BEZBEDNE RAČUNARSKE KOMUNIKACIJE KAO PREDUSLOV USPEŠNOG POSLOVANJA SPORTSKOG CENTRA "ČAIR"
SECURE COMPUTER COMMUNICATIONS AS A PRECONDITION TO SUCCESSFUL OPERATION OF THE SPORTS CENTRE "ČAIR"

Miodrag Nikolić, *Visoka škola strukovnih studija za poslovno industrijski menadžment, Kruševac*
Zoran Nikolić, *Fakultet za industrijski menadžment, Kruševac*
Bratislav Ignjatović, Dragan Bogojević, Dejan Radojević*, Sportski centar "Čair", Niš*

Sažetak - *U radu se razmatra neophodnost bezbednog prenosa podataka kroz distribuirani informacioni sistem. Objašnjena je tehnika uspostavljanja zaštićenih računarskih komunikacija kao i šifrovanja podataka koji se prenose takvim vezama. Cilj rada je da se ukaže na potrebu zaštite integriteta podataka sa aspekta stabilnog i kontinuiranog poslovanja sportskih centara čije je upravljanje podržano primenom savremenih informatičkih tehnologija. Posebno je naglašena obaveza obezbeđenja delikatnih zdravstvenih i ličnih podataka iz elektronskih kartona sportista, skladištenih u jedinstvenoj bazi poslovnog Intranet-a koji se oslanja na javne računarske mreže i u takvoj organizaciji podložan zlonamernim napadima. U radu se ta problematika razmatra sa aspekta poslovanja sportskih centara podržanog strukturno kompleksnim informacionim sistemom. Izložena su rešenja Informacionog sistema Sportskog centra "Čair". Predstavljeni su dosadašnji rezultati i konceptualno rešenje koje je u procesu projektovanja i implementacije.*
Ključne reči - Informacioni sistem sportskog centra, bezbedne računarske komunikacije, elektronski karton sportiste
Abstract – *The paper deals with the necessity of secure data transfer through the distributed informational system. The technique of setting up secure computer communications and encryption of transferring data has been explained. The purpose of the paper is to draw attention to the need to protect data integrity from the aspect of stable and continual operations of sports centers whose management is supported with the applications of modern informational technologies. The paper emphasizes the responsibility of securing the confidential medical and personal data from the athletes' electronic file, which are stored in the unique Intranet database reliant on public computer networks and, in such an organization, are prone to malicious attacks. This problem is deliberated upon in the paper from the aspect of sports centers' operations supported by structurally complex informational system. The paper details the solutions of the Sports Centre Čair's Informational system and presents current results and conceptual solution that is in the process of design and implementation.*
Key words: Sport center informational system, secure computer communications, athlete's electronic file

1. UVOD

Primena savremenih informatičkih tehnologija u uspešnom poslovanju privrednih i društvenih subjekata je realnost i imperativ današnjice. Sva proizvodna preduzeća koja se bore za svoj deo profita na tržištu, primenjuju informacione sisteme kako bi opstali u nemilosrdnoj borbi sa konkurencijom. Primenom savremenih računarskih tehnologija organizuju, prate i nadgledaju proizvodne kao o sve ostale procese u preduzeću. Koriste Web tehnologije za reklamu i predstavljanje svojih proizvoda, za pridobijanje novih i zadržavanje poverenja starih kupaca. Ovakvi informatički sistemi tipa ERP primenjuju se ne samo u proizvodnim sistemima, već i u uslužnim i saobraćajnim sistemima [1] kao i u organizacijama državne uprave. Uvođenjem savremenog integrisanog informacionog sistema preduzeća dostižu viši nivo stabilnosti i sigurnosti u poslovanju. Dobijaju potpun uvid i kontrolu troškova, podižu nivo usluga i unapređuju upravljanje ljudskim resursima. Krajnji efekat ovakvih promena je veća rentabilnost, kvalitetniji proizvod ili usluga i efikasnije poslovanje.

Značaj primene integrisanih informacionih sistema u efikasnom poslovanju prepoznao je i menadžment Sportskog centra "Čair" u Nišu. Efikasno poslovanje za ovu upravljačku strukturu ne znači samo poboljšanje materijalnih efekata poslovanja već, posredno, stvaranje optimalnih uslova za rad svih sportskih terena i pratećih objekata. Time se integrisani informacioni sistem stavlja u funkciju efikasne organizacije, monitoringa i održavanja sportskih objekata i obezbeđuje kontinuitet kvalitetnog trenažnog procesa [2].

