UNIVERZITET U SARAJEVU
FAKULTET POLITIČKIH NAUKA
ODSJEK ZA SIGURNOSNE I MIROVNE STUDIJE

# ZAŠTITA LIČNIH PODATAKA U ZDRAVSTVENIM INFORMACIONIM SISTEMIMA

**-magistarski rad-**

Kandidatkinja:
Vesna Simikić
Broj indeksa: 16-IS/22

Mentor:
prof.dr. Saša Mrdović

Sarajevo, oktobar 2023. godine

| | | |
|---|---|---|
| 2023. | Vesna Simikić | Zaštita ličnih podataka u zdravstvenim informacionim sistemima |

# SADRŽAJ

**Zaštita ličnih podataka u zdravstvenim informacionim sistemima**

Vesna Simikić

**Sažetak:**

Podaci su jednostavne i proste činjenice koje izolovane nemaju poseban značaj ali njihovom obradom stvaraju se informacije koje imaju najširu primjenu u savremenom svijetu. S pravom se smatra da su podaci izuzetno vrijedan resurs a trka za njihovim prikupljanjem odnosno raspolaganjem stvara platformu za ostvarivanje postavljenih ciljeva. Svi podaci nisu javni i ne koriste se samo u ostvarivanju dobrih namjera. Pojam zloupotrebe podataka obično se vezuje za skupinu koju nazivamo osjetljivi podaci. Razvoj svijesti o zaštiti osjetljivih kategorija podataka, naročito ličnih podataka, doveo je do potrebe za definisanjem normativnih okvira i smjernica za zaštitu ličnih podataka kako na međunarodnom, tako i na lokalnom nivou. Zdravstveni podaci predstavljaju posebnu kategoriju ličnih podataka koja se organizuje i obrađuje kroz zdravstvne informacione sisteme. Usvajanje Opšte uredbe Evropske unije o zaštiti ličnih podataka značajno je uticalo na obradu ličnih podataka u zdravstvenim informacionim sistemima. Cilj ovog rada je da pokaže da je zaštita ličnih podataka u zdravstvenim informacionim sistemima obaveza svih aktera sistema i da bez efikasnog provođenja standardizovanih mjera ne postoji mogućnost adekvatne zaštite ličnih podataka. Ovim radom je omogućen uvid u rezultate analize ispunjenosti zahtjeva Zakona o zaštiti ličnih podatka Bosne i Hercegovine na primjeru integrisanog zdravstvenog informacionog sistema Republike Srpske (IZIS).

**Ključne riječi:** lični podaci, ISO 27001, GDPR, sigurnosne mjere, IZIS, sigurnosna politika

# UVOD

Zdravstveni podaci pripadaju skupini ličnih podataka i kao takvi predstavljaju povjerljive i osjetljive kategorije. Kako bi zdravstveno stanje svakog pacijenta bilo praćeno na adekvatan i objektivan način, neophodno je vršiti preciznu evidenciju i obradu zdravstvenih podataka. Navedeni podaci se pribavljaju tokom liječenja, intervencija i/ili terapija koje se propisuju pacijentu. S obzirom da se radi o velikoj količini podataka za njihovo prikupljanje, obradu i čuvanje primjena savremenih informaciono-komunikacionih tehnologija je moguća samo uz praćenje propisanih standarda poslovanja.

Zdravstveni informacioni sistemi predstavljaju jedan od načina organizacije i čuvanja velikih količina zdravstvenih podataka. Funkcionalan zdravstveni informacioni sistem pojednostavljuje prikupljanje, selektovanje, prosleđivanje i čuvanje pomenutih podataka, čime se zdravstvenim radnicima olakšava dostupnost informacija potrebnih za donošenje odluka presudnih za dalji tok liječenja pacijenata. Međutim, postoje mnoge neusklađenosti u kreiranju informacionih sistema u sklopu zdravstvenih ustanova. Zakon o zaštiti ličnih podataka Bosne i Hercegovine definisao je načine organizacije i obrade ličnih podataka ali do pojave Smjernica Svjetske zdravstvene organizacije nisu postojali jasno definisani načini organizacije i obrade elektronskih zdravstvenih podataka.

Veliki broj zdravstvenih ustanova razvio je svoje infomacione sisteme i prilagodio ih potrebama svog poslovanja. Nerijetko je pristutna činjenica da je više pažnje posvećivano formi (vizuelnom prikazu, statističkom izvještavanju) nego bezbjednosti pohranjenih podataka. Dešavale su se i situacije da su softverske kuće koje su izrađivale pomenute zdravstvene informacione sisteme zadržavale vlasništvo nad podacima uskladištenim na svojim serverima. Upotreba lokalizovanih zdravstvenih informacionih sistema ograničavala je dijagnostikovanje medcinskog stanja ili čak liječenje pravog vlasnika podataka, odnosno pacijenta, u drugim zdravstvenim ustanovama.

Razvojem integrisanog zdravstvenog informacionog sistema u Republici Srpskoj omogućeno je povezivanje svih informacionih sistema koji su služili za prikupljanje i obradu zdravstvenih podataka osiguranika u cjelinu. Glavni nedostatak ovakvog sistema je u tome što u njemu postoji izuzetno veliki broj korisnika a veoma mali broj administratora čime je povećan rizik od gubitka ili „curenja" povjerljivih podataka. Pored toga, dodatni problem za zaštitu ličnih podataka krajnjih korisnika predstavlja nedostatak svijesti zdravstvenih ustanova o potrebi procjene rizika od gubitka ili zloupotrebe povjerljivih podataka.

Imajući u vidu da su zaposleni u zdravstvenim ustanovama u stalnom kontaktu sa podacima čija zloupotreba može dovesti do izuzetno štetnih posledica, neophodno je precizno definisati prava pristupa osjetljivim podacima i u skladu sa tim stepen odgovornosti korisnika.

Usvajanjem Zakona o zdravstvenoj dokumentaciji i evidencijama u oblasti zdravstva Republike Srpske elektronski zdravstveni podaci dobili su zakonsku formu i kroz integrisani zdravstveni informacioni sistem omogućena je organizacija i obrada u zakonskim okvirima. Ovaj rad stavlja u fokus tematiku zaštite ličnih podataka u zdravstvenim informacionim sistemima sa osvrtom na integrisani zdravstveni informacioni sistem Republike Srpske.

Materija ovog rada biće izložena u pet poglavlja i to:

1. Teorijsko – metodološki okvir rada
2. Metode zaštite podataka u informacionim sistemima
3. Standard za upravljanje informacijskom sigurnošću ISO 27001
4. Zakonski okvir zaštite ličnih podataka
5. Upravljanje zaštitom ličnih podataka u integrisanom zdravstvenom informacionom sistemu Republike Srpske

U prvom poglavlju preciziran je predmet i problem istraživanja, opisano šta predstavljaju lični podaci, čime se defnišu i kako se utiče na njihovu bezbjednost. Precizirani su ciljevi istraživanja, dat pregled sistema hipoteza, definisani načini istraživanja, opravdanost, vremenski i prostorni okvir istraživačkog rada. Važnost posjedovanja sigurnosne politike, postojanja fizičkog obezbjeđenja informatičke opreme i prostorija namijenjenih za čuvanje podataka, neophodnost uspostavljanja klasifikacije i kontrole pristupa informacijama predstavljene su u drugom poglavlju. Treće poglavlje se bavi međunarodnim standardom za upravljanje informacijskom sigurnošću ISO/IEC 27001, njegovim karakteristikama, strukturom i postupkom implementacije. Objašnjen je i način upravljanja sigurnošću informacija u zdravstvu kroz kratak osvrt na standard ISO 27799. Četvrto poglavlje se bavi normativnim aktima koji se odnose na područje zaštite ličnih podataka. U njemu su razmotreni dokumenti od međunarodnog značaja, odnosno Zaštita ličnih podataka u zdravstvenim informacionim sistemima – principi i procesi za javno zdravlje Svjetske zdravstvene organizacije i Opšta uredba Evropske unije o zaštiti ličnih podataka (engl. The EU General Data Protection Regulation - GDPR), kao i propis od regionalnog i lokalnog značaja Zakon o zaštiti ličnih podataka Bosne i Hercegovine. U petom poglavlju analizirano je upravljanje zaštitom ličnih podataka u integrisanom zdravstvenom informacionom sistemu Republike Srpske kroz definisanje funkcionalnosti i primjene integrisanog zdravstvenog informacionog sistema, način organizacije, upravljanje i pristup podacima, kao i njegova usklađenost sa zahtjevima Zakona o zaštiti ličnih podataka Bosne i Hercegovine.

# 1. TEORIJSKO - METODOLOŠKI OKVIR RADA

## *1.1. Pojam ličnih podataka*

Informacije predstavljaju osnovni resurs računarskih sistema kojima je neophodno obezbjediti zaštitu od neovlaštenog otkrivanja, eventualne izmjene, kao i mogućnosti uskraćivanja upotrebe ovlaštenim korisnicima. Navedeni uslovi predstavljaju osnov teorije sigurnosti informacija.[1]

Pojava modernizovanijih načina obrade podataka uslovili su potrebu za drugačijim prisupom zaštiti informacija. Rasprostanjena upotreba društvenih mreža, pametnih uređaja i interneta uopšte, dovela je do pojave dijeljenja i prenošenja ličnih podataka daleko izvan fizičkih granica država. Reforma direktive koja definiše oblast zaštite ličnih podataka odnosno usvajanje Opšte uredbe Evropske unije o zaštiti ličnih podataka smatra se najvećom reformom u ovoj oblasti još od postanka weba.[2]

Lični podaci su, prema definiciji iz Uredbe svi oni podaci koji se odnose na pojedinca „čiji je identitet utvrđen ili se može utvrditi („ispitanik"); pojedinac čiji se identitet može utvrditi jeste lice koje se može identifikovati direktno ili indirektno, naročito uz pomoć identifikatora kao što su ime, identifikacioni broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više faktora svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca."[3]

Pod pojmom „lični podaci" podrazumijeva se: lično ime i prezime, identifikacioni broj lične isprave (lične karte, pasoša, studentskog indeksa), jedinstveni matični broj građanina (JMBG), glasovni zapis, adresa prebivališta i boravišta, broj telefona (mobilnog i fiksnog), IP adresa, broj zdravstvene kartice, broj zdravstvenog osiguranja, poreski broj, broj bankovnog računa. U lične podatke se ubrajaju i obilježja poput godina starosti, zaposlenja, poslovne funkcije, položaj i status u radnoj organizaciji. U ovu kategoriju se ubrajaju i biometrijski podaci poput DNK, otisaka prstiju, ušiju i skeniranog zapisa mrežnjače oka.

U kategoriju osjetljivih podataka o ličnosti mogu se uvrstiti i: pol, rasa, nacionalna pripadnost, vjeroispovjest, jezik, zdravstveno stanje, sindikalno i političko članstvo, zdravstveni status, seksualno opredjeljenje, osuda za krivično djelo i dr.

---

[1] Mrdović, Saša, Sigurnost računarskih sistema, ETF UNSA, Sarajevo, 2014, str. 24-26,

[2] Za više informacija posjetiti: http://azlp.ba/GDPR_Menu/Sta_je_GDPR/default.aspx?id=2373&langTag=bsBA&template_id=149&pageIndex=1

[3] Opšta uredba Evropske unije o zaštiti ličnih podataka, 2016, član 2

Uredbom je definisano i pravilo da prije prikupljanja ličnih podataka, subjekt koji ih prikuplja ima obavezu pružanja informacija o tome za koju svrhu se oni prikupljaju, na osnovu kojeg pravnog osnova, kome se podaci otkrivaju, te o pravu pojedinca da svojim podacima pristupi, zahtijeva njihov ispravak ili eventualno brisanje.[4]

Potrebno je imati u vidu da svi podaci koji se jednom nađu na internetu, tamo i ostaju. Rizici za bezbjednost ličnih podataka su u doba četvrte indrustrisjke revolucije[5] i više nego brojni. Neki od njih su: krađa identiteta, prevare načinjene zloupotrebom ličnih podataka (online kupovina), zloupotreba ličnih podataka sa ciljem postizanja materijalne koristi (preprodaja ličnih podaka drugih lica, spam poruke), maltretiranje u virtuelnom svijetu, seksualno uznemiravanje, iznuđivanje.

Veoma je važno imati razvijenu svijest po pitanju zaštite ličnih podataka. Funkcija interneta i informacionih tehnologija jeste da pruži olakšice u što više oblasti: poslovanju, komunikaciji, obrazovanju, kupovini, prodaji. Međutim, bez adekvatnog sigurnosnog pristupa svim servisima može se lako postati žrtvom. S toga je potrebno imati na umu da je sigurnost naših ličnih podataka u našim rukama tako da je neophodno preduzeti sve mjere opreza kako ti podaci ne bi bili predmet zloupotrebe.

### *1.2. Predmet istraživanja*

Zdravstveni podaci pripadaju kategoriji osjetljivih podataka i kao takvi moraju biti zaštićeni na adekvatan način. Bezbjednost zdravstvenih podataka ogleda se kroz obezbjeđivanje informacionih sistema kroz koje se navedeni podaci prikupljaju i obrađuju, te fizičkih i tehničkih mjera koje se provode nad informatičkom opremom, kao i definisanja i upravljanja pravima pristupa korisnika sistema. Postojanje svijesti o potrebi zaštite, kako softverskog i hardverskog dijela zdravstvenih informacionih sistema, tako i zdravstvenih i ličnih podataka, omogućava jasno sagledavanje bezbjedonosnih rizika i tretman istih.

### *1.3. Problem istraživanja*

Naglim razvojem digitalnih tehnologija ugroženo je jedno od osnovnih ljudskih prava a to je pravo na zaštitu ličnih podataka i privatnosti. Zaštita navedenog prava postala je globalni problem današnjice. Sve veća pažnja se posvećuje zaštiti zdravstvenih podataka pacijenata. Do pojave Smjernica za izradu zdravstvenih informacionih sistema Svjetske zdravstvene

[4] Za više informacija posjetiti: https://www.nosbih.ba/bs/o-nama/zastita-licnih-podataka/
[5] Za više informacija posjetiti: https://www.weforum.org/focus/fourth-industrial-revolution

organizacije i Opšte uredbe Evropske unije o zaštiti ličnih podataka način organizacije zdravstvenih podataka zavisio je isključivo od zahtjeva vlasnika zdravstvenih informacionih sistema. Različitošću sistema otežana je dostupnost medicinskih podataka pacijenata usled nemogućnosti njihovog sinhronizovanog rada i skladištenja podataka vezanih za jednog pacijenta u jedinstven elektronski karton.

Uvezivanjem više različitih privatnih i javnih zdravstvenih informacionih sistema kroz projekat integrisanog zdravstvenog informacionog sistema vlada Republike Srpske uspjela je omogućiti veću dostupnost medicinske dokumentacije i podataka. Međutim, pitanje sigurnosti ličnih podataka iniciralo je sledeća istraživačka pitanja:

a) Da li su u slučaju integrisanog zdravstvenog informacionog sistema Republike Srpske ispoštovana sva pravila zaštite ličnih podataka navedena u odgovarajućim normativnim aktima?
b) Da li su zdravstvene ustanove svjesne rizika koji postoje u zdravstvenim informacionim sistemima?
c) Da li su zdravstvene ustanove omogućile bezbjedan pristup ličnim podacima kroz adekvatnu zaštitu informatičke opreme i korisnika?

### *1.4. Ciljevi istraživanja*

Ciljevi istraživanja su sadržani u odgovorima na prethodna istraživačka pitanja i mogu se podijeliti na naučne i društvene.

Naučni cilj ovog rada je da se metodološkim pristupom utvrdi hipotetički okvir zaštite ličnih podataka u zdravstvenim informacionim sistemima kao obaveze i dužnosti svih aktera zdravstvenih inoformacionih sistema.

Društveni cilj ovog rada je podizanje svijesti institucija i pojedinaca u Bosni i Hercegovini o važnosti zaštite ličnih i zdravstvenih podataka, kako kroz primjene odgovarajućih normativnih akata na međunarodnom i lokalnom nivou, tako i kroz implementacije mjera zaštite definisanih međunarodnim standardom za bezbjednost podataka i informacija.

### *1.5. Sistem hipoteza*

Glavna hipoteza ovog rada glasi da je zaštita ličnih podataka u zdravstvenim informacionim sistemima obaveza i dužnost kako vlasnika sistema, tako i impementatora i korisnika.

Posebne-pojedinačne hipoteze su sledeće:

- Primjena smjernica i ispunjavanje zahtjeva iznesenih u normativnim aktima na svjetskom i lokalnom nivou omogućavaju veću bezbjednost ličnih podataka u zdravstvenim informacionim sistemima.
- Razvijena svijest zdravstvenih ustanova o bezbjednosti ličnih podataka predstavlja glavnu ulogu u uspješnoj implementaciji sigurnosnih mjera.

### *1.6. Način istraživanja*

Istraživanje na ovom radu provedeno je kombinacijom kvantitativno-kvalitativnih metoda. Narativna analiza postojećeg stanja vezano za bezbjednost ličnih podataka u integrisanom zdravstvenom informacionom sistemu Republike Srpske izvršena je na osnovu dostupnih normativnih akata vlasnika sistema.

Dobijeni rezultati su upoređeni sa aktuelnim propisima na međunarodnom i lokalnom nivou koji se bave zaštitom ličnih podataka.

### *1.7. Naučna i društvena opravdanost istraživanja*

U doba lake dostupnosti ličnih podataka putem društvenih mreža i interneta javila se potreba za razvijanjem svijesti pojedinaca i institucija o zaštiti ličnih podataka.

Bezbjednost podataka se više ne vezuje samo za mrežne administratore, nego postaje obaveza svih nas. Način na koji pristupamo ovoj temi pruža nam priliku da sagledamo sve aspekte zaštite koje je moguće provesti. Sve veća mogućnost zloupotrebe ličnih podataka navodi nas na stalnu analizu sistema zaštite i preispitivanje aktuelnih zakonskih akata kojima su nam prava na zaštitu ličnih podataka i privatnost zagarantovana.

Doprinos ovog rada ogleda se u identifikaciji i analizi tačaka regulative o zaštiti ličnih podataka u zdravstvenim informacionim sistemima na primjeru integrisanog zdravstvenog informacionog sistema Republike Srpske. Takođe pruža uvid u mehanizme zaštite pojedinaca, opreme i podataka, kao i postupke definisane međunarodnim standardom za bezbjednost podataka.

### *1.8. Vremensko i prostorno određenje istraživanja*

Vremenski okvir istraživanja odnosi se na period od početka implementacije integrisanog zdravstvenog informacionog sistema Republike Srpske, odnosno od 2018. godine, do perioda u kom su sve javne zdravstvene ustanove primarnog, sekundarnog i tercijarnog nivoa

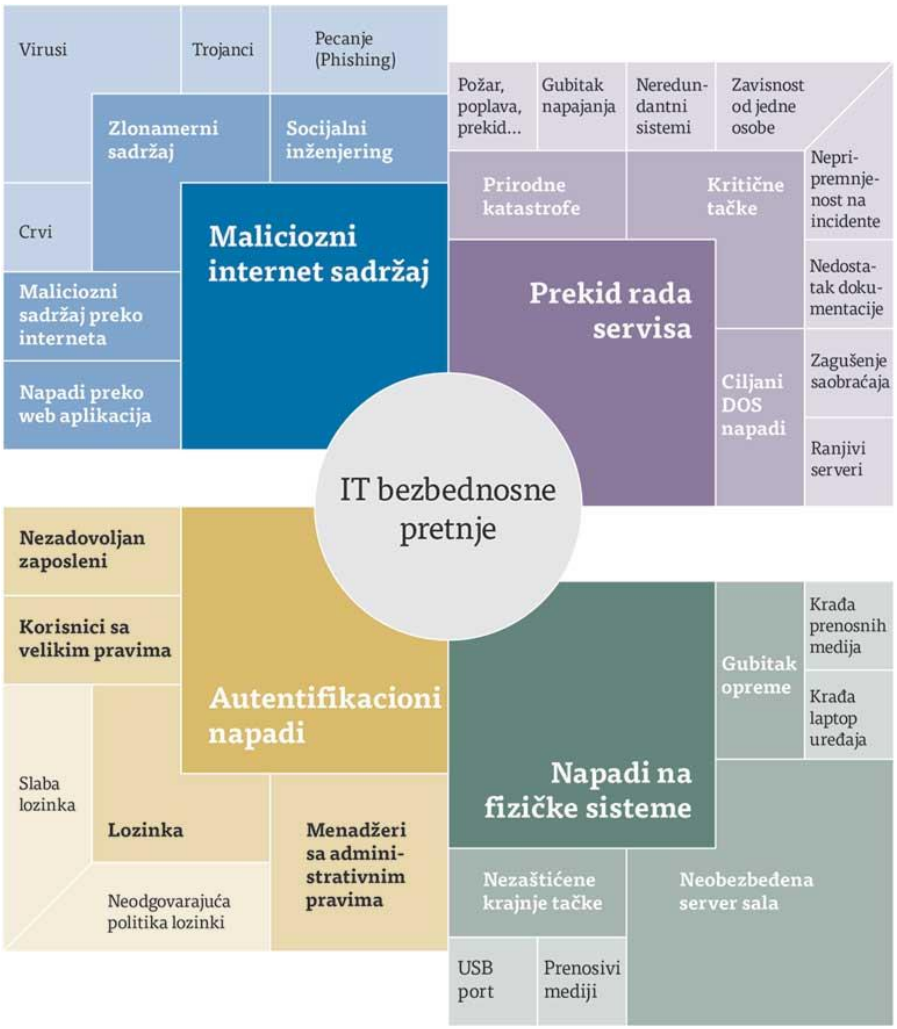
Republike Srpske uvezane u sistem integrisanog zdravstvenog informacionog sistema, odnosno do početka 2023. godine.

Prostorni okvir istraživanja obuhvata entitetsko područje Bosne i Hercegovine pod nazivom Republika Srpska.

## 2. METODE ZAŠTITE PODATAKA U INFORMACIONIM SISTEMIMA

Intenzivnom upotrebom interneta i pametnih uređaja povećana je upotreba elektronske razmjene podataka (engl. e-mail), elektronskog poslovanja i novih načina komunikacije. Problem sigurnosti resursa informacionog sistema i bezbjednosti podataka je postao jedan od dominantnih i najznačajnijih u oblasti informacionih tehnologija. Veliki broj prijetnji kojima smo svakodnevno izloženi na internetu (slika 1.) zahtijeva primjenu različitih mjera zaštite.

Postojanje loših mjera za fizičku bezbjednost podataka i računarske opreme, nepostojanje sigurnosne politike, neadekvatno čuvanje mrežne i komunikacijske opreme, nedostatak stručnog nadzora nad lokalnom mrežom dodatno može uzrokovati narušavanje bezbjednosti podatka kao i cjelokupnog informacionog sistema.




Slika 1. IT bezbjedonosne prijetnje[6]

[6] Za više informacija posjetiti: https://coming.rs/business-and-it/business-and-it-broj-4/informaciona-bezbednost-pretnje-za-koje-se-moramo-pripremiti/

### *2.1. Važnost posjedovanja sigurnosne politike*

Sigurnosna politika[7] predstavlja skup dokumenata koji opisuju postupke i uloge u procesu zaštite ispravnog i kvalitetnog funkcionisanja informacionog sistema u smislu pouzdanosti, tačnosti i pristupačnosti informacija i servisa. Uvođenje sigurnosne politike predstavlja jedinstven i cjelovit pristup zaštiti informacija te propisuje procedure i pravila koja su obavezna za sve zaposlene (korisnici informacionog sistema, administratori sistema) kao i za druga lica kojima su data privremena ili stalna prava pristupa informacionom sistemu.

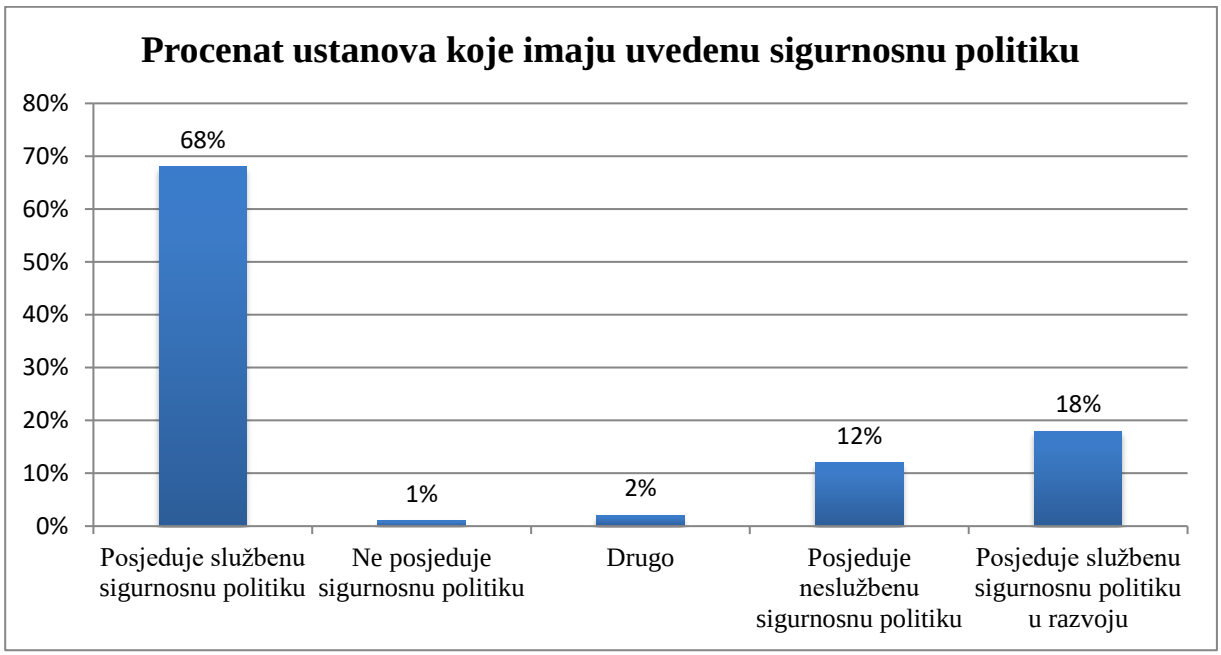
Imajući u vidu da se sve veći broj poslovnih procesa odvija primjenom elektronskih medijuma, tj. korištenjem resursa informacionog sistema, potrebno je obezbjediti neophodne mehanizme zaštite u cilju postizanja pouzdanog i ispravnog funkcionisanja. Upotrebom globalne svjetske mreže (interneta) znatno se povećavaju rizici gubitka, krivotvorenja, uništenja ili neovlaštenog korištenja resursa, čime razvoj sigurnosti postaje strateški važno pitanje.

Sigurnosna politika sadrži niz mjera, procedura i pravila koja se odnose na cjelokupno funkcionisanje informacionog sistema a sve u cilju povećanja njegove sigurnosti i ispravnog funkcionisanja. Svaki korisnik informacionog sistema trebao bi prilikom priključenja u isti biti obavezan da poštuje procedure i pravila definisane u sigurnosnoj politici. Poštovanje obaveza sigurnosne politike osigurava se kroz potpisivanje izjave o sigurnosti u kojoj je navedeno da je korisnik upoznat sa elementima sigurnosne politike i da ih prihvata. Takve izjave su obavezne za sve osobe kojima je odobren pristup bez obzira na vremensi period i način pristupa.

Na osnovu statističkog izvještaja za 2008. godinu Istituta za kompjutersku bezbjednost[8] može se zaključiti da je većina ustanova svjesna rizika kojima su izloženi njihovi informacioni sistemi, kao i važnosti samih podataka koji se obrađuju kroz navedene sisteme. U Dijagramu 1. navedeno je da je 68% ustanova ima uvedenu službenu sigurnosnu politiku, a na razvoju iste radi 18% ustanova. Neslužbenu sigurnosnu politiku u primjeni ima 12% ustanova dok samo 1% ne posjeduje nikakvu. Neformalna pravila koja ne pripadaju opsegu sigurnosne politke, u dijagramu 2. navedena kao „drugo" posjeduje 2% ustanova. Iz navedenog se može zaključiti da veliki broj ustanova, preciznije njih 80% ima uvedenu službenu sigurnosnu politiku.

[7] Hrvatska akademska i istraživačka mreža, 2009, Sigurnosna politika CCERT, str. 5

[8] Richardson, Robert, 2008, The latest results from the longest-running project of its kind, CSI Computer Crime & Security Survey




Dijagram 1. Procentualni prikaz ustanova koje imaju uvedenu sigurnosnu politiku[9]

### *2.2. Fizička sigurnost*

Svaka organizacija posjeduje prostorije koje su otvorene za javnost, prostorije kojima pristup imaju samo zaposleni i prostorije u kojima je ulaz dozvoljen samo određenoj grupi zaposlenih, zavisno od odobrenja i posla koji obavljaju. Oprema koja omogućava obavljanje ključnih funkcija za rad informacionog sistema i/ili ona na kojoj se pohranjuju povjerljive informacije trebala bi da se nalazi u tzv. serverskoj ili sistemskoj sobi.[10]

Ključnu infrastrukturu informacionog sistema čine: serveri, sve vrste mrežnih komunikacionih uređaja, razvodni ormari instalacija, glavna baza telefonskih linija i slično. Pristup takvim prostorijama trebao bi biti dozvoljen samo ovlaštenim licima koja se bave održavanjem ili administriranjem mrežne i komunikacione opreme. Ključna oprema potrebno je da bude zaštićena od prirodnih katastrofa, poplava, požara, zemljotresa i sl. Svaka organizacija je dužna da obezbjedi vatrootporne i vodootporne ormare namjenjene za čuvanje rezervnih kopija važnih sistemskh i korisničkih podataka.

Prostorije u kojima se nalaze serveri i oprema za podršku informacionom sistemu moraju se štititi adekvatnim uređajima za klimatizaciju.[11] Serverske sobe moraju biti obezbjeđene od

[9] Richardson, Robert, 2008, The latest results from the longest-running project of its kind, CSI Computer Crime & Security Survey, str.25

[10] Telecommunications Infrastructure Standard for Data Centers TIA-942, 2005, Telecommunications industry association, Arlington, str. 26-33

[11] Za više informacija posjetiti: https://bs.itpedia.nl/2019/05/15/de-it-equipment-room-mer-ser-en-der/

ulaska neovlaštenih osoba posredstvom digitalnog panela koji posjeduje šifru za otvaranje vrata ili nekim drugim sistemom fizičke zaštite od neovlaštenog pristupa.

Svaki korisnik, odnosno grupa korisnika, potrebno je da ima odgovornost za dio opreme koju koristi. Sva oprema koja je u upotrebi predstavlja vlasništvo organizacije, izuzev ako nije drugačije definisano posebnim pravilima. Poslovna oprema ne treba da se koristi u privatne svrhe. Privatna oprema se priključuje na poslovnu mrežu, odnosno na informacioni sistem, samo uz neke posebno definisane uslove i odobrenje uz obavezno posredovanje sistem administratora organizacije.[12]

Eksterni uređaji (brze memorije, CD, DVD, tvrdi diskovi) predstavljaju veliku opasnost za bezbjednost podatka i bezbjednost samog informacionog sistema. Veliku štetu mogu nanijeti uređaji koji su namjenjeni za iznošenje i upotrebu van prostorija organizacije. Navedene uređaje je potrebno držati izvan mrežnog okruženja i pod nezavisnom kontrolom do potrebe za njihovim korištenjem.

### *2.3. Upravljanje korisničkim nalozima i lozinkama*

Pravo pristupa informacionom sistemu treba biti jasno propisana kroz kategorizaciju korisničkih naloga. Korisničke naloge bi trebali posjedovati isključivo registrovani korisnici sistema (radnici u organizaciji, saradnici) uz jasno predočena pravila o zaštiti i čuvanju tajnosti podataka. Privilegije pristupa podacima za svakog korisnika trebaju biti definisane u zavisnosti od kategorije povjerljivosti podataka. Na taj način se vrši zaštita ovlaštenog prisupa podacima i programima.

Ograničavanjem korisničkih naloga može se obezbjediti efikasnija kontrola pristupa i korištenja operativnih sistema, programa i datoteka, kao i instaliranje softvera. Takođe, može se omogućiti da samo određeni korisnik može imati prisup određenoj datoteci ili fascikli na serveru ili pokrenuti određenu aplikaciju na serveru u mrežnom okruženju. Ova ograničenja provodi administrator sistema. Samo administrator može imati potpun pristup sistemu, dok svi drugi korisnički nalozi trebaju imati limitiran pristup.

Ograničenje je moguće provesti na samom računaru kroz podešavanja operativnog sistema ili zahtijevati identifikaciju korisnika, pa na osnovu toga definisati prava pristupa određenoj grupi podataka. Sigurnost računarskih sistema se realizuje obično kroz tri procesa, a to su: autentifikacija, autorizacija i evidentiranje aktivnosti. Proces autentifikacije, odnosno provjere korisničkog identiteta, je prvi korak u prijavi korisnika na informacioni sistem i predstavlja

[12] Bjelajac Đ. Željko, Vesić Lj. Slavimir, Bezbednost informacionih sistema, Pravo-teorija i praksa, 2020, str. 63-76

veoma je važan element informacijske sigurnosti.[13] Pod autorizacijom se podrazumijeva provjera prava pristupa sistemu za konkretnog korisnika čiji je identitet potvrđen.[14] Napredna autentifikacijska rješenja su bazirana na oznakama (engl. tokenima), tako što se prilikom jedne autentifikacije stvara jedinstvena i jednom iskoristiva oznaka kojom se korisnik predstavlja resursu za kojeg je autorizovan.[15]

Evidencija aktivnosti odnosi se na evidenciju podataka o svim aktivnostima korisnika sistema. Svaki korisnik sistema neophodno je da posjeduje jedinstven identifikator za prijavu na lokalni računarski sistem kako bi se sve aktivnosti za definisani nalog mogle povezati i pratiti. Na taj način uvijek postoji pojedinačna odgovornost za stanje računarske opreme i sistema.

Sistem upravljanja lozinkama osigurava dokazivanje identiteta korisnika. S toga je za kreiranje lozinke neophodno:

- kroz upotrebu individualnih lozinki (kreiranih prilikom prve prijave korisnika na sistem) obezbjediti utvrđivanje odgovornosti;
- definisati oblik kvalitetne i snažne lozinke;
- eliminisati mogućnost upotrebe postojećih lozinki;
- lozinke čuvati kripotovane algoritmima za jednosmjernu enkripciju, potpuno odvojene od podataka koji se čuvaju iz aplikacija.

Da bi se postigao odgovarajući psihološki efekat na korisnike neophodno je da sistem posjeduje sledeće elemente:

- da prikazuje upozorenje koje naglašava da računaru smiju pristupiti samo ovlašteni korisnici uz minimalan broj informacija neovlaštenom korisniku;
- prilikom prikazivanje forme za prijavu ne smije prikazivati nikakve sugestivne poruke;
- usled neuspješnog logovanja ne smije naznačavati koji dio unešenih podataka je netačan;
- mora posjedovati ograničenje za maksimalan broj neuspješnih prijava.

Sve aktivnosti unutar sistema neophodno je pratiti i dokumentovati u cilju analize i pravovremene reakcije na situacije koje odstupaju od politike kontrole pristupa. Informacije koje je potrebno čuvati su:

- korisničko ime, datum i vrijeme neuspješnih pokušaja prijava;

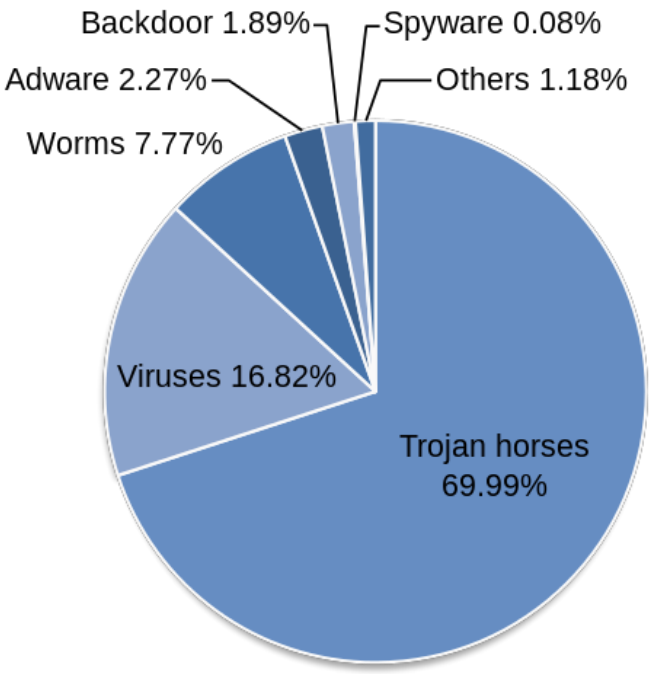
[13] Pavić, Tihomir , Jelenković Lejla, Autentifikacija i autorizacija korisnika na jednom mjestu, Fakultet elektrotehnike i računarstva, Zagreb, 2006.
[14] Za više informacija posjetiti: https://www.rječnik.com/Autorizacija
[15] Pavić, Tihomir , Jelenković Lejla, Autentifikacija i autorizacija korisnika na jednom mjestu, Fakultet elektrotehnike i računarstva, Zagreb, 2006.

- korisničko ime, datum i vrijeme uspješnih prijava i odjava, datoteke kojima je pristupano, programi koji su korišteni;
- podatke o računaru sa koga se prijavljuje korisnik.

Sačuvane informacije neophodno je redovno pregledati i analizirati kako bi se obezbjedilo izvršavanje samo onih aktivnosti koje su dodijeljene korisnicima.

### *2.4. Antivirusna politika (maliciozni softveri)*

Informacioni sistem, pored komunikacione infrastrukture obuhvata i resurse koji su podložni dejstvu aplikacija sa malicioznim kodom. Mrežno okruženje izuzetno pogoduje širenju aplikacija sa malicioznim kodom koje imaju mogućnost samostalnog širenja. Takve aplikacije su opremljene modulima za podršku raznim vrstama komunikacionih protokola i u stanju su da za izuzetno kratko vrijeme zaraze veliki broj računara u mreži i onemoguće ispravno funkcionisanje informacionog sistema. U maliciozni tj. zlonamjerni kod (engl. malware) (slika 4.) spadaju virusi, trojanci, crvi, špijunski softver (engl. spyware).




Slika 2. Vrste malicioznog softvera[16]

Samo jednim pokretanjem maliciozni softveri mogu konstantno obavljati određene zadatke, a da korisnik pritom nije ni svjestan da takav program postoji na njegovom računaru. Maliciozni program može biti, na primjer, programiran da šalje na određenu elektronsku

[16] Za više informacija posjetiti: https://kiber.ba/2023/02/09/sta-je-malware/

adresu arhivski fajl u kome je sačuvana kombinacija pritisnutih tastera na računaru, pa na taj način i korisnička imena i lozinke. Osim toga, maliciozni programi mogu izazvati štetu poput brisanja svih podataka na računaru.

Neki od malicioznih programa mogu se naći u okviru instalacionih fajlova softvera koji imaju prepoznatljiv brend, ali znaju biti bezopasni ili čak i korisni. Za većinu tih „pratećih" programa se ispostavi da su virusi ili trojanci. Skriveno ili nesvjesno instaliranje ovih dodatnih programa u najboljem slučaju inficira računar nepoželjnim reklamnim softverom, ili ga u gorem slučaju pretvara u hakerskog botneta. Ovaj vid „podmetanja" lažnog softvera u okviru instalacionog paketa softvera poznatog brenda predstavlja jedan od vidova socijalnog inženjeringa.[17] Da bi se spriječio ulazak malicioznog koda u informacioni sistem neophodno je implementirati zaštitu mrežnih resursa organizovanjem zaštite na nekoliko nivoa. Zaštita od malicioznog koda se odnosi na zaštitu podataka i progama koji se nalaze na korisničkim računarima i serverima.

Svrha korištenja zaštite od malicioznog koda je da se u realnom vremenu spriječi ulaz malicioznog koda u informacioni sistem. U slučaju prodora zaštita mora imati mogućnost sprječavanja njegovog aktiviranja i daljeg širenja. Virusi i druge vrste malicioznog koda mogu dospjeti u računarsku mrežu na više načina, u zavisnosti od mogućnosti razmjene podataka sa okruženjem, kao npr. putem:

- internet konekcije;
- elektronske pošte;
- prenosom datoteka;
- zaraženih prenosivih medijuma (CD, DVD, USB flash memory disk, eksterni disk).

Da bi se mreža zaštitila u što je moguće većoj mjeri, neophodno je sprovesti mjere na više nivoa:

- na nivou mrežnog prolaza (gateway, firewall);
- na nivou servera elektronske pošte;
- na nivou radnih stanica, fajl i aplikativnih servera.

Osnovna funkcija prva dva nivoa je da spriječi prodor malicioznog koda u mrežu, dok je funkcija trećeg nivoa da direktno štiti korisničke računare na kojima se nalaze podaci i aplikacije. U smislu klasifikacije navedenih nivoa zaštite po značaju, smatra se da je zaštita na nivou radnih stanica, tj. korisničkih računara obavezna, zaštita na nivou servera elektronske pošte i mrežnih prolaza preoporučljiva, dok se optimalno rješenje postiže kombinovanom zaštitom na sva tri nivoa.

[17] Kaspreska, Natalija , Ašmanov, Igor, Digitalna higijena, Riznica +, Beograd, 2021, str. 46-47

### *2.5. Zaštita na nivou mrežnog prolaza*

Zaštita na nivou mrežnog prolaza se postavlja na ulazima u mrežu, tj, na mjestima gdje se mreža priključuje na druge mreže, bilo da je u pritanju javna mreža (internet) ili računarske mreže drugih organizacija. Zaštita na nivou mrežnog prolaza realizuje na nekoliko načina. Jedan od njih je upotrebom hardverskih uređaja ili sofverskih aplikacija poput zaštitnog zida (engl. firewall).

Mrežni zaštitni zid je najčešće hardverski uređaj koji ima ulogu barijere između mreža, sprječavajući malicioznu komunikaciju i hakerske pokušaje upada. Korisnički zaštitni zid je program koji se izvršava na korisničkom računaru i štiti računar na kome se izvršava. U oba slučaja zaštitni zid pregleda mrežni saobraćaj, bilo dolazni ili odlazni, te na osnovu predefinisanih kriterijuma određuje da li je komunikacija dozvoljena ili ne.

Drugi način zaštite na nivou mrežnih prolaza je upotrebom hardverskih „web appliance“ uređaja, koji pružaju zaštitu od svih vrsta prijetnji sa interneta uključujući spyware, viruse, trojanske konje, phishing napade i neželjene aplikacije. Ovi uređaji putem aktivnog web filtering-a omogućavaju implemetnaciju sigurnosne politike organizacije u dijelu sigurnosnog i prihvatljivog poslovnog korištenja interneta.

Treći način zaštite na nivou mrežnih prolaza je primjenom softverskih administratorskih alata ili namjenskih hardverskih uređaja za nadzor mrežnog saobraćaja koji prikupljaju i analiziraju oprerativne i sistemske zapise (log fajlove). Ovi fajlovi omogućavaju uvid u aktivnosti resursa informacionog sistema te se s toga koriste u sljedeće svrhe:

- u cilju otkrivanja neovlaštenog pristupa i korištenja podatka, programa i ostalih resursa informacionog sistema;
- dijagnostike, tj, identifikovanja problema u radu mreže;
- rekonstrukcije događaja, npr, kao pomoć u istrazi kojom se utvrđuje kako, kada i zašto je određena redovna operacija prekinuta, te ko je, kada i kako obavio određenu radnju;
- podsticanje korisnika na savjesno korištenje resursa s obzirom da su korsnici upoznati sa mogućnošću da se njihove radnje mogu naknadno analizirati.

Osnovni doprinos zaštite na nivou mrežnog prolaza u ukupnoj zaštiti mreže jeste da će najveći broj malicioznog koda koji dolazi spolja biti uočen i uklonjen već na samoj ulaznoj tački u mrežu. Na taj način se sprječava prodor većeg dijela malicioznog koda u unutrašnjost mreže, što znatno olakšava posao antivirusnim programima koji rade na donjim nivoima zaštite.

### *2.6. Zaštita servera elektronske pošte*

Zaštitom servera elektonske pošte se stvaraju uslovi na osnovu kojih se pošta provjerava na prisustvo zlonamjernog koda prije nego što se isporuči krajnjem korisniku. Imajući u vidu visok procenat učešća elektonske pošte u razmjeni malicioznog koda, jasno je da se na ovaj način eliminiše najveći broj opasnosti po resurse informacionog sistema.

Zaštita servera elektronske pošte vrši se instalacijom odgovarajućeg antivirusnog softvera na server elektronske pošte ili pomoću posebnog hardverskog uređaja (e-mail appliance). Osim antivirusne zaštite, na severu elektronske pošte treba da bude instalirana i anti-spam zaštita. Spam je neželjena poruka najčešće reklamnog karaktera. Administator servera elektronske pošte je dužan da server konfiguriše na način da se što više neželjenih poruka zaustavi. Anti-spam zaštita treba da ima mogućnost konfigurisanja ulaznog filtera koji kontorliše ulazne poruke. Ukoliko se ustanovi da je u pitanju spam, poruka se odstranjuje ili premiješta na određeno vrijeme u karantin, tj. posebno mjesto na serveru na kojem se privemeno smještaju pritstigle spam poruke. Na taj način poruka koja nije spam, a protumačena je kao spam, može naknadno da se proslijedi korisniku.

Korištenjem uređaja e-mail appliance postiže se dodatna pogodnost u vidu djelimičnog oslobađanja propusnog opsega zakupljenog internet linka od nepotrebnog saobraćaja uzrokovanog spamom. To se postiže posredstvom funkcionalnosti uređaja koja mu omogućava da izvrši odbacivanje dijela spama prije kompletnog preuzimanja sa servera provajdera.

S obzirom na izuzetan značaj zaštite na nivou elektronske pošte na bebzjednost cijele mreže, potrebno je pažljivo pristupiti izboru antivirusnog softvera. Posebnu pažnju je potrebno posvetiti izboru servera elektronske pošte sa ciljem da isti posjeduje mogućnost impelementacije određenih antivirusnih rješenja većeg broja proizvođača antivirusnog softvera.

### *2.7. Zaštita radnih stanica i servera*

Antivirusna zaštita korisničkih računara i severa (fajl i aplikativnih servera) je obavezan nivo zaštite. Ovaj nivo zaštite obavezan je iz više razloga. Jedan od njih je taj što se na korisničkim računarima i serverima nalaze aplikacije i programi koji se zapravo štite, Većina virusa i drugih vrsta zlonamjernog koda namijenjena za izvršavanje na računarima ovog niova a vrlo rijetko je virus namijenjen za direktni napad na zaštitni zid ili server elektronske pošte.

U zavisnosti od prirode i načina konfigurisanja zaštite na nivou mrežnog prolaza i servera elektronske pošte određeni broj zlonamjernih programa neće biti prepozant, kao npr. fajlovi arhivirani sa lozinkom ili šifrovani saobraćaj, obzirom da samo krajnji korisnik može da dobije pristup izvornom sadržaju.

Antivirusni programski paketi namijenjeni korisničkim računarima i serverima mogu da sadrže veći broj različitih komponenti, od kojih su obavezne monitorski program, skenerski program i programski modul.

Osnovna funkcionalnost monitorskog programa je da u realnom vremenu provjerava svaki programski kod i podatke koji treba da se nađu u meomoriji računara. Monitorski program se aktivira prilikom svake akcije programa ili korisnika i analizaira sadržaj memorije. U slučaju pokušaja virusa da se aktivira, monitorski program će ga blokirati i spriječiti njegovo dalje izvršavanje, te preduzeti odgovarajuću radnju (obavještavanje korisnika, smještanje zaraženog fajla u karantin, brisanje fajla itd). Radi efikasne zaštite monitorski program treba da bude uvijek aktivan. Skenerski program se aktivira po potrebi ili unaprijed definisanom rasporedu, te detaljno provjerava sadržaj čvrstog diska. Programski modul ažurira bazu definicija virusa na računaru preuzimanjem novih definicija sa centralnog servera.

Da bi se obezbjedila antivirusna zaštita administrator je dužan da instalira i održava antivirusne programe na svim računariam i serverima u organizaciji. Obaveza administrtora je da korisničke računare konfiguriše tako da se redovne izmjene u bazi antivirusnog programa na centralnom serveru automatski prezuzimaju sa centralne lokacije u mreži bez aktivnog učešća korisnika. Antivirusna zaštita treba biti konifgurisana tako da korisnik nema mogućnost samostalnog isključenja antivirusne zaštite na svom računaru.

Pored antivirusne zaštite, na radnim stanicama i serverima je potrebno vršiti redovnu nadogradnju operativnih sistema, što predstavlja jednu od osnovnih i obaveznih linija odbrane od bezbjedonosnih problema.

### *2.8. Obaveze korisnika*

Korisnik može unošenjem malicioznih programa preko interneta i elektronske pošte ugroziti sigurnost informacionog sistema. Po statističkim podacima 88% slučajeva uzrok je ljudska greška ili nesavjesnost zaposlenih u smislu niske svijesti o potrebi poštovanja odredbi o prihvatljivom korištenju interneta.[18]

Kako bi se povećala sigurnost sistema i podataka potrebno je pridržavati se sljedećih uputstava:

[18]Za više informacija posjetiti: https://cisomag.com/security-awareness/

- prisup internetu i e-mailu dozvoliti korisnicima kojima je internet neophodan za obavljanje redovnih poslova;
- ne treba dozvoljavati pristup intenetu korisnicima na čijim računarima se nalaze povjerljivi podaci i podaci od izuzetne važnosti.

Posebnu pažnju treba posvetiti obaveznoj edukaciji korisnika o opasnostima na internetu. Obuka korisnika predstavlja aktivnost koja se sprovodi konstantno jer jedino povećavanjem nivoa osposobljenosti korisnika možemo uticati na smanjenje pojave grešaka uzrokovanih lošim rukovanjem opremom ili nepoštovanjem propisanih pravila.[19] Samo edukovan korisnik može znati kojim opasnostima je izložen ukoliko ne poštuje definisana pravila.

[19] Banković, Miroljub, 2008, *Menadžment informacionih sistema*, VTŠ Kragujevac, Kragujevac, str. 64

## 3. STANDARD ZA UPRAVLJANJE INFORMACIJSKOM SIGURNOŠĆU ISO 27001

Informacijska sigurnosti obuhvata primjenu širokog spektra zaštitnih mjera. U osnovi podrazumijeva implementaciju ne samo tehničkih, nego i fizičkih i administrativnih mjera zaštite. Kombinacijom svih pomenutih mjera postiže se adekvatna zaštita informacionih sistema organizacije. Međutim, jedini mehanizam kojim je moguće izvršiti efikasnu implementaciju i nadzor svih potrebnih mjera zaštite jeste dobro razvijen sistem za upravljanje sigurnošću informacija (engl. Information Security Management System - ISMS).

Sistem upravljanja sigurnošću informacija čine „politike, procedure, smjernice, povezani resursi i aktivnosti kojima rukovodi organizacija u nastojanju da zaštiti svoju informacionu imovinu" i predstavlja način „uspostavljanja, primjene, sprovođenja, praćenja, pregleda, održavanja i unapređivanja sigurnosti informacija organizacije" a sve u svrhu postizanja poslovnih ciljeva.[20] Osnova ISMS-a predstavlja precizno procjenjivanje rizika (ljudskih, tehnoloških, fizičkih) koji su u vezi sa informacijskom sigurnošću organizacije, njihove analize, jasnog definisanja granica prihvatljivosti, te efikasnih mjera za tretiranje i upravljanje rizicima.

Implementacijom ISMS-a utiče se na smanjenje vjerovatnoće ostvarenja rizika po sigurnost informacija. Prednosti koje organizacija može imati usvajanjem ISMS standarda su:

a) strukturirani okvir koji omogućava specifikaciju, implementaciju, provođenje i održavanje koncizno definisanog, vrednonosnog i usklađenog ISMS-a;
b) pomoć rukovodstvu u upravljanju na odgovoran način sigurnošću informacija unutar konteksta i korporativnim rizikom kroz edukacije i obuke vlasnika poslova i sistema;
c) promovisanje dobrih praksi sigurnosti informacija omogućava usvajanje i unapređivanje relevantnih kontrola i njihovo održavanje shodno unutrašnjim i vanjskim promjenama;
d) obezbjeđivanje lakšeg uspostavljanja povjerenja s poslovnim partnerima i kompatibilnim ISMS-om;
e) povećanje povjerenja zainteresovanih strana;
f) zadovoljavanje društvenih potreba i očekivanja; i
g) efektivnije upravljanje investicijama u polju informacione sigurnosti.[21]

[20] Institut za standardizaciju Bosne i Hercegovine, https://isbih.gov.ba/p/sistemi-upravljanja-sigurnoscu-informacija
[21] Institut za standardizaciju Bosne i Hercegovine, https://isbih.gov.ba/p/sistemi-upravljanja-sigurnoscu-informacija

Sve navedene pogodnosti predstavljaju reference i savjete iz normativnih akata vezanih za uspostavljanje sigurnosti u informacijskim sistemima. Najpoznatiji normativni akti su međunarodni standardi.

„Standard je dokument za opštu i višekratnu upotrebu, donešen koncenzusom i odobren od priznatog tijela, koji sadrži pravila, smjernice ili karakteristike aktivnosti, ili njihove rezultate i koji ima za cilj postizanje optimalnog stepena uređenosti u datom kontekstu."[22] Dva tijela koji zajedno čine sistem za međunarodnu standardizaciju su Međunarodna organizacija za standardizaciju ISO (engl. The International Organization for Standardization) i Međunarodna elektrotehnička komisija IEC (engl. The International Electrotechnical Commission).[23]

U ovom radu će biti razmotren međunarodni standard ISO/IEC 27001 i njegova podkategorija ISO 27799.

### *3.1. Karakteristike standarda ISO 27001*

ISO/IEC 27001 Informacione tehnologije – Tehnike bezbjednosti – Sistemi menadžmenta bezbjednošću informacija – Zahtjevi (engl. Information technology – Security techniques – Information security management systems – Requirements) predstavlja međunarodni standard koji daje zahtjeve za ISMS – Sisteme menadžmenta bezbjednošću informacija.[24]

Prva verzija ovog standarda, objavljena 2005. godine, razvijena je na temeljima standarda BS 7799 (egl. British Standards), preciznije njegovog drugog dijela. Posljednja verzija ovog standarda je objavljena 2013. godine. U Bosni i Hercegovini standard ISO/IEC 27001 je usvojilo državno tijelo za standarde Bosne i Hercegovine, pa standard nosi i nacionalni prefiks i označava se kao BAS ISO/IEC 27001.

Ovaj standard propisuje metodologiju za primjenu upravljanja informacijskom sigurnošću i omogućava organizacijama dobijanje potvrde (sertifikata) od strane nezavsinog sertifikacijskog tijela o uspješnosti implementacije protokola i rješenja koji pružaju informacijsku sigurnost u skladu sa zahtjevima standarda ISO/IEC 217001.

Prednost implementacije ISO 27001 za organizaciju su:

- povećavanje povjerenja u poslovanje organizacije po pitanju sigurnosti podataka i informacija;

[22] Bijelić, Drago, Vodič kroz standardizaciju, pitanja i odgovori, Republički zavod za standradizaciju i metrologiju, Banja Luka, 2015, str. 23

[23] Urankar, Danijel, Mjere procjene sigurnosti i zaštite poslovnog korisnika, Fakultet prometnin znanosti, Sveučilište u Zagrebu, Zagreb, 2015

[24] Za više informacija posjetiti: https://gemserv.com/wp-content/uploads/2019/09/ISO-IEC-27001-and-GDPR-v1.0.pdf

- uticaj na smanjenje rizika od gubitka i/ili oštećenja informacija;
- jasno definisane odgovornosti na svim nivoima organizacije u vezi sa bezbjednošću informacija;
- potpuno usaglašavanje sa važećim zakonskim propisima;
- smanjenje troškova poslovanja;
- dobijanje konkurentske prednosti.[25]

ISO 27001 je moguće implemetirati u bilo kojoj organizaciji. Nastao je kao rezultat saradnje najboljih svjetskih stručnjaka sa polja informacijske sigurnosti. Ova serija standarda obuhvata standarde koji obezbjeđuju podršku, daju detaljna uputstva i instrukcije za cjelokupan proces planiraj-uradi-proveri-deluj PDCA (detaljnije objašnjeno kasnije u tekstu); daje uputstva i ocenjivanje usaglašenosti za ISMS.

Upotrebom serije standarda ISO 27001 organizacija dobija pomoć u procesima upravljanja tokovima informacija.

### *3.2. Struktura standarda ISO 27001*

Standard ISO 27001 je standard koga karakteriše široko polje djelovanja jer obuhvata više aspekata i to:

- informatički aspekt, koji obuhvata analizu i definisanje performasi IT opreme, administrativni aspekt, lozinke, prava pristupa, kripotovanje, te aspekt pojave rizika po sigurnost informacija;
- administrativni aspekt, u kom se definišu politike, uputstva i procedure u svrhu generisanja informacija, dalje upotrebe i na kraju skladištenja, odnosno arhiviranja; i
- fizički aspekt, koji se odnosi na utvrđivanje fizičkog nadzora u vidu video nadzora, evidencije zaposlenih, kontrole pristupa poslovnim prostorijama, zaštita pomenutih prostorija itd.

Često se pogrešno zaključuje da standard ISO 27001 pokriva samo sigurnost IT područja. Međutim, imajući u vidu aspekte djelovanja koje obuhvata za ovaj standard se može reći da se odnosi i na ,,upravljanje fizičkom i tehičkom zaštitom, ljudskim resursima, odnosima sa dobavljačima, partnerima i klijentima, zakonskim i regulatornim obavezama, kontinuitetom poslovanja i sl.”[26]

[25] Kokić, Momčilo i Tasevski Petar, Primena standarda ISO/IEC 27001 kao faktora konkurentske prednosti organizacija, Infoteh – Jahorina, 2016, str. 485-490

[26] Kulašin,Džemal,Unkić Faruk i Dalila Goran, Sistem upravljanja informacijskom sigurnošću prema standardu ISO/IEC 27001, Univerzitetska hronika – časopis Univerziteta u Travniku, 2012, str. 31-38

Standard je struktuiran u jedanaest poglavlja. Prva tri poglavlja su uvodna, dok preostala sadrže zahtjeve koje je svaka organizacija koja implementira ovaj standard u obavezi da ispoštuje.

Poglavlja standarda ISO 27001 su sljedeća:

- Poglavlje 0: Uvod (engl. Introduction). Predstavlja svrhu i kompatibilnost ISO 27001 sa drugim standardima.
- Poglavlje 1: Područje primjene (engl. Scope). Definiše opšte zahtjeve ISMS-a.
- Poglavlje 2: Upućivanje na standarde (engl. Normative references). Definiše ISO/IEC 27000 kao esencijalni standard za uspostavljanje ISMS-a.
- Poglavlje 3: Termini i definicije (engl. Terms and definitons). Navodi da se u ovom standardu primjenjuju termini i definicije sadržane u ISO/IEC 27000.
- Poglavlje 4: Kontekst organizacije (engl. Context of the organization). Jasno definiše organizacijski kontekst, te omogućava razumijevanje potreba i očekivanja „zainteresovanih strana". Definiše i područje primjene ISMS-a.
- Poglavlje 5: Liderstvo (engl. Leadership). Naglašava da najviše rukovodstvo mora da pokaže liderstvo i opredijeljenost za ISMS, definiše sigurnosnu politiku, a zatim i uloge, odgovornosti i ovlaštenja u organizaciji.
- Poglavlje 6: Planiranje (engl. Planning). Definiše aktivnosti po pitanju procjene i tretmana rizika, sačinjavanja izjave o primjenjljivosti SOA (engl. State of Applicability), te obaveze oko uspostavljanja ciljeva sigurnosti informacija i planiranja njihovog ostvarivanja.
- Poglavlje 7: Podrška (engl. Support). Navodi uslove neophodne za dostupnost resursa, kompetentnosti, savjesnosti, komunikacije, te obaveza oko dokumentovanja informacija,od kreianja, ažuriranja do upravljanja.
- Poglavlje 8: Funkcionisanje (engl. Operation). Definiše operativno planiranje i kontrolu, te model za procjenu i tretman rizika.
- Poglavlje 9: Ocjenjivanje performansi (engl. Performance evaluation). Određuje uslove za praćenje, mejerenje, analizu i vrjednovanje, internu reviziju, te postupke preispitivanja od rukovodstva.
- Poglavlje 10: Poboljšavanja (engl. Improvement). Definiše uslove vezane za neusklađenost, izmjene, korektivne mjere i stalna poboljšavanja ISMS-a.[27]

[27] Za više informacija posjetiti: http://www.iso27001security.com/html/27001.html

Poseban dio u standardu predstavlja Aneks A koji sadrži spisak sigurnosnih kontrola koje je neophodno primijeniti u cilju zaštite informacija. Jasno je da ovaj dokument predstavlja najvažniji dio standarda ISO 27001.

Sigurnosne kontrole Aneksa A (preciznije, 114 kontrola) raspoređene su u 14 sekcija, kako slijedi:

- A.5. Politike sigurnosti informacija (engl. Information security policies) – dvije kontrole
- A.6. Organizacija sigurnosti informacija (engl. Organization of information security) – sedam kontrola
- A.7. Sigurnost ljudskih resursa (engl. Human resource security) - šest kontrola
- A.8. Upravljanje imovinom (engl. Asset management) - deset kontrola
- A.9. Kontrola pristupa (engl. Access control) -četrnaest kontrola
- A.10. Kriptografija (engl. Cryptography) – dvije kontrole
- A.11. Fizička sigurnost i sigurnost okruženja (engl. Physical and environmental security) – petnaest kontrola
- A.12. Sigurnost operacija (engl. Operations security) - četrnaest kontrola
- A.13. Sigurnost komunikacija (engl. Communications security) - sedam kontrola
- A.14. Nabavka, razvoj i održavanje sistema (engl. System acquisition, development and maintenance) - trinaest kontrola
- A.15. Odnosi sa dobavljačima (engl. Supplier relationships) - pet kontrola
- A.16. Upravljanje incidentima sigurnosti informacija (engl. Information security incident management) - sedam kontrola
- A.17. Aspekti sigurnosti informacija u upravljanju kontinuitetom poslovanja (engl. Information security aspects of business continuity management) - četiri kontrole
- A.18. Usaglašenost (engl. Compliance) - osam kontrola [28]

Iz navedenog možemo zaključiti da pojedine sekcije u Aneksu A imaju različit broj sigurnosnih kontrola. Shodno tome možemo ocijeniti „težinu" određene sekcije. Potrebno je napomenuti da organizacija koja implementira standard ISO 27001 nije u obavezi da sprovede sve sigurnosne mjere koje su predviđene Aneksom. Broj mjera za sprovođenje isključivo zavisi od rezultata procjene rizika tokom uspostavljanja sistema za upravljanje informacijskom sigurnošću.

[28] Za više informacija posjetiti: https://advisera.com/27001academy/what-is-iso-27001/

### *3.3. Principi implementacije standarda ISO 27001*

Standard ISO 27001 se fokusira na zaštitu ključnih temelja sigurnosti informacija tzv, CIA trougao (slika 1.), odnosno na:

- povjerljivost (engl. Confidentiality), odnosno ograničenja u otkrivnaju informacija neovlaštenim licima;
- cjelovitost (engl. Integrity), odnosno obezbjeđivanje originalnosti i potpunosti informacija sprječavanjem neovlaštene izmjene sadržaja istih;
- raspoloživost (engl. Availability), odnosno dostupnost informacija samo ovlaštenim licima u trenutku kada su im potrebne.[29]


Slika 3. CIA bezbjedonosni trougao[30]

Pomenutu zaštitu je moguće sprovesti samo uspješnim prepoznavanjem potencijalnih problema koji se mogu desiti sa informacionim sistemom, te definisanjem mjera koje treba preduzeti da bi se takvi problemi spriječili. To ujedno predstavlja procjenu i tretman rizika, što je i suštinska filozofija standarda ISO 27001.

Osnova karakteristika kvaliteta i uspješnosti implementacije sistema upravljanja informacijskom sigurnošću može se prikazati Demingovim ili PDCA ciklusom (Plan-Do-Check-Act) (Slika 4.). U skladu sa ISO 9001 ovaj ciklus predstavlja jedno od osnovnih načela upravljanja kvalitetom i zasnovan je na pretpostavci da je za uspješno funkcionisanje organizacije neophodno utvrditi njene procese rada i njihovu povezanost, te upravljati njima na jednostavan i efikasan način. Sama metodologija se temelji na prethodno primijenjenom

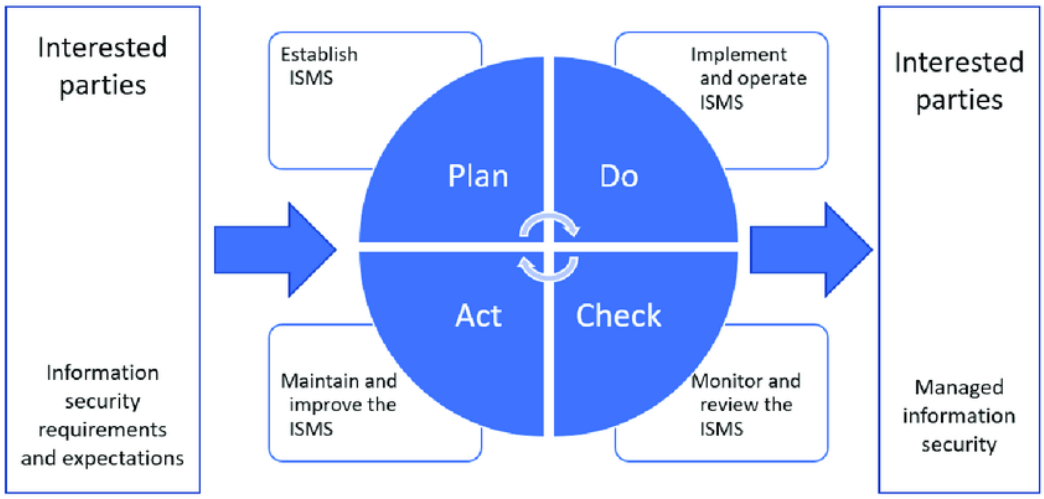
[29] Yee,Chai K. ,Zolkipli, Mohamad F., Review on Confidentiality, Integrity and Availability in Information Security, Journal of ICT in Education, 2021, vol 8. no 2.

[30] Nikander, Jussi, Menninen, Onni, Laajalahti, Mikko, Requirements for cybersecurity in agricultural communication networks, Computers and Electronics in Agriculture, 2020

procesnom prisupu i činjenici da se za sve identifikovane poslovne procese primjenjuju sljedeće radnje:

- planiranje (engl. Plan) i uspostavljanje ciljeva i procesa koji su neophodni za ostvarivanje rezultata u skladu sa zahtjevima zainteresovanih strana;
- primjenu procesa (engl. Do);
- nadzor i evaluacije procesa u odnosu na definisanu politiku, ciljeve i zahtjeve (engl. Check);
- preduzimanje aktivnosti za dalje poboljšavanje procesa (engl. Act).[31]

Interakcija PDCA metodologije i procesnog pristupa predstavljaju suštinu sistema upravljanja kvalitetom prema ISO 9001. Primjena PDCA modela na procese ISMS-a prikazana je na slici 3.




Slika 4. PDCA model primijenjen na procese ISMS -a[32]

Za ISMS koji obuhvata područje informacijsko-komunikacijskih tehnologija (IKT), procesni pristup je važan zbog brzine tehnoloških promjena i čestih sigurnosnih incidenata proisteklih kako iznutra, tako i izvan sistema. [33] U ovom kontekstu, PDCA ima drugačije značenje.

Politika, ciljevi i definisane mjere ISMS-a vezano za unapređenje informacijske sigurnosti predstavljaju „Plan-Planiraj" dio ISMS-a za ISO 27001. Zahtjevima korisnika i uspostavljanjem politike ISMS-a organizacija ulazi u fazu planiranja ISMS-a u kojoj se provode aktivnosti definisanja kriterijuma i metodologije za ocjenu rizika, kao i nivoi prihvatljivosti. Provođenje se odnosi na akcije prethodno definisanih mehanizama za

[31] Za više informacija posjetiti: https://www.svijet-kvalitete.com/index.php/upravljanje-kvalitetom/948-pdca-krug

[32] Donatas, Mažeika and Butleris Rimantas, MBSEsec: Model-Based Systems Engineering Method for Creating Secure Systems, Applied Siences, 2020, str. 1-18

[33] Kulašin,Džemal,Unkić Faruk i DalilaGoran, Sistem upravljanja informacijskom sigurnošću prema standardu ISO/IEC 27001, Univerzitetska hronika – časopis Univerziteta u Travniku, 2012, str. 31-38

upravljanje ciljevima, zatim na izradu i primjenu plana smanjenja rizika, edukacije za razvijanje svijesti o primjeni ISMS-a, upravljanje resursima, kontrole dokumenata, spremnošću na reagovanje u vanrednim situacijama i dr. Sve ove aktivnosti predstavljaju „Do-Sprovedi" dio ISMS-a prema ISO 27001.

U fazi „Check-Provjeri" prema ISO 27001 se izvršavaju aktivnosti preispitivanja ISMS-a po definisanim procedurama za:

- provođenje internih provjera;
- vrjednovanje neusaglašenosti;
- provođenje korektivnih i preventivnih mjera;
- upravljanje zapisima;
- ažuriranje planova za smanjenje rizika;
- mjerenje efektivnosti upravljačkih mehanizama i dr.

Dio „Act-Poboljšavanje" ISMS-a prema zahtjevima ISO 27001 se realizuje preko preispitivanja od strane rukovodstva koje zaokružuje cijeli ciklus djelovanja sistema upravljanja i vraća ga na početak, odnosno na planiranje (engl. Plan) koje treba da predstavlja nastavak ciklusa konstantnog poboljšavanja. Ovaj završni korak se provodi kroz postupke preuzimanja preventivnih i korektivnih mjera, provjerom održivosti poboljšanja i sl.

PDCA ciklus je moguće uočiti i u nekim zahtjevima samog standarda ISO 27001 i to:

- Planiranje (engl. Plan) u:
    - Poglavlju 4. Kontekst organizacije;
    - Poglavlju 5. Liderstvo;
    - Poglavlju 6. Planiranje;
- Sprovođenje (engl. Do) u:
    - Poglavlju 8. Funkcionisanje;
- Provjeravanje (engl. Check) u:
    - Poglavlju 9. Ocjenjivanje performansi;
- Poboljšavanje (engl. Act) u:
    - Poglavlju 10. Poboljšavanja.

PDCA ciklus je proces koji se stalno ponavlja i pruža osnovu za neprekidno unapređenje sistema upravljanja. Implementiranjem ISO 27001 organizacija pokazuje da ima jasan cilj u čvrstom opredjeljenju najvećeg rukovodstva za stalnim poboljšavanjem sistema upravljanja, kao i za stalnim intelektualnim i infrastrukturnim poboljšanjima postojećeg sistema.

### *3.4. Upravljanje sigurnošću informacija u zdravstvu*

U informacionim sistemima u zdravstvu evidentiraju se različite informacije o pacijentima, zaposlenima, opremi, poslovnim procesima i dr. Sve te informacije neophodno je da budu zaštićene sa aspekta povjerljivosti, cjelovitosti i raspoloživosti.

U zdravstvu se posebna pažnja posvećuje:

- povjerljivosti podatka, odnosno omogućavanju pristupa podacima samo od strane ovlaštenih osoba;
- cjelovitosti podataka, odnosno sprječavanju neovlaštenog mijenjena podataka o pacijentu, i
- raspoloživosti podataka, odnosno pravovremenoj dostupnosti sistema.

U zdravstvenim informacionim sistemima postoji više različitih tipova informacija koje je potrebno štiti, a neki od njih su:

- lični podaci pacijenata;
- metapodaci generisani sa ciljem istraživanja;
- informacije koje su izvedene iz zdravstvenih informacija pacijenata bez identifikacijskih podataka, a koje se koriste u statističke svrhe;
- kliničko/medicinsko znanje bez direktne poveznice sa pacijentom i njegovim ličnim podacima (npr. reakcije na lijekove);
- informacije o medicinskom osoblju, saradnicima i volonterima;
- informacije iz oblasti javnog nadzora i sudskih procesa;
- informacije koje su proizvodi obrade nekog kompjuterizovanog sistema (radiološki nalazi, laboratorijske analize);
- identifikacijski parametri korisnika sistema (lozinke, korisnička imena).

Usled ranjivosti sistema na ključne aspekte informacijske sigurnosti mogu uticati mnogi rizici koji mogu uključivati različite faktore:

- medicinske (bolničke infekcije, dijagnostičke greške i sl.);
- finansijske (loše upravljanje finansijama, velika zaduživanja i sl.);
- administrativne (nepoštovanje i/ili nepoznavanje zakona, propisa, i sl.);
- kadrovske (loša obučenost i/ili nestručnost odgovornih lica, nedostatak permanentne edukovanosti i sl.).

Zaštitom informacionih sistema neke rizike je moguće smanjiti na prihvatljiv nivo. Rizici sa najmanjim nivoom prihvatljivosti u medicinskim ustanovama su rizici od nedostupnosti podataka, neovlaštenog prisupa ili neovlaštene izmjene podataka pacijenata.

Standard ISO 27799 predstavlja standard za upravljanje sigurnošću informacija u sektoru zdravstva. Preduslov za uspješno upravljanje sigurnošću informacija predstavlja upravljanje rizicima.

Specifične prijetnje sigurnosti informacija i informacionih sistema u zdravstvu su:

- neovlašten pristup informacijama spolja i iznutra (zaboravljen logout, upotreba naloga drugog korisnika sistema);
- neautorizovana upotreba zdravstvenog informacionog sistema (loša autentifikacija korisnika, loša kontrola pristupa i upravljanje privilegijama korisničkih naloga);
- nezaštićenost sistema od malicioznog softvera (virusi, trojanci, crvi);
- presretanje interne komunikacije;
- odbijanje prijema ili slanja osjetljivih informacija zbog nepostojanja zaštite digitalnim potpisom;
- greške kod povezivanja na mrežne servise (neizmirene finansijske usluge ka internet provajderu, prekid usluga mobilnog operatera);
- pogrešno adresiranje osjetljivih podataka;
- hardverske greške (serveri, mrežna oprema, radne stanice);
- nepostojanje rezervnih varijanti kod vanrednih situacija (nestanka struje, požara, poplava);
- greške u funkcionisanju informacionog sistema (nemogućnost korištenja servisa, greške u povezivanju sa bazom);
- greške u funkciionisanju aplikativnog softvera (dotrajalost licenci i sigurnosnih sertifikata);
- greške operatera (sistem administratora, mrežnih administratora);
- greške u održavanju (loše urađeni servisi opreme);
- greške korisnika;
- manjak stručno kvalifikovanog osoblja;
- krađe podataka unutar/izvan organizacije;
- namjerno uništavanje opreme unutar/izvan organizacije.[34]

Može se zaključiti da je upravljanje rizicima po sigurnost informacija i informacionih sistema u zdravstvu vrlo kompleksna oblast. Obzirom da je cilj svake organizacije zaštita kritične imovine, to se i zaštiti informacija u zdravstvenim informacionim sistemima pridaje posebna važnost. Međutim, upravljanju zaštitom informacija u zdravstvu ne može se prići

[34] Božić, Velibor, Upravljanje informacijskom sigurnošću u zdravstvu, Medicinska informatika, 2013, str. 254-263

samo sa informatičkog aspekta, nego je potreban multidiciplinaran pristup kako bi se postigao željeni efekat.

# 4. ZAKONSKI OKVIR ZAŠTITE LIČNIH PODATAKA

Većina digitalnog okruženja kreirana je tako da stvara zavisnost korisnika od raznih aplikacija sa ciljem prikupljanja što veće količine podataka. Zaštita osnovnih ljudskih prava u sajber prostoru postala je veoma komplikovana iz razloga što digitalni svijet ne poznaje granice. Potreba za prenošenjem ličnih podataka digitalnim putem stvorila je preduslove za donošenje normativnih akata koji regulišu pravila tog prenosa.

Prvi normativni akt kojim je ličnim podacima dat značaj bila je Direktiva 95/46/E3 Evropske unije koja je predstavljala skup minimalnog broja pravila koja moraju biti ispunjena da bi se prenos ličnih podataka obavio u zakonskom okviru. Na osnovu tih smjernica zemlje članice Evropske unije donosile su svoje zakone o zaštiti ličnh podataka.

Nova Uredba Evropske unije o zaštiti ličnih podataka uvela je jedinstven kriterijum zaštite i omogućila svim građanima da imaju lakši pristup svojim podacima, kao i veoma jednostavan način informisanja o cilju obrade njhovih podataka.

U nastavku ovog poglavlja biće detaljnije pojašnjeni sledeći propisi:

- Zaštita ličnih podataka u zdravstvenim informacionim sistemima – principi i procesi za javno zdravlje Svjetske zdravstvene organizacije;
- Opšta uredba Evropske unije o zaštiti ličnih podataka (GDPR);
- Zakon o zaštiti ličnih podataka Bosne i Hercegovine.

## *4.1. Zaštita ličnih podataka u zdravstvenim informacionim sistemima – principi i procesi za javno zdravlje Svjetske zdravstvene organizacije*

Usled konstantne potrebe za obezbjeđivanjem zaštite podataka i provođenjem sajber bezbjednosti zemlje Evropske unije su bile primorane da uvode nove ili dopunjavaju stare zakone koje su se bavili pomenutom tematikom. Ovi zakonski akti imali su indirektan uticaj na zdravstvene informacione sisteme i aktivnosti u polju javnog zdravlja. Dokument Zaštita ličnih podataka u zdravstvenim informacionim sistemima – principi i procesi za javno zdravlje Svjetske zdravstvene organizacije usvojen 2011. godine ima za cilj da „istraži konceptualne implikacije i da da neke smjernice o tome sprovesti konkretne odluke koje neizbježno moraju da balansiraju između prava i interesa koji su u pitanju."[35]

Posebna pažnja u Smjernicama posvećena je istraživanju koncepta i principa zaštite podataka. Važno je napomenuti da zaštita podataka podrazumijeva praćenje jasno definisanih

[35] WHO, The protection of personal data in health information systems – principles and processes for public health, 2011. str.1

koraka za njenu uspješnu implementaciju u sistem upravljanja informacijama u zdravstvu. Takođe, usklađivanje zaštite podataka ne predstavlja skupu investiciju u smislu ulaganja u ljudske resurse ili tehnologije. Uz nekoliko koraka koji se lako primjenjuju, bilo koja organizacija u javnom zdravstvu može značajno povećati svoj nivo usklađenosti zaštite podataka. Ove smjernice omogućavaju određeni uvid u „provođenje“ zaštite podataka i kroz šest poglavlja precizno i jasno definišu principe zaštite ličnih podataka u zdravstvenim informacionim sistemima.

Pošto je zaštita podataka zasnovana na principima koji su evoluirali tokom vremena, drugo poglavlje daje kratak istorijski pregled, nakon čega slijedi opis pravnih principa zaštite podataka, principe vezane za informisani pristanak i transparentnost pri obradi podataka.[36] U trećem poglavlju je prikazana praktična primenu pomenutih principa, pa se ovo poglavlje bavi i pravima vlasnika podataka poput prava na pristup podacima, prava na informisanje, prava na prigovor, te prava na prenos podataka u različitim formatima (digitalnim, štampanim).[37] Četvrto poglavlje ispituje elemente koji trebaju biti u ravnoteži sa ovim pravima – posebno sa pravom na zdravlje i javno zdravlje uopšte. U cilju bezbjednosti informacionih tehnologija, javno zdravlje je u obavezi da se rukovodi istim standardima kao i bilo koja druga oblast.

U skladu sa tim obrađuje sledeće oblasti: zakonski okvir zaštite podataka u zdravstvenim informacionim sistemima, detaljno pojašnjenje načina zaštite podataka u zdravstvenim informacionim sistemima kroz ključna pravila zaštite podataka (povjerljivost, dostupnost, tačnost) i namjene prikupljenih podataka, te zaštitu podataka i IT bezbjednost.[38] U petom poglavlju ponovo se razmatra sekundarna upotreba podataka u svrhe javnog zdravlja i to kroz definisanje pravila upotrebe ličnih podataka kroz upravljanje zdravstvenim informacionim sistemima, za medicinska istraživanja, te postizanja ravnoteže između zaštite podataka i javnog zdravstva.[39] Šesto poglavlje daje pregled koraka koje treba preduzeti da bi se sve navedeno realizovalo, uz mehanizme podrške, nadzora, edukacija, internih kontrola u cilju stalnih poboljšanja.[40]

[36] WHO, The protection of personal data in health information systems – principles and processes for public health, 2011. str. 2-7
[37] WHO, The protection of personal data in health information systems – principles and processes for public health, 2011. str. 8-9
[38] WHO, The protection of personal data in health information systems – principles and processes for public health, 2011. str 10-14
[39] WHO, The protection of personal data in health information systems – principles and processes for public health, 2011. str 15-18
[40] WHO, The protection of personal data in health information systems – principles and processes for public health, 2011. str 19-22

### *4.2. Opšta uredba Evropske unije o zaštiti ličnih podataka (GDPR)*

Opšta uredba evropskog parlamenta i Savjeta Evropske unije o zaštiti lica u vezi sa obradom ličnih podataka (engl. The EU General Data Protection Regulation – GDPR) donijeta je 2016. godine. Nastala je na temeljima Direktive 95/46/E3 i omogućila je povećanje sigurnosti pojedinaca u vezi sa obradom njihovih ličnih podataka. Time se nastojalo postići jačanje povjerenja u rukovaoce i obrađivače podataka i nesmetano kretanje podataka kako na tradicionalnom, tako na digitalnom tržištu. Ovome je trebao doprinijeti jedinstven usklađen pravni okvir i usklađena primjena propisa na teritoriji Evropske unije, jasnije definisane obaveze rukovaoca i obrađivača podataka, precizija pravila za zaštitu podataka, kao i njihovo iznošenje van granica Evropske unije. Prema članu 2. Uredbe ovaj propis se primjenjuje na „obradu podataka o ličnosti koja se u cjelosti ili djelimično obavlja automatski" kao i na „neautomatizovanu obradu podataka o ličnosti koji čine dio zbirke podataka ili su namijenjeni zbirci podataka".[41]

Uredba ima primjenu i na kontrolore podataka van Evropske unije koji se bave obradom podataka građana EU. Takođe donosi mnogo novosti, a najvažnija je ta da su ojačana prava nosioca podataka i obaveze onih koji obrađuju lične podatke. Uvode se nove i pojednostavljuju neke već postojeće definicije odnosno preciznije opisuju postojeći pojmovi, određuju biometrijski i genetski podaci, smanjuju i pojednostavljuju pojedine administrativne obaveze voditelja zbirke ličnih podataka, a ujedno i jačaju nadzorna ovlašćenja, kao i mogućnost izricanja kazni od strane tijela za zaštitu ličnih podataka. [42]

Za obične građane GDPR je omogućio lakši pristup njihovim ličnim podacima i načinu i svrsi njihove obrade. Uredba definiše „pravo na zaborav" preciznije mogućnost da sam građanin zatraži od organizacija koje su vršile prikupljanje njegovih podataka brisanje istih iz baze organizacije. Takođe naglašava da je sam obrađivač dužan da obavijesti nadzorno tijelo ukoliko je došlo do povrede zaštite ličnih podataka. U određenim stavkama Uredba naglašava potrebu za obavještavanjem nosica podataka o narušavanju sigurnosti njegovih ličnih podataka. Takođe se definiše potreba za imenovanjem službenika za zaštitu podataka.

Imajući u vidu da djeca pripadaju ranjivoj skupini, Uredba prepoznaje važnost nadzora nad njihovim ličnim podacima i dozvoljava djeci, izričito uz roditeljsku saglasnost, upotrebu usluga i servisa internet mreže koji koriste lične podatke.

---

[41] Opšta uredba Evropske unije o zaštiti ličnih podataka, 2016, član 2

[42] Za više informacija posjetiti: http://azlp.ba/GDPR_Menu/Sta_je_GDPR/default.aspx?id=2373&langTag=bsBA&template_id=149&pageIndex=1

Novi propisi definisani Uredbom odnose se u istoj mjeri na sve organizacije i preduzeća. Manje organizacije i preduzeća neće biti pod strogim nadzorom, ali veće organizacije i preduzeća, naročito one koje prikupljaju i obrađuju velike količine podataka (informatičke kompanije, banke, preduzeća za vele i malo prodaju, osiguravajuće agencije, ustanove koje pružaju zdravstvene usluge i dr.) u obavezi su da definišu kategorije podataka koje obrađuju i u skladu sa tim da im obezbjede adekvatnu zaštitu.

Propisi iz člana 25. definišu primjenu zaštitnih (tehničkih i integrisanih) mjera u sam postupak proizvodnje, odnosno obrade. Naglašeno je da je primjena zaštite privatnosti podataka na visokom nivou neophodna od samog početka obrade podataka, te da je obrađivač u obavezi da obezbjedi odgovarajuće mehanizme, kako tehničke, tako proceduralne, da spriječi obradu ličnih podataka za koje nije definisana svrha obrade.

U izvještaju Agencije Evropske unije za mrežnu i informacionu sigurnost navodi se da sve aktivnosti vezane za zaštitu podataka u vidu enkripcije i dekripcije moraju da se obavljaju lokalno jer je neophodno da ključevi budu u vlasništvu obrađivača podataka, kako bi se ispoštovala zaštita privatnosti podataka u potpunosti. Takođe navodi da je skladištenje podataka na „cloud" dozvoljeno u slučaju gdje jedino vlasnik podataka ima ključeve za dekripciju.

Primjena novih propisa o zaštiti ličnih podataka na nivou Bosne i Hercegovine odvijaće se posredstvom Zakona o zaštiti ličnih podataka Bosne i Hercegovine. Za sada nije moguće procijentiti do koje mjere će se stavke nove Uredbe odraziti na poslovanje javnih i privatnih organizacija i preduzeća u Bosni i Hercegovini. Jasno je samo da svaka obrada ličnih podataka mora imati precizno definisanu svrhu, te da mora biti usaglašena sa EU standardima i važećim zakonodavstvom Bosni i Hercegovini.

### *4.3. Zakon o zaštiti ličnih podataka Bosne i Hercegovine*

Zakon o zaštiti ličnih podataka Bosne i Hercegovine usvojen je 2006. godine. Izmjene i dopune zakona urađene u 2011. godine. Cilj ovog Zakona je da se „na teritoriji Bosne i Hercegovine svim licima, bez obzira na njihovo državljanstvo ili prebivalište, osigura zaštita ljudskih prava i osnovnih sloboda a naročito prava na privatnost i zaštitu podataka u pogledu obrade ličnih podataka koji se na njih odnose."[43] Primjenjuje se na „lične podatke koje obrađuju svi javni organi, fizička i pravna lica."[44]

[43] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 1
[44] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 2

Navedeni zakon je dobio na značaju razvojem modernog poslovanja, baziranog na elektronskom prikupljanju i obradi podataka. Aktivna upotreba novih informacionih tehnologija prouzrokovala je sve češću zloupotrebu ličnih podataka korisnika. Nerazvijena svijest pojedinaca o načinima zaštite ličnih podataka dovela je do zloupotrebe navedenih podataka najčešće u svrhe marketinga i plasiranja proizvoda. Na internet portalima se ne mogu često naći smjernice za zaštitu ličnih podataka. U Zakonu o zaštiti ličnih podatka Bosne i Hercegovine u glavi 2. definisani su osnovni principi zakonite obrade ličnih podataka. U članu 5. naglašeno je da je brada ličnih podataka dozvoljena isključivo uz pristanak nosioca, odnosno vlasnika podataka. Prije bilo kakvog prikupljanja i obrade podataka, vlasnik podataka mora biti obavješten o tome i dati svoju saglasnost.[45] Članom 6. uređuju se uslovi obrade ličnih podataka bez saglasnosti vlasnika podataka. Zakon obavezuje kontrolora da prije obrde podataka provjeri njihovu autentičnost i tačnost[46], te da obavezno ,,poštuje prava na zaštitu privatnog i ličnog života nosioca podataka".[47] U članu 11. naglašava se da se ,,kontrolor podataka i, u okviru svoje nadležnosti, obrađivač podataka staraju o bezbjednosti podataka te preduzimaju sve tehničke i organizacione mjere i utvrđuju pravila postupka, koji su neophodni da bi se sproveo ovaj zakon i drugi propisi u vezi sa zaštitom i tajnošću podataka." Obaveze čuvanja tajnosti podatka preciznije su definisane u članu 16. dok se članom 17. definišu uslovi za davanje podataka trećoj strani, pa se tako navodi da ,,kontrolor podataka ne može da daje lične podatke trećoj strani prije nego što o tome obavijesti nosioca podataka. Ako nosilac podataka ne odobri da se daju lični podaci, oni ne mogu da se otkriju trećoj strani osim ako to nije u javnom interesu."[48] Članom 20. preciziran je način obrade podataka u statističke, istorijske i naučne svrhe.

U glavi 3. Zakona o zaštiti ličnih podatka BiH definisana su prava nosioca podataka. Tako je članom 22. definisano da ,,kontrolor podataka prije nego što počne da prikuplja podatke obavještava nosioca podataka, ako on o tome već nije obaviješten"[49]. U članu 24. kojim je regulisano pravo o pristupu ličnim podacima naglašeno je da ,,kontrolor podataka obavještava nosioca podataka na njegov zahtjev o toku obrade njegovih podataka koju vrši kontrolor ili obrađivač podataka, svrsi obrade podataka, zakonskoj osnovi i trajanju obrade, da li su podaci pribavljeni od nosioca podataka ili od treće strane i o pravu na pristup ličnim podacima, kao i o tome ko je primio ili ko će da primi podatke i za koju svrhu."[50] Ispravljanje, brisanje i blokiranje podataka vrši se na zahtjev nosioca podataka ali samo za podatke koje se utvrdi da

[45] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 5
[46] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 7
[47] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 8
[48] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 17
[49] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 22
[50] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 24

su „netačni ili da su pogrešno navedeni ili obrađeni na drugi način koji je suprotan zakonu i pravilima koji se odnose na obradu podataka."[51] U situacijama sumnje na povredu prava zaštite ličnih podataka nosilac podataka ima pravo da podnese prigovor Agenciji za zaštitu ličnih podataka Bosne i Hercegovine što je definisano članom 30.

U glavi 4. Zakona o zaštiti ličnih podataka Bosne i Hercegovine definisana su sva pitanja vezana za „funkcionisanje Agencije kao upravne organizacije, kao što je donošenje pravilnika o unutrašnjoj organizaciji i ostalih podzakonskih propisa, upravni nadzor, odnos između institucija Bosne i Hercegovine, te odnos Agencije prema pravnim i fizičkim licima".[52]

U glavi 5. navedene su odgovarajuće kaznene odredbe u slučaju kršenja pravila koja su propisana ovim Zakonom.

Imajući u vidu da veliki broj problema vezanih za zaštitu ličnih podataka nastaje usled nedostatka pravne pismenisti građana Bosne i Hercegovine po pitanju zaštite ličnih podataka, jasno je da Zakon sam po sebi nije dovoljan da bi spriječio sve zloupotrebe ličnih podataka građana, nego da je neophodno da svaki pojedinac postupa sa velikom pažnjom sa svojim ličnim podacima, te da se redovno informiše o svrsi prikupljanja i obrade ličnih podataka posebno na internet servisima. Jedino se tako može efikasno uticati na smanjenje slučajeva zloupotrebe ličnih podataka.

[51] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 27

[52] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 34

# 5. UPRAVLJANJE ZAŠTITOM LIČNIH PODATAKA U INTEGRISANOM ZDRAVSTVENOM INFORMACIONOM SISTEMU REPUBLIKE SRPSKE

U ovom poglavlju biće analizirano upravljanje zaštitom ličnih podataka u integrisanom zdravstvenom informacionom sistemu Republike Srpske kroz definisanje funkcionalnosti i primjene, organizaciju, upravljanje i pristup podacima, kao i usklađenost sa odredbama Zakona o zaštiti ličnih podataka Bosne i Hercegovine.

## *5.1. Funkcionisanje i namjena integrisanog zdravstvenog informacionog sistema*

U Republici Srpskoj je od 2020. godine u aktivnoj upotrebi integrisani zdravstveni informacioni sistem (u daljem tekstu: IZIS) koji je u vlasništvu Fonda zdravstvenog osiguranja Republike Srpske (FZO RS). Navedeni sistem funkcioniše po principu uvezivanja podataka iz više republičkih ustanova (Agencija za identifikacione dokumente, evidenciju i razmjenu podataka Bosne i Hercegovine - IDDEEA, Ministarstvo unutrašnjih poslova Republike Srpske, Fond zdravstvenog osiguranja Republike Srpske, Ministarstvo zdravlja i socijalne zaštite RS, Institut za javno zdravstvo, Agencija za sertifikaciju, akreditaciju i unapređenje kvaliteta zdravstvene zaštite Republike Srpske - ASKVA, Agencija za lijekove i medicinska sredstva RS, javne zdravstvene ustanove primarnog, sekundarnog i tercijarnog nivoa, apoteke) a sve u cilju unapređenja sistema zdravstvene zaštite. (slika 5.)

Ovim projektom izvršeno je povezivanje zdravstvenih ustanova različitih nivoa zdravstvene zaštite u jedinstven sistem koji omogućava razmjenu medicinskih podataka pacijenata uz formiranje jedinstvenog elektronskog zdravstvenog kartona za svakog stanovnika Republike Srpske. Projekat sadrži i komponente poput elektronske uputnice, elektronskog recepta te elektronske kartice zdravstveno osiguranih lica i zdravstvenih radnika. Aktivnom upotrebom sistema formira se jedinstvena baza podataka o zdravstvenom stanju korisnika usluga u zdravstvenim ustanovama u Republici Srpskoj.


Slika 5. Šema IZIS-a[53]

IZIS se organizuje i razvija radi planiranja i efikasnog upravljanja sistemom zdravstvene zaštite, pristupa zdravstvenim podacima i efikasnosti pružanja zdravstvenih usluga i poboljšanja kvaliteta, kao i prikupljanja i obrade podataka u vezi sa zdravstvenim stanjem stanovništva, funkcionisanjem zdravstvene službe, odnosno prikupljanja i obrade zdravstvenih informacija, te evidencije iz oblasti zdravstvenog osiguranja.

*5.2. Način organizovanja podataka u integrisanom zdravstvenom informacionom sistemu*

Razvoj i održavanje IZIS-a vrši se od strane Fonda zdravstvenog osiguranja RS kroz centralno mjesto IZIS-a, odnosno organizacionu jedinicu za razmjenu zdravstvenih podataka. Prije IZIS-a prikupljanje podataka realizovano je na više lokacija. FZO RS je putem regionalnih filijala prikupljao podatke vezano za usluge konsultativno-specijalističke zdravstvene zaštite (KSZ), dio evidencije dijagnostičkih i bolničkih usluga. Institut za javno zdravstvo prikupljao je podatke vezane za evidenciju o zaraznim bolestima dok je Agencija za sertifikaciju i akreditaciju RS prikupljala i obrađivala indikatore kvaliteta zdravstvenih usluga, te putem svojih servisa omogućavala obračun bolničkih usluga.

Uvođenjem IZIS-a omogućeno je „generisanje, pohranjivanje i razmjena podatka između svih ustanova i institucija koje koriste IZIS”[54] u okviru jedne organizacione jedinice koja je

[53] Za više informacija posjetiti: https://www.zdravstvo-srpske.org/novosti/pocela-integracija-privatnih-ustanova-u-izis.html

sastavni dio Fonda zdravstvenog osiguranja. Izvor podataka IZIS-a su zdravstvene ustanove, koje u sklopu svog rada prikupljaju neophodne podatke.

Način prikupljanja podataka je omogućen na dva načina:

1) upotrebom aplikacija Centralnog aplikativnog sistema,

2) upotrebom servisa Centralnog integracionog sistema.

Centralni aplikativni sistem prikuplja podatke iz modula koji je direktno implementiran korisnicima u zdravstvenim ustanovama koje nisu imale ili nisu zadržale svoj informacioni sistem. Centralni aplikativni sistem čine:

- podsistem primarne zdravstvene zaštite;
- podsistem konsultativno-specijalističke zaštite (primarni i vanbolnički);
- bolničko-klinički podsistem.

Ovaj sistem funkcioniše po principu prikupljanja medicinskih podataka (engl. Electronic Medical Record - EMR) na nivou određene zdravstvene ustanove (doma zdravlja ili bolnice). Za poslovanje svake službe, odjeljenja ili odsjeka kreiran je adekvatan aplikacioni modul čime je omogućeno da se „lični podaci prikupljaju za posebne, izričite i zakonite svrhe i ne obrađuju na bilo koji način koji nije u skladu s tom svrhom".[55]

U cilju formairanja elektronskog zdravstvenog kartona (engl. Electronic Health Record - EHR) omogućen je vid povezivanja ustanova putem elektronskih servisa IZIS-a. Centralni integracioni sistem se sastoji od:

- podsistema elektronskog zdravstvenog kartona (EHR);
- podsistema elektronskih uputnica – eUputnica;
- podsistema elektronskih recepata – eRecept;
- podsistema za elektronsku razmjenu nemedicinskih podataka uz formiranje jedinstvenih registara;
- podsistema za administraciju.

EHR omogućava adekvatno smještanje i razmjenu medicinskih podataka i sadrži odgovarajuće komponente za povezivanje sa institucijama koje su veoma bitne za njegovo funkcionisanje, kao npr. Ministarstvo unutrašnjih poslova Republike Srpske u cilju validacije ličnih podataka pacijenata[56],Poslovno informacioni sistem Fonda zdravstvenog osiguranja u cilju provjere statusa osiguranja pacijenata, ažuriranja liste lijekova, liste medicinskih usluga i

[54] Uredba o integrisanom zdravstvenom informacionom sistemu, 2018, član 8.

[55] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 4, stav b

[56] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 7, stav 1

sl. Time je omogućeno da sistem obrađuje „samo autentične i tačne lične podatke, te da ih ažurira kada je to potrebno".[57]

Podsistem elektronskih uputnica pruža mogućnost upravljanja elektronskim uputnicama na nivou cijelog sistema. Nezavisno od toga da li se ustanova odlučila za upotrebu Centralnog aplikativnog sistema ili Centralnog integracionog sistema IZIS „lične podatke čuva u obliku koji dozvoljava da se nosioci podataka identifikuju ne duže no što je to potrebno za svrhu u koju se podaci prikupljaju ili dalje obrađuju."[58] Podisistem elektronskih recepata omogućava razmjenu elektronskih recepata između zdravstvenih ustanova i apoteka. Time je omogućena „obrada ličnih podataka samo u mjeri i obimu koji je neophodan da bi se ispunila određena svrha".[59] Podsistem za administraciju omogućava administratorima sistema upravljanje korisnicima sistema, organizacionim jedinicama i osnovnim šifarnicima.

Svaki od navedenih podsistema razdvojen je cjelinama koje omogućavaju „da se lični podaci koji su prikupljeni u različite svrhe ne objedinjuju ili kombinuju."[60]

### *5.3. Osvrt na usklađenost integrisanog zdravstvenog informacionog sistema sa Zakonom o zaštiti ličnih podataka Bosne i Hercegovine*

Zakonom o zaštiti ličnih podataka Bosne i Hercegovine pravno je uređena zaštita ličnih podataka svih lica na teritoriji Bosne i Hercegovine. Svrha ovog zakona je da obezbjedi svim licima u Bosne i Hercegovine zaštitu prava na privatnost i zaštitu njihovih ličnih podataka koji se obrađuju u sistemima na prostoru Bosne i Hercegovine. Primjer jednog takvog sistema predstavlja integrisani zdravstveni informacioni sistem Republike Srpske (IZIS). U nastavku ovog poglavlja biće detaljno razmotreni osnovni principi zaštite ličnih podataka u IZIS-u sa zahtjevima definisanim Zakonom o zaštiti ličnih podataka Bosne i Hercegovine.

U Zakonu o zaštiti ličnih podataka Bosne i Hercegovine u članu 2. naglašeno je da se „ovaj zakon primjenjuje na lične podatke koje obrađuju svi javni organi, fizička i pravna lica"[61] što obuhvata zdravstvene podatke prikupljene iz javnih zdravstvenih ustanova, privatnih zdravstvenih ustanova i od osiguranika lično.[62]

U članu 4. se kroz principe obrade ličnih podataka naglašavaju obaveze kontrolora, odnosno Fonda zdravstvenog osiguranja kroz centralni aplikacioni i integracioni sistem IZIS-a. U stavu b se izričito navodi obaveza kontrolora da „lične podatke koje prikuplja za

[57] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 4, stav d
[58] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 4, stav g
[59] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 4, stav c
[60] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 4, stav h
[61] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 2
[62] Uredba o integrisanom zdravstvenom informacionom sistemu, 2018, član 5

posebne, izričite i zakonite svrhe ne obrađuje na bilo koji način koji nije u skladu s tom svrhom"[63] što u IZIS-u predstavlja prikupljanje zdravstvenih podataka iz aplikacionih modula svake službe, odjeljenja ili odsjeka u centralni sistem. Stav c u kome je definisano da se vrši ,,obrada ličnih podataka samo u mjeri i obimu koji je neophodan da bi se ispunila određena svrha"[64] realizovan je kroz podsistem razmjene elektronskih recepata između zdravstvenih ustanova i apoteka. Realizacijom elektronskog recepta ispunjava se zahtjev stava f odnosno pravila da se prikupljeni lični podaci ,,obrađuju samo u vremenskom periodu koji je neophodan da bi se ispunila svrha za koju su podaci prikupljeni".[65]

,,Obrađivanje samo autentičnih i tačnih ličnih podataka" i njihovo ,,ažuriranje kada je to potrebno"[66] iz stava d osigurano je kroz ažuriranje liste lijekova i liste medicinskih usluga u poslovnom infomacionom sistemu Fonda zdravstvenog osiguranja Republike Srpske. Omogućavanjem razmjene elektronskih uputnica između različitih modula (aplikacija ili servisa) IZIS ispunjava zahtjeve iz stava g jer ,,lične podatke čuva u obliku koji dozvoljava da se nosioci podataka identifikuju ne duže nego što je to potrebno za svrhu u koju se podaci prikupljaju ili dalje obrađuju".[67] Stav h koji kaže da je potrebno da se ,,lični podaci koji su prikupljeni u različite svrhe ne objedinjuju ili kombinuju"[68] je ispunjen kroz razdvojenost podsistema IZIS-a.

Član 5. se bavi zahtjevima vezanim za saglasnost nosioca podataka. U IZIS-u je nosilac podataka osiguranik (fizičko lice) koje popunjavanjem zahtjeva za vođenje elektronskog kartona daje saglasnost iz stava 2. koja služi ,,za obradu posebne kategorije ličnih podataka" i ,,mora da bude u pisanoj formi".[69] Saglasnost iz ove stavke ,,mora da potpiše nosilac podataka, mora da ima tačnu naznaku podataka u vezi sa kojima se saglasnost daje, te mora da sadrži ime kontrolora, svrhu i vremenski period na koji se saglasnost daje."[70] Fizički dokument saglasnosti se predaje filijali Fonda zdravstvenog osiguranja kojoj korisnik osiguranja pripada a gdje ostaje arhiviran po pravilima Zakona o evidenciji medicinske dokumentacije čime su ispunjene stavke 4. i 5. ovog člana.

Uslovi za sticanje prava na obradu ličnih podataka bez saglasnosti nosioca podataka definisani su u članu 6. i članu 7. Prikupljanjem podataka iz elektronskog kartona pacijenta (nosioca podataka) o obavljenim zdravstvenim uslugama, realizovanim terapijama, korištenim

[63] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 4, stav b
[64] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 4, stav c
[65] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 4, stav f
[66] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 4, stav d
[67] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 4, stav g
[68] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 4, stav h
[69] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 5, stav 2
[70] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 5, stav 2

medicinskim sredstvima, zaraznim oboljenjima i slično, sa ciljem izvještavanja viših instanci zdravstvenog sistema Republike Srpske (Ministarstva zdravlja i socijalne zaštite Republike Srpske, Instituta za javno zdravlje Republike Srpske, Agencije za lijekove i medicinska sredstva Republike Srpske, a po obavezama iz Zakona o zdravstvenoj zaštiti Republike Srpske), ispunjavaju se zahtjevi iz člana 6. i to:

- zahtjev iz stava a koji glasi da ,,ako kontrolor vrši obradu ličnih podataka u skladu sa zakonom ili je obrada neophodna da bi se ispunile nadležnosti utvrđene zakonom"[71] i
- zahtjev iz stava d koji glasi ,,ako je obrada ličnih podataka potrebna da bi se ispunio zadatak koji se izvršava u javnom interesu"[72].

Samim tim zadovoljena je uslovljenost koja je definisana članom 6. a koja kaže da ,,kontrolor može da obrađuje podatke bez saglasnosti nosioca podataka ako je ispunjen jedan od navedenih uslova"[73].

Član 7. određuje dužnosti vezane za provjeru autentičnosti i tačnosti podataka. U IZIS-u je ovaj član ispoštovan kroz provjeru podataka za zaposlene i pacijente kroz servis koji povezuje centralnu bazu IZIS-a sa Ministarstvom unutrašnjih poslova Republike Srpske. Upotrebom korisničkih zdravstvenih kartica u sistemu se vrši identifikacija zaposlenog a putem elektronske knjižice identifikuje se osiguranik.

Svaka uputnica i svaki kreirani nalaz ili otpust imaju svoj identifikacioni broj kojim su jednoznačno prepoznati kroz sistem. Objedinjavanje svih uputnica i nalaza koji su kreirani za jednog osiguranika (nosioca podataka) vrši se u elektronskom medicinskom kartonu osiguranika, poštujući „prava na zaštitu privatnog i ličnog života nosioca podataka".[74] Navedeni dokumenti se mogu povezivati isključivo u IZIS sistemu, za svakog osiguranika ponaosob, nezavisno od tipa uputnice, vrste nalaza, odjeljenja ili ustanove u kojoj je pacijent boravio. Shodno svim navodima ispunjeni su svi uslovi izrečeni u članu 8.

Član 11. jasno definiše stavke vezane za bezbjednost podataka. Kroz Politiku bezbjednosti integrisanog zdravstvenog informacionog sistema Fond zdravstvenog osiguranja je detaljno obradio i predočio sve postupke „o bezbjednosti podataka te preduzimanju svih tehničkih i organizacionih mjera i utvrđivanja pravila postupka, koji su neophodni da bi se sproveo ovaj zakon kao i drugi propisi u vezi sa zaštitom i tajnošću podataka"[75]. Tehničke mjere navedene

[71] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 6, stav a
[72] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 6, stav d
[73] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 6
[74] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 8
[75] Politika bezbjednosti integrisanog zdravstvenog informacionog sistema Republike Srpske, 2018, član 11

su u poglavlju „Politika fizičke bezbjednosti" dok je organizaciona bezbjednost IZIS-a definisana u poglavlju „Politika kontrole pristupa", autentifikacija i autorizacije korisnika.
Stav 3. koji kaže da je „javni organ kao kontrolor dužan da, u okviru svojih nadležnosti, donese propis s ciljem sprovođenja ovog Zakona"[76] ispunjen je postojanjem Politike bezbjednosti integrisanog zdravstvenog informacionog sistema.

Svaki korisnik IZIS-a, nezavisno od pozicije koju ima u sistemu, dužan je da potpiše Izjavu o čuvanju poslovne tajne, pristupu raučnarskim sistemima, pravima intelektualnog vlasništva, obavezi povrata informacija i pravu nadzora propisanu od strane FZO RS u kojoj su sadržane stavke kojima su ispunjene obaveze iz stava 2. a koje se odnose na „mjere protiv neovlašćenog ili slučajnog pristupa ličnim podacima, mijenjanja, uništavanja ili gubitka podataka, neovlašćenog prenosa, drugih oblika nezakonite obrade podataka, kao i mjere protiv zloupotrebe ličnih podataka.".[77]

Politikom bezbjednosti IZIS-a obuhvaćen je i plan odgovora na bezbjednosne incidente[78] kojim su „ određene tehničke i organizacione mjere za bezbjednost ličnih podataka"[79] i time ispunjen stav 4.

Obaveze čuvanja tajnosti podataka nabrojane su u članu 16. Pod stavom 1. naznačeno je da „zaposleni kod kontrolora ili obrađivača i ostala lica koja rade na obradi ličnih podataka na osnovu ugovora sa kontrolorom ili obrađivačem mogu da obrađuju lične podatke samo pod uslovima i u obimu koje odrede kontrolor ili obrađivač"[80] što se kroz IZIS odnosi na administratore zdravstvenih ustanova, odnosno, na sve korisnike IZIS sistema kojima je kroz ovlašćenje rukovodstva zdravstvenih ustanova data saglasnost za pristup IZIS-u.

Potpisivanjem Izjave o čuvanju poslovne tajne, pristupu raučnarskim sistemima, pravima intelektualnog vlasništva, obavezi povrata informacija i pravu nadzora propisanu od strane FZO RS svi korisnici sistema IZIS iz stava 2. odnosno „zaposleni kod kontrolora ili obrađivača, ostala fizička lica koja obrađuju lične podatke na osnovu ugovora zaključenog sa kontrolorom ili obrađivačem i ostala lica koja u okviru primjene zakonom propisanih prava i obavljanja dužnosti dođu u kontakt sa ličnim podacima u prostorijama kontrolora ili obrađivača" pod krivičnom i materijalnom odgovornošću su „dužna da čuvaju tajnost ličnih podataka i da se pridržavaju utvrđenog načina obezbjeđivanja".[81]

[76] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 11, stav 3
[77] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 11, stav 2
[78] Politika bezbjednosti integrisanog zdravstvenog informacionog sistema Republike Srpske, 2018, član 18
[79] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 11, stav 4
[80] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 16, stav 1
[81] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 16, stav 2

Kroz Izjavu o čuvanju poslovne tajne, pristupu računarskim sistemima, pravima intelektualnog vlasništva, obavezi povrata informacija i pravu nadzora, i član 17. stav 2. Uredbe o IZIS-u ispunjeni su zahtjevi stava 3. i stava 4. da „lični podaci koje obrađuju kontrolor ili obrađivač podataka za zaposlene,, predstavljanju službenu tajnu"[82]

Obrada podataka „za potrebe statistike, istorije i nauke bez saglasnosti nosioca podataka"[83] a „uz poštovanje prava na zaštitu privatnosti i ličnog života nosioca podataka"[84] realizovano je kroz Uredbu o IZIS-u u članu 17, stav 1. Time su ispunjeni zahtjevi navedeni u članu 20. Zakona o zaštiti ličnih podataka Bosne i Hercegovine. Nosilac podataka, odnosno pacijent, se ne obavještava o obradi ličnih podataka u navedenim situacijama, a po zahtjevu člana 24. stav 2, alineja 1.

U članu 24. stav 1. naglašeno je da se nosilac podataka (pacijent), na svoj lični zahtjev, obavještava o „ toku obrade njegovih podataka koju vrši kontrolor ili obrađivač podataka, svrsi obrade podataka, zakonskoj osnovi i trajanju obrade, da li su podaci pribavljeni od nosioca podataka ili od treće strane i o pravu na pristup ličnim podacima, kao i o tome ko je primio ili ko će da primi podatke i za koju svrhu."[85] Primjena ovog člana ogleda kroz aktivnu upotrebu elektronskog kartona pacijenta od strane porodičnog ljekara, elektronske recepte i nalaze koji se na licu mjesta pojašnjavaju pacijentu, te upućivanju na dalje liječenje putem elektronskih uputnica.

Posebna pažnja se poklanja bezbjednosti posebno osjetljivih kategorija medicinskih podataka pa se pacijent ne obavještava ni u zahtjevu definisanom kroz član 24. stav 2. alineju 2, odnosno da „podatak ili činjenica da su podaci bili pohranjeni mora biti održana u tajnosti na osnovu zakona ili s obzirom na njihovu vrstu, posebno zbog prevladavajućeg opravdanog interesa treće strane"[86] Ovi podaci, kao i ostala medicinska dokumentacija se štite „od neovlašćenog pristupa, uvida, kopiranja i zloupotrebe, nezavisno od oblika u kom su podaci sačuvani".[87]

### *5.4. Uloga administratora integrisanog zdravstvenog informacionog sistema Republike Srpske*

Administratori baza podataka u Fondu zdravstvenog osiguranja Republike Srpske (tzv. super administratori) imaju pristup i mogućnost upravljanja podacima o zaposlenima u

[82] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 16, stav 3
[83] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 20, stav 2
[84] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 20, stav 3
[85] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 24, stav 1
[86] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 24, stav 2, alineja 2
[87] Uredba o integrisanom zdravstvenom informacionom sistemu, 2018, član 17, stav 2

zdravstvenim ustanovama. Uspostavljeni su principi delegirane administracije kojima se odgovarajuće procedure i mehanizmi za dodjeljivanje prava pristupa sistemu radnicima ustanove prenose na administratore zdravstvenih ustanova (tzv. administratori sa prenesenim pravima pristupa). Na taj način su omogućeni višestruki nivoi bezbjednosti prilikom autentifikacije i autorizacije korisnika.[88]

Pristup Centralnom aplikativnom sistemu IZIS-a odvija se kroz autorizovan pristup fizičkih lica kojima je putem Podsistema za administraciju IZIS-a dodijeljeno pravo pristupa u skladu sa ovlašćenjima za obavljanje određenih poslova[89] za administratora sistema. Prema Uputstvu za delegiranu administraciju IZIS-a administratori kroz Podsistem za upravljanje resursima i šifranicima vrše upravljanje korisnicima centralnog aplikativnog sistema IZIS-a (ovlašćena lica koja koriste jednu ili više aplikacija navedenog podsistema).[90]

Prilikom prijave ili odjave korisnika, te definisanja pravila pristupa svaka ustanova je dužna dostaviti svom administratoru popunjen Sigurnosno-tehnički obrazac (SGT obrazac), propisan od strane FZO RS, a koji sadrži:

- ime, prezime i JMBG korisnika;
- spisak aplikacija koje je potrebno dodijeliti korisniku;
- spisak rola (uloga) po pojedinim aplikacijama koje je neophodno dodijeliti korisniku.[91]

Svaka zdravstvena ustanova je dužna da pomenuti obrazac dostavi i Fondu zdravstvenog osiguranja Republike Srpske.

U skladu za članom 16. Zakona o zaštiti ličnih podataka svi administratori sistema zdravstvenih ustanova su dužni potpisati Izjavu o čuvanju poslovne tajne, pristupu raučnarskim sistemima, pravima intelektualnog vlasništva, obavezi povrata informacija i pravu nadzora i pridržavati se utvrđenog načina obezbjeđivanja ličnih podataka. Ista obaveza odnosi se za svakog kreiranog korisnika u sistemu IZIS-a.[92]

Određivanje autentifikacijskih parametara (jedinstvenog korisničkog imena i inicijalne šifre) i dalje upravljanje korisnicima centralnog aplikativnog sistema IZIS-a vrši nadležni (delegirani) administrator. U njegovom domenu je i određivanje inicijalne šifre za novi nalog korisnika, koju je korisnik dužan promijeniti nakon prvog prijavljivanja (logovanja) na sistem.

[88] Uputstvo za delegiranu administraciju integrisanog zdravstvenog informacionog sistema Republike Srpske, 2018

[89] Pravilnik o izgledu i sadržaju identifikacione elektronske kartice zdravstvenog radnika, 2018

[90] Uputstvo za delegiranu administraciju integrisanog zdravstvenog informacionog sistema, 2018, tačka 8-9

[91] Uredba za delegiranu administraciju integrisanog zdravstvenog informacionog sistema Republike Srpske, 2018, tačka 13.

[92] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 16

Prilikom prestanka/prekida radnog odnosa vrši se odjava korisnika sa sistema, uz deaktivaciju njegovog naloga (ili više njih) i automatsko poništavanje kartice zdravstvenog radnika.[93]

Upravljanje autorizacijom podrazumijeva dodjeljivanje odgovarajućih uloga (rola) korisnicima (zaposlenia u ustanovi) u sistemu od strane nadležnog administratora na osnovu dostavljenog SGT obrasca od strane ustanove. Korisniku se dodjeljuju odgovarajuća prava na pojedinim aplikacijama koje omogućavaju pristup i dalji rad u modulima za evidenciju i obradu medicinskih podataka. Pristup podacima iz elektronskog zdavstvenog kartona pacijenata, odnosno korisnika zdravstvene zaštite, imaju zdravstveni radnici sa odgovarajućim pravima pristupa, a u svrhu pružanja odgovarajuće zdravstvene zaštite.[94]

### *5.5. Pristup podacima i njihova bezbjednost*

Baza podataka IZIS-a predstavlja centralizovanu i jedinstvenu bazu sa svim potrebnim mehanizmima zaštite i kao takva sačinjena je od više jedinstvenih registara i šifarnika. Da bi se podaci između različitih informacionih sistema mogli razmjenjivati na sistematizovan i klasifikovan način uspostavljeni su jedinstveni registri za osnovne skupove podataka poput podataka o pacijentu, šifarnicima lijekova, organizacionim jedinicama, medicinskim uslugama itd.

Pristup bazama IZIS-a definisan je Politikom bezbjednosti integrisanog zdravstvenog informacionog sistema Republike Srpske u poglavlju „Politika kontrole pristupa"[95] kroz identifikaciju i provjeru vjerodostojnosti korisnka, praćenje pristupa i korišćenja sistema, kao i bilježenje aktivnosti nad sistemom u vidu dnevnika zapisa. U cilju bezbjednosti podataka preduzimaju se sve tehničke i organizacione mjere, te se utvrđuju pravila postupaka neophodnih za adekvatnu zaštitu i tajnost prikupljenih podataka.[96] Obezbjeđivanje autentifikacija i autorizacije korisnika sistema, kontrole pristupa aplikacijama, definisanje korisničkih usluga u sistemu i pristupa podacima vrši se preko odgovarajućeg modula za upravljanje korisničkim nalozima i modula za upravljanje resursima.[97]

Elektronski zdravstveni karton otvara se za svakog korisnika zdravstvene zaštite za koga postoji adekvatan zdravstveni karton u fizičkom obliku. Elektronski karton predstavlja izvod

[93] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 13, stav i
[94] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 24, stav 1
[95] Politika bezbjednosti integrisanog zdravstvenog informacionog sistema Republike Srpske, 2018, poglavlje 3, str 11-18
[96] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 11, stav 1
[97] Uredba o integrisanom zdravstvenom informacionom sistemu, 2018, član 9

podataka iz osnovne medicinske dokumentacije koja se vodi u elektronskoj formi o jednom korisniku zdravstvene zaštite i objedinjuje sve zdravstvene podatke o korisniku.[98]

Korisnik zdravstvene zaštite, kao nosilac podataka, ima pravo da odluči da li će se o njemu u IZIS-u voditi elektronski zdravstveni karton, odnosno da da saglasnost FZO RS „da može da obrađuje lične podatke uz saglasnost nosioca podataka".[99] Ukoliko se korisnik odluči za vođenje elektronskog kartona dužan je dostaviti zdravstvenoj ustanovi pismenu izjavu o tome[100] uz prethodnu ispunjenost odgovarajućih tehničkih i bezbjedonosnih uslova za pristup putem interneta, biće mu omogućen uvid u svu medicinsku dokumentaciju smještenu u njegovom elektronskom kartonu.

Prikupljeni lični podaci korisnika zdravstvene zaštite čuvaju se i obrađuju na način kojim se obezbjeđuje ostvarenje prava na privatnost i povjerljivost podataka[101] o pacijentu kroz sprovođenje tehničkih i organizacionih mjera, odnosno definisanja politike fizičke bezbjednosti i politike bezbjednosti pristupa podacima.

Elektronska kartica radnika služi kao jedinstven identifikator fizičkog lica, odnosno zaposlenog, dok elektronska zdravstvena knjižica pacijenta predstavlja jedinstven identifikator pacijenta (osiguranika). Svako fizičko lice prijavljuje se na sistem putem jedinstvenog korisničkog imena i lozinke. Administrator sistema kroz svoje ovlaštenje u Podsistemu za administraciju IZIS-a vrši kreiranje naloga za pristup fizičkom licu na osnovu sigurnosno tehničkog obrasca popunjenog iz dva dijela: podacima iz evidencije kadrovske službe PIS-a ustanove i dodjeljenim prava pristupa u IZIS-u radniku na osnovu izjašnjenja rukovodećih lica.

Pacijent (osiguranik) ostvaruje svoja zakonska prava na zdravstvenu zaštitu omogućavanjem pristupa zdravstvenim radnicima svojim zdravstvenim podacima putem elektronske zdravstvene knjižice. Pomenuta isprava ne sadrži jedinstvene podatke o korisniku (JMBG ili fotografiju) pa se utvrđivanje identiteta vrši na osnovu lične karte osiguranika (pacijenta).

Kroz politiku kontrole pristupa FZO RS jasno su izdefinisana prava pristupa pojedinaca ili grupe informacijama, jedinicama za obradu informacija i poslovnim procesima unutar IZIS-a. U okviru centralnog sistema kontrola pristupa mreži i mrežnim resursima uspostavljena je zarad osiguravanja pristupa isključivo korisnicima koji za to imaju definisana prava pristupa. Ukoliko ta prava nisu dodijeljena, pristup je zabranjen.

[98] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 8
[99] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 5, stav 1
[100] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 5, stav 2
[101] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 11

Definisanjem bezbjedonosnog puta za pristup od terminala do servisa predstavlja bezbjedonosnu kontrolu koja sprječava zlonamjernog korisnika da iskoristi neautorizovan pristup aplikacijama i uređajima za obradu podataka.[102] Definisana pravila odnose se na centralizovani sistem FZO RS, ali ne obuhvataju pravila poslovanja lokalnih korisnika iz bolnica, domova zdravlja i drugih zdravstvenih ustanova. Zdravstvenim ustanovama stavljeno je na odgovornost definisanje pravila šta treba štititi a šta ne po pitanju računarskih resursa, kao i sama procjena rizika po računarsko poslovanje. Svaka ustanova bi trebala da ima jasno definisanu sigurnosnu politiku, posebno po pitanju fizičkog ograničenja pristupa i kontrole nad računarskim resursima, kao i uspostavljene bezbjedonosne mehanizme koji će unutar samog operativnog sistema biti funkcionalne.

Imajući u vidu činjenicu da se podaci evidentirani kroz sistem IZIS-a u elektronskom obliku čuvaju trajno, neophodno je da se vodi računa o očuvanju njihove upotrebne vrijednosti.[103] Uvođenje dovoljno jakog odbrambenog mehanizma za zaštitu podataka od neovlašćenog pristupa, kopiranja i zloupotrebe svake vrste i na svim nivoima pristupa sistemu je jedan korak u obezbjeđivanju podataka.[104] U skladu sa tim postojanje plana odgovora na bezbjedonosne incidente na svim nivoima pristupa IZIS-u je vrlo važan korak u sprovođenju zaštite podataka.[105]

[102] Politika bezbjednosti integrisanog zdravstvenog informacionog sistema Republike Srpske, 2018, str. 11-19

[103] Uredba o integrisanom zdravstvenom informacionom sistemu, 2018, član 16

[104] Uredba o integrisanom zdravstvenom informacionom sistemu, 2018, član 17

[105] Zakon o zaštiti ličnih podataka Bosne i Hercegovine, 2011, član 11, stav 4

## ZAKLJUČAK

Bezbjednost podataka i informacionih sistema realizuje se primjenom velikog broja sigurnosnih mjera i postupaka. Cilj ovih mjera je osiguravanje optimalnog funkcionisanja informacionih sistema bez narušavanja integriteta poslovanja i bez obrzira na rizike kojima su izloženi. Oblast zaštite podataka je postala znatno izloženija zloupotebi usled rasprostranjene upotrebe digitalnih tehnologija. Da bi se izvršila adekvatna zaštita neophodno je izvršiti njeno provođenje na nekoliko nivoa.

Prvi nivo definiše razvoj svijesti korisnika o postojanju opasnosti od zloupotrebe ličnih podataka. Drugi nivo se odnosi na obezbjeđivanje fizičke zaštite kroz bezbjednost informatičke opreme koja se koristi za obradu ličnih podataka. U tu svrhu je neophodno shvatiti važnost posjedovanja sigurnosnih politika poslovanja. Kroz ove politike vrši se rukovođenje i zaštita informatičke opreme (radnih stanica, mrežne i komunikacijske opreme) kao i regulisanje korisničkih pristupa podacima. Zloupotreba podataka, naročito ličnih podataka, može dovesti do veoma štetnih posljedica usled čega je neophodno precizno definisati prava pristupa osjetljivim podacima, te u skladu sa tim i stepen odgovornosti svakog korisnika u organizaciji.

Opasnost od malicioznog koda se spječava postavljanjem zaštite na nivou mrežnih prolaza, servera elektronske pošte, radnih stanica, fajl i aplikativnih servera. Pažljivim odabirom antivirusnog softvera ispunjava se prvi korak zaštite kako podataka, tako i informacionog sistema uopšte. Obezbjeđivanje informacijske sigurnosti vrši se implementacijom tehničkih, fizičkih i administrativnih mjera zaštite, koristeći koncept sistema upravljanja informacijskom sigurnošću, preciznije primjenom odgovarajućih sigurnosnih mjera koje se odnose na politiku sigurnosti, poslovne procese, procedure, uputstva, organizacijsku strukturu, te funckionalnost hardvera i softvera. Smjernice za sve navedeno date su u međunarodnom standardu ISO/IEC 27001.

Kako bi se obrada ličnih podataka odvijala u zakonskim okvirima definisani su normativni akti na međunarodnom i lokalnom nivou. Pravila koja se definišu na međunarodnom nivou objedinjena su Smjernicama za zaštitu ličnih podataka u zdravstvenim informacionim sistemima – principi i procesi za javno zdravlje Svjetske zdravstvene organizacije i Opštom uredbom Evropske unije o zaštiti ličnih podataka (GDPR). Propis od lokalnog značaja koji precizira način obrade i zaštitu ličnih podataka je Zakon o zaštiti ličnih podataka Bosne i Hercegovine. Akti kojima su definisani zakonski okviri obrade ličnih podataka obuhvataju i zaštitu ličnih podataka u zdravstvenim informacionim sistemima. Činjenica je da njihova primjena zavisi od kompleksnosti same strukture zdravstvene organizacije, kao i kvaliteta

zdravstvenog informacionog sistema ali principi koje definišu moraju biti sprovedeni u cilju sigurnosti svih podataka korisnika sistema.

**SKRAