MOGUĆNOSTI DALJNJEG RAZVOJA NACIONALNE INFORMACIJSKE INFRASTRUKTURE U DOMENI ZAŠTITE NA RADU

Franović, Kristina

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij Sigurnosti i zaštite

Kristina Franović

MOGUĆNOSTI DALJNJEG RAZVOJA NACIONALNE INFORMACIJSKE INFRASTRUKTURE U DOMENI ZAŠTITE NA RADU

ZAVRŠNI RAD

Karlovac, 2019.

Karlovac University of Applied Sciences

Safety and Protection Department

Professional graduate Study of Safety and Protection

Kristina Franović

POSSIBILITIES OF FURTHER DEVELOPMENT OF THE NATIONAL INFORMATION INFRASTRUCTURE IN THE DOMAIN OF SAFETY AT WORK

FINAL PAPER

Karlovac, 2019.

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij Sigurnosti i zaštite

Kristina Franović

MOGUĆNOSTI DALJNJEG RAZVOJA NACIONALNE INFORMACIJSKE INFRASTRUKTURE U DOMENI ZAŠTITE NA RADU

ZAVRŠNI RAD

Mentor:

dr.sc. Damir Kralj, prof.v.š.

Karlovac, 2019.

VELEUČILIŠTE U KARLOVCU

KARLOVAC UNIVERSITY OF APPLIED SCIENCES
Trg J.J.Strossmayera 9
HR-47000, Karlovac, Croatia
Tel. +385 - (0)47 - 843 - 510
Fax. +385 - (0)47 - 843 – 579

HRN EN ISO 9001:2009

VELEUČILIŠTE U KARLOVCU

Stručni / specijalistički studij: Specijalistički diplomski stručni studij sigurnosti I zaštite
(označiti)

Usmjerenje: Zaštita na radu

Karlovac _16.05.2019.

ZADATAK ZAVRŠNOG RADA

Student: Kristina Franović

Matični broj: 0422416001

Naslov: MOGUĆNOSTI DALJNJEG RAZVOJA NACIONALNE INFORMACIJSKE INFRASTRUKTURE U DOMENI ZAŠTITE NA RADU

Opis zadatka:

- Na osnovi: dosadašnjih iskustava, prakse, aktualne domaće regulative te aktualnih EU smjernica i obvezujućih projekata, analizirati i istaknuti bitne čimbenike koji ukazuju na nužnost razvoja i konačnog oblikovanje nacionalne informacijske infrastrukture u domeni ZNR;
- Analizirati aktualne napredne oblike primjene interneta u području javne uprave i javnih usluga na području Republike Hrvatske (npr. e-građani, CEZIH - nacionalna informacijska infrastruktura u zdravstvu) kao dobre primjere s visokim stupnjem završenosti;
- Na osnovi saznanja iz prethodnih dviju analiza pristupiti analizi postojećih segmenata započetog projekta pod nazivom "Središnji nacionalni informacijski sustav ZNR" (tzv. "Data Collector") kao temelja informacijske infrastrukture te predložiti logične mogućnosti njegovog daljnjeg razvoja vodeći računa o postizanju dnevno-operativnih, taktičkih i strateških ciljeva poslovnog sustava u domeni ZNR.

Zadatak zadan:	Rok predaje rada:	Predviđeni datum obrane:
16.05.2019.	24.06.2019.	03.07.2019.

Mentor:

dr.sc. Damir Kralj, prof.v.š.

Predsjednik Ispitnog povjerenstva:

mr.sc. Snježana Kirin, v.pred.

PREDGOVOR

Ovim putem željela bih se zahvaliti mentoru dr.sc. Damiru Kralju, prof.v.š. na nesebičnoj pomoći, strpljenju i stručnim savjetima pruženim tijekom izrade ovog završnog rada. Hvala i svim nastavnicima i kolegama Veleučilišta u Karlovcu, Odjela sigurnosti i zaštite, na pomoći, podršci i prenesenom znanju tijekom studiranja, koje sam primjenjivala u pisanju ovog rada, ali kojeg ću primjenjivati i u daljnjem životu i radu.

Veliko hvala mojim dragim prijateljima, a posebice Vlatki, Ivani i Valentini koje su uvijek bile tu za mene, bodrile me i pokušale razumjeti i Ivanu koji mi je pomogo svojim stručnim znanjem u izradi ovog završnog rada, ali i drugim zadacima tijekom dugogodišnjeg studiranja.

Posebice veliko hvala mojim najdražim roditeljima, koji su mi omogućili školovanje i bili mi velika potpora na ovom putu i koji su zajedno sa mnom gubili živce, te me motivirali da ustrajem u svom naumu. Također hvala mojoj užoj obitelji i rodbini s kojima sam mnogo toga naučila, koji su nesebično pomagali i prije svega bili strpljivi i razumni u mnogim situacijama tijekom studiranja.

Veliko hvala mom dečku Kristijanu i djedu Slavomiru koji su me konstantno bodrili i vjerovali u mene, te zajedno sa mnom proživljavali i teške i sretne trenutke.

I na kraju još jedno veliko hvala svima navedenima bez kojih ovaj veliki uspjeh, koji mi jako puno znači, ne bi bio moguć.

SAŽETAK

Predmet ovog rada je analiza mogućnosti daljnjeg oblikovanja nacionalne informacijske infrastrukture u domeni zaštite na radu. Kroz analizu nacionalne zakonske regulative i EU smjernica u domeni zaštite na radu, mogućnosti primjene globalnih mrežnih usluga, uspješnih primjera razvoja nacionalnih informacijskih sustava u domeni javne uprave i zdravstva, stvoreni su temelji za spekulativni pristup analizi mogućnosti daljnjeg razvoja nacionalne informacijske infrastrukture u domeni zaštite na radu. Opisane su i aktualne aplikacije koje se koriste za vođenje poslova zaštite na radu, a koje bi poslužile kao klijentske aplikacije za središnji nacionalni informacijski sustav (SNIS) ZNR. Posebno je analiziran zdravstveni informacijski sustav CEZIH kao dobar funkcionalni uzor za daljnji razvoj ovog sustava. Na kraju je osmišljena i prikazana ideja o predvidivom razvoju SNIS-a koji se oslanja na središnji registar podataka i resursa ZNR pod nazivom "Data Collector" sa svim potrebnim funkcionalnostima koje jamče unaprjeđenje zaštite na radu u RH.

Ključne riječi: zaštita na radu, mrežne usluge, nacionalna informacijska infrastruktura, zakonska regulativa, EU smjernice, Data Collector.

SUMMARY

The subject of this paper is an analysis of the possibilities of further development of the national information infrastructure in the domain of safety at work. Through the analysis of: national legislation and EU directives in the field of occupational safety and health, possibilities of application of the web services and successful examples of the development of national information systems in the domain of public administration and health care, the basis for the speculative approach to the analysis of the possibilities of further development of national information infrastructure in the field of safety at work is created. The applications used to manage safety at work, which would serve as client applications for the central national information system are also presented. The health information system CEZIH has been analyzed as a good functional example for the further development of subject system.

In the end, the idea of predictable development of the central national information system, which relies on the central data and resource register of the safety at work, called „Data Collector", has been designed and presented with all the necessary functionalities that guarantee the improvement of Croatian safety at work.

Keywords: safety at work, web services, national information infrastructure, legislation, EU directives, Data Collector.

SADRŽAJ

1. UVOD

Zaštita na radu je skup tehničkih, zdravstvenih, pravnih, psiholoških, pedagoških i drugih djelatnosti pomoću kojih se otkrivaju i otklanjaju rizici, odnosno rizične pojave kao što su opasnosti, štetnosti i napori, a koje mogu ugroziti život i zdravlje osoba na radu. Svrha i cilj zaštite na radu je osigurati sigurne radne uvjete kako bi se spriječile ozljede na radu, odnosno umanjile štetne posljedice, ako se opasnost ne može otkloniti. Za organizaciju i provedbu zaštite na radu odgovoran je poslodavac neovisno o tome da li je zaposlio stručnjaka zaštite na radu ili je ugovorio suradnju s ovlaštenom stručnom ustanovom. Poslodavac je dužan osigurati radniku uvjete za rad na siguran način koji ne ugrožava njegovo zdravlje te je obavezan utvrditi i obavljati poslove zaštite na radu u skladu s procjenom rizika, stanjem zaštite na radu i brojem zaposlenika.

Danas zaštita na radu ima najvažniju ulogu u uspješnom proizvodnom procesu jer sustav zaštite na radu osigurava sigurnost i neprekinutost procesa s naglaskom na kontinuirano praćenje i poboljšavanje. Unaprjeđivanje djelatnosti i suvremeni način poslovanja nezamisliv je bez sustavnog provođenja politike zaštite na radu te unaprjeđivanja sigurnosti i zaštite zdravlja radnika. Unaprjeđenje sustava zaštite na radu u tvrtkama moguće je postići stalnim stručnim praćenjem razvoja tehnologije i samog radnog procesa, djelovanjem u skladu s njima i pružanjem stručne podrške, edukacijom te podizanjem svijesti o važnosti dobre organizacije i provedbe zaštite na radu. Neprovođenje zaštite na radu i nepoduzimanje preventivnih mjera može svojim neželjenim posljedicama ugroziti poslovanje, stabilnost pa i sam opstanak svake tvrtke, posebno onih manjih, jer troškovi koji mogu nastati zbog ozljeda na radu i inspekcijskih kazni višestruko nadmašuju svako ulaganje u prevenciju i sigurnost na radu. Zaštita na radu kao najvažnije područje u jednom uspješnom poduzeću ima i mora za potrebu imati primjenu najsuvremenijih mrežnih tehnologija te usmjeriti pozornost na utjecaj informacijske i komunikacijske tehnologije na svakodnevne radne procese i radno okruženje.

Cilj ovog rada je na osnovi znanja stečenih tijekom studija i iskustava iz prakse uz oslonac na aktualnu domaću regulativu, EU direktive, norme i aktualne projekte analizirati i istaknuti bitne činjenice i čimbenike koje ukazuju na prijeko potrebno oblikovanje nacionalne informacijske infrastrukture u domeni zaštite na radu, sagledati do sada ostvarene dijelove informacijskog sustava koji bi trebao ostvariti postavljene ciljeve te predložiti logične

mogućnosti njegovog daljnjeg razvoja vodeći računa o postizanju dnevno-operativnih, taktičkih i strateških ciljeva poslovnog sustava u domeni zaštite na radu.

Metodologija predviđena za ostvarenje cilja rada obuhvaća istraživanje i analizu dostupnih pisanih i mrežnih izvora koji sadrže i obrađuju navedene regulativne, normativne i projektne sadržaje te radova koji se bave problemima razvoja, implementacije i prihvaćanja ključnih informacijsko-komunikacijskih projekata na području Republike Hrvatske.

2. INTERNET

2.1. Što je internet?

Internet je globalna računalna mreža koja povezuje računala i druge računalne mreže radi međusobne razmjene podataka. Pristupanjem internetu moguće je koristiti razne sadržaje i usluge koje su dostupne u svakom trenutku i na bilo kojem uređaju. Danas je život bez interneta praktički nezamisliv.

Razvoj interneta kao globalne mreže ponajprije je ovisio o razvoju sredstava komuniciranja. Izumi telegrafa, telefona, radija i računala bili su, u okviru svojih granica primjene, podloga za pojavu interneta. Internet je nastavak računalne mreže uspostavljene u Sjedinjenim Američkim Državama (SAD) tijekom 1960. godine od ARPA (eng. *Advanced Research Projects Agency*), koja je povezivala nekoliko računala. Prva računalna mreža nazvana je ARPANET (*ARPA* + eng. *NETwork*). Znanstvenici su izgradili ARPANET s namjerom da to bude mreža koja će još uvijek uspješno raditi i u slučaju da dio mreže bude oštećen. Takav koncept bio je važan vojnim organizacijama koje su proučavale načine da održe komunikacijske mreže u funkciji i u slučaju nuklearnog rata. Prvotno zamišljen kako bi omogućio visoku učinkovitost u komunikaciji između istraživačkih centara, sveučilišta i vladinih agencija SAD-a, internet je ubrzo prerastao u internacionalnu mrežu dostupnu svima. Kako je ARPANET rastao u 1970-ima, sa sve više i više sveučilišta i institucija koji su se spajali na njega, korisnici su uvidjeli potrebu razvijanja standarda za put kojim će podaci biti prenošeni internetom.

Internet nitko ne posjeduje, ali kao vršno tijelo osnovana je W3C (eng. *WWW Consortium*) kao neprofitabilna međunarodna udruga koja predlaže i donosi ključne norme za njegovu funkcionalnost. Postoji nekoliko mreža visoke razine koje su međusobno povezane preko IXP točaka. Internet IXP (eng. *exchange point)* je fizička infrastruktura kroz koju davatelji internetskih usluga međusobno razmjenjuju podatke između svojih autonomnih sustava. Uređaji povezani na internet komuniciraju koristeći TCP/IP (eng. *Transmission Control Protocol/Internet Protocol*) komunikacijski protokol. Glavna funkcija mu je usmjeravanje i jednoznačno adresiranje kroz mreže. Poruke se sa izvora šalju u razloženim paketima koji se ponovno spajaju na odredištu, a ispravnost prijenosa paketa provjerava se generiranjem tzv. „provjernog zbroja“ u zaglavlju (eng. *checksum*). TCP/IP protokoli imaju komunikacijska kašnjenja reda desetaka ili stotina milisekundi, koja su najčešće promjenjiva i

nepredvidljivog iznosa u slučaju smetnji. Svako računalo ima IP adresu, pridruženu njegovoj mrežnoj kartici, koja predstavlja jedinstvenu brojčanu oznaku računala na Internetu. IP adrese se dijele na javne i privatne. Javne su jedinstvene, globalne i normirane, dok privatne mogu biti duplicirane uz uvjet da se ne nalaze u istoj lokalnoj mreži. Prilikom izlaska korisnika iz lokalne mreže na internet, privatna adresa pretvara se u javnu pomoću NAT *(*eng. *Network Address Translation)* i PAT *(* eng. *Port Address Translation)* metoda. Međunarodna organizacija IANA *(*eng. *Internet Assigned Numbers Authority)* se brine o raspodjeli IP adresnog prostora zadužujući za određen raspon adresa regionalne internet registre (RIR) [1].

2.2. Načini povezivanja na internet

Način povezivanja na internet ovisi o dostupnosti mrežne infrastrukture na mjestu gdje se želi ostvariti pristup internetu te o uslugama koje će se najviše rabiti. Povezivanje se može ostvariti korištenjem:

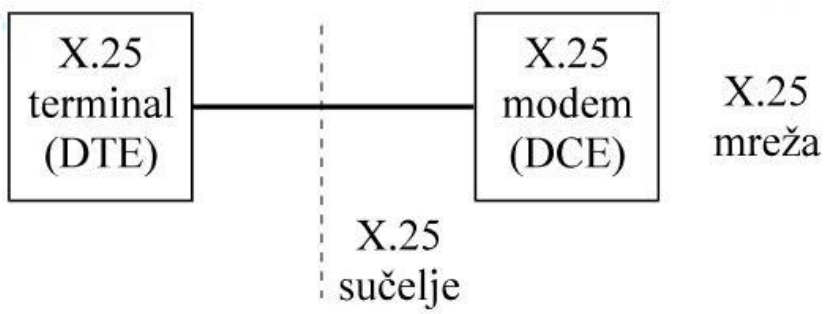
- **Žičnog telefonskog priključka (DSL tehnologija).** Jedan od najkorištenijih načina povezivanja koji omogućuje stalan pristup internetu preko telefonske mreže. DSL uređaj se s računalom može povezati preko mrežnog kabela na mrežnu karticu ili preko USB kabela na USB sučelje. DSL uređaji su uglavnom kombinacija modema, usmjerivača i pristupne točke pa je moguće žično ili bežično povezivanje na internet.
- **Kabelske televizije.** Kabelski internet se može ostvariti samo ako je uvedena kabelska televizija, tako da koristi istu infrastrukturu. Pomoću razdjelnika korisnik može istodobno primati signal kabelske televizije i imati stalan pristup internetu.
- **Bežične mobilne mreže.** Mobilna širokopojasna mreža omogućuje brzi pristup internetu pomoću prijenosnih uređaja s bilo kojeg mjesta gdje je dostupan signal mobilne mreže.
- **Javnog bežičnog interneta (eng. *HotSpot*).** Pristup internetu se može ostvariti pod uvjetom da je korisnik u dosegu signala neke od tzv. *HotSpot* lokacija gdje su postavljene pristupne točke. Veza se ostvaruje pomoću bežične mrežne kartice koja se nalazi u uređaju koji se spaja na internet, a brzina pristupa ovisi o broju korisnika koji istodobno pristupaju *HotSpot* lokaciji.

2.2.1. X.25 mrežni protokol

Mrežna razina osigurava prijenos poruke s kraja na kraj mreže. Primarni problemi ovog sloja su adresiranje, usmjeravanje prometa kroz mrežu te kontrola pogreške i kontrole zagušenja. Optimalno rješenje za korisnike je da podaci stižu sa minimalnim kašnjenjem i s najvećom mogućom točnošću. Paket je jedinica informacije koju je moguće prosljeđivati zasebno ili virtualnim kanalom. Kod zasebnog slanja svaki paket mora nositi globalnu adresu odredišta. Prosljeđivanje virtualnim kanalom zahtjeva da prvi paket nosi globalnu adresu, dok ostali nose samo kratki identifikator virtualnog kanala.