2. INFORMATIČKO KOMUNIKACIONE TEHNOLOGIJE U FUNKCIJI USPEŠNOG POSLOVANJA SPORTSKIH OBJEKATA

Usavršavanje računarske opreme i pojeftinjenje hardvera do neslućenih razmera doveo je do razvoja jeftinih a moćnih

informacionih sistema baziranih na platformi personalnih računara. Skupi računarski sistemi, zatvorene arhitekture i specijalizovane programske podrške, zastarevaju i izlaze iz upotrebe [3]. Njih zamenjuje koncept otvorene arhitekture baziran na mreži radnih stanica tipa PC i široko raširenim operativnim sistemima i aplikativnim programima koji su često čak i otvorenog koda [4]. Time primena informacionih sistema u poslovanju prestaje da bude privilegija visoko profitabilnih organizacija. Stiču se uslovi da i male društvene organizacije sa skromnim budžetom unaprede svoje poslovanje primenom savremenih informaciono komunikacionih sistema.

Rukovodstvo Sportskog centra "Čair" odlučilo je da uvede savremeno koncipiran integrisani informacioni sistem sa ciljem da pokrije sve procese u organizaciji rada. Cilj ovog poduhvata je integracija procesa planiranja i upravljanja svim resursima i njihovo korišćenje u čitavom kompleksu sportskog centra. To se postiže softverskim paketom koji obezbeđuje integraciju toka raznorodnih informacija kroz razuđeni sportski kompleks, kombinujući različite izvore informacija u jednu softversku aplikaciju i jedinstvenu bazu podataka. Osim standardnih izvora informacija čiju obradu objedinjuju različiti podsistemi ERP softverskih rešenja [5], u slučaju poslovne integracije sportskog centra poseban akcenat se stavlja na podatke i parametre koji se tiču tehničkog sektora kompleksa. Misli se pre svega na mašinsko postrojenje za grejanje vode bazena i toplane za zagrevanje hala i fiskulturnih sala. Proizvođači ERP softverskih rešenja predviđaju podsisteme održavanja sa sledećim modulima: hardver (tehnički uređaji), održavanje, servis [6]. Sa aspekta poslovanja sportskog kompleksa "Bazen Čair", zahtevi vezani za modul održavanja idu i dalje od računarske obrade radnog naloga za održavanje. Implementirani podsistem održavanja treba da ima mogućnost dinamičkog nadgledanja svake merne tačke tehničkog sektora, čime se na efikasan način sprečavaju moguće havarije i kvarovi a samim tim izbegava zastoj u upotrebi sportskog objekta.

Sa aspekta finansijskog poslovanja odgovarajući podsistem Integrisanog informacionog sistema treba da ispuni, pored standardnih, i neke posebne zahteve. Oni su vezani za specifičnost poslovanja vezanog za organizovanje sportskih, zabavnih i poslovnih priredbi. Informacionim sistemom se uvedi potpuni nadzor nad prodajom karata. Veza automata na svim ulaznim mestima sa informacionim sistemom SC, obezbediće efikasnu kontrolu prodatih karata a posrednom vezom sa Informacionim sistemom policije i evidenciju i kontrolu gledaoca.

Rukovodstvo Sportskog centra postavlja još jedan specifičan zahtev pred projektante Informacionog sistema. To je briga o svakom sportisti, korisniku nekog od sportskih objekata. To se ostvaruje uvođenjem **"sportskog elektronskog kartona",** kako za sportiste pojedince tako i za sportske organizacije i timove. U toj "elektronskoj sportskoj knjižici" prati se kompletan razvoj dečaka i devojčica od njihovih prvih koraka vezanih za fizičko vaspitanje i aktivnost [2]. Priroda nastajanja tih podataka podrazumeva daljinski pristup informacionom sistemu. Poseban zadatak i specifičnost integrisanog informacionog sistema sportskog kompleksa "Čair" je povezivanje njegove baze podataka sa bazom podataka Zdravstvenog Informacionog Sistema (ZIS). Rezultati sistematskih pregleda sportista u sportskim ambulantama slivaće se u "elektronski karton pacijenata" u jedinstveni ZIS države, isto kao i rezultati specijalističkih pregleda. Vezom ova dva informaciona sistema, sve iformacije o zdravstvenom stanju sportiste biće uvek dostupne klupskom lekaru i treneru bilo da se nalaze na nekom od objekata Sportskog centra, na planini na visinskim pripremama ili nekom drugom trenažnom kampu [7].

3. BEZBEDNOST INFORMACIONOG SISTEMA

Sportski centar predstavlja složen poslovni sistem povezan sa velikim brojem kako proizvodnih organizacija tako i državnih institucija. S obzirom na njegovu funkciju očuvanja i unapređenja zdravstvenog stanja stanovništva i na njegovu opšte društvenu funkciju, veoma je značajan segment za lokalne zajednice i državu u celini. Informacioni sistem sportskih centara je u razvoju i ima osnovni zadatak da podrži i učini efikasnijim poslovanje ovih društvenih subjekata. Njegov osnovni cilj je organizacija, racionalizacija i funkcionisanje sportskih centara na optimalan način, odnosno poboljšanje kvaliteta uslužne delatnosti i da obezbedi tačne, potpune i blagovremene informacije u cilju smanjenja troškova poslovanja. S obzirom na potrebu njegovog daljeg povezivanja sa informacionim sistemima elektronske uprave u društvu kao i Zdravstvenim Informacionim Sistemom, bezbednost i integritet podataka skladištenih u njemu postaje ključni problem ne samo za informacioni sistem sportskog centra već i za navedene informacione sistema na koje se oslanja. Prilikom kreiranja Informacionog sistema sportskog centra važno je pridržavati se važećih standarda koji se odnose na formate podataka zbog njihove razmene sa ostalim društvenim i proizvodnim organizacijama. Neophodno je ostvariti uslove za njihovu bezbednost sa posebnim akcentom na bezbednu komunikaciju pri prenosu podataka sa ostalim informacionim sistemima. Zaštitom Informacionog sistema SC "Čair" ostvaruje se i bezbednost čitavog integrisanog informacionog sistema u državi.

Bezbednost bilo kog informacionog sistema čine tri osnovna principa: **poverljivost** (*Confidentality*) - sprečavanje namernog ili nenamernog neovlašćenog pristupa podacima, **celovitost** (*Integrity*) - podatke u sistemu mogu menjati lica ili procesi koji su za to ovlašćeni i da podaci moraju biti interno i eksterno konzistentni, **raspoloživost** (*Availability*) - podaci su dostupni korisnicima sistema na pouzdan način i u trenutku kada su korisniku potrebni [8]. Očuvanje ova tri principa su osnovni ciljevi zaštite u svakom sistemu i, s obzirom na osetljivost ličnih i poslovnih podataka i sam distribuirani proces rada, posebno su naglašeni u Informacionom sistemu sportskog centra.

S obzirom da jedan informacioni sistem nije samo skup međusobno povezanih tehničkih aparata već on predstavlja interakciju svih ljudi koji su uključeni u sistem, tzv "nosioca" informacionog sistema - *stakeholders*-a, veoma je značajno da se prilikom dizajna sistema u celini obuhvate svi bezbedonosni aspekti. Ovo podrazumeva planiranje kontinuiteta poslovanja, odnosno očuvanja osnovnih principa bezbednosti za veliki broj scenarija od onih koji podrazumevaju prirodne katastrofe pa do pretnji koje se

mogu desiti od svakog pojedinca u sistemu. Narušavanje osnovnih ciljeva bezbednosti moguće je na mnogo načina i ono može nastati zbog:

1. fizičkog uništenja opreme;
2. napada na fizičkom nivou;
3. napada na mrežnom nivou;
4. napada na nivou operativnog sistema;
5. napada malicioznim kodom (trojanci, virusi);
6. napada na aplikativnom nivou, napadima socijalnim inženjeringom, itd.

Imajući u vidu navedeno, bezbedonosni aspekti u informacionom sistemu se mogu podeliti na one tehničke prirode kao i na one koji se odnose na učesnike u sistemu [9].

Servisi i mehanizmi zaštite, sami po sebi, ne znače mnogo ukoliko nema odgovarajuće strategije ostvarivanja bezbednosti. **Strategija ostvarivanja bezbednosti** u IS-u je plan koji pokazuje pravac ostvarivanja usluga, tj. određuje ko je odgovoran za koji aspekt bezbednosti i kojim resursima će se ti aspekti realizovati. Da bi strategija bila uspešna, mora se izvršiti klasifikacija podataka, isprojektovati pravila i procedure ponašanja na sistemu, izvršiti dodeljivanje uloga učesnicima u sistemu pri čemu one sa sobom povlače određena prava i odgovornosti i, što je najvažnije, svo osoblje sistema mora biti obučeno u tolikoj meri da svojim delovanjem doprinosi sprovođenju strategije bezbednosti. Sam pojam bezbednosti ne treba da se posmatra kao „gotov proizvod“ već kao proces koji ciklično treba da prolazi kroz određene faze, a to su:

1. razmatranje i uočavanje pretnji i ranjivosti;
2. vršenje procene rizika;
3. vršenje korektivnih radnji kao i
4. stalna kontrola nad sprovođenjem definisanih procedura i pravila.

Kod planiranja zaštite podataka, odnosno očuvanja osnovih principa bezbednosti kod IS-a, potrebno je prevenstveno obezbediti zaštitu podataka na fizičkom nivou. Ona podrazumeva da serveri i mrežno-komunikaciona oprema koja služi za skladištenje i transport podataka moraju biti smešteni u posebno osiguranim prostorijama. Te prostorije treba da ispunjavaju određene uslove koji obezbeđuju neprekidno napajanje, adekvatno hlađenje kao i da poseduju sisteme za zaštitu od požara i sprečavanje neovlašćenog pristupa [9].

Na polju zaštite mreža jedna od najefikasnijih i najraširenijih strategija ostvarivanja bezbednosti je s*lojevita zaštita* koja se zasniva na formiranju zaštitnih slojeva (prstenova) oko sistema [8]. U ovakvom sistemu korisnik mora da prođe kroz nekoliko slojeva kako bi pristupio podacima, a svaki od slojeva podrazumeva upotrebu određenih zaštitnih mehanizama koji zadržavaju potencijalnog napadača, odnosno, minimiziraju njegov pristup podacima. Slojeviti pristup zaštite treba da, u skladu sa strategijom ostvarivanja bezbednosti, obezbedi kombinaciju sigurnosnih mehanizama i tehničkih rešenja koji obuhvataju dovoljno široku lepezu sigurnosnih zahteva. Njegova bitna karakteristika je da eventualno probijanje jednog od slojeva sistema nema kritične posledice na bezbednost celog sistema.

Sa aspekta dislokacije objekata Sportskog centra i njegovog razuđenog IS-a, od posebnog je značaja "*treći zaštititni sloj "* čiji je zadatak da štiti sistem od “unutrašnje“ mreže i sadrži mehanizme kao što su infrastruktura za sertifikovanje javnih ključeva (PKI), virtuelne privatne mreže (VPN) i mrežne barijere. Veliki radijus kretanja korisnika IS-a SC-a nalaže "definisanje mobilnog pristupa i rada" koji se obavlja bežičnom komunikacijom kao i preko Interneta. Za taj vid rada definišu se posebne politike koje se odnose na sam uređaj sa kojeg se vrši pristup, tip uspostavljanja sigurnog prenosa podataka, način šifrovanja, odgovornosti kao i obaveze i plan u slučaju otuđivanja mobilnog uređaja.

4. ZAŠTIĆENE RAČUNARSKE KOMUNIKACIJE

Analize bezbednosti mreže na Internetu ukazuju da su Virtuelne privatne mreže (Virtual Private Networks – VPN) danas najbezbednija tehnologija za komunikaciju svih vrsta podataka preko otvorene javne globalne mreže kao što je Internet [10]. One emuliraju vezu tačka-tačka tunelovanjem podataka, sa enkapsulacijom i enkripcijom pomoću bezbedonosnih protokola, čime ostvaruju privatnost, integritet i raspoloživost, što su osnovni elementi bezbednosti svake mreže. Ipak i ove mreže pokazuju ranjivost na neke standardne napade Internet okruženja [11], tako da generalno tretiranje ovih mreža kao bezbedne nije moguće.

Može se reći da je Virtuelna privatna mreža skup uređaja, povezanih korišćenjem Interneta ili tuđe privatne mreže kao transportnog medijuma, koji krajnjem korisniku daje privid potpuno ili delimično izolovane privatne mreže. Ona pruža mogućnost da se privatne komunikacije obavljaju preko javne mreže kao što je Internet. Sam termin se odnosi na kombinaciju tehnologija i tehnika koje osiguravaju komunikacije između dve krajnje tačke uspostavljanjem tunela neprobojnog za prisluškivanje i ometanje.

Sa aspekta koncepta realizacije mogu se podeliti na:

- VPN na nivou aplikacije;
- VPN na nivou protokola mrežnog sloja;
- VPN na nivou protokola sloja veze.

Virtuelna privatna mreža omogućava korisnicima da razmenjuju podatke vezom koja je emulirana kao direktna veza (*point-to-point* link - PPP) između klijenta i servera. PPP emulacija dobija se enkapsulacijom podataka zaglavljem koje omogućava rutiranje kroz javnu mrežu do odredišta koje je deo privatne mreže. Podaci su šifrirani i paketi koji su presretnuti u okviru javne ili deljene mreže ne mogu se pročitati bez ključa za dešifrovanje. Infrastruktura javne mreže je nebitna jer korisnik logički vidi samo svoj privatni link, odnosno nalazi se logički u lokalnoj mreži, iako je od drugih korisnika razdvojen javnom mrežom.

Tunelovanje je najvažnija komponenta tehnologije virtuelnih privatnih mreža i predstavlja prenos paketa podataka namenjenih privatnoj mreži preko javne mreže. Ruteri javne mreže nisu svesni da prenose pakete koji pripadaju privatnoj mreži i VPN pakete tretiraju kao normalan saobraćaj. Tunelovanje ili enkapsulacija je metod pri kome se koristi infrastruktura jednog protokola za prenos paketa podataka drugog protokola. Umesto da se šalju originalni paketi, oni su enkapsulirani dodatnim zaglavljem.

Dodatno zaglavlje sadrži informacije potrebne za rutiranje, odnosno usmeravanje paketa kroz mrežu, tako da novodobijeni paket može slobodno putovati transportnom mrežom. Sigurnost, niska cena, lakoća implementacije, univerzalnost su prednosti koje značajno doprinose upotrebi ove tehnologije.

Tehnologija tunelovanja koristi tri vrste protokola: protokol nosač, protokol za enkapsulaciju i transportni protokol. Rešenja koja se primenjuju su: PPTP (*Point-to-Point Tunneling Protocol) - Microsoft i* L2TP (*Layer 2 Tunneling Protocol)- Microsoft & Cisco.*

Sa stanovišta upravljanja postoje dva pristupa Virtuelnim privatnim mrežama: VPN kojima upravljaju korisnici i VPN kojima upravljaju provajderi mrežnih usluga (npr. *Internet Service Provider* - ISP). Virtuelne privatne mreže kojima upravljaju provajderi mrežnih usluga dele se na osnovu toga gde se nalazi oprema koja implementira VPN: na strani provajdera (PE - *provide edge*) ili na strani korisnika (CE - *customer edge*).

Bezbednost je integralni deo VPN usluge. Postoji veliki broj pretnji VPN mrežama:

- neovlašćeni pristup VPN saobraćaju;
- izmena sadržaja VPN saobraćaja;
- ubacivanje neovlašćenog saobraćaja u VPN (*spoofing*);
- brisanje VPN saobraćaja;
- DoS (*denial of service*) napadi;
- napadi na infrastrukturu mreže preko softvera za upravljanje mrežom;
- izmene konfiguracije VPN mreže;
- napadi na VPN protokole.

Odbrana od VPN napada realizuje se i na korisničkom i na nivou provajdera VPN usluga:

- kriptozaštita paketa;
- kriptozaštita kontrolnog saobraćaja;
- filteri;
- firewall;
- kontrola pristupa;
- izolacija.

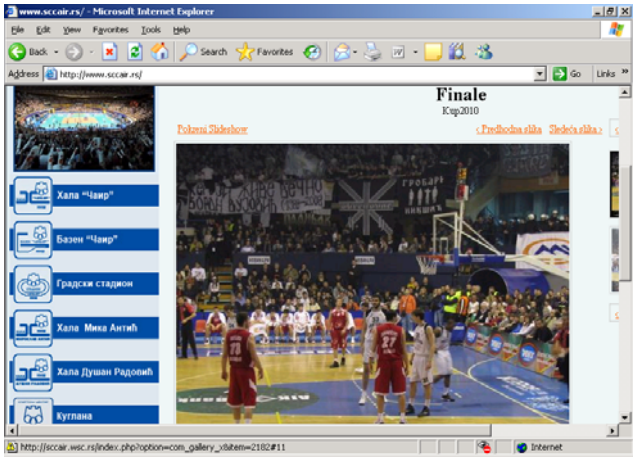
VPN mreže koje koriste Internet ili druge nebezbedne mreže obično koriste razne metode kriptozaštite. Korisnici VPN mreža sa posebnim zahtevima za bezbednost, na primer banke, obično implementiraju i dodatnu infrastrukturu za zaštitu podataka.

5. IMPLEMENTACIJA ZAŠTITE INFORMACIONOG SISTEMA SC "ČAIR"

U nastojanju da unapredi svoje poslovanje primenom Integrisanog informacionog sistema, menadžment Sportskog centra "Čair" izvršio je projektovanje informacionog sistema [12], definisao sve posebne zahteve i planirao faze njegovog uvođenja.

Sa aspekta bezbednosti IS-a preduzeto je niz mera. Server sala na centralnoj lokaciji Sportskog centra zadovoljava osnove uslove koji obezbeđuju neprekidnost napajanja, adekvatno hlađenje, sistem za dojavu požara, video nadzor itd.

Segmentacija mreže izvršena je tako da je svaka lokacija u posebnom adresnom prostoru i može da vrši razmenu podataka samo sa pripadajućim aplikativnim serverima. Serveri pojedinih sistema su takođe organizovani kao zasebni LAN. Upravljanje i monitoring celokupnog sistema obavlja se iz posebnog *Management* modula.



Slika 1. Internet prenos utakmice [www.sccair.rs]

Na svim dislociranim objektima mora biti odvojen segment računara koji radi na aplikaciji od onih koji imaju pristup Internetu. Ovo je posebno značajno zbog daljinskog pristupa Informacionom sistemu i korišćenja Web tehnologija za prenose sportskih takmičenja (slika 1). Na svakom od računara postavljene su polise koje onemogućavaju korišćenje tih računara u bilo koje druge svrhe osim rada na aplikaciji kao i upotrebu prenosnih medija.

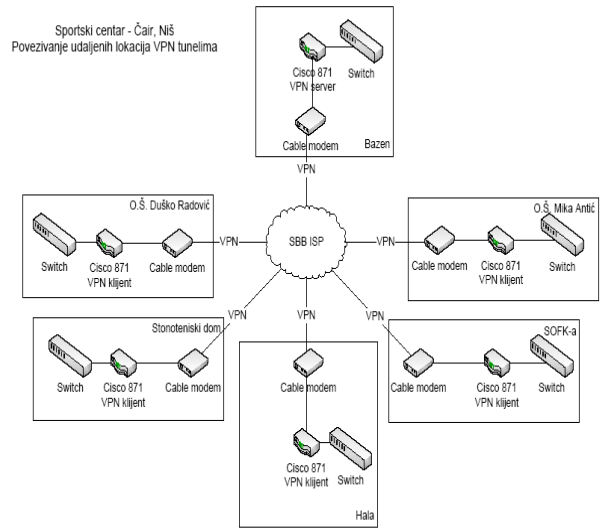
Shvatajući značaj komunikacionih tehnologija u implementaciji integrisanog informacionog sistema rukovodstvo je pristupilo instalaciji zaštićenih računarskih komunikacija. Dva su dominantna razloga uvođenje sigurnih veza: dislocirani sportski objekti koji su u sastavu sportskog kompleksa "Čair" i obaveza zaštite integriteta poslovnih podataka i ličnih podataka sportista. Razmeštaj sportskih objekata Sportskog centra "Čair" prikazan je na slici 2.

Slika 2. Razmeštaj sportskih objekata Sportskog centra "Čair"

Sa slike se vidi da su lokalne računarske mreže SOFKE, Hale sportova "Čair", sportskih hala pri osnovnim školama "Duško Radović" i "Mika Antić" i Stonoteniskog doma povezane sa LAN-om bazena "Čair" u kojoj je server centralizovane baze podataka. U postupku projektovanja i implementacije angažovana je konsultantska firma "Telelink" [13]. Ugovoreno je da komunikacija udaljenih podsistema bude ostvarena VPN tehnologijom baziranoj na opremi renomiranog proizvođača komunikacione opreme "Cisco" [14]. Slika 3. prikazuje šemu povezivanja udaljenih lokacija Sportskog cetra "Čair" u Nišu VPN tunelima [2].

6. PRAVCI DALJEG RAZVOJA

Proces uvođenja novih informacionih sistema, kao i zamena starih, praćen je različitim vrstama problema. Rukovodstvo Sportskog centra, svesno mogućih problema, izvršilo je njihovu analizu i plan prevazilaženja. Očekuje se da će dominirati dva problema: problem obezbeđivanja potrebnih finansijskih sredstava i izrada posebnih podsistema Integrisanog informacionog sistema za pokrivanje specifičnih procesa u Centru.



Slika 3. Povezivanje udaljenih lokacija Sportskog cetra Čair u Nišu VPN tunelima [2]

I pored mnoštva modernih tehnoloških rešenja koja za cilj imaju očuvanje osnovnih principa bezbednosti, ni jedan informacioni sistem nije "neprobojan". Svesni te činjenice, menadžment SC "Čair" posvetiće posebnu paznju zaštiti informacionog sistema i razmene podataka primenom tehnologija javnih i tajnih ključeva, elektronskog potpisa i drugih. S obzirom da ektronski ili digitalni potpis predstavlja prvi stepen u identifikaciji stranaka koje razmenjuju poruke, rukovodstvo sprovodi korake dobijanja elktronskog potpisa i njegovog korišćenja u poslovnoj komunikaciji. Ova tehnologija, koja se primenjuje u sistemima elektronskog poslovanja i omogućava proveru potpisnika, štiti integritet podataka koji se prenose i tačnost elektronskog potpisivanja poruke ili dokumenta, predmet je rada koji je u proceduri objavljivanja.

7. ZAKLJUČAK

U radu je pokazana neophodnost primene informaciono komunikacionih tehnologija u savremenom poslovanju svih društvenih subjekata sa posebnim osvrtom na potrebe sportskih centara. Razmatran je problem bezbednosti informacionih sistema. Zbog specifičnosti organizacije SC "Čair" i njegovih veza sa okruženjem, posebna pažnja posvećena je analizi sigurnih računarskih komunikacija. Prikazani su dosadašnji rezultati Sportskog centra „Čair" u implementaciji Integrisanog informacionog sistema i njegovoj zaštiti. Naznačeni su pravci daljeg razvoja i zaštite IS-a.

8. LITERATURA

[1] http://www.saga-infotech.net/viewPage.do?ID=23

[2] Игњатовић, Б., Богојевић, Д., Радојевић, Д., Николић, З., Николић, М., *"Примена на информациски комуикациски технологии како еден од предусловите за оптимална припрема на спортската омладина"*, 13ти Симпозијум за спорт и физичко образование на младите, Охрид, Октобар 2009.

[3] Nikolić, M., Nikolić, Z., Petrović, Ž., *"Razvoj jednog rešenja fabričkog informacionog sistema*", YU INFO 2009, Kopaonik, Mart 2009.

[4] Kajan, E.**,** *Otvoreni sistemi Koncepti, Komponente i Aplikacije za budućnost***,** Prosveta, Niš, 1994.

[5] http://www.sap.com/solutions/business-suite/erp/

[6] http://www.saga-infotech.net/viewPage.do?ID=419

[7] Nikolić, Z. , Milosavljević, B., Nikolić, M., *"Radn na daljinu - oblik rada budućnosti"*, YU INFO 2009, Kopaonik, mart 2009.

[8] Pleskonjić, D., Maček, N., Đorđević, B., Carić, M., *Sigurnost računarskih sistema i mreža*, Mikro knjiga, Beograd, 2007.

[9] Reković, D., Balota, A., Glomazić, Z., Šendelj, R., *"Bezbjednost informacionog sistema u zdravstvu"*, YU INFO, Kopaonik, mart 2009, Zbornik radova na CD-u.

[10] Kovačević, F., *"Ocena bezbednosti i zaštita mreže na Internetu"*, ETRAN, Herceg Novi, jun 2003.

[11] Schneier & Mudge, Cryptoanalysis of Microsoft Point-to- Point Tunneling Protocol, www.counterpane.com

[12] Veljović, A., *Projektovanje informacionih sistema***,** Kompjuter biblioteka, "Svetlost" Čačak, 2003.

[13] http://www.telelink.co.yu/sr/index.html

[14] http://www.cisco.com/en/US/products/ps5743/