 2011.
13. Gojko Grubor „Projektovanje menadžment sistema zaštite informacija“, Univerzitet Singidunum, Beograd 2011.
14. Kozak, M., Crotts, J. C. and Law, R., 2007. *The impact of the perception of risk on international travellers*. *International Journal of Tourism Research*, 9 (4), 233-242.
15. Lepp, A. and Gibson, H., 2003. *Tourist roles, perceived risk and international tourism*. *Annals of Tourism Research*, 30 (3), 606-624.
16. Lepp, A. and Gibson, H., 2008. *Sensation seeking and tourism: Tourist role, perception of risk and destination choice*. *Tourism Management*, 29, 740-750.
17. Mansfeld, Y. and Pizam, A., 2006. *Tourism, security and safety: from the theory to practice*, Butterworth-Heinemann.

18. Miljević Milan, *Metodologija naučnog rada, Filozofski fakultet, Univerzitet u istočnom Sarajevu, Pale*, 2007.
19. Njeguš, A. (2013) „Bezbednost informacione imovine u hotelskom poslovanju“, *Seminar o zaštiti podataka o ličnosti u hotelskoj industriji, JPM & HORES, Beograd*
20. Petrović R. S., *Strani pravni život- dilema Institut za uporedno pravo, Beograd 2012. godine*
21. *Teorijsko stručni časopis Ministarstva unutrašnjih poslova Republike Srbije, Kosmos, Zemun*, 2006.
22. www.unwto.org
23. www.balkanmagazin.net
24. www.today.reuters.com
25. www.maplecroft.com
26. [www.politika.rs/ magazin](http://www.politika.rs/magazin)
27. www.travelmedicine.com
28. www.pressonline.rs
29. www.emins.org
30. [www.swissbusiness .org.sg](http://www.swissbusiness.org.sg)
31. www.časopis horizont.com
32. www.travelmagazin.rs
33. www.stetoskop.info
34. www.who.int
35. www.beuc.org (BEUC- The European Consumers Organization)
36. www.safety.com
37. www.smedia.rs
38. www.mojaputovanja.com
39. [http://www.cis.hr/files/Celuska Osnove_upravljanja_rizikom.pdf](http://www.cis.hr/files/Celuska_Osnove_upravljanja_rizikom.pdf)
40. www.crnarupa.singidunum.ac.rs
41. <http://www.cqm.rs/2011/2/pdf/28.pdf>
42. www.tqmkonsalting.com
43. <http://www.prointer.rs/sr/bellevue-hotel-software>
44. <http://www.hiltonworldwide.com/portfolio/>
45. www.marriott.com

46. <http://www.hyatt.com/hyatt/about/security-safety>

47. <http://www.starwoodhotels.com>

48. www.hotelparkbeograd.rs