X.25 mreža se dijeli na javnu i privatnu. Javna pruža usluge svim potencijalnim korisnicima, a privatna se koristi za potrebe jednog ili više korisnika koji razmjenjuju informacije unutar svog zatvorenog sustava.

X.25 mrežni protokol je spojevni protokol koji uspostavlja numeraciju paketa i oporavak od pogreški ponovnim slanjem (*retransmisijom*). Paketi se prosljeđuju po virtualnom kanalu i adresa je potrebna samo u fazi njegove uspostave (nosi je samo prvi paket), a ostali paketi koriste 12-bitni identifikator virtualnog kanala. Identifikator virtualnog kanala nije jedinstven i mijenja se od čvora do čvora prema tablicama virtualnog kanala.



Slika1. Struktura X.25 mreže [2]

DCE (eng. *Data circuit-terminating equipment*) je uređaj na mrežnoj strane veze „korisnik-mreža“. Omogućava fizičko povezivanje na mrežu, prosljeđivanja prometa i sinkronizaciju prijenosa podataka između DCE i DTE uređaja.

DTE (eng. *Data terminal equipment*) je uređaj na korisničkoj strane veze „korisnik-mreža“. Služi kao izvorište i/ili odredište, a na mrežu se povezuje kroz DCE uređaj i koristi signal za sinkronizaciju koji dobiva od DCE uređaja.

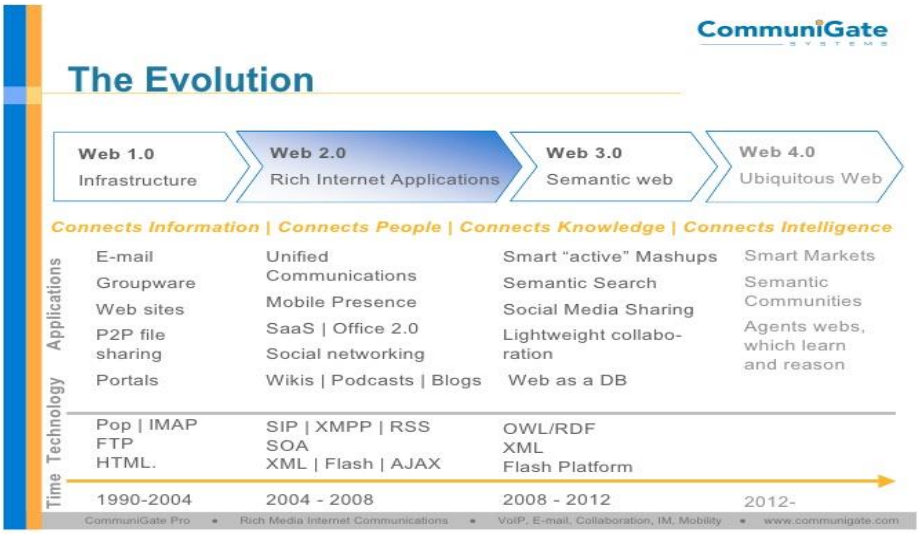
X.25 standard obuhvaća tri sloja:

- **Fizički sloj**. Mehaničko i električno sučelje između računala korisnika i mreže.
- **Sloj veze**. Bavi se uspostavljanjem, kontrolom i raskidanjem veze između korisnika i mreže te greškama nastalim tijekom prijenosa na liniji između njih.
- **Paketni sloj**. Bavi se formiranjem paketa, adresiranjem, kontrolom protoka, potvrđivanjem isporuke, prekidima i multipleksiranjem.

Prijenos podataka se obavlja spojno ili bespojno. Spojni prijenos se vrši preko virtualne komutirane linije koja se dinamički uspostavlja ili fiksnom linijom koja unaprijed dogovorena. Bespojni prijenos se vrši pomoću datagram servisa gdje je svaki paket nezavisan te sadrži izvorišnu i odredišnu adresu.

2.3. Mogućnosti primjene interneta

Suvremeni život i poslovanje nezamislivi su bez interneta. Internet posjeduje poslužitelje usluga kojim se olakšala njegova uporaba. Najznačajniji internetski poslužitelji su: WWW (eng. *World Wide Web*), elektronička pošta (eng. *e-mail*), daljinsko preuzimanje datoteka (FTP, eng. *file transfer protocol*), mrežne novine (eng. *news*), forum, čavrljanje (eng. *chat*) i udaljeni rad (*telnet*). WWW je najraširenija i najpopularnija internetska usluga koja obuhvaća i neke druge usluge (*e-mail*, *chat*). Njome se omogućuje razmjena podataka.



Slika 2. Etape razvoja mrežnih usluga [3]

Ovaj skup globalnih usluga i tehnološka razvojna epoha najčešće se naziva "web". Kako je prikazano na slici 2, Web je prolazio i još prolazi kroz razvojne etape. Sama evolucija weba je velika i može se podijeliti u četiri faze. Prva faza je Web 1.0 u kojoj su postavljene osnove infrastrukture, uvedene su osnovne mrežne usluge (e-pošta, FTP, HTML), a mrežne stranice su služile uglavnom jednosmjernoj prezentaciji uz relativno manji stupanj dvosmjerne dinamičnosti. Druga faza Web 2.0 je osim tehnološki razvijenije platforme od Weba 1.0 imala i novi pristup vizualnoj komunikaciji s korisnikom. Uvodi dinamičnost i interaktivnost, a dopušta i potiče sve korisnike na izradu, dijeljenje i distribuiranje informacija, te obuhvaća globalne mrežne tehnologije i usluge kao što su blogovi, društvene mreže, wiki stranice, komunikacijske alati i alate koji su usmjereni na dijeljenje sadržaja i suradnju preko Weba . Još jedan od važnijih sustava koji je proizašao iz ove faze, a uvelike olakšava današnje obrazovanje, je sustav za upravljanje učenjem *(eng. Learning Management System, LMS).* Uslijedila je treća faza Web 3.0 koju nazivamo još i "semantički web", a koja je usmjerena na razumijevanje informacija na Webu od strane računala u svrhu pružanja produktivnijih i intuitivnijih korisničkih iskustava. Web 3.0 daje naglasak na integriranje podataka, znanja i aplikacija na Webu kako bi isti mogli surađivati u svrhu stvaranja tzv. smislenog i sveprisutnog Weba (eng. *smart web & ubiquitous web*). Dakle, sljedeću fazu Web 4.0 još nazivamo i „ smisleni i sveprisutni Web“ zbog usmjerenosti na interakciju i razumijevanje od strane računala i ljudi te mogućnost "posvudašnje" dostupnosti. Njezin osnovni cilj je postizanje više razine inteligencije na Webu preko softverskih agenata i sustava koji se međusobno razumiju, komuniciraju i surađuju kako bi postigli ciljeve korisnika te ukidanje prostornog i vremenskog ograničavanja korisnika.

Svaka faza obilježava svoje ciljeve, probleme, tehnologije i mogućnosti. Razvojem jedne faze nije "umrla" druga faza već su jedna temelj za drugu. Sve faze su prirodan slijed događanja i razvoja interneta koji prate brzo rastući trend novih tehnologija i načina života.

Razvojem interneta i prihvaćanjem novih era weba proizašle su mnoge web-zasnovane aplikacije i sustavi koji znatno olakšavaju i nadopunjavaju današnji stil života. Razvojem novih tehnologija nametnula se potreba da se stvari brzo i jednostavno odvijaju, bez odlaganja, bez isprika, bez obzira na vrijeme i mjesto. Zbog takve potrebne spontano se i gotovo neprimjetno dogodila i tranzicija iz pasivnog korištenja interneta u aktivno korištenje interneta ne samo u privatne, već i u poslovne svrhe . Uz otvorenost i dostupnost interneta došlo je do širenja poslovne suradnje i razmjene informacija na globalnoj razini, dakle do globalnog oblika poslovne integracije

Faza Web 2.0 donijela je velike promjene, inovacije i razvoj poslovanja te je donijela termin "računalstvo u oblaku" (eng. *cloud computing*). Računalni oblak (slika 3) je naziv poslovnog modela i tehnološke platforme za komunikaciju te razvoj i izvršavanje programskih rješenja koji se danas sve više koriste. Može se definirati kao mogućnost iznajmljivanja virtualnog poslužitelja na kojem korisnici mogu pohranjivati podatke i po volji im pristupati. Također se može definirati i kao pohranjivanje i osiguravanje ogromnih količina podataka kojima mogu pristupati samo ovlaštene aplikacije ili korisnici. Razlikujemo razne vrste računalstava u oblaku a to su: B2B (eng. *Business to Business*), A2A (eng. *Application to Application*), IoT (eng. *Internet of Things*) i mnoge druge. Ova koncepcija računalstva u oblaku u potpunosti je promijenila način poslovanja i funkcioniranja tvrtki. Oblak tvrtkama omogućuje uštedu, evoluciju u načinu na koji informacijska tehnologija (IT) podržava poslovanje tvrtke i inovacije u kreiranju poslovnih rješenja koje tvrtkama osiguravaju prednost na tržištu. Zahvaljujući i oblaku, zaposlenici sad pristupaju dokumentima poduzeća koji su tradicionalno bili dostupni samo u uredima s bilo kojeg mjesta u bilo koje vrijeme, dokle god postoji mrežna veza. Prednost oblaka je niža cijena programske podrške jer se plaća usluga onoliko koliko se troši, odnosno prema ostvarenom mrežnom prometu i usluzi koja se koristi. Programska podrška, njena najnovija verzija i podaci su dostupni sa svake lokacije gdje korisnik ima pristup internetu. Nije potrebno kupovati sklopovlje i baze podataka te ih instalirati i održavati, nego su samo prisutni manji troškovi održavanja i nadogradnje programske podrške. Usluga uključuje i profesionalnu antivirusnu zaštitu i arhiviranje podataka. Osim brojnih prednosti potrebno je spomenuti i poneki nedostatak. Mogući su problemi s dostupnosti, sigurnosti i ovisnosti o jednom pružatelju programske podrške, odnosno usluge. Problem dostupnosti uzrokuje loša internetska veza ili njen prekid, dok je problem sigurnosti vezan uz povjerenje pružatelju usluga da ih neće ukrasti, prodati ili zloupotrijebiti naše podatke i dokumente. Također postoji opasnost od prisluškivanja komunikacije između klijentskih uređaja i poslužiteljskih središta.

Slika 3. Računalstvo u oblaku - načelna funkcionalna shema [4]

Isporuka usluge računalstva u oblaku podijeljena je na tri arhitekturna modela i različite izvedbene kombinacije. Mogući modeli pružanja usluge su:

- **SaaS** (eng. *Software as a Service*) – korisniku je pružena mogućnost uporabe dostupnih aplikacija koje se nalaze u infrastrukturi oblaka. Aplikacije su dostupne preko klijentskog sučelja, a korisnik pri tome ne provjerava pozadinsku infrastrukturu ni individualne aplikacijske mogućnosti. Usluge se unajmljuju prema potrebi, umjesto da se kupuju kao zaseban program koji treba instalirati na uredskim računalima. Korisnici nemaju dodatnih ulaganja u poslužitelje ili programske licence, a davatelji usluga imaju male troškove u odnosu na tradicionalnu uslugu držanja datoteka na poslužitelju. Primjeri takvih aplikacija su: Sustav za upravljanje odnosima s korisnicima *(*eng. *Customer relationship management*) i Sustav za planiranje sredstava poslovanja (eng. E*nterprise resource planning*);
- **PaaS** (eng. *Platform as a Service*) – dodatna usluga u odnosu na SaaS strukturu je razvojna okolina. Korisnik sam gradi vlastite aplikacije koje se pokreću na infrastrukturi davatelja usluge. Poslužitelji su u vlasništvu davatelja usluga, a usluge su ograničene dizajnom i mogućnostima isporučitelja tako da korisnik nema potpunu slobodu. Korisnik ne može provjeravati strukturu oblaka niti mrežu, ali uz nadzor razvijenih aplikacija ponekad ima i mogućnost nadzora okolne konfiguracije. Primjer takve platforme je "Microsoft Azure";

- **IaaS** (eng. *Infrastructure as a Service*) – korisnici ne kupuju poslužitelje, programe, prostore za pohranu podataka ili mrežnu opremu, već kupuju navedene resurse kao vanjsku uslugu. Korisnik može pokrenuti različite vrste programske podrške, od operacijskih sustava do aplikacija, ali nema nadzor nad infrastrukturom oblaka. Ipak ima nadzor nad operacijskim sustavima, pohranom podataka i razvojem aplikacija, a može čak imati i nadzor nad odabranim komponentama umrežavanja.

Neovisno o modelima pružanja usluga postoje četiri različita modela provođenja usluga računalstva u oblaku koji su izvedeni na različite načine, ovisno o specifičnim potrebama:

- **Javni oblak** (eng. *Public Cloud*) – u vlasništvu je tvrtke koja prodaje usluge računalstava u oblaku, a platforma je dostupna i otvorena za javnost. Aplikacije različitih korisnika nalaze se na istim poslužiteljima, sustavima za pohranjivanje i mrežama. Javni oblaci čine privremeno zakupljenu infrastrukturu organizacija te smanjuju sigurnosne rizike i troškove pružanjem promjenjive infrastrukture. Mogu biti puno veći od privatnih oblaka, a nude i mogućnost prebacivanja odgovornosti s organizacija na davatelja usluga u slučaju pojave neplaniranih rizika. Dijelovi javnog oblaka mogu biti i pod isključivom uporabom samo jednog korisnika, čineći tako privatni podatkovni centar. Tada korisnici mogu upravljati ne samo slikama virtualnih strojeva, nego i poslužiteljima, sustavima pohrane, mrežnim uređajima i mrežnim topologijama;
- **Privatni oblak** (eng. *Private Cloud*) – infrastruktura je dostupna isključivo jednoj organizaciji koja želi veći nadzor nad podacima nego što ga mogu imati korištenjem javnog oblaka. Organizacija posjeduje infrastrukturu i ima nadzor nad raspodjelom aplikacija na vlastitoj infrastrukturi. IT službe kompanija ili davatelji usluga grade privatne oblake i upravljaju njima, a organizacije mogu na njemu instalirati programe, aplikacije, pohranjivati podatke i upravljati strukturom oblaka;
- **Zajednički oblak** (eng. *Community Cloud*) – nekoliko organizacija dijeli strukturu oblaka, a infrastruktura podržava posebne zajednice koje imaju zajedničke potrebe, misije, zahtjeve sigurnosti i slično;
- **Hibridni oblak** (eng. *Hybrid Cloud*) – čine ga dva ili više različitih oblaka koji ostaju jedinstveni entiteti, ali su međusobno povezani normiranim tehnologijama koje omogućavaju efikasan prijenos podataka. Mogućnost proširivanja privatnog oblaka s resursima javnog oblaka može se koristiti za održavanje uslužnih razina kako bi se lakše

izdržala velika opterećenja. Ako su podaci mali ili aplikacije ne pamte stanja, hibridni oblak može biti bolje rješenje od prepisivanja velike količine podataka u javni oblak

Možemo zaključiti da je oblak ključan za svakodnevno uspješno poslovanje tvrtke, a analiza podataka i aplikacije vezane uz njega dodatno su pripomogle razvoju IT sektora. Omogućuje jednostavnije upravljanje podacima, dokumentima i aplikacijama. Uz pomoć oblaka tvrtke koriste IT resurse na zahtjev i po potrebi ovisno o rastu posla. Zbog velike količine podataka koje treba skladištiti, analizirati oblak je odlično rješenje i vođenju poslova zaštite na radu u određenim tvrtkama. Svaki stručnjak na radu ili ovlaštena osoba za poslove zaštite na radu mora u svakom trenutku i na različitim mjestima imati uvid u dokumente, a oblak je ta koncepcija poslovanja koja mu nudi novi način pristupa osobnim podacima i aplikacijama, koji više nisu smješteni na računalu već u "oblaku" – što znači da programu, evidencijama, dokumentaciji i svemu što mu je potrebno možete pristupiti sa više uređaja, u bilo koje vrijeme i s različitih lokacija [5].

2.4. Primjeri uspješnih infrastrukturnih projekata u Republici Hrvatskoj

2.4.1. e-Hrvatska

Strategija e-Hrvatska 2020 [6] prikazuje pregled informatizacije i e-usluga u javnom sektoru te ciljeve daljnjeg razvoja. Glavni cilj Strategije je osigurati povezivanje informacijskih sustava tijela javne uprave iz svih sektora na način da se građanima pruži što veći broj kompleksnih e-usluga i smanji opterećenje građana u osobnoj interakciji s javnom upravom. Aktivnosti se provode sukladno Akcijskom planu i financiraju prvenstveno iz Europskih fondova te iz nacionalnih sredstava. Prema smjernicama Europske komisije utvrđene su razine zrelosti po kojima se mjeri dostupnost javnih usluga na Internetu [6].

Svaka e-usluga definirana je različitim razinama informatiziranosti s pripadajućim značenjem:

1. **Informacija**: na mreži je dostupna samo informacija o usluzi (npr. opis postupka);
2. **Jednosmjerna interakcija**: dostupnost formulara u e-obliku za pohranjivanje na računalu, prazne formulare je moguće otisnuti na pisaču;
3. **Dvosmjerna komunikacija**: interaktivno ispunjavanje formulara i prijava uz autentifikaciju, ispunjavanjem formulara pokreće se pojedina usluga;

4. **Transakcija**: cijela usluga je dostupna na mreži, popunjavanje formulara, autentifikacija, plaćanje i isporuka potvrda, narudžbe ili drugi oblici potpune usluge putem mreže;
5. **Ciljana usluga (proaktivnost/automatizacija)**: obavljanje usluge je proaktivno/automatizirano na način da se od korisnika traži samo potvrda ili suglasnosti.

