

K. Franović, D. Kralj\*

# MOGUĆNOSTI DALJNJEG RAZVOJA NACIONALNE INFORMACIJSKE INFRASTRUKTURE U PODRUČJU ZAŠTITE NA RADU

UDK 331.45:004.7](497.5)  
PRIMLJENO: 16.9.2020.  
PRIHVaćENO: 30.4.2021.

Ovo djelo je dano na korištenje pod Creative Commons Attribution 4.0 International License



*SAŽETAK: Predmet ovog rada je analiza mogućnosti daljnjeg oblikovanja nacionalne informacijske infrastrukture u području zaštite na radu. Temelji ove infrastrukture postavljeni su kroz početni razvoj informacijskog sustava zaštite na radu (IS ZNR) pod vodstvom Ministarstva rada, mirovinskog sustava, obitelji i socijalne politike. Analizom nacionalne zakonske regulative i EU smjernica u području zaštite na radu, mogućnosti primjene globalnih mrežnih usluga, uspješnih primjera razvoja nacionalnih informacijskih sustava u području javne uprave i zdravstva, stvoreni su temelji za spekulativni pristup analizi mogućnosti daljnjeg razvoja nacionalne informacijske infrastrukture u području zaštite na radu. Osmišljena je i prikazana ideja o predviđivom daljnjem razvoju i strukturi budućeg središnjeg nacionalnog informacijskog sustava zaštite na radu koji se oslanja na središnji registar podataka i resursa zaštite na radu (inicijalno nazvanom Data Collector) te na sve potrebne funkcionalnosti koje jamče sigurnost, sveprisutnost i longitudinalnost elektroničkih zapisa, a na temelju toga jamče i unapređenje zaštite na radu u Republici Hrvatskoj.*

**Ključne riječi:** zaštita na radu, mrežne usluge, nacionalna informacijska infrastruktura, zakonska regulativa, Data Collector, IS ZNR

## UVOD

Prema Zakonu o zaštiti na radu, zaštita na radu (ZNR) je sustav pravila, načela, mjera, postupaka i aktivnosti, čijom se organiziranom primjenom ostvaruje i unapređuje sigurnost i zaštita zdravlja na radu, s ciljem sprečavanja rizika na radu, ozljeda na radu, profesionalnih bolesti, bolesti u vezi s radom te ostalih materijalnih i nematerijalnih šteta na radu i u vezi s radom. Unapređivanje djelatnosti i suvremeni način poslovanja nezamisliv je bez sustavnog provođenja politike ZNR te unapređivanja sigurnosti i zaštite zdravlja radnika. Unapređenje sustava zaštite na radu u tvrtkama moguće je postići stalnim stručnim praćenjem razvoja tehnologije i samog radnog procesa, dje-

lovanjem u skladu s njima i pružanjem stručne podrške, edukacijom te podizanjem svijesti o važnosti dobre organizacije i provedbe zaštite na radu. Međutim, u današnje vrijeme nije dovoljno pratiti stupanj uspješnosti ZNR samo na razini tvrtke tj. na operativnoj i taktičkoj razini, već se njezin uspjeh ili neuspjeh odražavaju i na stanje nacionalnog pa i šireg regionalnog gospodarstva, čime se problem podiže na stratešku razinu. Za oblikovanje strateških ciljeva i planova bitne su pravovremene i točne informacije, a njih se može osigurati samo putem učinkovite informacijske infrastrukture (II).

Cilj ovog rada, koji su si autori postavili, bio je da se - na osnovi znanja stečenih tijekom specijalističkog studija zaštite na radu, iskustava iz prakse uz oslonac na aktualnu domaću regulativu i EU smjernice, normi i tehnološki sličnih aktualnih projekata koji su u visokom stupnju gotovosti - analiziraju i istaknu bitne činjenice i čimbenici

\*Kristina Franović, struč. spec. ing. sec., (kfranovic08@gmail.com), Linija koda d.o.o., Ulica Marijane Radica 6, 10000 Zagreb, dr. sc. Damir Kralj, profesor visoke škole, (damir.kralj@vuka.hr), Veleučilište u Karlovcu, Odjel sigurnosti i zaštite, Trg J. J. Strossmayera 9, 47000 Karlovac.

koji ukazuju na prijeko potrebno oblikovanje nacionalne II u području zaštite na radu, sagledaju do sada ostvareni dijelovi informacijskog sustava koji bi trebao ostvariti postavljene ciljeve te istraže i predlože logične mogućnosti njegovog daljnjeg razvoja vodeći računa o postizanju dnevno-operativnih, taktičkih i strateških ciljeva poslovnog sustava u području ZNR. Pri tome treba uzeti u obzir činjenicu da je ovo jedan spekulativni pristup mogućnostima razvoja jednog budućeg sveobuhvatnog nacionalnog informacijskog sustava u području ZNR. Idejno rješenje, koje je zastupao bivši Zavod za unaprjeđenje zaštite na radu (ZUZNR) zasnivalo se na oblikovanju i izgradnji tzv. Središnjeg nacionalnog informacijskog sustava zaštite na radu (SNIS ZNR) koji se temelji na središnjoj bazi podataka nazvanoj *Data Collector*. Ono što je od te inicijalne ideje ostvareno je početak gradnje jednog središnjeg aplikativnog rješenja pod nazivom Informacijski sustav zaštite na radu (IS ZNR), kojim upravlja i koordinira njegov daljnji razvoj Ministarstvo rada, mirovinskog sustava, obitelji i socijalne politike (MRMS) i koji je trenutno u fazi inicijalnih punjenja te još nije u potpunosti funkcionalan. SNIS ZNR je uglavnom ostao na ideji te kao takav, u sklopu postojećeg sustava, nema jasno definiranu budućnost, linije odgovornosti i nadležnosti su nejasne pa je takav projekt za sada teško provediv. Stoga su autori objektivne elemente pristupa gradili na prezentaciji činjenica o postojećim projektima zasnovanim na analizi javnih dokumenta kreatora istih, kao i iskustava autora u samom postupku izgradnje i kasnijim projektima evaluacije njihove funkcionalnosti, dok spekulativni dio izvode iz tehnoloških temelja analiziranih realiziranih sustava i aktualnom stanju i potrebama u području ZNR. Kako bi se osigurala distinkcija između aktualnog sustava (IS ZNR) i našeg prijedloga novog sustava, za predloženi sustav autori će koristiti termine iz inicijalnog idejnog rješenja (SNIS ZNR, Data Collector).

## METODOLOGIJA

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 sličnih ključ-

nih informacijsko-komunikacijskih projekata na području Republike Hrvatske (RH). Po izvršenoj analizi navedenih izvora, čimbenika i projekata, predviđen je i proveden sintetički pristup okvirnom prijedlogu oblikovanja i razvoja nacionalne informacijske infrastrukture u području ZNR.

## PRIMJERI ZAVRŠENIH PROJEKATA

Kako bi se odredila polazna točka za spekulativni prijedlog razvoja predmetne II u području ZNR, analizirano je nekoliko kardinalnih projekata u RH, koji su završeni ili su, bolje rečeno, u visokoj fazi gotovosti. Naime, ovakvi projekti nisu nikad u potpunosti završeni i u trajnom mirovanju, već su podložni dopunama, promjenama i unapređenjima svojih funkcionalnosti u skladu s potrebama i tehnološkim napretkom. Ove promjene, kao i postupak izgradnje, provode se prema projektnim fazama.

### e-Hrvatska

Strategija e-Hrvatska 2020 (*Ministarstvo uprave, 2019.*) 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 njihovo opterećenje osobnom interakcijom s javnom upravom. Aktivnosti se provode u skladu s Akcijskim planom i financiraju prvenstveno iz europskih fondova te iz nacionalnih sredstava. Prema smjericama Europske komisije, utvrđene su razine zrelosti po kojima se mjeri dostupnost javnih usluga na internetu. Svaka e-usluga definirana je različitim razinama informatiziranosti s pripadajućim značenjem:

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

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

Današnje stanje u RH 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 pružiti 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
- neinformiranost 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 jedinstvenog podružja *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 (najviša). Lista prihvaćenih vjerodajnica s naznačenim razinama prikazuje se na stranici prijave. 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 (*FINA, 2019.*).

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 povezane s pojedinim upravnim područjem. 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 za pristup katastarskim i zemljišnoknjižnim podacima.

Portal otvorenih podataka RH, 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 grāde koju posjeduju tijela državne uprave je jedan od preduvjeta za njegovo ostvarenje.

## e-Zdravstvo

Centralni zdravstveni informacijski sustav Republike Hrvatske (CEZIH) je informacijski sustav koji povezuje niz aplikacija i sustava zdravstva. Ministarstvo zdravstva (MZ) je vlasnik, a Hrvat-

ski zavod za zdravstveno osiguranje (HZZO) je operator središnjeg dijela integriranog informacijskog sustava (HZZO, 2019.).

Jedan od najvećih uspjeha sustava CEZIH je elektronički recept (e-Recept), 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.

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.

Koncepcija sustava je takva da klijentske aplikacije razmjennom poruka, a koristeći mrežne usluge sustava 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).

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.
- Vjerodostojnost. Svi partneri moraju imati privatne ključeve kojima se potpisuju sadržaji i dokazuje njihova vjerodostojnost (cjelovitost, autentičnost, neporecivost).
- Autentifikacija. Uspostavlja se identitet sudionika i osigurava integritet podataka.
- Detekcija neovlaštenog mijenjanja podataka.

Osnovne komponente PKI sustava su: krajnji entitet, certifikacijski centar, registracijski centar, opozvani certifikati. Krajnji entitet odnosi se na sve što može biti identificirano imenom na certifikatu. 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 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 ostvaruju se od svakog klijenta po načelu udaljenog pristupa (eng. *remote access*). Prije početka rada korisničke aplikacije moraju uspostaviti VPN tunel prema CEZIH sustavu. VPN definira se 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 ko-



jima se razdvajaju CEZIH poslužitelji te definiraju pristupni protokoli i portovi. Vatrozidom je krajnjim korisnicima omogućen pristup samo preko sigurne tj. *https* 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. *balansere* 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 (oznaka G1) 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 (oznaka G2) i tako izvodi interakciju sa CEZIH sustavom. Aplikacija tada radi prvi upit prema CEZIH G1 uslugama. Liječnik nije upoznat s 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 uspoređuju certifikat i korisnički zapis. Svaki korisnik u imeničkom servisu korisnika CEZIH sustava ima pridijeljenu ulogu koja se provjerava autorizacijom te ako dodijeljena uloga dopušta slanje poruka u CEZIH sustav, korisnik dobiva dopusnicu. CEZIH zahtijeva

da sve poruke koje se upućuju prema centralnom sustavu budu potpisane. Osiguravanjem povjerljivosti i integriteta direktno se osigurava i neporecivost na razini same poruke. Sve poruke koje ulaze u CEZIH sustav pohranjuju se te se naknadnim pretraživanjem može utvrditi koji su podaci ušli u sustav te tko ih je kreirao. Svaki ulazni podatak prolazi procjenu valjanosti. Za sva polja za unos podataka kontroliraju se tip i veličinu podataka (HZZO, 2019., Gvozdanović, 2015.).

## IDEJA IZGRADNJE SNIS ZNR

Međunarodna organizacija rada (eng. *International Labour Organization*, ILO) je u povodu Međunarodnog dana sigurnosti i zdravlja na poslu, 28. travnja 2017. godine, predstavila ideju prikupljanja i obrade podataka u vezi sa ZNR na međunarodnom planu (ILO, 2017.). 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 o ozljedama na putu do 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 pridonositi međunarodnoj pozi-

tivnoj statistici. Nacionalni sustav trebao bi imati ugrađen sustav definicija i klasifikacija ozljeda na radu te osiguravati odgovarajuće djelotvorne sustave za naknadu štete. Ove aktivnosti obuhvaćene su i nedavno predstavljenim prijedlogom dokumenta "Nacionalni plan zaštite na radu za razdoblje 2021.-2027. godine" (MRMS, 23. studenoga 2020.). 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 ocijenile stanje i napredak ZNR. Posebna istraživanja, poput anketa o radnom okruženju i pitanja u vezi sa ZNR, mogu se uključiti u nacionalne ankete o zdravlju i anketiranje zaposlenih. Neki od izazova za uspostavu učinkovitih sustava za bilježenje i izvještavanje koji pružaju pouzdane podatke su sljedeći:

- 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 zahtijeva 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 razli-

kuju 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 zbog odgovarajućeg praćenja mogućeg podrijetla bolesti s dugim razdobljima latencije;
- podsustav zdravstvenih evidencija o zdravstvenom stanju pojedinih radnika koji će se pratiti tijekom cijelog radnog vijeka.

ZUZNR, prije nego je postao integralni dio MRMS, predstavio je u siječnju 2016. godine program razvoja pomoću kojega bi unaprijedio ZNR, zdravlje i produktivnost radnika u RH, koji je do sada samo djelomično implementiran. Njegova vizija bila je razvijati kulturu prevencije i unapređivanja ZNR zbog osiguranja sigurnih i zdravih radnih mjesta koja pridonose dobrobiti radnika i poslodavca te 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 istaknuta je potreba za oblikovanjem sveobuhvatne baze podataka koja je prema inicijalnoj zamisli nazvana "Data Collector". 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 istaknuta je kao važan parametar koji treba zadovoljiti kako bi realizacija projekta bila opravdana (ZUZNR, 2016.).

### Data Collector

Središnji nacionalni informacijski sustav zaštite na radu, odnosno njegova središnja baza podataka nazvana popularnim nazivom "Data Collector" (u nastavku rada označavat će se skraćenicom „DC“) integrirao bi, prema osnovnoj zamisli, podatke u vezi sa zaštitom na radu u jedinstvenu bazu podataka s ciljem podizanja kvalitete ukupnog stanja ZNR u RH. Sve institucije, korisnici podataka ZNR, trenutno koriste interne baze podataka koje nisu međusobno povezane i ne omogućuju međusobnu razmjenu podataka. Krajnji korisnici DC bili bi poslodavci te pravne i fizičke osobe ovlaštene za obavljanje poslova ZNR. Sustav bi omogućavao generiranje različitih cjelovitih podataka koji bi se koristili za praćenje stanja ZNR, izradu stručnih elaborata, provođenje statističkih istraživanja, izrađivanje metoda i modela ZNR, utvrđivanje kriterija i postupaka u vezi s organizacijom rada. DC osigurao bi da se u bazu podataka dostavljaju svi relevantni podaci na osnovi odgovarajućeg Pravilnika.

Različite skupine korisnika trebale bi unositi odgovarajuće podatke u DC:

- Porezna uprava – pristup podacima o pravnim i fizičkim osobama na temelju OIB-a;
- Ministarstvo gospodarstva – integracija podataka iz obrtnog registra;
- MRMS – prijava i odjava radnika te evidencija ovlaštenja za pravne i fizičke osobe i unos podataka direktno u aplikaciju;
- DZS – Državni zavod za statistiku – integracija klasifikacijskih podataka;
- HZZO i HZJZ – unos podataka o ozljedama na radu i profesionalnim bolestima izravno u bazu ili učitavanje iz postojeće interne baze podataka;
- Državni inspektorat - unos podataka o nepravilnostima nakon provedenih inspeksijskih nadzora;
- Poslodavci - omogućen unos podataka preko web sučelja i učitavanje podataka iz po-

stojećih baza propisano Zakonom o ZNR i pravilnicima;

- Ovlaštene osobe (pravne i fizičke) - omogućen unos podataka preko web sučelja.

S druge strane, izlaz DC omogućavao bi generiranje normiranih izvješća na zahtjev te pristup javnosti preko web sučelja (ZUZNR, 2016.).

## PRIJEDLOG MODELA USTROJA NOVOG SUSTAVA

U skladu sa do sada analiziranim realiziranim projektima u području javne uprave i javnog zdravstva, planovima i idejama (sada već bivšeg) ZUZNR, preporukama ILO, kao i aktualnim stanjem informatizacije ZNR u RH, ovdje se donosi okvirni prijedlog ostvarenja jednog budućeg sveobuhvatnog nacionalnog informacijskog sustava (nacionalne II) u području ZNR u RH. S obzirom na to da se ovaj spekulativni prijedlog nadograđuje na ideju i planove ZUZNR, u sklopu daljnjih razmatranja koristit će se (kako je već navedeno u Uvodu) postojeće, u njima predloženo, osnovno nazivlje.

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

- registru osoba;
- registru korisnika;
- registru resursa ZNR.

*Registar osoba* sadržavao bi dva podregistra:

- podregistar tvrtki;
- podregistar radno sposobnih građana.

U podregistar tvrtki bile bi upisane sve tvrtke iz registra Porezne uprave i obrtnog registra Ministarstva gospodarstva, čime bi se riješio problem punjenja i ažuriranja podregistra tvrtki.

U podregistru radno sposobnih građana kreirao bi se svojevrsni karton (profil) za svakog radnika, koji bi se popunjavao tijekom radnog vijeka, otprilike poput zdravstvenog kartona u CEZIH-u koji otvara HZZO.

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

- ovlaštene osobe za vođenje zaštite na radu;
- inspektorat rada;
- medicina rada;
- MRMS;
- HZZO;
- HZJZ-Služba za medicinu rada.

*Registar resursa ZNR* sadržavao bi sljedeće podregistre:

- podregistar zakona i pravilnika povezanih sa zaštitom 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 HZJZ (funkcije bivšeg 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 različita osposobljavanja koja se provode. Osim edukativnih materijala, podregistar bi sadržavao dokumentaciju propisanu zakonskim aktima.

Podregistar ozljeda na radu i profesionalnih bolesti sadržavao bi podatke o nastalim ozljedama na radu i profesionalnim bolestima. Hrvatski zavod za javno zdravstvo, u skladu s nacionalnim propisima, prikuplja podatke o ozljedama na radu i profesionalnim bolestima Hrvatskog zavoda za

zdravstveno osiguranje te ih obrađene prema ESAW klasifikacijskom sustavu dostavlja Eurostatu. Hrvatski zavod za javno zdravstvo u djelatnosti medicine rada bilježi podatke o zdravstvenoj zaštiti radnika, preventivnim pregledima, ozljedama na radu i profesionalnim bolestima, a pregledni podaci dostupni su u Hrvatskim zdravstvenostatističkim ljetopisima i na mrežnoj stranici.

Podregistar mjera i aktivnosti sadržavao bi podatke o provedbi mjera i aktivnosti u svrhu unapređenja ZNR. Sadržavao bi informacije o aktivnostima nacionalne politike koje se provode kako bi se podigla kvaliteta ZNR. 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 obvezne upute o ispitivanju, pripadajuću dokumentaciju 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 koja bi bila grupirana u skladu sa zakonima i pravilnicima za radnu opremu i radni okoliš. Sadržavao bi još popis opasnosti i štetnosti na radnom mjestu te rizike u vezi s radnom opremom (*HZZO, 2019., Gvozdanović, 2015., ZUZNR, 2016.*).

### Aplikacije za pristup DC-u

Za prethodno navedene skupine 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 s mogućnošću povezivanja na DC po uzoru na G2 aplikacije CEZIH-a, odnosno trebalo bi prilagoditi već postojeće aplikacije koje se koriste za vođenje poslova ZNR kod poslodavaca. Na primjer, WebZNR i slične aplikacije, trebalo bi funkcionalno i podatkovno uskladiti potrebama punjenja i sinkronizacije s DC-om. U Tablici 1 nalazi se popis mogućih skupina korisničkih aplikacija koje bi se povezivale s DC-om.



**Tablica 1. Popis aplikacija za korisnike DC****Table 1. List of applications for DC users**

Oznaka	Naziv aplikacije
A1	Aplikacija za poslodavce
A2	Aplikacija za MRMS (ZNR)
A3	Aplikacija za medicinu rada
A4	Aplikacija za HZZO i HZJZ

Aplikacija za poslodavce (A1) koristila bi se za evidencije ZNR od strane djelatnika zaduženih za obavljanje tih zadataka.

Aplikacija za MRMS (A2) omogućila bi zaposlenicima MRMS pohranjivanje u DC materijala za edukacije koje provode u području ZNR, statističko praćenje ozljeda na radu i profesionalnih bolesti te provedbu istraživanja i analiza na osnovi pouzdanih i pravovremenih podataka. Osim toga, omogućila bi im planiranje i provedbe preventivnih i drugih mjera u sustavu unapređenja ZNR. Imali bi mogućnost izdavanja, nadzora i revidiranja izdanih ovlaštenja.

Aplikacija za medicinu rada (A3) omogućila bi specijalistima medicine rada izradu svih potrebnih dokumenata i edukativnog materijala.

Aplikacija za HZZO i HZJZ (A4) omogućila bi unos podataka o prijavljenim ozljedama na radu i profesionalnim bolestima, izradu i unos statističkih podataka o istima, 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 izdancima za liječenje istih i izgubljenih dana tijekom izostanka s posla. Dio namijenjen za HZJZ (Služba za medicinu rada) omogućavao bi unos materijala za stručne edukacije, evidencije i analize ozljeda na radu i profesionalnih bolesti, evidencije radnika izloženih opasnostima i štetnostima na radu te evidencije stručnog nadzora ordinacija medicine rada. Postojala bi i kategorija inovacija koja bi sadržavala polja u koja bi korisnici upisivali aktivnosti koje su osmislili i koje su proveli ili će provesti. Te aktivnosti sadržavale bi polja kao što su predlagani zakoni, izrada elaborata i doktorata, problemi i rješenja istih, mjere za unapređenje sigurnosti i poboljšanje zdravlja te stručna i znanstvena istraživanja nacionalnih i EU projekata.

Osim klijentskih aplikacija postojala bi i web aplikacija kojoj bi se pristupalo preko jedinstvenog internetskog portala - dobar primjer je Web-ZNR aplikacija sa svojim korisničkim portalom tj. posebnim modulom za izravnu razmjenu podataka iz te aplikacije u središnji sustav (trenutno je to IS ZNR) (*Linija koda d.o.o., 2020.*). Portal bi se u konačnici izradio po uzoru na sustav „e-Građani“ i omogućavao bi različite kategorije usluga kreirane za korisnike koji bi imali pravo pristupa.

### Primjena NIAS-a i infrastrukture javnog ključa

SNIS ZNR bi za pristup DC-u, kao i CEZIH, trebao primjenjivati visoke standarde u vezi s implementacijom sigurnosti. Za razmjenu podataka s drugim sustavima (MRMS, HZZO, porezna uprava) koristile bi se VPN veze. Vatrozidom bi se blokirali sumnjivi izvori i vrste sadržaja te bi se nakon filtriranja mrežnog prometa stvorila sigurna zona.

Za pristup krajnjih korisnika koristio bi se HTTPS protokol za uspostavu sigurnog transportnog kanala (SSL/TLS) između poslužitelja i internetskog preglednika.

### Primjer funkcioniranja SNIS ZNR

U ovom potpoglavlju na primjeru jedne hipotetske tvrtke opisat će se kako bi ustvari funkcionirao SNIS ZNR.

Poslodavac bi nakon otvaranja tvrtke zatražio od MRMS da ga se upiše u podregistar tvrtki te bi nakon toga MRMS dodijelio prava pristupa ovisno o ovlaštenju. Autentikacija u sustav provodila bi se uz pomoć NIAS-a vjerodajnicom razine 4. 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, isti mogao prijaviti u aplikaciju sa svojim NIAS vjerodajnicama. Ovlaštena osoba može zatim pročitati njegove podatke iz DC-a i ažurirati podatke kad nastupi njihova promjena. Prvo što radnik treba nakon što se zaposli je pohađati osposobljavanje za rad na siguran način koje provode stručnjaci zaštite na radu zaposleni kod poslodavca, odnosno stručnjaci zaštite na radu II. stupnja zaposleni

kod osobe ovlaštene za osposobljavanje radnika. Osposobljavanje se provodi prema programu osposobljavanja koji se temelji na procjeni rizika. Sastoji se od teoretskog i praktičnog dijela, a poslovi s malim rizicima imaju samo teoretski dio. Radnici bi prijavom na korisnički portal mogli pristupiti edukativnim materijalima i prezentacijskim sadržajima za teoretski dio, nakon čega bi pristupili ispitu. Nakon završetka ispita, rezultati bi automatski bili poslani stručnjaku zaštite na radu zaposlenom kod poslodavca, odnosno kod osobe ovlaštene za osposobljavanje radnika. Osim osposobljavanja za rad na siguran način, radnik mora obaviti i liječnički pregled kod specijaliste medicine rada ako radi na poslu s posebnim uvjetima rada. Na pregled bi se naručivao kroz klijentske aplikacije poslodavca i medicine rada koje bi imale sličnu ulogu kao i klijentske G2 aplikacije u CEZIH-u. Aplikacije bi se sinkronizirale putem SOAP+MQ sustava poruka te imale module za automatski pristup nekim portalskim segmentima DC-a. Ovlaštena osoba u tvrtki generirala bi 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 bili obaviješteni radnik, njegov ovlaštenik i stručnjak zaštite na radu. Analogija tome je e-upućivanje i e-naručivanje u CEZIH-u. Specijalist medicine rada bi u svoju aplikaciju mogao učitati radnikov karton i ažurirati ga nakon obavljenog pregleda s donesenim zaključcima iz nalaza te bi nakon toga poslodavac imao uvid u radnu sposobnost radnika tj. medicina rada bi odmah unijela uvjerenje RA2 iz kojeg je sve vidljivo. Nakon prestanka rad-

nog odnosa, radnik bi automatski bio uklonjen s popisa aktivnih radnika u tvrtki na temelju podataka preuzetih iz sustava MRMS-a, ali bi njegovi podaci i karton (profil) i dalje bili dostupni u DC-u, kako bi ih mogla povući tj. koristiti tvrtka u kojoj bi radnik zasnovao svoj slijedeći radni odnos.

Ovlaštene osobe (definirane Pravilnikom o ovlaštenjima za poslove zaštite na radu) bi kroz aplikaciju unosile sve elemente zaštite na radu u tvrtki koji su opisani u prethodnim poglavljima i potpoglavljima.

U slučajevima ozljede na radu, u lokalnoj aplikaciji poslodavca generirao bi se OR obrazac te bi se kao XML izvješće prosljedio i pohranio 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 pohranjivao bi se 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 (*HZZO-ISPZZ, 2019., ZUZNR, 2016.*).

## Ciljevi

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

**Tablica 2. Poslovni ciljevi SNIS-a**

**Table 2. Business goals of SNIS**

Dnevno-operativni ciljevi	Taktički ciljevi	Strateški ciljevi
<ul style="list-style-type: none"> <li>osnovne evidencije o ZNR</li> <li>izvješća o ozljedama</li> <li>uputnice</li> </ul>	<ul style="list-style-type: none"> <li>brza dostupnost ukupnim podacima o stanju za željeno razdoblje</li> <li>analiza poboljšanja po razdobljima</li> <li>izrada i klasifikacija modela rizika</li> </ul>	<ul style="list-style-type: none"> <li>daljnja konsolidacija nacionalnih strategija – koordinacijom politika i uzajamnim učenjem</li> <li>pružanje praktične potpore malim i mikropoduzećima</li> <li>poboljšanje provedbe evaluacijom rezultata nacionalnih inspektorata rada</li> <li>pojednostavljivanje postojećeg zakonodavstva</li> <li>unapređenje prikupljanja statističkih podataka zbog osiguranja kvalitetnijih dokaza i razvijanja alata za praćenje</li> <li>jačanje koordinacije s međunarodnim organizacijama</li> </ul>

## ZAKLJUČAK

U ovome radu pokušala se iznijeti ideja razvoja hipotetskog sveobuhvatnog nacionalnog informacijskog sustava ZNR ili, drugim riječima, izgradnje informacijske infrastrukture u području ZNR u RH. Idejno se ovaj spekulativni pristup gradi na započetim planovima bivšeg ZUZNR koji su polazili od ideje sustava SNIS ZNR sa sveobuhvatnom bazom podataka u području ZNR nazvanom "Data Collector" (često korištenom kao sinonim za cijeli SNIS) s uključenim dobrim primjerima iz prakse i već započetim radovima na oblikovanju konkretnog sustava pod nazivom Informacijski sustav zaštite na radu ili drugim riječima, prvim koracima oblikovanja nacionalne II u području ZNR. Dok se ovaj spekulativni pristup opisa ustroja i funkcionalnosti ovakvog središnjeg informacijskog sustava može učiniti zahtjevnijem čitatelju možda neobjektivnim, treba uzeti u obzir da je pri njegovu oblikovanju primijenjen objektivni pristup analizi i prezentaciji postojećih aktivnih informacijskih sustava i tehnoloških rješenja na kojima su zasnovani, dosadašnjih planova i zacrtanih ciljeva za izgradnju predloženog sustava, postojećih obveza RH u informatizaciji ZNR, kao i aktualnog stanja informatizacije u ovom području.

RH je kroz EU projekte IPA2007 i IPA 2012 (Uredbe Vijeća EU: 1085/2006, 718/2007) dobila zadaću oblikovanja nacionalne II u ZNR. U izvršavanju te zadaće RH se sa svojim stručnjacima našla u problemima kako izvesti odgovarajući SNIS i njegov središnji registar podataka i resursa ZNR u RH. Do svog ukidanja, ZUZNR kao tadašnje izvršno tijelo investitora u gradnji sustava, uspio je implementirati samo dio funkcionalnosti i to kroz aplikativno rješenje IS ZNR koji se suočio s mnogim problemima koje bi trebalo otkloniti kako bi se omogućio daljnji razvoj inicijalno planiranog SNIS-a. U sadašnjoj funkcionalnoj fazi, IS ZNR sadržava podatke o ovlaštenim osobama za obavljanje poslova zaštite na radu i njihovom obavljanju poslova zaštite na radu za poslodavce te različite podatke koje svi poslodavci prema ZZNR i drugim važećim propisima imaju obvezu redovno dostavljati MRMS. Ovi podaci koriste se za stručni nadzor i reviziju poslovanja ovlaštenih osoba za obavljanje poslova ZNR u odnosu na dobivena ovlaštenja, praćenje stanja,

izradu stručnih mišljenja za različite subjekte, provođenje statističkih istraživanja, izrađivanje programa, vodiča, metoda i modela ZNR, utvrđivanje kriterija i postupaka u vezi s organizacijom rada, pružanje pomoći udruženjima poslodavaca, sindikatima, ovlaštenim osobama za poslove ZNR te tijelima uprave, provođenje akcija s pojedinih područja ZNR i zaštite zdravlja na radu te za unapređivanje ukupnog stanja ZNR. U prvoj fazi punjenja baze podataka utakani su podaci iz evidencija kontrolnih kuća, a slijedi i faza uvezivanja aplikacija za vođenje evidencija po ZNR u tvrtkama koje dobivaju dodatne module za izravnu razmjenu podataka sa IS ZNR (npr. programsko rješenje WebZNR). U smislu portalskog načina rada, osim same prijave u IS ZNR, kroz mrežnu stranicu MRMS omogućen je i jednostavan unos podataka o osobama koje je poslodavac odredio za obavljanje poslova zaštite na radu.

Ako se IS ZNR gleda kao polazna točka, daljnji razvoj i njegova transformacija u sustav očekivane veličine i kompleksnosti zahtijeva vrlo velika financijska ulaganja. Osim financijskih problema, postoje pravni i tehnički problemi. Tehnički problem IS ZNR je nepostojanje integracije s NIAS-om tj. nepovezanost s e-Građani, korištenje zastarjelih verzija poslužiteljskog i razvojnog programskog sustava, a što dodatno otežava mogućnost integracije s vanjskim sustavima. Što se tiče pravnih problema, IS ZNR podložan je Zakonu o državnoj informacijskoj infrastrukturi. Tim Zakonom definirane su obveze svakog registra, između ostalog i kroz članak 7., stavak 3., članak 9., stavak 5. i 7. te članak 22., stavak 8. Iz Pravilnika je jasno da se radi o uspostavi Registra i potrebama koordinacije s ostalim projektima državne informacijske infrastrukture. Investitori i izvođači projekta IS ZNR trebali bi demonstrirati volju te odlučiti poštovati planove i strategije donesene od strane Vlade, pogotovo o pitanju sigurnosti IS-a koji bi trebao biti usklađen s Nacionalnom strategijom kibernetičke sigurnosti i Akcijskim planom za provedbu nacionalne strategije kibernetičke sigurnosti. Morao bi biti implementiran sustav nadzora pristupa podacima koji će transparentno biti dostupan, kako korisnicima, tako i svim obveznicima dostave podataka, koji su navedeni u funkcionalnom opisu sustava. Prema nekim tumačenjima, to je i jedan od zahtjeva GDPR-a, a iako su javna tijela izuzeta iz plaćanja kazni, ne znači da time nisu i obveznici poštovanja GDPR-a.

Kako bi se IS ZNR uskladio s akcijskim planom Vlade RH o smanjenju administrativnog opterećenja poslodavaca, sve operacije koje je poslodavac već obavio putem drugih informacijskih sustava ne smiju biti ponovljene. Na primjer, novozaposleni radnik mora se automatski pojaviti na listi aktualnih zaposlenika ako je isti prijavljen putem MRMS-a.

Autori ovu ideju i prijedlog mogućnosti daljnjeg razvoja sustava po uzoru na zdravstveni informacijski sustav CEZIH smatraju ispravnim i logičnim putem. Cilj autora je, osim isticanja važnosti i potrebe izgradnje, bio i uputiti čitatelje u probleme i kompleksnost pokretanja i provođenja ovakvog projekta. U iznošenju ideje za razvoj sustava korištena su stečena teoretska znanja, iskustva iz prakse, uz oslonac na aktualnu domaću regulativu, EU smjernice, norme i aktualne projekte i projektnu dokumentaciju. ZNR je u europskim okvirima na vrlo visokoj razini na kojoj bi trebala biti i u RH, ali nažalost još nije. Unapređenje ZNR može se postići samo zajedničkim naporima nadležnih državnih tijela, poslodavaca kao i drugih čimbenika u sustavu ZNR. Provođenjem izgradnje ovakvog sveobuhvatnog sustava, RH bi znatno unaprijedila ZNR i podigla ju na jednu znatno višu razinu jer cilj ZNR nije samo smanjiti broj ozljeda na radu, već uspostava sustava u kojemu su sve stavke i sudionici sigurni u svakom trenutku.

## LITERATURA

Fina: *Web aplikacije i servis*, dostupno na: <https://www.fina.hr/e-servisi>, pristupljeno: 29.5.2019.

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](https://www.fer.unizg.hr/download/repository/Healthcare_information_system_in_Croatia_16-9_RevD_-_FER_-_2015.pdf), pristupljeno: 10.6.2019.

Hrvatski zavod za javno zdravstvo: *Hrvatski zavod za zaštitu zdravlja i sigurnost na radu*, 2019. dostupno na: <http://hzzsr.hr/>, pristupljeno: 29.5.2019.

Hrvatski zavod za zdravstveno osiguranje: *CEZIH – koncept sustava*, dostupno na: [http://www.cezih.hr/pzz/dokumentacija/01\\_00\\_CEZIH\\_koncept\\_sustava.pdf](http://www.cezih.hr/pzz/dokumentacija/01_00_CEZIH_koncept_sustava.pdf), pristupljeno: 10.5.2019.

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](http://www.cezih.hr/pzz/dokumenti_pzz/Opis_NISHI_sustava.pdf), pristupljeno: 12.6.2019.

International Labour Organization; *Data Sources for Optimizing the Collection and Use of OSH data*, 2017. dostupno na: [https://www.ilo.org/wcmsp5/groups/public/---ed\\_protect/---protrav/---safework/documents/publication/wcms\\_546703.pdf](https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/publication/wcms_546703.pdf), pristupljeno: 1.6.2019.

Linija koda d.o.o.: *WebZNR – modul IS ZNR*, 2020. dostupno na: <https://www.zastitanaradu.hr/isznr/>, pristupljeno: 1.9.2020.

Ministarstvo rada, mirovinskog sustava, obitelji i socijalne politike: *IS ZNR, 2020*. dostupno na: <http://uznr.mrms.hr/znr/is-znr/>, pristupljeno: 1.9.2020.

Ministarstvo rada, mirovinskog sustava, obitelji i socijalne politike: *NACIONALNI PLAN ZAŠTITE NA RADU za razdoblje 2021.-2027. godine - prijedlog*, 23. studenoga 2020. dostupno na: <https://esavjetovanja.gov.hr/ECon/MainScreen?entityId=4571>, pristupljeno: 1.12.2020.

Ministarstvo uprave Republike Hrvatske: *Strategija e-Hrvatska 2020*, dostupno na: [https://uprava.gov.hr/UserDocsImages/Istaknute%20 teme/e-Hrvatska/Strategija\\_e-Hrvatska\\_2020.pdf](https://uprava.gov.hr/UserDocsImages/Istaknute%20 teme/e-Hrvatska/Strategija_e-Hrvatska_2020.pdf), pristupljeno: 8.5.2019.

*Odluka o donošenju Nacionalne strategije kibernetičke sigurnosti i Akcijskim planu za provedbu nacionalne strategije kibernetičke sigurnosti*, N.N., br. 108/15.

*Pravilnik o obavljanju poslova zaštite na radu*, N.N., br. 112/14.

*Pravilnik o obavljanju poslova zaštite na radu*, N.N., br. 126/19.

*Zakon o državnoj informacijskoj infrastrukturi*, N.N., br. 92/14.

Središnji državni ured za razvoj digitalnog društva: *Središnji katalog službenih dokumenata*, dostupno na: <http://www.digured.hr/>, pristupljeno: 2.6.2019.

ZUZNR: *Zajedno za zaštitu na radu, zdravlje i produktivnost*, Zagreb, 2016., dostupno na: [http://www.hzos.hr/upload\\_data/site\\_files/zuznr\\_hzos\\_sijecanj\\_2016.pptx](http://www.hzos.hr/upload_data/site_files/zuznr_hzos_sijecanj_2016.pptx), pristupljeno: 6.5.2019.



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

*SUMMARY: The subject of this paper is the analysis of the possibilities of further design of the national information infrastructure in the field of occupational safety. The foundations of this infrastructure were laid through the initial development of the Information System of Occupational Safety and Health (IS OSH) under the leadership of the Ministry of Labor. Through the analysis of: national legislation and EU guidelines in the field of occupational safety, the possibilities of applying global network services, successful examples of development of national information systems in the field of public administration and health; the foundations for a speculative approach to the analysis of further development of this national information infrastructure were created. The idea of predictable further development and structure of the future central Information System of Occupational Safety and Health was conceived and presented. It relies on the central register of data and resources for safety at work (initially called Data Collector) and all necessary functionalities that guarantee security, ubiquity and longitudinal electronic records. This guarantees the improvement of safety at work in the Republic of Croatia.*

**Key words:** *safety at work, web services, national information infrastructure, legislation, Data Collector, IS OSH*

*Professional paper  
Received: 2020-09-16  
Accepted: 2021-04-30*