Današnje stanje u Republici Hrvatskoj je takvo da je još uvijek velika većina e-usluga na razini zrelosti 2 (razdoblje 2012-2015.), tj. da se radi o jednosmjernoj interakciji.

Svako tijelo, koje je htjelo pružati personalizirane usluge, moralo je razviti svoj sustav izdavanja mehanizma za verifikaciju e-identiteta. Pri tome su probleme predstavljali:

- nepostojanje jedinstvenog mehanizma za verifikaciju e-identiteta;
- nepostojanje središnjeg servisa za izdavanje vjerodajnica;
- nepostojanje mehanizma za sigurnu dostavu personaliziranih informacija korisnicima;
- raspršenost informacija i e-usluga po različitim stranicama te
- neinformirnost javnosti o dostupnosti e-usluga.

Svi navedeni problemi riješeni su puštanjem u rad i daljnjim razvojem platforme e-Građani 10. lipnja 2014. godine. Platforma se ostvaruje kroz tri glavne sastavnice: Sustav središnjeg državnog portala, Nacionalni identifikacijski i autentifikacijski sustav (NIAS) te Sustav osobnog korisničkog pretinca.

Središnji državni portal integrira informacije i e-usluge na jednom mjestu i na taj način rješava raspršenost. Realiziran je unutar jedinstvene domene gov.hr i njegov cilj je pružiti informacije o svim uslugama javne uprave.

NIAS je cjelovito informacijsko-tehnološko rješenje za identifikaciju i autentifikaciju korisnika na nacionalnoj razini koje omogućava uključivanje više tipova vjerodajnica različitih razina sigurnosti od razine 2 (najniža) do 4. Lista prihvaćenih vjerodajnica nalazi se u prilogu 1. NIAS je posrednik između korisnika e-usluge, pružatelja e-usluge i izdavatelja vjerodajnice. Osobni identifikacijski broj (OIB) je jedinstveni e-identitet, koji dobivaju sve fizičke i pravne osobe za koje postoji potreba praćenja u službenim evidencijama, a koji NIAS prosljeđuje e-usluzi za jednoznačnu identifikaciju korisnika.

U Osobni korisnički pretinac (OKP) zaprimaju se poruke od javne uprave bez da korisnik mora pokrenuti neku e-uslugu. OKP omogućuje personalizaciju poruka od strane korisnika i prosljeđivanje informacija o porukama na e-mail adresu.

Vjerodajnica najviše razine je elektronička osobna iskaznica (eOI) s identifikacijskim certifikatom koji omogućuje pristupanje svim elektroničkim uslugama.

Danas, osim e-Građani, postoje i druge platforme vezane uz pojedina upravna područja. Neke od tih su:

- e-Porezna za usluge Porezne uprave;
- e-Carina za usluge Carinske uprave;
- CEZIH portal za zdravstvene djelatnike;
- CARNet i Srce za usluge sustava znanosti i obrazovanja;
- Zajednički informacijski sustav katastra i zemljišnih knjiga (ZIS) kao centralno mjesto o katastarskim i zemljišnoknjižnim podacima.

Portal otvorenih podataka Republike Hrvatske, po uzoru na druge slične projekte u Europi i svijetu, predstavlja katalog metapodataka (podataka koji pobliže opisuju skupove podataka) te pomoću njega korisnici lako dolaze do traženih otvorenih podataka.

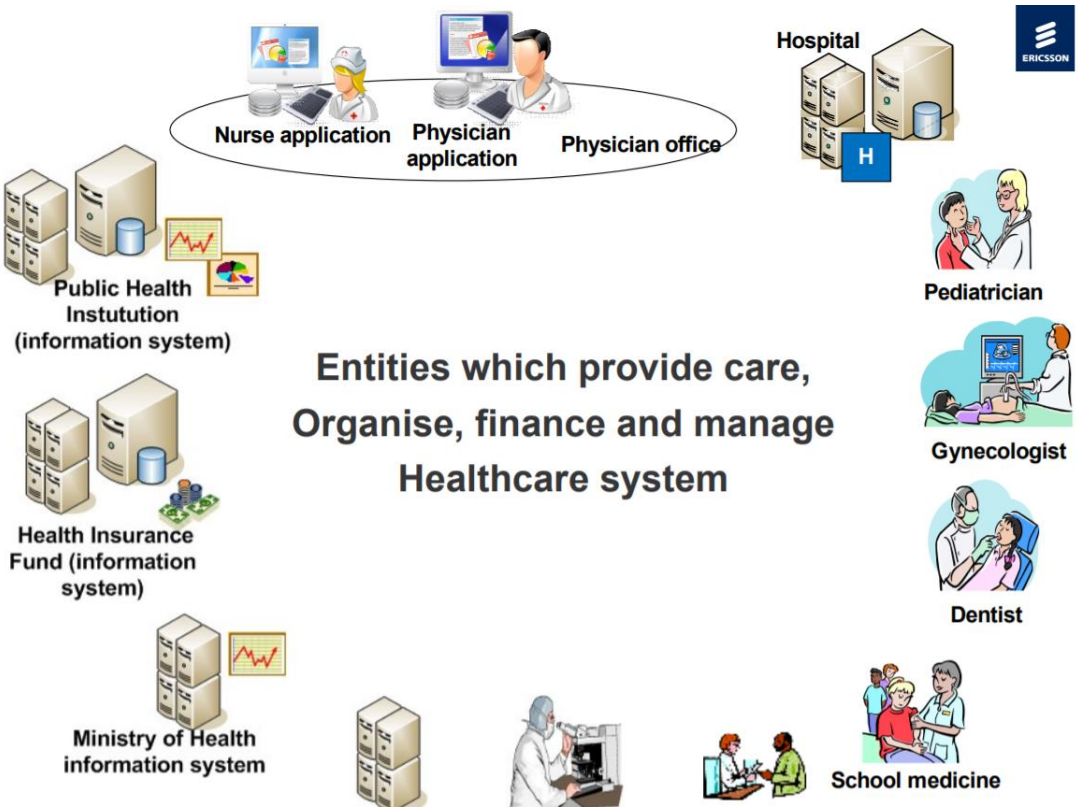
Projekt izgradnje sigurne osnovice za razmjenu podataka između javnih registara je u pripremi. U tijeku su i razmišljanja o uvođenju načela "*Big Data*" za pretraživanje i obradu velikih količina nestrukturiranih podataka. Digitalizacija građe koju posjeduju tijela državne uprave je jedan od preduvjeta za njegovo ostvarenje.

2.4.2. e-Zdravstvo

Centralni zdravstveni informacijski sustav Republike Hrvatske (CEZIH) je informacijski sustav koji povezuje niz aplikacija i sustava zdravstva. Ministarstvo zdravlja (MZ) je vlasnik, a Hrvatski zavod za zdravstveno osiguranje (HZZO) je operator središnjeg dijela integriranog informacijskog sustava [7].

Jedan od najvećih uspjeha sustava CEZIH je elektronički recept (eRecept), prva prava nacionalna implementacija elektroničkog propisivanja i izdavanja lijekova u svijetu. Implementacijom elektroničke uputnice u izvanbolničku specijalističko konzilijarnu zaštitu

CEZIH je planirano prerastao iz sustava primarne zdravstvene zaštite u Centralni zdravstveni informacijski sustav.



Slika 4. Pregled sustava CEZIH [8]

CEZIH je s projektnog gledišta zasnovan na sustavu NISHI (eng. *National Information System on Health Infrastructure*) razvijenom od tvrtke Ericsson NT koji korištenjem virtualne privatne mreže povezuje ordinacije primarne zdravstvene zaštite, HZZO, Hrvatski zavod za javno zdravstvo (HZJZ) te u daljnjem razvoju i ostale partnere koji sačinjavaju sustav javnog zdravstva. Središnji dio ovog informacijskog sustava primarne zdravstvene zaštite čine tzv. državni registri:

- **Elektronički populacijski registar (EPR).** Sadrži osobne i demografske podatke o pacijentima koji su registrirani u NISHI sustavu.
- **Registar resursa u zdravstvu (RRZ).** Sadrži informacije o resursima u zdravstvu kao što su sve zdravstvene ustanove i svi liječnici.
- **Arhiva elektroničkih zdravstvenih kartona (EHCR).** Sadrži zdravstvene kartone s povijestima bolesti svih pacijenata poznatih sustavu, od prvog registriranja pacijenta u sustav pa do isteka željenog vremenskog intervala nakon smrti pacijenta. Za razliku pd prethodna dva registra, ovaj je još u razvoju.

Koncepcija sustava je takva da klijentske aplikacije razmjenom poruka, a koristeći mrežne usluge ustava CEZIH mogu komunicirati međusobno ili prema drugim korisnicima koji imaju pristupne ovlasti pojedinim dijelovima sustava. Integracijska komponenta je sastavni dio isporuke i sustava odgovarajuće funkcionalnosti koji se brine o dostupnosti CEZIH-a. Upravljanje medicinskim zapisima, podrška pri izmjeni kliničkih i administrativnih informacija te podsustav izvještaja glavne su funkcionalnosti integracijske komponente. U slučaju nedostupnosti sustava ili asinkronih poruka integracijska komponenta ih čuva i isporučuje prvom prilikom. Temelj ovog načina komunikacije je sustav za upravljanje tzv "redom za čekanje poruka" (eng. *message queue,* MQ).

Uvedeni su sljedeći lokalni nazivi aplikacija koje komuniciraju s CEZIH-om:

- G2 – liječničke aplikacije opće/obiteljske medicine;
- G3 – aplikacije za ordinacije za zdravstvenu zaštitu predškolske djece („pedijatrija“);
- G4 – aplikacije za ordinacije za zdravstvenu zaštitu žena („ginekologija“);
- G5 – aplikacije za stomatološku zdravstvenu zaštitu;
- G6 – aplikacije za ordinacije za preventivno-odgojne mjere za zdravstvenu zaštitu školske djece i studenata;
- G7 – aplikacije za laboratorijsku dijagnostiku;
- G8 – aplikacije za ljekarne;
- G9 – aplikacije za izvanbolničku specijalističko-kozilijarnu zdravstvenu zaštitu;
- G100 – bolnički informacijski sustavi;
- G110 – aplikacije za sestrinsku dokumentaciju.

Infrastruktura javnog ključa (eng. *private key infrastructure,* PKI) predstavlja sigurnosne norme i tehnike prijenosa podataka putem interneta. Ispunjava sljedeće obveze:

- **Šifriranje/dešifriranje.** Šifrirana poruka od strane korisnika u potpuno nečitljivom obliku se šalje primatelju koji ju zatim dešifrira. Razlikujemo šifriranje simetričnim ključem i šifriranje javnim ključem. Šifriranje javnim ključem uključuje par ključeva, jedan javni i virtualno poznat svima i jedan tajni poznat samo primatelju. Ono zahtjeva više računanja i nije uvijek povoljno za velike količine podataka. Obrnuti način kod javnog ključa uz još neke parametre se koristi za digitalni potpis. Podaci se šifriraju tajnim ključem, a onda se dešifriraju javnim ključem te je tako moguće utvrditi identitet pošiljatelja. Certifikatom se provjerava pripada li javni ključ zaista osobi koja se

predstavlja kao pošiljatelj. Primijenjeno na SNIS ZNR, ZUZNR bi kao trebao objaviti svoj javni ključ kojim bi svi sudionici-partneri kriptirali promet koji šalju prema DC-u, a svi partneri bi imali privatne ključeve kojima bi se potpisivali sadržaji i dokazivala njihova vjerodostojnost.

- **Detekcija neovlaštenog mijenjanja podataka.** Digitalnim potpisom se uspostavlja identitet sudionika i osigurava integritet podataka. Omogućuje primatelju da pomoću *hash* funkcije izračunava sažetak te ga kriptira privatnim ključem pošiljatelja.
- **Autorizacija.** Pouzdana identifikacija jedne strane od druge strane.
- **Neporecivost poslanih podataka.** Sprječava pošiljatelja poruke da kasnije tvrdi kako nije poslao poruku.

Osnovne komponente PKI sustava su: krajnji entitet, certifikacijski centar, registracijski centar, baza valjanih i opozvanih certifikata te izdavač opozvanih certifikata.

Krajnji entitet se odnosi na sve što može biti identificirano imenom na certifikatu. Certifikacijski centar je ustanova koja potpisuje i izdaje certifikate te svojim potpisom jamči ispravnost podataka u certifikatu. Registracijski centar ima ulogu u registraciji krajnjih entiteta, a provjerava i posjeduje li korisnik privatni ključ koji odgovara javnom. Baza certifikata predstavlja sustav distribuiranih sustava koji pohranjuju certifikate te listu opozvanih certifikata. Izdavač opozvanih certifikata identificira svaki opozvani certifikat serijskim brojem te ga čini javno dostupnim svima.

Sve kvalificirane ključeve i certifikate izdaje Fina kao glavna i jedina certifikacijska agencija. Sve poruke prema HZZO-u potpisane su elektroničkim potpisom pošiljatelja (privatnim ključem) i kriptirane javnim ključem HZZO-a, koji ih nakon primitka dekriptira svojim privatnim ključem.

Arhitektura CEZIH sustava je u skladu s osnovama informacijske sigurnosti i to: povjerljivosti, integritetom i dostupnošću. CEZIH sadrži osjetljive podatke pa iz tog razloga visoki standardi vezani uz implementaciju sigurnosti zahtijevaju: povjerljivost podataka, kontrolu pristupa, visoku dostupnost i višeslojnu implementaciju rješenja. CEZIH je odvojen od ostatka interneta uspostavljanjem virtualne privatne mreže (eng. *virtual private network,* VPN) i bez uspostavljanja VPN tunela onemogućen je pristup do CEZIH poslužitelja. VPN veze se ostvaruju od svakog klijenta po načelu udaljenog pristupa (*eng. remote access*). Prije početka rada korisničke aplikacije moraju uspostaviti VPN tunel prema CEZIH sustavu. VPN se definira kao međuveza lokalne mreže koja koristi kriptirane načine međusobne

komunikacije, uobičajeno putem interneta. Tako se produžava privatna mreža preko javne mreže što omogućava korisnicima slanje i primanje osjetljivih podataka kao da su njihova računala spojena na istu privatnu lokalnu mrežu (eng. *local area network*, LAN), iako fizički nisu na istoj mreži. CEZIH infrastruktura obuhvaća i vatrozide kojima se razdvajaju CEZIH poslužitelji te definiraju pristupni protokoli i portovi. Vatrozidom je krajnjim korisnicima omogućen pristup samo preko sigurne tj. *htpps* veze na definiranim pristupnim adresama i portovima te direktan pristup poslužiteljima od strane krajnjih korisnika nije moguć.

Uravnoteženje opterećenja i visoka raspoloživost postižu se propuštanjem prometa od strane korisnika kroz poslužitelje za uravnoteženje prometa tzv. *balansera* prometa. Svaka od web aplikacija instalirana je na barem dva poslužitelja, a promet se balansira između niza poslužitelja na web sloju (*eng. gate servers*).

Unutar CEZIH sustava koristi se pet tipova certifikata kojima se potvrđuje autentičnost klijenta. Prvi tip certifikata je poslužiteljski certifikat koji se koristi za uspostavu transportnog kanala. Drugi tip certifikata su aplikativni certifikati koji se izdaju web aplikacijama koje se spajaju na CEZIH *web servis*, a služe za prijavu web aplikacija kao klijentski certifikati. Treći tip certifikata je certifikat izdan središnjem CEZIH sustavu za potpisivanje odlaznih poruka iz G1 sustava. Četvrti tip certifikata je potpisni certifikat koji se koristi u svrhu potpisivanja koda i tim certifikatom je potpisan sav kod koji se izvršava na strani korisnika kroz internetske preglednike. Peti tip su klijentski certifikati koji se izdaju zdravstvenim djelatnicima na pametnim karticama (eng. *smart cards*), a koriste se za prijavu na CEZIH programska rješenja te za potpisivanje poruka koje se razmjenjuju preko *web servisa*.

Liječnik na početku radnog vremena otvara svoju aplikaciju i tako vrši interakciju sa CEZIH sustavom. Aplikacija tada radi prvi upit prema CEZIH G1 uslugama. Liječnik nije upoznat sa detaljima implementacije procesa autentifikacije, već su oni dio unutrašnjeg načina funkcioniranja aplikacije koja se spaja na CEZIH sustav. Djelatnikov certifikat mora biti izdan od strane CEZIH certifikacijskog tijela te mora biti valjan. Također mora postojati djelatnikov korisnički zapis u imeničkom servisu pa se preko jedinstvenog matičnog broja vrši usporedba certifikata i korisničkog zapisa. Svaki korisnik u imeničkom servisu korisnika CEZIH sustava ima pridijeljenu ulogu koja se provjerava autorizacijom te ukoliko dodijeljena uloga dozvoljava slanje poruka u CEZIH sustav, slanje je dozvoljeno. CEZIH zahtjeva da sve poruke koje se upućuju prema centralnom sustavu budu potpisane. Osiguravanjem povjerljivosti i integriteta direktno se osigurava i neporecivost na nivou same poruke. Sve poruke koje ulaze u CEZIH

sustav se pohranjuju te se naknadnim pretraživanjem može utvrditi koji su podaci ušli u sustav te tko ih je kreirao. Svaki ulazni podatak prolazi kroz procjenu valjanosti. Za sva polja za unos podataka kontroliraju se tip i veličinu podataka. [7, 8]

3. ZAKONSKA REGULATIVA U DOMENI ZNR

Zaštita na radu iznimno je važan dio radno-pravnog sustava svake države. Prvi korak u uspješnom provođenju zaštite na radu je provođenje iste u skladu sa zakonima i propisima u RH, ali i težnja sa usklađivanjem i unaprjeđenjem s EU direktivama i normama.

Tijekom posljednjih 27 godina EU je predvodnik u postavljanju visokih standarda zaštite radnika od rizika za zdravlje i sigurnost na radnom mjestu na svojem području te promiče visoke razine zaštite i u trećim zemljama. Politika sigurnosti i zdravlja na radnom mjestu doprinosi cilju poboljšanja sigurnosti i zdravlja radnika unutar EU-a. Zakonodavni okvir EU-a imao je ključnu ulogu u oblikovanju strategija za sigurnost i zdravlje na radnom mjestu na nacionalnoj razini i razini poduzeća. Zakonski okvir EU-a temelji se na Okvirnoj direktivi 89/391/EEZ i 23 povezane direktive. Iz istoga proizlazi važnost shvaćanja definicije direktiva. Direktive su pravni akt čije je donošenje predviđeno u Ugovoru o EU-u i odnose se na gospodarstvo, kulturu, znanost, industriju, osiguranje i sl. U svim ovim područjima posebno mjesto ima zaštita na radu. Direktive su u potpunosti obvezujuće i obvezuju države članice da ih prenesu u svoje nacionalno pravo u određenom vremenskom roku i države članice ih moraju prevesti u okviru svoje legislative. One nas u osnovi i obavezuju na informacijsku integraciju u cilju unaprjeđenja stanja sigurnosti na radu zasnovanog na brzim i točnim aktualnim analitičkim podacima. Državama članicama dopušta se, naime, donijeti zaštitne mjere strože od onih koje su predviđene direktivama EU-a. Isto tako, primarnu odgovornost za provođenje nacionalnih odredaba, kojima se prenose direktive, snose nadležna nacionalna tijela, uobičajeno inspektorati rada

Prije ulaska u Europsku uniju Hrvatska je bila primorana preuzimati nove direktive, norme i propise te ih implementirati u svoj zakonodavni okvir. Republika Hrvatska je svoju pristupnicu za pristupanje Europskoj uniji veoma ozbiljno shvatila, što se tiče zaštite na radu i njenih zakonskih okvira koji se moraju ispuniti, pa se tako već davne 1996. godine, tadašnji članovi povjerenstva ministarstva nadležnog za rad, izradili zakonski prijedlog čija su najvažnija rješenja ostala na snazi još i danas. Već tada su prepoznali važnost okvirne Direktive 89/391/EFZ o uvođenju mjera za poticanje poboljšanja sigurnosti i zdravlja koja utvrđuje načela koja čine temelj ukupnog zakonodavstva Zajednice o zaštiti na radu. Nakon izrade zakonskog

prijedloga, Hrvatski Sabor je 28. lipnja 1996. donio Zakon o zaštiti na radu, a na snazi je od 1. siječnja 1997. godine. U tom periodu primjenjivalo se preko pedeset podzakonskih propisa.

Republika Hrvatska je krajem 2005. godine započela pregovore s Europskom unijom (EU). S pregovorima su došle i nove obaveze svih stručnjaka koji su se bavili zaštitom na radu. Trebalo je uskladiti naše propise s odgovarajućim direktivama EU i osigurati njihove provedbe prije nego li Hrvatska postane članicom EU.

Prva faza u usklađivanju našeg zakonodavstva s područja zaštite na radu bila je provedba analize usklađenosti kako bi se utvrdilo jesu li i u kojoj mjeri hrvatski propisi s ovog područja usklađeni s odredbama direktiva EU. Težište analize usklađenosti s direktivama EU bilo je prije svega usmjereno na analizu usklađenosti hrvatskih propisa s područja zaštite na radu s okvirnom Direktivom 89/391/EEC kao i s dodacima na koje se ona poziva.

Na temelju obavljene analize stupnja usklađenosti zakonodavstva Republike Hrvatske s pravnom stečevinom EZ-a (fra. *aquis*) iz područja zdravlja i sigurnosti na radu utvrđeno je sljedeće:

• naši su propisi u potpunosti usklađeni s ovim direktivama:

1. Direktivom 89/391/EEC o uvođenju mjera za poticanje poboljšanja sigurnosti i zdravlja radnika pri radu;

2. Direktivom 1999/92/EC o minimalnim zahtjevima za poboljšanje sigurnosti i zdravlja radnika koji su izloženi potencijalno eksplozivnim atmosferama (15. pojedinačna direktiva u smislu članka 16. Direktive 89/391/EEC).

• naši su propisi u znatnoj mjeri usklađeni s ovim direktivama:

1. Direktiva 89/654/EEC o minimalnim zahtjevima za sigurnost i zdravlje na radnom mjestu (1. pojedinačna direktiva u smislu članka 16. Direktive 89/391/EEC);

2. Direktiva 89/655 o minimalnim zahtjevima za sigurnost i zdravlje pri uporabi radne opreme (2. pojedinačna direktiva u smislu članka 16. Direktive 89/391);

3. Direktiva 92/85/EEC od 19. listopada 1992. o uvođenju mjera za poticanje poboljšanja sigurnosti i zdravlja pri radu trudnica, rodilja i dojilja (10. pojedinačna direktiva u smislu članka 16(1) Direktive 89/391/EEC);

4. Direktiva 92/91/EEC koja se odnosi na minimalne zahtjeve za unapređivanje sigurnosti i zaštite zdravlja prilikom dobivanja ruda bušenjem (11. pojedinačna direktiva u smislu članka 16. Direktive 89/391/EEC);

5. Direktiva 92/104/EEC o minimalnim zahtjevima za poboljšanje sigurnosti i zdravlja radnika zaposlenih na iskorištavanju rudnog bogatstva s površine i ispod površine zemlje (12. pojedinačna direktiva u smislu članka 16. Direktive 89/391/EEC);

6. Direktiva 98/24/EC o zaštiti zdravlja i jamčenju sigurnosti pred rizicima zbog izloženosti kemijskim tvarima pri radu (14. pojedinačna direktiva u smislu članka 16. Direktive 89/391/EEC);

7. Direktiva 2000/39/EC kojom se utvrđuje prva upućujući popis granica profesionalnog izlaganja vezano za primjenu Direktive 98/24/EC o zaštiti radnika od rizika izlaganja kemijskim tvarima pri radu;

8. Direktiva 2000/54/EC Europskog parlamenta i Vijeća od 18. rujna 2000. o zaštiti radnika od rizika u svezi s izlaganjem biološkim tvarima pri radu.

Nakon provedene analize usklađenosti ostalo je još 12 direktiva s kojima naši propisi nisu usklađeni.

Zatim je slijedila druga faza u poslu na usklađivanju odredaba naših propisa s odredbama direktiva EU. Bila je to horizontalna analiza učinaka na temelju odgovarajućih upitnika dobivenih od Ministarstva za europske integracije kojom su bile obuhvaćene ove direktive EU:

- Direktiva 86/188/EEC o zaštiti radnika zbog izloženosti buci pri radu;
- Direktiva 89/654/EEC o minimalnim zahtjevima za sigurnost i zdravlje na radnom mjestu;
- Direktiva 89/655 o minimalnim zahtjevima za sigurnost i zdravlje pri uporabi radne opreme;
- Direktiva 89/656/EEC o minimalnim zahtjevima za sigurnost i zdravlje pri uporabi osobne zaštitne opreme;
- Direktiva 90/269/EEC o minimalnim zahtjevima za sigurnost i zdravlje pri ručnom rukovanju teretima, pri čemu postoji mogućnost oštećenja leđa;

- Direktiva 90/270/EEC o minimalnim zahtjevima za sigurnost i zdravlje pri radu sa zaslonima;
- Direktiva 92/57/EEC o osiguranju minimalnih zahtjeva za sigurnost i zdravlje na privremenim radilištima;
- Direktiva 92/58/EEC o minimalnim zahtjevima za znakove koji se odnose na sigurnost i zdravlje pri radu;
- Direktiva 92/85/EEC od 19. listopada 1992.o uvođenju mjera za poticanje poboljšanja sigurnosti i zdravlja pri radu trudnica, rodilja i dojilja;
- Direktiva 98/24/EC o zaštiti zdravlja i jamčenju sigurnosti od rizika zbog izloženosti kemijskim tvarima pri radu;
- Direktiva 1999/92/EC o minimalnim zahtjevima za poboljšanje sigurnosti i zdravlja radnika koji su izloženi potencijalno eksplozivnim atmosferama;
- Direktiva 2000/54/EC Europskog parlamenta i Vijeća od 18. rujna 2000. o zaštiti radnika od rizika u svezi s izlaganjem biološkim tvarima pri radu.

Iz gore navedenog vidljivo je da je Republika Hrvatska išla dobrim putem ka usklađivanju naših propisa s odredbama direktiva EU u području zaštite na radu. Potrebno je još mnogo posla u usklađivanju kako bi se postigla povećana razina sigurnosti i zaštite zdravlja radnika i kako bi se mogli izračunati i smanjiti troškovi koji će biti nužni da se stanje u pogledu zaštite na radu u Republici Hrvatskoj dovede u sklad s odredbama direktive Europske unije.

Slijedile su višestruke izmjene i dopune Zakona koje su bile velikim dijelom uvjetovane usklađivanjem nacionalnog zakonodavstva s opsežnom pravnom stečevinom Europske unije na području zaštite zdravlja i sigurnosti na radu.

Prema Izvješću Komisije o napretku za 2007. godinu proizlazi da se u području zaštite zdravlja i sigurnosti na radu bilježi znatan napredak. U odnosu na zahtjeve pojedinačnih direktiva hrvatsko je nacionalno zakonodavstvo do tada bilo usklađeno kako slijedi:

- Pravilnik o zaštiti na radu za radne i pomoćne prostorije (NN 5/84 i 42/05) usklađen je s Direktivom Vijeća 89/654/EEZ od 30. studenoga 1989. o minimalnim sigurnosnim i zdravstvenim zahtjevima za radno mjesto (prva pojedinačna direktiva u smislu članka 16. stavka 1. Direktive 89/391/EEZ);
- Pravilnik o uporabi osobnih zaštitnih sredstava (NN 39/06) usklađen je s Direktivom Vijeća 89/656/EEZ od 30. studenoga 1989. o minimalnim sigurnosnim i zdravstvenim

zahtjevima za upotrebu osobne zaštitne opreme na radnom mjestu (treća pojedinačna direktiva u smislu članka 16. stavka 1. Direktive 89/391/EEZ);

- Pravilnik o sigurnosnim znakovima (NN 29/05) usklađen je s Direktivom Vijeća 92/85/EEZ od 19. listopada 1992. o provođenju mjera za poboljšanje sigurnosti i zdravlja trudnih radnica te radnica koje su nedavno rodile ili doje na radnome mjestu (deseta pojedinačna direktiva u smislu članka 16. stavka 1. Direktive 89/391/EEZ);
- Pravilnik o sigurnosti i zaštiti zdravlja radnika pri radu s računalom (NN 69/05) usklađen je s Direktivom Vijeća 90/270/EEZ od 29. svibnja 1990. o minimalnim zahtjevima u pogledu sigurnosti i zaštite zdravlja pri radu s opremom sa zaslonom (peta pojedinačna direktiva u smislu članka 16. stavka 1. Direktive 89/391/EEZ);
- Pravilnik o zaštiti na radu pri ručnom prenošenju tereta (NN 42/05) usklađen je s Direktivom Vijeća 90/269/EEZ od 29. svibnja 1990. o minimumu zdravstvenih i sigurnosnih uvjeta pri manualnom rukovanju teretom gdje postoji rizik osobito u slučaju ozljede leđa radnika (četvrta pojedinačna direktiva u smislu članka 16. stavka 1. Direktive 89/391/EEZ);
- Pravilnik o tehničkom nadzoru električnih postrojenja, instalacija i uređaja namijenjenih za rad u prostorima ugroženim eksplozivnim atmosferama (NN 39/06) usklađen je s Direktivom 1999/92/EZ Europskog parlamenta i Vijeća od 16. prosinca 1999. o minimalnim zahtjevima za poboljšanje sigurnosti i zaštite zdravlja radnika potencijalno izloženih riziku od eksplozivnih atmosfera (15. zasebna Direktiva u smislu članka 16. stavka 1. Direktive 89/391/EEZ);
- Odluka o tehničkim pravilima za statutarnu certifikaciju ribarskih brodova (NN 77/07) usklađena je s Direktivom Vijeća 93/103/EZ od 23. studenog 1993. o minimalnim zahtjevima za sigurnost i zdravlje pri radu na plovilima za ribolov (trinaesta pojedinačna direktiva u smislu članka 16. stavka 1. Direktive 89/391/EEZ);
- Pravilnik o minimalnim zahtjevima za poboljšanje sigurnosti i zdravstvene zaštite radnika u industrijama koje se bave vađenjem minerala bušenjem (NN 40/07) usklađen je s Direktivom 92/91/EEZ o minimalnim zahtjevima za poboljšanje sigurnosti i zdravstvene zaštite radnika u industrijama koje se bave vađenjem minerala bušenjem;
- Pravilnik o minimalnim zahtjevima za poboljšanje sigurnosti i zaštite zdravlja radnika u industrijama koje se bave vađenjem minerala iz površinskih ili podzemnih kopova (NN 40/07) usklađen je s Direktivom Vijeća 92/104/EEZ od 3. studenoga 1992. o minimalnim uvjetima za poboljšanje sigurnosti i zaštite zdravlja radnika u industrijama

ekstrahiranja minerala bušenjem (jedanaesta pojedinačna Direktiva u smislu članka 16. stavka 1. Direktive 89/391/EEZ);

- Pravilnik o zaštiti radnika od rizika povezanih s izlaganjem karcinogenima ili mutagenim tvarima na radu (NN 40/07) usklađen je s Direktivom 2004/37/EZ o zaštiti radnika od rizika povezanih s izlaganjem karcinogenima ili mutagenima na radu (šesta pojedinačna direktiva u smislu članka 16. stavka 1. Direktive 89/391/EEZ);
- Pravilnik o zaštiti radnika od rizika vezanih uz izloženost azbestu na radnom mjestu (NN 40/07) usklađen je s Direktivama 83/477/EEZ od 25. lipnja 1991. kojom se izmjenjuje i dopunjuje Direktiva 83/477/EEZ o zaštiti radnika od rizika vezanih uz izloženost azbestu na radnom mjestu (druga pojedinačna Direktiva u smislu članka 8. Direktive 80/1107/EEZ) i 2003/18/EZ Europskoga parlamenta i Vijeća od 27. ožujka 2003. kojom se izmjenjuje i dopunjuje Direktiva Vijeća 83/477/EEZ o zaštiti radnika od rizika vezanih uz izloženost azbestu na radnom mjestu;
- Pravilnik o minimalnim zahtjevima i uvjetima pružanja medicinske skrbi na brodovima, brodicama i jahtama (NN 14/08) usklađen je s Direktivom Vijeća 92/29/EEZ od 31. ožujka 1992. godine o minimalnim sigurnosnim i zdravstvenim zahtjevima za poboljšanje liječničke pomoći na brodovima.

Također su, uz naprijed navedeno, dovršene aktivnosti izrade konačnih prijedloga:

- Pravilnika o minimalnim zahtjevima u pogledu sigurnosti i zaštite zdravlja radnika pri upotrebi radne opreme na radnom mjestu (89/655/EEZ);
- Pravilnika o zaštiti radnika od izloženosti buci na radu (2003/10/EZ);
- Pravilnika o minimalnim zdravstvenim i sigurnosnim zahtjevima koji se odnose na izloženost radnika rizicima koji potječu od elektromagnetskih polja (2004/40/EZ);
- Pravilnika o zaštiti na radu na privremenim ili pokretnim radilištima (92/57/EEZ).

U zakonodavstvu zaštite na radu i dalje se pokazuje problem administrativnih kapaciteta, odnosno, sposobnosti relevantnih tijela za implementaciju i nadzor istoga. Nadalje je potrebno nastaviti obučavati inspektore zaštite na radu s ciljem povećavanja razine njihovog znanja i mobilnosti. Također je potrebno inspekciju zaštite na radu tehnološki bolje osposobiti tj. uvesti korištenje odgovarajuće, modernije opreme.

Nakon detaljne analize usklađenosti RH počinje koristiti i mogućnosti pristupnog programa IPA. Uredba o programu IPA primjenjuje se od 1. siječnja 2007. godine. Ovom se

Uredbom propisuju provedbena pravila kojima se uređuje pružanje pretpristupne pomoći od strane Zajednice koja je uspostavljena Uredbom Vijeća (EU) br.1085/2006 (IPA) tj. Uredbom o programu IPA. Sve detalje o korištenju i obavezama svih zemalja koje pristupaju EU pa tako i Republike Hrvatske u vezi pristupnog programa može se pročitati u uredbi Uredba Komisije (EU) br. 718/2007 od 12. lipnja 2007. godine o provedbi Uredbe Vijeća (EU) br.1085/2006 kojom se uspostavlja instrument pred pristupne pomoći. Osnovni cilj ovog programa je pomoć državama kandidatkinjama za članstvo u EU i državama potencijalnim kandidatkinjama u usklađivanju nacionalnog zakonodavstva i provedbi pravne stečevine EU (fra. *Acquis Communautaire*) u procesu pridruživanja u članstvo EU, kao i pripremi za korištenje kohezijskog i strukturnih fondova.

Republika Hrvatska je korisnica IPA programa od 2007. godine i imala ga je pravo koristiti do pristupanja u članstvo EU. Republika Hrvatska kao zemlja kandidatkinja za punopravno članstvo u EU imala je mogućnost korištenja sredstava iz svih pet komponenti:

1. Pomoć u tranziciji i jačanje institucija;

2. Prekogranična suradnja;

3. Regionalni razvoj – promet, zaštita okoliša, regionalna konkurentnost;

4. Razvoj ljudskih potencijala;

5. Ruralni razvoj.

Opći cilj programa IPA je razvoj djelotvornog sustava zaštite zdravlja i sigurnosti na radu u Hrvatskoj u skladu sa standardima EU, kao i jačanje administrativnih kapaciteta svih relevantnih institucija vezanih uz zaštitu zdravlja i sigurnost na radu, u skladu sa mjerilima za Poglavlje 19 - Socijalna politika i zapošljavanje u pregovorima, u procesu pristupanja Hrvatske EU i uvođenje metodologije EU statistike prema EODS-u i ESAW-u.

Glavni cilj je uspostaviti učinkovit sustav i mrežu institucija za zaštitu na radu radi uz povezivanje postojećih i novih baza podataka, kao i sustava upravljanja zaštitom na radu. Pojedine komponente ugovora bih istaknula kao bitnu činjenicu nastanka i razvoja ovog diplomskog rada, a to su: „Europska statistika ozljeda na radu", „Procjena opasnosti", „Razrada koncepta IT mreže među sudionicima projekta" i „Pružanje pomoći pri razvoju i pripremi smjernica za provedbu praćenja, nadzora, statistika i analiza vezanih uz EU direktive te izrada Priručnika kojim bi stručnjak zaštite na radu provodio unutarnji nadzor".

Program IPA u sklopu kojeg su provedeni razni projekti je pridonio jačanju kapaciteta u smislu kadrovskih kompetencija, kako bi bili u mogućnosti obavljati potrebne dužnosti i aktivnosti na najučinkovitiji način u smislu organizacije. Jačanjem kapaciteta institucija uključenih u projekt, koje su dio sustava zaštite zdravlja i sigurnosti na radu, poboljšala se kvalitetna, pristupačna zdravstvena zaštita i prevencija bolesti. Razmjena informacija i iskustava, na kojoj se radilo između dionika omogućila je bolju povezanost svih relevantnih podataka o bolesnim i ozlijeđenim radnicima, analizu podataka i izradu zaključaka na temelju tih analiza, što je doprinijelo razvoju informacijskog sustava i učinkovitog sustava zaštite zdravlja i sigurnosti na radu.

Iz svega gore navedenog vidljivo je da je program IPA uvelike pomogao Republici Hrvatskoj, no, ona nije stala samo na tome. Od početka 2013. godine na snazi je novi obrazac prijave ozljede na radu koji sadrži podatke o ozljedi na radu sukladne metodologiji Europske statistike ozljeda na radu po tzv. ESAW (*eng. European Statistics on Accidents at Work*) metodologiji, jer je Republika Hrvatska od početka punopravnog članstva u EU obvezna dostavljati podatke o ozljedama na radu Europskom uredu za statistiku u obliku koji je sukladan ovoj metodologiji. Slijedom navedenog Hrvatski zavod za zaštitu zdravlja i sigurnost na radu analizira podatke o ozljedama na radu koje su se dogodile na mjestu rada po parametrima koji su sukladni metodologiji Europske statistike ozljeda na radu a to su:

- mjesto i vrijeme ozljeđivanja;
- podaci o radniku koji je ozlijeđen (spol, državljanstvo, zaposlenički status, zanimanje, osposobljenost iz ZNR i dr.);
- podaci o poslodavcu (djelatnost i veličina poslodavca kod kojeg je zaposlen ozlijeđeni radnik);
- podaci o vrsti ozljede i ozlijeđenom dijelu tijela, poslu koji je obavljan i prostoru u kojem je obavljan posao kada se radnik ozlijedio, prema specifičnoj aktivnosti i poremećaju koji je doveo do ozljede, načinu nastanka ozljede i materijalnim sredstvima koja su pri tom korištena ili sudjelovala u ozljedi;
- medicinski pokazatelji (ozlijeđeni dio tijela, MKB) i pojedinačna analiza za područja djelatnosti u kojima se ozlijedila većina radnika u odnosu na ukupan broj analiziranih ozljeda.

Na osnovu podataka Državnog zavoda za statistiku o broju zaposlenih u RH po granama djelatnosti i podatka o broju ozljeda na radu prijavljenih Hrvatskom zavodu za zdravstveno

osiguranje, Hrvatski zavod za zaštitu zdravlja i sigurnost na radu izračunava i stopu ozljeda na radu na 1000 zaposlenih.

Novi Zakon o zaštiti na radu donesen je 2014. godine i objavljen je u Narodnim novinama br.71 i počeo se primjenjivati od 19.lipnja 2014. godine. Ovim Zakonom se propisuju obveze poslodavaca i radnika, institucije nadležne za praćenje i unapređivanje područja zaštite na radu te se na drugačiji način propisuju ovlasti inspekcijskog nadzora. Cilj donošenja novog Zakona je u prvom redu smanjenje broja njegovih provedbenih propisa, njegova jednostavnija primjena i smanjivanje administrativnih troškova izrade dokumentacije, ali i uz novu ulogu inspektora zaštite na radu. Novi Zakon o zaštiti na radu u potpunosti je usklađen sa svim propisima Europske unije u tom području, kao i s mjerodavnom praksom Suda pravde Europske unije (eng. *Court of Justice of the European Union*) i njegovim tumačenjem propisa Europske unije u tom području.

Početkom 2019. godine, točnije 1. siječnja na snagu je stupio Zakon o izmjenama i dopunama Zakona o zaštiti na radu. Izmjene i dopune ovog Zakon usklađene su sa svim direktivama EU na području sigurnosti i zaštite na radu.

Najvažnije promjene koje su izmijenjene u zakonu su slijedeće:

- zavod za unapređivanje zaštite na radu s danom 1. siječnja 2019. godine prestao je s radom, a postojeće zaposlenike i poslove Zavoda preuzelo je Ministarstvo rada i mirovinskog sustava;
- uvela se prekršajna sankcija prema poslodavcu ako pri izradi procjena rizika ne sudjeluju radnici, odnosno njihovi predstavnici;
- utvrđuje se da se Zakon o zaštiti na radu ne primjenjuje na obrtnika koji obrt obavlja sam kao niti na poslodavca kojeg zastupa jedna fizička osoba koja je ujedno i jedini radnik kod poslodavca, ali samo kada izolirano kao pojedinci obavljaju određene poslove na svojim mjestima rada. Ukoliko samozaposlene osobe rade zajedno s drugom osobom ili s više drugih osoba obavljaju poslove na istom mjestu rada, tada se na njih primjenjuju odredbe Zakona o zaštiti na radu. Također, samozaposlene osobe u obvezi su ispunjavati obveze propisane Zakonom o zaštiti na radu kada za njih određene aktivnosti obavljaju osobe na radu (studenti, volonteri, osobe na stručnom osposobljavanju, učenici na praksi i sl.);

- smanjila se dinamika održavanja redovnih sjednica Odbora zaštite na radu, sa najmanje jednom u 3 mjeseca na najmanje jednom u 6 mjeseci, s tim da se dopunjuje prekršajna odredba u vezi neodržavanja redovnih sjednica odbora;
- smanjio se potreban broj osposobljenih radnika za pružanje prve pomoći na ukupan broj radnika (umjesto najmanje 1 do 20 radnika, najmanje 1 do 50 radnika);
- izostavilo se pojam „teške ozljede“ na mjestu rada kod poslodavca, ali se određuje pojam događaja ozljede na mjestu rada kojeg poslodavac ima obvezu prijaviti, budući da je neprijavljivanje takvoga događaja inspekcijskom tijelu, i to odmah po nastanku, sankcionirano kao prekršaj.

Kroz analizu povijesti razvoja zakonske regulative na području Republike Hrvatske može se zaključiti da je ista znatno napredovala. Nadležna tijela Republike Hrvatske su shvatila da se implementiranjem europskih direktiva i normi stvara sigurnije radno okruženje u kojem radnici rade s manje opasnih tvari i supstanci koje na ovaj način manje štete kako radniku tako i okolišu. Današnji temeljni zakon koji uređuje zaštitu na radu u RH jest Zakon o zaštiti na radu (NN br. 71/14., 118/14, 154/14, 94/18, 96/18). Uz Zakon o zaštiti na radu, široko područje zaštite na radu uređuje se i drugim zakonskim propisima. Prava, obveze i odgovornosti u svezi zaštite na radu uređuju se na izravan i neizravan način i propisima radnog zakonodavstva, mirovinskog osiguranja, zdravstvenog osiguranja i zdravstvene zaštite, tehničkim i drugim propisima kojima se štite sigurnost i zdravlje osoba na radu i drugih osoba te kolektivnim ugovorima.

Neki aktualni drugi zakonski propisi koji uređuju i zaštitu na radu su:

- Zakon o zdravstvenom osiguranju zaštite zdravlja na radu (NN br. 85/06, 67/08.);
- Zakon o listi profesionalnih bolesti (NN br. 162/98., 107/07);
- Zakon o normizaciji (NN br. 163/03);
- Zakon o općoj sigurnosti proizvoda (NN br. 30/09);
- drugi zakonski propisi u skladu sa Zakonom o sigurnosti i zdravlju na radu.

Upravna tijela za područje zaštite na radu u Republici Hrvatskoj su:

- Hrvatski zavod za zaštitu zdravlja i sigurnost na radu;
- Hrvatski zavod za zdravstveno osiguranje;
- Državni inspektorat rada;

- Ministarstvo rada i mirovinskog sustava.

Provedbu zakonskih obavezna nadzire Državni inspektorat temeljem pravilnika o unutarnjem ustrojstvu Državnog inspektorata.

Zakonom o zaštiti na radu uređen je sustav zaštite na radu u Republici Hrvatskoj, a osobito nacionalna politika i aktivnosti, opća načela prevencije i pravila zaštite na radu, obveze poslodavca, prava i obveze radnika i povjerenika radnika za zaštitu na radu, djelatnosti u vezi sa zaštitom na radu te nadzor i prekršajna odgovornost. Svrha ovog zakona je uvođenje mjera za poticanje unaprjeđenja sigurnosti i zdravlja ranika na radu, sprečavanje ozljeda na radu te profesionalnih bolesti i drugih bolesti u svezi sa radom. Odredbe ovog Zakona primjenjuju se u svim djelatnostima u kojima radnici obavljaju poslove za poslodavca izuzev Oružanih snaga RH, policije, poslova zaštite i spašavanja, poslova zaštite i imovine te poslova vatrogasaca i pirotehničara.

Na temelju Zakona o zaštiti na radu ministar nadležan za rad donosi podzakonske akte kojima se detaljnije uređuju određeni uvjeti i pravila zaštite na radu. Podzakonskim aktima se pobliže utvrđuju određeni zahtjevi sigurnosti koji proizlaze iz odgovarajućih direktiva propisanih od vijeća EU. Poveznice za sve najvažnije hrvatske zakone i propise koji su na snazi i odnose na zaštitu na radu su: Narodne novine [9] i Središnji katalog službenih dokumenata RH [10]. Vlada Republike Hrvatske dužna je pratiti najnovija dostignuća u području zaštite na radu, te raditi i vrednovati politiku zaštite zdravlja i zdravlja na radu i usklađivati ih s promjenama koje donosi EU.

4. AKTUALNI STUPANJ PRIMJENE IKT U DOMENI ZNR U RH

Sustav zaštite na radu u RH suočen je s vremenom brzih promjena, sve većom uporabom novih tehnologija u svakodnevnom životu i radu, ali i učenju i podučavanju. U današnje doba stručnjaci zaštite na radu kao i sami poslodavci susreću se u praksi s ogromnim listama i evidencijama koje su vezane za određene djelatnike i njihova radna mjesta, te velikim količinama dokumenata, registratora i datoteka. Stoga se u okviru tih institucija koje su primarni korisnici podataka zaštite na radu u RH uočilo potrebu i neophodnost da se u razvojnim strategijama napravi most između informacijsko-komunikacijske tehnologije (IKT) i korisnika podataka zaštite na radu.

Na području zaštite na radu postoji više razina aktivnosti, kao i više područja djelovanja. Razina neposredne organizacije, provođenje i kontrola provođenja mjera zaštite na radu moraju svakako biti vezane uz samo radno mjesto i radnike koji tu rade. Zaštita na radu zahtijeva i značajniji dio stručnih i specijalističkih znanja na razini analize, planiranja i organiziranja cjelovitih mjera zaštite na radu. Također tu spadaju različite evidencije, administrativno-tehnički poslovi, kontakti s vanjskim institucijama, te čitava grupa stručnih i administrativnih poslova vezanih uz povrede na radu. Djelatnosti poduzeća, kao i tehnologija koju poduzeće koristi mogu u određenim slučajevima značajno utjecati na obujam i sadržaj poslova zaštite na radu. Tijekom svog studiranja i obavljanja stručne prakse imala sam uvid u stanje zaštite na radu u tvrtkama i velike napretke što se tiče same provedbe zaštite na radu u skladu sa novim tehnologijama i razvojem interneta.

Analiza stanja zaštite na radu u tvrtkama diljem RH provodi se kroz obradu troškova poslodavca u provedbi zaštite na radu vezano uz edukaciju i osposobljavanja, troškove nabave zaštitnih sredstava, obradu i analizu postojećih podataka o ozljedama na radu te izračune troškova za poslodavce i državu. Analizom stanja zaštite na radu i provjere provedbe osposobljavanja radnika za rad na siguran način, izrade procjene rizika, provedbe raznih ispitivanja radne okoline i radne opreme utvrđuje se stvarno stanje i stupanj primjene i provedbe pravila zaštite na radu, ali po mom mišljenju, ovi rezultati su nedovoljno povezani na nacionalnoj razini između poslodavaca te pravnih i fizičkih osoba ovlaštenih za obavljanje poslova zaštite na radu.

U današnje vrijeme većina tvrtki za vođenje evidencija i organiziranje poslova za zaštitu na radu koristi lokalne i globalne mrežne aplikacije čime značajno pojednostavljuju, unaprjeđuju

i osiguravaju dobro poslovanje svoje tvrtke. Na tržištu u ponudi nalazimo više proizvođača, odnosno verzija tih aplikacija koje su kroz svoj razvoj pratile napredak tehnologije i napredovale od samostalnih aplikacija, preko lokalnih mrežnih aplikacija pa do globalnih mrežnih aplikacija ili, kako ih najčešće jednostavnije nazivamo, web aplikacija. Proučavajući današnje web aplikacije koje su u aktualnoj ponudi na tržištu, mišljenja sam da sve rade na sličnim načelima i uvelike olakšavaju i ubrzavaju posao.

Suvremene web aplikacije za vođenje poslova zaštite na radu namijenjene su djelatnicima zaduženim za vođenje zaštite na radu. Pomoću ovih aplikacija korisnici vode evidencije podataka potrebne za ispunjenje evidencija propisanih Zakonom i Pravilnicima s područja zaštite na radu. Većinom ih čak i ne treba posebno instalirati u IT infrastrukturu tvrtke koja želi biti korisnik, jer rade na načelu računalstva u oblaku, o kojem sam pisala u prethodnim poglavljima. Proizvođači korisnicima na ovaj način omogućuju stalni pristup najnovijim verzijama. Temeljni podaci koje sadrže ove aplikacije odnose se na evidencije podataka o djelatnicima što uključuje uvjerenja o osposobljenosti na rad na siguran način i zaduženja zaštitnih sredstava koje koriste tijekom obavljanja radnog procesa. Nadalje se tu nalaze evidencije o ispitivanjima radne opreme i provedbom njihovih periodičkih pregleda, ispitivanja radne okoline, liječničke uputnice koje se razlikuju ovisno o izloženosti rizika na radnom mjesto, a to su RA-1, RO-1, RO-2 i NR-1. Vode se i evidencije o prijavama ozljede na radu i profesionalnih bolesti, kompletna izvješća o ozljedama na radu. Na temelju evidentiranih podataka omogućena je izrada liječničkih uputnica i izvještaja te evidencijskih kartona a to su:

- EK - 1 - o osposobljenosti radnika za rad na siguran način;
- EK - 2 - o radniku raspoređenom na poslove s posebnim uvjetima rada;
- EK - 4 - o ispitivanju strojeva i uređaja s povećanim opasnostima;
- EK - 5 - o ispitivanju radne okoline;
- EK - 6 - o pregledu ili ispitivanju osobnog zaštitnog sredstva.

Evidencijski kartoni i liječničke uputnice imaju propisani zakonski obrazac. Aplikacije omogućuju praćenje i planiranje troškova za pojedine gore navedene obveze stručnjaka zaštite na radu. Sve gore navedene evidencije i ispitivanja imaju svoje rokove, stoga aplikacija omogućava praćenje rokova, te putem kalendara i elektroničke pošte, upozorava korisnike na vrijeme o nadolazećim obavezama. Takvo načelo rada samim stručnjacima zaštite na radu, tj. korisnicima, uvelike olakšava posao jer na vrijeme mogu planirati svoje obaveze te smanjuju mogućnost pogrešaka koje se u zaštiti na radu jako skupo naplaćuju. Tijekom ispunjavanja

određenih uputnica ili obrazaca za pojedinog radnika podaci koji su već uneseni u bazu podataka aplikacije bit će u te obrasce uneseni automatski, što uvelike ubrzava cijeli postupak. Svi podaci koji se unose usklađeni su sa zakonima i zakonskim promjenama u RH. Administratori stalno ažuriraju aplikaciju i usklađuju je sa svim promjenama u području zaštite na radu. Podaci iz mrežnih aplikacija o evidencijama zaštite na radu lako se prenose iz jedne u drugu mrežnu aplikaciju, što je jedna od ključnih ugovorenih usluga na koju se obvezuju pružatelji ovih mrežnih usluga (proizvođači aplikacija), a koja osigurava tzv. *longitudinalnost* zapisa o djelatnicima i događajima. Ovo je također jedan od ključnih zahtjeva na elektroničke zapise koji se kao kriterij mogu preuzeti od zdravstvenih informacijskih sustava i svojstava elektroničkog zdravstvenog kartona (EZK).

Neke mrežne aplikacije sadrže mogućnost uvoza podataka iz CSV, Excel ili PDF datoteka. Uz evidentirane podatke moguće je priložiti datoteke poput skeniranih uvjerenja, upute za rad na siguran način i drugu potrebnu dokumentaciju. Sve postojeće dokumente koji su do sada bili raspodijeljeni i rasipani na različitim mjestima moguće je staviti na jedno mjesto u obliku digitalne arhive. Neke od mrežnih aplikacija svojim korisnicima nude i modul procjene rizika unutar same aplikacije. Procjena rizika je temeljni i najvažniji dokument u pogledu unaprjeđenja zaštite zdravlja i sigurnosti radnika. Skupina alata koje koristi ovaj modul pripremaju poslodavce i radnike za procjenu rizika, pomažu u prepoznavanju rizika i izradi plana mjera za prevenciju mogućih opasnosti te zaštitu zdravlja radnika. Sastoji se od pet modula koji uključuju organizaciju i provođenje zaštite na radu te informacije o uvjetima rada. Također, navedene su i mjere zaštite od požara. Završno izvješće može se pohraniti i ispisati kao dokument procjene rizika, jednako kao i plan mjera. Modul procjene rizika unutra mrežne aplikacije prati istu programsku logiku gdje korisnik prolazi kroz navedene elemente procjene te na taj način iste odabire i dodaje u postupak obrade. Na ovaj način omogućena je jednostavna, kvalitetna i brza izrada procjene rizika za tvrtku.

Svi podaci uneseni u aplikacije nalaze se na certificiranim poslužiteljima te proizvođači aplikacija jamče apsolutnu sigurnost i zaštitu, uključujući automatsku izradu sigurnosnih kopija. Proizvođači aplikacija prikupljaju podatke o IP adresama zbog sigurnosnih razloga, za potrebe dijagnostike i statističke analize prometa radi poboljšanja kakvoće te upotrebljivosti usluga koje nude. Prikupljanje svih osobnih podataka i sama razmjena podataka između klijenta i mrežnih poslužitelja provodi se preko kriptirane veze te su svi podaci pohranjenu iza vatrozida sukladno najvišim IT normama. Aplikacija omogućava kontrolu pristupa podacima. Još jedna dobra strana *cloud aplikacija* je što su svi podaci uvijek dostupni i s vama bez obzira gdje se

nalazili te se mogu koristiti s bilo kojeg uređaja koji se može spojiti na internet. Prednost je što više korisnika istodobno može raditi sa istim podacima. Putem korisničkih portala za stručnjake zaštite na radu može se dozvoliti kontrolirani pristup podacima iz evidencije, a pri tome stručnjaci zaštite na radu cijelo vrijeme imaju potpunu kontrolu nad tim podacima koji se pokazuju na korisničkim portalima. Korištenje *cloud* aplikacija riješilo bi problem ograničenog pristupa i zahtjev za internom pohranom podataka koje imaju *web* aplikacije. Potpuno bi se riješio problem pohrane te bi zbog svojstva sveprisutnosti bile dostupne s raznih uređaja i raznih lokacija. Lokalne mrežne i *web* aplikacija trebale bi s vremenom migrirati u *cloud* aplikacije te će se u nastavku koristiti izraz aplikacija bez obzira na detalje izvedbene tehnologije. Te aplikacije trebale bi postati klijenti za DC, kao što su G2 aplikacije klijenti za CEZIH (G1 grupu).

4.1. Ideja izgradnje SNIS ZNR

Međunarodna organizacija rada (eng. *International Labour Organization,* ILO) je povodom međunarodnog dana sigurnosti i zdravlja na poslu, 28. travnja 2017. godine, predstavila ideju prikupljanja i obrade podataka vezanih uz ZNR na međunarodnom planu [11]. Prema njihovim procjenama tada je bilo 313 milijuna ozljeda na radu, a te ozljede na radu smanjuju BDP za 4%. Vrlo je važno da zemlje povećaju svoje kapacitete za prikupljanje i analizu podataka o ZNR u svrhu prevencije. Podaci su neophodni za određivanje prioriteta i mjerenje napretka kako na razini tvrtke, tako i na nacionalnoj razini. Nadležno tijelo može biti ministarstvo rada koje je ovlašteno izdavati propise ili naloge koji imaju zakonsku snagu u odnosu na sustav. Ministarstvo u suradnji s reprezentativnom organizacijom poslodavaca i radnika treba osigurati uspostavu i primjenu sljedećih postupaka:

- izvješćivanje o ozljedama na radu i profesionalnim bolestima;
- izvješćivanje u ozljedama na putu da posla;
- istrage nesreća koje uzrokuju ozljede;
- izrade godišnjih statistika o ozljedama na radu, bolestima i smrtnim slučajevima;
- izvješćivanje o slučajevima pojava opasnih profesionalnih bolesti.

Nacionalni sustav za bilježenje i izvještavanje o ozljedama na radu i profesionalnim bolestima trebao bi težiti pokrivanju svih grana gospodarske djelatnosti, svih tvrtki i radnika, neovisno o opisu radnog mjesta. Osim toga trebao bi pružiti sveobuhvatne i pouzdane podatke o učestalosti ozljeda na radu i profesionalnim bolestima u cilju izrade preventivnih mjera zaštite na radu na razini tvrtke, sektora kojem tvrtka pripada te na nacionalnoj razini. Potrebno je objavljivati usporedne nacionalne statistike i izvješća u preventivne svrhe te na taj način doprinositi međunarodnoj pozitivnoj statistici. Nacionalni sustav trebao bi imati ugrađen sustav definicija i klasifikacija ozljeda na radu te osiguravati odgovarajuće djelotvorne sustave za naknadu štete. Mnoge zemlje nemaju dostupne pouzdane podatke o ozljedama na radu zbog nedovoljnog praćenja i izvještavanja. Uzrok tome su složeni postupci za evidentiranje, preopširna papirologija, neodlučnost da se odmah prijavi i zatraži pomoć od liječnika te odstupanja između zabilježenih i prijavljenih slučajeva. Zakašnjeli ili nepodneseni izvještaj otežava pravovremenu zamjenu ozlijeđenog radnika s adekvatnim radno sposobnim radnikom. Podaci drugih zemalja i međunarodni izvori informacija mogu biti korisna referenca, posebno za zemlje koje nemaju pouzdane nacionalne statistike. Zbog nedovoljnog evidentiranja i prijavljivanja ozljeda na radu neke zemlje dopunjuju zakonske odredbe podacima prikupljenim iz drugih izvora kako bi dobile cjelovitiju sliku te ocijenili stanje i napredak ZNR. Posebna istraživanja, poput anketa o radnom okruženju i pitanja vezanih uz ZNR, mogu se uključiti u nacionalne ankete o zdravlju i anketiranje zaposlenih. Ostali regionalni i nacionalni administrativni podaci o zdravstvu koji mogu pružiti informacije o zdravlju radnika, raspodjeli smrtnosti, bolestima i ozljedama u sektorima po zanimanjima su: popis stanovništva, evidencija primarnog i bolničkog liječenja, podaci o smrtnosti i izvješća medicinske inspekcije koje provodi zdravstvena inspekcija. Neki od izazova za uspostavu učinkovitih sustava za bilježenje i izvještavanje koji pružaju pouzdane podatke su:

- određene grane gospodarstva i kategorije radnika su isključene zbog izostanka sveobuhvatne pokrivenosti u nacionalnim pravnim okvirima;
- nacionalni sustavi evidentiranja i prijavljivanja ne smatraju se sastavnim dijelom upravljanja rizicima na radu;
- dijagnoza profesionalnih bolesti zahtjeva specifična znanja i iskustva koja nisu dostupna u mnogim zemljama pa zbog toga dolazi do razlika u kriterijima za priznavanje profesionalnih bolesti;

- odgovornosti za ZNR mogu se podijeliti na više nadležnih tijela pa to rezultira nekompatibilnošću prikupljenih podataka te posljedično nemogućnosti procjene i izrade nacionalnih i globalnih podataka;

- terminologija, definicije i klasifikacije razvijene su u svrhu kompenzacije i razlikuju se od zemlje do zemlje, a dostupni podaci nisu usklađeni na razini države, što otežava procjenu regionalnih ili globalnih trendova.

Na razini tvrtke bilježili bi se pogrešni koraci, a njihovo praćenje bilo bi ključno za uspješnost ZNR i pružanje informacija u slučajevima kada nadzor stvarnih ozljeda daje nedovoljno podataka. Kao izvori informacija mogu se koristiti i sustavi izvješćivanja o incidentima koji su razvijeni za brzu identifikaciju opasnosti, pravovremeno pokretanje preventivnih mjera i brzu reakciju kod velikih nesreća i industrijskih katastrofa.

Nacionalni sustav nadzora ZNR koristio bi između ostalog i za praćenje smrtnosti i morbiditeta profesionalnih ozljeda i bolesti te bi uključivao sljedeće:

- individualne i kolektivne procjene zdravlja, zdravstvene ankete, istrage i izvješća medicinskih inspekcija;

- sumnjive slučajeve bolesti radi odgovarajućeg praćenja mogućeg podrijetla bolesti s dugim periodima latencije;

- podsustav zdravstvenih evidencija o zdravstvenom stanju pojedinih radnika koji će se pratiti tijekom cijelog radnog vijeka.

Zavod za unaprjeđenje zaštite na radu (ZUZNR), prije nego je postao dio Ministarstva rada i mirovinskog sustava, predstavio je u siječnju 2016. godine program pomoću kojega bi unaprijedio ZNR, zdravlje i produktivnost radnika u Republici Hrvatskoj. Njihova vizija je razvijati kulturu prevencije i unaprjeđivanja ZNR radi osiguranja sigurnih i zdravih radnih mjesta koja pridonose dobrobiti radnika i poslodavca, rastu produktivnosti, konkurentnosti i gospodarskom rastu. Edukacijom u području ZNR podizala bi se razina svijesti i informiranosti. Osim edukacije uvedene u školskoj dobi, kao glavni projekt je naglašena sveobuhvatna baza podataka pod nazivom "*Data Collector* ZNR". Prije definiranja projektnog zadatka bilo je potrebno provesti detaljnu analizu postojećeg stanja (analiza raspoloživih resursa, procesa, ciljeva i potreba) te nakon toga definirati sve potrebne resurse i pripremiti natječajnu dokumentaciju. Nakon provedenog natječaja uslijedile bi faze izrade, testiranja i

implementacije informacijskog sustava te edukacija sudionika (budućih konzumenata informacijskog sustava). Održivost projekta je važan parametar koji treba zadovoljiti kako bi realizacija projekta bila opravdana.

4.2. Data Collector

Središnji nacionalni informacijski sustav zaštite na radu (SNIS ZNR) nazvan *Data Collector* (u nastavku rada označavat će se kraticom „DC“) integrirao bi podatke vezane uz zaštitu na radu u jedinstvenu bazu s ciljem podizanja kvalitete ukupnog stanja zaštititte na radu u Republici Hrvatskoj. Sve institucije, korisnici podataka zaštite na radu, trenutno koriste interne baze podataka koje nisu međusobno povezane i ne omogućuju međusobnu razmjenu podataka. Krajnji korisnici DC bit će poslodavci te pravne i fizičke osobe ovlaštene za obavljanje poslova zaštite na radu. Sustav bi omogućio generiranje različitih cjelovitih podataka koji bi se koristili za praćenje stanja zaštite na radu, izradu stručnih elaborata, provođenje statističkih istraživanja, izrađivanje metoda i modela zaštite na radu, utvrđivanje kriterija i postupaka u vezi s organizacijom rada. DC bi osigurao da se u bazu podataka dostavljaju svi relevantni podatci na osnovi odgovarajućeg Pravilnika.

Slika 5. Blok shema cjelokupnog SNIS ZNR [12]

Različite skupine korisnika trebale bi unositi odgovarajuće podatke u DC:

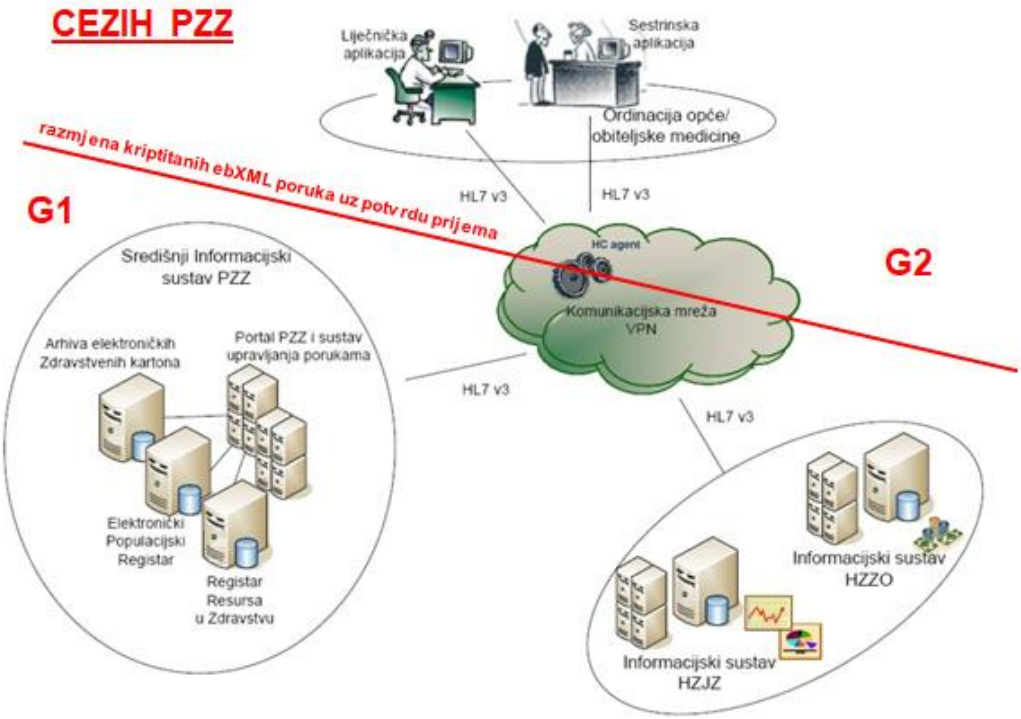
- **HZZO i HZZZSR**. Unos podataka o ozljedama na radu i profesionalnim bolestima izravno u bazu ili učitati iz postojeće interne baze;

- **Inspektorat rada**. Unos podataka o nepravilnostima nakon provedenih inspekcijskih nadzora;
- **Poslodavci**. Omogućen unos podataka preko web sučelja i učitavanje podataka iz postojećih baza propisano Zakonom o ZNR i pravilnicima;
- **Ovlaštene osobe (pravne i fizičke)**. Omogućen unos podataka preko web sučelja;
- **ZUZNR**. Evidencija ovlaštenja za pravne i fizičke osobe i unos podataka direktno u aplikaciju.

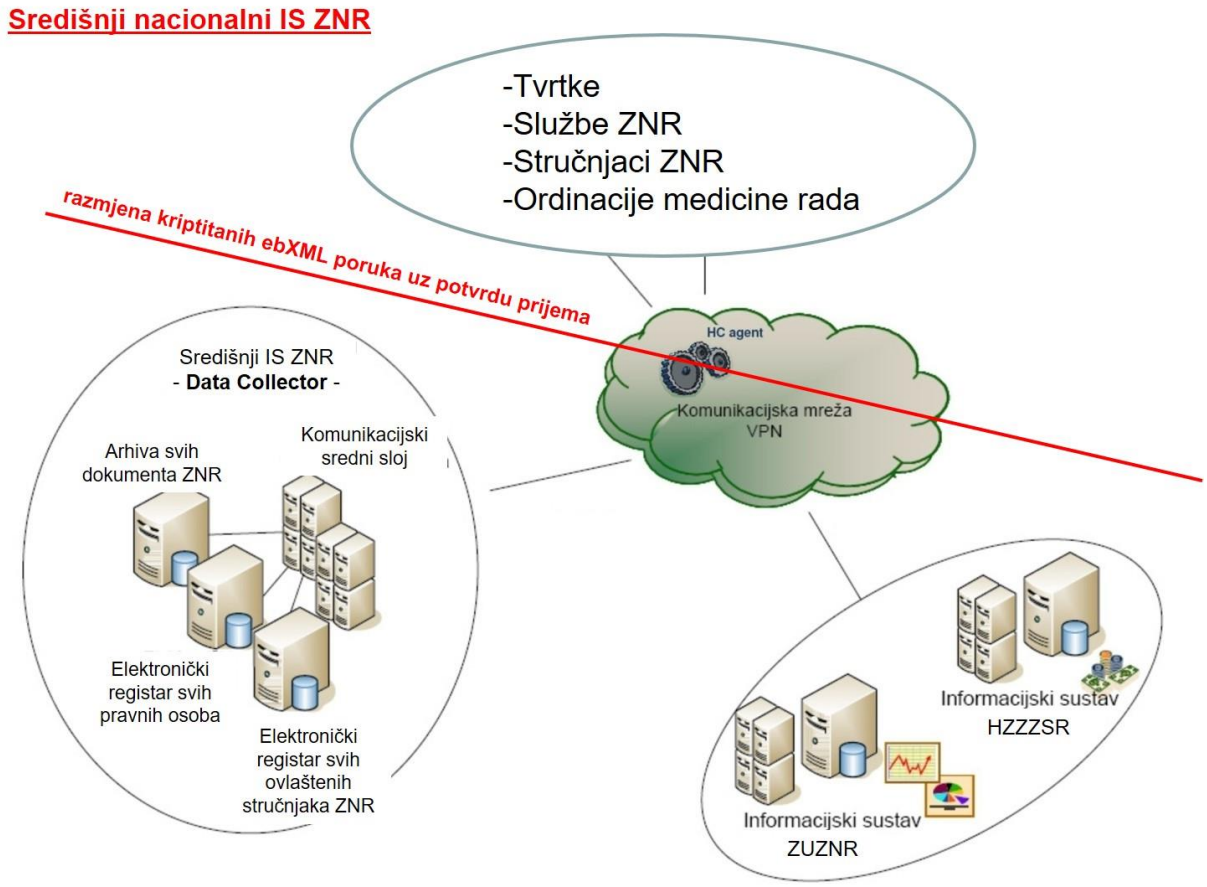
S druge strane, izlaz DC omogućavao bi generiranje normiranih izvješća na zahtjev te pristup javnosti preko web sučelja.

5. PRIJEDLOZI ZA UNAPREĐENJE STANJA

U ovom poglavlju bit će opisan prijedlog izvedbe SNIS-a ZNR povlačenjem paralela sa zdravstvenim informacijskim sustavom CEZIH koji se nalazi u visokom stupnju dovršenosti i postupno integrira nove funkcionalne elemente sukladno postavljenim planovima za ostvarenje strateških ciljeva poslovnog sustava javnog zdravstva. Također će biti predloženi načini uvezivanja i oblika transakcija između elektroničkih evidencija aplikacija pojedinih tvrtki, kontrolnih kuća, Ministarstva zdravstva i drugih partnera. Prema slici 6 koja prikazuje funkcionalnu shemu procesa razmjene kriptiranih poruka između G1 (CEZIH) i G2 (klijentskih aplikacija), oblikovana je funkcionalna shema na slici 7 koja prikazuje moguće sudionike u SNIS-u ZNR.



Slika 6. Središnji informacijski sustav primarne zdravstvene zaštite [13]



Slika 7. Prijedlog funkcionalne sheme SNIS-a ZNR

DC kao jedinstvena baza podataka i središnji dio SNIS-a bio bi organiziran po registrima. Korisnici s dozvolom pristupa mogli bi pristupati nekim od dostupnih registara:

- registru osoba;
- registru korisnika,
- registru resursa zaštite na radu.

i) **Registar osoba** sadržavao bi dva podregistra:

- podregistar tvrtki ;
- podregistar radno sposobnih građana.

U podregistar tvrtki bile bi upisane sve tvrtke iz Fina-inog Jedinstvenog registra računa (JRR), elektroničke baze svih poslovnih subjekta, financijskih institucija i drugih pravnih osoba koje

posluju u RH. Uvezivanjem DC-a s Fina-inim JRR-om riješio bi se problem punjenja i ažuriranja podregistra tvrtki.

U podregistru radno sposobnih građana kreirao bi se svojevrsni karton (profil) za svakog radnika koji bi se tijekom radnog vijeka popunjavao, nešto poput zdravstvenog kartona u CEZIH-u koji otvara HZZO. Nakon završenog školovanja, navršene punoljetnosti, odnosno steknutih uvjeta za prijavu na Hrvatski zavod za zapošljavanje građanin stječe status radno sposobnog. Karton bi se dakle kreirao iz već postojećih mehanizama, neovisno o tome je li građanin u radnom odnosu, i pohranio u podregistar te osim osnovnih osobnih podataka sadržavao i podatke o stečenom obrazovanju. Više o sadržaju kartona bit će rečeno u nastavku rada.

ii) **Registar korisnika** bi sadržavao sve subjekte koji bi imali pravo pristupa i uređivanja DC-a. Korisnici bi imali pravo pristupa određenim podacima, ovisno o tome kojoj grupi bi pripadali:

- ovlaštene osobe za vođenje zaštite na radu;
- ZUZNR;
- inspektorat rada;
- medicina rada;
- MRMS;
- Fina;
- HZZO;
- HZZZSR.

Prema Pravilniku o obavljanju poslova zaštite na radu [14] kod poslodavca poslove vođenja zaštite na radu može obavljati stručnjak zaštite na radu (čl.2) ili sam poslodavac (čl.4).

Medicina rada je sastavni i nezaobilazni dio radnog procesa koji se brine za smanjenje opasnosti i štetnosti na radu, siguran rad i zaštitu zdravlja na radu. Poslodavac odabire specijaliste

medicine rada koji u skladu s propisima o specifičnoj zdravstvenoj zaštiti i zdravstvenom osiguranju vrše preventivni pregled psihofizičkog stanja radnika.

MRMS je glavno upravno tijelo za sigurnost i zdravlje na radu u Republici Hrvatskoj. Sudjeluje u pripremi programa i projekata te provedbi projekata iz programa Europske unije i ostalih oblika međunarodne pomoći. MRMS obavlja poslove koji se odnose na sudjelovanje Republike Hrvatske u radu tijela Europske unije u područjima iz njegove nadležnosti. MRMS obavlja i druge poslove koji su mu stavljeni u nadležnost posebnim zakonom. Od stupanja na snagu dopuna i izmjena Zakona o zaštiti na radu [15] Zavod za unapređivanje zaštite na radu (ZUZNR) kao glavna nacionalna institucija za nadzor i unapređivanje zaštite na radu pripojen je MRMS u okviru Uprave za rad i zaštitu na radu.

Financijska agencija (Fina) je vodeća hrvatska tvrtka na području pružanja financijskih i elektroničkih usluga. Ona je jedinstveno mjesto susreta tržišnih dionika s poslovnim rješenjima financijskog posredovanja, kvalitetnim poslovnim informacijama i elektroničkim poslovanjem koje pruža elektroničkim putem te posredstvom razvijene poslovne mreže [16].

HZZO je ustanova pod upravom Ministarstva zdravlja koja provodi osnovno, dopunsko i dobrovoljno zdravstveno osiguranje. Zavod ima ulogu sustava zdravstvene zaštite što uključuje upravljanje zakonodavstvom, izradu proračuna, nadziranje zdravstvenog statusa i zdravstvenih potreba, edukaciju zdravstvenih djelatnika i nadgledanje procesa reforme zdravstvenog sustava u RH [17].

HZZZSR je središnja nacionalna institucija za zaštitu zdravlja i sigurnost na radu koja u okviru svoje osnovne djelatnosti provodi specifičnu zdravstvenu zaštitu, edukaciju i informiranje dionika u sustavu zaštite zdravlja i sigurnosti na radu te postavlja stručne doktrine i standarde. Objedinjuje i unapređuje stručne aktivnosti u području zaštite zdravlja i sigurnosti na radu u cilju poboljšanja radnih uvjeta, sprječavanja ozljeda na radu i profesionalnih bolesti, očuvanje zdravlja radnika i povećanja učinkovitosti gospodarstva Republike Hrvatske. Zavod je pod nadzorom Ministarstva zdravstva [18].

iii) Registar resursa zaštite na radu sadržavao bi sljedeće podregistre:

- podregistar zakona i pravilnika vezanih uz zaštitu na radu;
- podregistar ispita o provedenom osposobljavanju;
- podregistar ozljeda na radu i profesionalnih bolesti;

- podregistar mjera i aktivnosti koje su provedene u svrhu unapređenja zaštite na radu;
- podregistar ispitivanja radnog okoliša i radne opreme.

Podregistar zakona i pravilnika sadržavao bi sve zakone i pravilnike usklađene s direktivama i normama Europske unije koje bi ažurirao HZZZSR te time osigurao da svi sudionici budu pravovremeno informirani o izmjenama i dopunama zakonskih akata.

Podregistar ispita o provedenom osposobljavanju sadržavao bi materijale za osposobljavanje radnika za rad na siguran način, za rad s posebnim uvjetima rada, za rad na računalu, osposobljavanje poslodavaca ili njihovih ovlaštenika iz zaštite na radu, povjerenika za zaštitu na radu te zaštite od požara. Osim edukativnih materijala, podregistar bi sadržavao ispite, uvjerenja i zapisnike o položenom ispitu.

Podregistar ozljeda na radu i profesionalnih bolesti sadržavao bi podatke o nastalim ozljedama na radu i profesionalnim bolestima koje su posljedica zastoja i pogrešaka u radnim procesima ili nepravilnog provođenja zaštite na radu te godišnje i mjesečne statističke izvještaje o istima podijeljenim prema djelatnostima.

Podregistar mjera i aktivnosti sadržavao bi podatke o provedbi mjera i aktivnosti u svrhu unapređenja zaštite na radu. Sadržavao bi informacije o aktivnostima nacionalne politike koje se provode kako bi kvaliteta zaštite na radu podigla. Ove mjere i aktivnosti provodile bi se na osnovi raznih izvještaja i analiza do kojih bi se moglo doći iz određenih registara unutar DC-a.

Podregistar radnog okoliša i radne opreme sadržavao bi obavezne upute o ispitivanju, uvjerenja i zapisnike o provedenom ispitivanju u radnom okolišu i radnoj opremi te mjesečna i godišnja statistička izvješća o nepravilnostima na određenoj radnoj opremi ili unutar radnog okoliša koje bi bile grupirane prema zakonima i pravilnicima za radnu opremu i radni okoliš. Sadržavao bi još popis opasnosti i štetnosti na radnom mjestu te rizike u svezi sa radnom opremom. [7, 8, 12]

5.1. Aplikacije za pristup DC-u

Za prethodno navedene grupe s pravom pristupa DC-u trebalo bi izraditi aplikacije pomoću kojih će imati pristup određenim registrima, mogućnost dopune, izmjene i ažuriranja podataka te pohranjivanja istih u DC. Aplikacije bi se izrađivale po uzoru na aplikacije CEZIH-

a i već postojeće aplikacije koje se koriste za vođenje poslova zaštite na radu kod poslodavaca. U tablici ispod nalazi se popis mogućih aplikacija koje bi se povezale s DC-om.

Tablica 1. Popis aplikacija za korisnike DC

A1	Aplikacija za poslodavce
A2	Aplikacija za ZUZNR
A3	Aplikacija za medicinu rada
A4	Aplikacija za HZZO i HZZZSR

Aplikacija za poslodavce (A1) koristila bi se za evidencije zaštite na radu od strane djelatnika zaduženih za obavljanje tih zadataka. Sadržavala bi sljedeće kategorije:

i) **Organizacijska.** Jedinice bi bile podijeljene prema procjeni rizika, radnicima, radnom okolišu i radnoj opremi te obveznim obrascima i evidencijskim kartonima.

ii) **Procjena rizika.** Izrađuje se prema Pravilniku o izradi procjene rizika.

iii) **Radnik.** Sadržavala bi polja za osobne podatke te podatke o osposobljenosti ovisno o mjestu rada i poslovima koje obavlja na tom radnom mjestu, liječničko uvjerenje o osposobljenosti za rad.

iv) **Radni okoliš.** Sadržavala bi polja s popisima svih ispitivanja koja se provode u radnom okruženju, polje za uvjerenja i zapisnike koji se izdaju za to ispitivanje.

v) **Radna oprema.** Sadržavala bi polje u kojem bi bio popis radnika koji koriste radnu opremu, polje s popisom radne opreme koja je u funkciji ili van funkcije u tvrtki, polje o ispitivanju radne opreme te zasebno polje s uvjerenjima i zapisnicima o ispitivanjima istih.

vi) **Obvezni obrasci**. Sadržavala bi grupirana polja obveznih obrazaca koji se koriste u vođenjima poslova zaštite na radu prema zakonima i pravilnicima koju su usklađeni s EU direktivama i normama.

Aplikacija za ZUZNR (A2) omogućila bi zaposlenicima zavoda pohranjivanje u DC materijala za edukacije koje provode u području zaštite na radu, statističko praćenje ozljeda na radu i profesionalnih bolesti, provedbu istraživanja i analiza na osnovi pouzdanih i pravovremenih podataka, omogućila bi im planiranje i provedbe preventivnih i drugih mjera u sustavu

unapređenja zaštite na radu. Imali bi mogućnost izdavanja, nadzora i revidiranja izdanih ovlaštenja.

Aplikacija za medicinu rada (A3) omogućila bi specijalistima medicine rada izradu obrazaca RA-1 (uputnica za utvrđivanje zdravstvene sposobnosti radnika) i obrazac NR-1 (uputnica za utvrđivanje zdravstvene sposobnosti radnika koji rade noću), izradu izvještaja o zdravstvenom pregledu za rad s računalom, izradu i izdavanje kontrolne liste za smetnje radnika, dokumenata za obilazak radnih mjesta, upute za korištenje i metode za ocjenjivanja opterećenja pri ručnom prenošenju tereta. Svi izvještaji i obrasci bi se kroz aplikaciju pohranjivali u DC i pridruživali osobnom kartonu radnika koji je obavio liječnički pregled.

Aplikacija za HZZO i HZZZSR (A4) omogućila bi unos podataka o prijavljenim ozljedama na radu i profesionalnim ozljedama i izradu i unos statističkih podataka o istim, o provedenim edukacijama i materijalima za iste, popis propisa iz Zaštite zdravlja na radu, rezultate o utvrđenim ili neutvrđenim pravima u slučaju ozljede na radu ili profesionalne bolesti te same informacije o novčanim izdacima za liječenje istih i izgubljenih dana tijekom izostanka s posla. Dio namijenjen za HZZZSR omogućavao bi unos materijala za stručne edukacije, evidencije i analize ozljeda na radu i profesionalnih bolesti, evidencije radnika izloženih opasnostima i štetnostima na radu, evidencije stručnog nadzora ordinacija medicine rada. Postojala bi i kategorija inovacija koja bi sadržavala polja u koje bi korisnici upisivali aktivnosti koje su osmislili i koje su proveli ili će provesti, a te aktivnosti bi sadržavale polja kao što su predlagani zakoni, izrada elaborata i doktorata, problemi i rješenja istih, mjere za unapređenje sigurnosti i poboljšanja zdravlja, stručna i znanstvena istraživanja nacionalnih i EU projekata.

Osim klijentskih aplikacija postojala bi i web aplikacija kojoj bi se pristupalo preko jedinstvenog internetskog portala. Portal bi se izradio po uzoru na sustav „e-Građani“ i omogućavao bi različite kategorije kreirane za korisnike koji bi imali pravo pristupa. Prva grupa korisnika bili bi radnici koji bi se registrirali pomoću OIB-a i vjerodajnice koju bi zatražili od Fina-e. Prilikom registracije radnik bi unio svoje osobne podatke te stupanj obrazovanja koji bi se pohranili u DC u obliku osobnog kartona, slično kao zdravstveni karton u CEZIH-u. Rubrika s nazivom poslodavca bi bila prazna sve dok osoba nije u radnom odnosu. Prilikom zapošljavanja poslodavac bi kroz svoju aplikaciju generirao šifru za novog djelatnika koju bi radnik na svom profilu unio u rubriku te bi nakon pohrane u DC poslodavac, odnosno ovlaštena osoba za provođenje ZNR, imao pristup radnikovom kartonu te pravo na njegovo uređivanje. Prilikom prestanka radnog odnosa, poslodavac bi kroz svoju aplikaciju uklonio radniku u DC-

u status zaposlenja te mu na taj način omogućio da se istim gore opisanim postupkom prijavi kod novog poslodavca. Osim registracije i izmjene osobnih podataka, radnik bi kroz web aplikaciju pristupao materijalima za učenje te također i ispitima o provedenom osposobljavanju. Bitno je naglasiti da radnik ne bi imao potpuni uvid u svoj karton, nego samo u osobne podatke. Druga grupa korisnika bio bi ZUZNR koji bi kroz administratorsku ulogu objavljivao podatke o projektima i programima koje MRMS provodi iz programa Europske unije, sudionicima samog projekta, rokovima početka i završetka istih, mjerama i aktivnostima koje su poduzete i koje bi trebale biti poduzete tijekom i po završetku projekta i programa. Treća grupa korisnika bio bi inspektorat rada kojemu bi bio omogućen unos podataka o nepravilnostima nakon provedenih inspekcijskih nadzora. Osim toga trebali bi unositi datume izlaska na teren te razlog izlaska ako je neki specifični kao što su ozljede na radu ili ozljede na radu uslijed kojih je nastupila smrt ili neke veće nezgode na radnoj opremi ili u radnom procesu, izvještaje o provedenim inspekcijama na mjesečnoj i godišnjoj bazi te rezultate istih koji bi govorili o nepravilnostima ali i dobrim stranama zatečenim pri nadzoru. Četvrta grupa korisnika bi bili svi građani koji bi bez registracije i autentifikacije mogli pregledavati novosti, planove, edukativne materijale i izvještaje koji se odnose na stanje ZNR na razini Hrvatske, ali i EU. [7, 8,12]

5.2. Infrastruktura javnog ključa (PKI)

DC bi kao i CEZIH trebao primjenjivati visoke standarde vezane uz implementaciju sigurnosti. Potrebno je osigurati povjerljivost podataka, kontrolu pristupa, visoku dostupnost te višeslojnu implementaciju rješenja. Kao i CEZIH, DC bi se VPN-om odvojio od ostatka mreže te bi se klijentskim certifikatima moglo pristupiti VPN poslužiteljima. Klijentski certifikat bi se izdavao na *smart* kartici korisnika te bi se samo pomoću valjanih certifikata moglo pristupiti VPN poslužiteljima.

Vatrozidom bi se blokirali sumnjivi izvori i vrste sadržaja te bi se nakon filtriranja mrežnog prometa stvorila sigurna zona.

Povjerljivost podataka bi se, kao i u CEZIH-u, osigurala šifriranjem transportnog kanala pomoću SSL/TLS sloja kojim bi se također potvrđivala i autentičnost poslužitelja na koji se spajaju klijenti.

Certifikati s obzirom na namjenu za koju se koriste mogli bi se podijeliti na pet tipova, isto kao u CEZIH-u.

Prvi tip certifikata bi bio poslužiteljski i koristio bi se za uspostavu sigurnog transportnog kanala (SSL/TLS). Drugi tip certifikata bi bili aplikativni certifikati i oni bi se izdavali web aplikacijama koje se spajaju na web servise, a služili bi kao klijentski certifikati za prijavu web aplikacija. Treći tip certifikata bio bi izdan centralnom DC sustavu, a koristio bi se za potpisivanje odlaznih poruka iz DC sustava. Četvrti tip bio bi potpisni certifikat kojim bi se potpisivao sav kod koji se izvršava na strani korisnika kroz Internet preglednike. Peti tip certifikata bili bi klijentski certifikati izdani krajnjim korisnicima izdani na pametnim karticama pomoću kojih bi se prijavljivalo na DC te potpisivale poruke koje se izmjenjuju s DC-om. [7, 8, 13]

5.3. Primjer funkcioniranja SNIS ZNR

U ovom podpoglavlju će biti na primjeru jedne tvrtke opisano kako bi ustvari funkcionirao SNIS. Poslodavac bi nakon otvaranja tvrtke zatražio od MRMS da ga se upiše u podregistar tvrtki te bi mu nakon toga ZUZNR kao dio MRMS-a izdao klijentski certifikat na pametnoj kartici koju bi koristila ovlaštena osoba za poslove ZNR u tvrtki. Zatim bi poslodavac instalirao aplikaciju kojom bi se nakon autentifikacije mogao spajati na DC. Aplikacija bi podržavala uvoz/izvoz podataka iz Excel tablica te CSV i XML zapisa pa bi se tako olakšalo ponajprije unošenje podataka u DC. Aplikacija bi imala opciju za dodavanje novog radnika na popis zaposlenih te bi se, nakon unosa osobnih podataka i OIB-a radnika, generirala šifra koju bi radnik dobio da ju unese u svoj profil. Radnik bi nakon zapošljavanja u tvrtki, ukoliko već nema, trebao kreirati svoj profil preko web sučelja i zatim unijeti šifru koju mu je dao poslodavac na za to predviđeno mjesto u osobnim podacima. Nakon što radnik pohrani šifru koju mu je dao poslodavac, njegov karton iz DC-a postaje dostupan ovlaštenoj osobi u tvrtki te se on počinje voditi kao zaposlenik tvrtke. Ovlaštena osoba može zatim povlačiti njegov karton iz DC-a i ažurirati podatke s vremenom, ali ti podaci koji se unesu od strane tvrtke ne bi bili vidljivi radniku na njegovom profilu. Nakon provedenog osposobljavanja o ZNR radnik bi pristupio rješavanju ispita preko web sučelja, a pristupnu šifru bi dobio od ovlaštene osobe u tvrtki. Prije rješavanja ispita mogao bi dodatno proučiti edukativne materijale koji bi također bili dostupni na internetskom portalu. Nakon što bi pohranio rezultate ispita, sustav bi ga ispravio te bi ovlaštenoj osobi došla poruka u aplikaciju o uspješnosti polaganja ispita. Osim ispita o provedenom osposobljavanju radnik mora proći i liječnički pregled kod specijalista medicine rada. Naručivanje na pregled bi se odvijalo kroz klijentske aplikacije poslodavca i

medicine rada, koje bi imale istu ulogu kao i klijentske G2 aplikacije u CEZIH-u. Aplikacije bi vršile sinkronizaciju putem SOAP+MQ poruka te imale module za automatski pristup nekim portalskim segmentima DC-a. Ovlaštena osoba u tvrtki bi generirala zahtjev za liječnički pregled kod partnera medicine rada, a on bi u svoju aplikaciju dobio zahtjev te bi zatim zakazao termin pregleda o čemu bi ovlaštena osoba bila obaviještena. Analogija tome je e-upućivanje i e-naručivanje u CEZIH-u. Specijalist medicine rada bi u svoju aplikaciju mogao povući radnikov karton i ažurirati ga nakon pregleda s donesenim zaključcima iz nalaza te bi nakon toga poslodavac imao uvid u radnu sposobnost radnika. Nakon prestanka radnog odnosa, ovlaštena osoba u tvrtki bi isključila radnika s popisa djelatnika i tako mu omogućila da pristupi novom poslodavcu.

Ovlaštena osoba bi kroz aplikaciju unosila sve elemente zaštite na radu u tvrtki koji su opisani u prethodnim poglavljima i podpoglavljima.

U slučajevima ozljede na radu ovlaštena osoba bi u lokalnoj aplikaciji generirala zapisnik te ga kao XML izvješće proslijedila i pohranila u DC. Zatim bi HZZO kroz svoju aplikaciju dobio obavijest o novom slučaju te bi nakon obrade poslao ažurirane podatke u DC. U radnikovom kartonu bi se pohranjivao status o bolovanju, ali bi se također i uz ime tvrtke pridruživali slučajevi ozljeda i profesionalnih bolesti. Na taj način bi se mogli izrađivati izvještaji o trajanjima i uzrocima bolovanja, odnosno prema skupinama radnika i poslodavaca analizirati na kojim mjestima se otvaraju bolovanja više nego je to uobičajeno. [7, 8, 12, 13]

5.4. Ciljevi

Prilikom razrade ideje o realizaciji projekta potrebno je navesti i analizirati ciljeve koje bi projekt trebao ostvariti. Ciljevi SNIS-a prikazani su u tablici 2, a podijeljeni su na: dnevno-operativne, taktičke i strateške. [12]

Tablica 2. Ciljevi izrade SNIS-a

DNEVNO-OPERATIVNI CILJEVI	TAKTIČKI CILJEVI	STRATEŠKI CILJEVI
• osnovne evidencije o ZNR • izvješća o povredama • uputnice	• brza dostupnost ukupnim podacima o stanju za željeni period • analiza poboljšanja po razdobljima • izrada i klasifikacija modela rizika	• daljnja konsolidacija nacionalnih strategija – koordinacijom politika i uzajamnim učenjem • pružanje praktične potpore malim i mikropoduzećima • poboljšanje provedbe evaluacijom rezultata nacionalnih inspektorata rada • pojednostavljivanje postojećeg zakonodavstva • unapređenje prikupljanja statističkih podataka zbog osiguranja kvalitetnijih dokaza i razvijanja alata za praćenje • jačanje koordinacije s međunarodnim organizacijama

6. ZAKLJUČAK

U ovom radu prošla sam kroz cijeli razvoj IT sustava od samih početaka nastanka interneta i funkcionalne analize njegovih razvojnih faza, primjenjivosti tih funkcionalnosti u ovom razmatranom slučaju, preko razvoja klijentskih aplikacija do razvoja samog sustava SNIS ZNR sa sveobuhvatnom bazom podataka u domeni ZNR nazvanom "Data Collector".

Približavanjem Europskoj Uniji, RH je sve više usklađivala svoje zakonodavstvo sa EU i počela je implementirati europske direktive za zaštitu na radu. Prije ulaska u EU, RH bila je korisnica pristupnog programa kroz projekte IPA 2007 i IPA 2012 kojima je glavni cilj bio uspostaviti učinkovit sustav i mrežu institucija za zaštitu na radu uz povezivanje postojećih i novih baza podataka, kao i sustava upravljanja zaštitom na radu. Razmjena informacija i iskustava, na kojoj se radilo između sudionika, omogućila je bolju povezanost svih relevantnih podataka o bolesnim i ozlijeđenim radnicima, analizu podataka i izradu zaključaka na temelju tih analiza, što je doprinijelo razvoju informacijskog sustava i učinkovitog sustava zaštite zdravlja i sigurnosti na radu. Stjecanjem punopravnog članstva u EU, od nas se tražilo da kao država nastavimo pratiti i usklađivati naše zakonodavstvo sa EU zakonodavstvom i njegovim direktivama i normama. Naime, kako je prethodno već navedeno, RH je kroz EU projekte IPA2007 i IPA 2012 dobila zadaću oblikovanja nacionalne infrastrukture u ZNR. U izvršavanju te zadaće RH se sa svojim stručnjacima našla u problemima kako izvesti odgovarajući SNIS. Dio SNIS-a je središnji registar podataka i resursa ZNR u RH pod nazivom "Data Collector". Ciljevi Data Collectora su prije svega elementarno čuvanje zdravlja i radne sposobnosti radnika kroz dobru provedbu evidencija u zaštiti na radu, taktički ciljevi u koje spada brza dostupnost ukupnim podacima o stanjima zaštite na radu kroz razna izvješća na mjesečnoj i godišnjoj razini i izrada modela rizika, zadnji ali ne manje važni strateški ciljevi koji bi doveli do visokog stupnja sigurnosti radnika, te smanjenju rizika. Zavod za unaprjeđenje zaštite na radu kao izvršno tijelo investitora u gradnji sustava uspio je implementirati samo dio funkcionalnosti na kojima se treba dalje graditi sustav.

U posljednjem poglavlju ovog završnog rada iznijela sam ideju o mogućnosti daljnjeg razvoja sustava po uzoru na zdravstveni informacijski sustav CEZIH, jer smatram da je to u stvari ispravan i logičan put. U iznošenju ideje za razvoj sustava koristila sam stečena teoretska iskustva tijekom studija i iskustava iz prakse uz oslonac na aktualnu domaću regulativu, EU direktive, norme i aktualne projekte. Zaštita na radu je u europskim okvirima na jako visokom

nivou na kojem bi trebala biti i u RH, ali nažalost još nije. Unapređenje zaštite na radu može se postići samo zajedničkim naporima nadležnih državnih tijela, poslodavaca kao i drugih čimbenika u sustavu zaštite na radu čije je funkcionalno usklađenje i načini suradnje objašnjeni u opisu sustava SNIS ZNR. Provođenjem izgradnje sustava SNIS i uspješnog razvoja DC, RH bi znatno unaprijedila zaštitu na radu i digla ju na jedan znatno viši nivo. Kao što znamo cilj zaštite na radu nije smanjiti broj ozljeda na radu. Cilj zaštite na radu je stvoriti sustav u kojemu su sve stavke sustava sigurne u svakom trenutku. Današnji sustav zaštite na radu u RH suočen je s vremenom brzih promjena, sve većom uporabom novih tehnologija u svakodnevnom životu i radu, ali i učenju i podučavanju, stoga se od njega zahtijeva da uvijek teži unaprjeđenju i bude korak naprijed. Iskreno se nadam da će se ovaj sustav realizirati i pomoći svim sudionicima u području zaštite na radu da budu korak naprijed.

7. LITERATURA

[1.] IANA, „Internet Assigned Numbers Authority“, dostupno na: https://www.iana.org/ (25. svibnja. 2019.)

[2.] Pale, P., „Sustavi za praćenje i vođenje procesa“, FER-LSS, Zagreb, 2017. dostupno na: https://www.fer.unizg.hr/_download/repository/SPVP-Internet-2017.pdf (21. svibnja. 2019.)

[3.] CommuniGate, „Web – The Evolution“, dostupno na: https://www.communigate.com/ (10. svibnja. 2019.)

[4.] Vujnović, G., „*Networking as a service* kao model računalstva u oblaku“, završni rad, Sveučilište u Zagrebu, FPZ, Zagreb, Hrvatska, 2015.

[5.] Letts, S., „What is Web 4.0?“, dostupno na: https://stephenletts.wordpress.com/web-4-0/ (20. svibnja. 2019.)

[6.] Ministarstvo uprave Republike Hrvatske, „Strategija e-Hrvatska 2020“, dostupno na: https://uprava.gov.hr/UserDocsImages/Istaknute%20teme/e-Hrvatska/Strategija_e-Hrvatska_2020.pdf (8. svibnja. 2019.)

[7.] Hrvatski zavod za zdravstveno osiguranje „CEZIH – koncept sustava“, dostupno na: http://www.cezih.hr/pzz/dokumentacija/01_00_CEZIH_koncept_sustava.pdf, (10. svibanj.2019.)

[8.] Gvozdanović, D., „E-Health implementation in Croatia (CEZIH)“, Ericsson NT / FER Zagreb, 2015. dostupno na: https://www.fer.unizg.hr/_download/repository/Healthcare_information_system_in_Croatia_16-9_RevD_-_FER_-_2015.pdf (10. lipnja 2019.)

[9.] Narodne novine, „Pravilnik o osposobljavanju iz zaštite na radu i polaganju stručnog ispita“, dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2014_09_112_2153.html (2. lipanj. 2019.)

[10.] Središnji državni ured za razvoj digitalnog društva, „Središnji katalog službenih dokumenata“, dostupno na: http://www.digured.hr/ (2. lipanj. 2019.)

[11.] International Labour Organization, „Data Sources for Optimizing the Collection and Use of OSH data“, dostupno na: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/publication/wcms_546703.pdf (01.lipanj .2019.)

[12.] ZUZNR, „Zajedno za zaštitu na radu, zdravlje i produktivnost , Zagreb, 15.01.2016.“, dostupno na: http://www.hzos.hr/upload_data/site_files/zuznr_hzos_sijecanj_2016.pptx (06. svibanj. 2019.)

[13.] Hrvatski zavod za zdravstveno osiguranje, „Središnji informacijski sustav primarne zdravstvene zaštite - ISPZZ“, dostupno na: http://www.cezih.hr/pzz/dokumenti_pzz/Opis_NISHI_sustava.pdf (12. lipanj. 2019.)

[14.] Narodne novine, „Pravilnik o obavljanju poslova zaštite na radu“, dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2014_09_112_2155.html , (29. svibanj. 2019.)

[15.] Narodne novine, „Zakon o izmjenama i dopunama Zakona o zaštiti na radu“ , dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_10_94_1819.html , (16. svibanj. 2019.)

[16.] Fina, „Web aplikacije i servisi“, dostupno na: https://www.fina.hr/e-servisi (29. svibanj. 2019.)

[17.] Hrvatski zavod za zdravstveno osiguranje, „Opis zdravstvenog sustava“, dostupno na: http://www.hzzo.hr/zdravstveni-sustav-rh/opis-zdravstvenog-sustava/ (29. svibanj. 2019.)

[18.] Hrvatski zavod za javno zdravstvo, „Hrvatski zavod za zaštitu zdravlja i sigurnost na radu“, dostupno na: http://hzzzsr.hr/ (29. svibanj. 2019.)

8. PRILOZI

8.1. Prilog 1 – lista prihvaćenih vjerodajnica

Tablica 3. Lista prihvaćenih vjerodajnica [6]

IZDAVATELJ	VJERODAJNICA ZA NIAS	SIGURNOSNA RAZINA	STATUS
MUP RH	Elektronička osobna iskaznica (eOI)	4	Trajna
CARNet	mToken za e-Građane	3	Trajna
FINA	E_Građani ePass	2	Trajna
SRCE	AAI@EduHr	2	Trajna
HZZO	Pametna kartica s certifikatom	3	Trajna
FINA	FinaSoft certifikat	3	Trajna
FINA	FinaCertRDC certifikat	4	Trajna
AKD	Osobni identifikacijski certifikat NCP+	4	Trajna
HPB	HPB token / mToken	3	Trajna
HP	ePošta	2	Trajna
ZABA	ZABA token / m-token	3	Trajna
PBZ	Mobilni token #withKEY / čitač kartice	3	Trajna
RBA	RBA token / mtokn i CAP čitač	3	Trajna
KentBank d.dd	SMS jednokratni pin	3	Trajna
OTP banka d.d.	OTP token	3	Trajna
Hrvatski telekom	HT telekom ID	2	Trajna
AKD	kID certifikat	4	Trajna
HZMO	Korisničko ime i lozinka	2	Privremena
REGOS	Korisničko ime i lozinka	2	Privremena
HZZ	Korisničko ime i lozinka	2	Privremena

8.2. Popis slika

Stranica

8.3. Popis tablica

Stranica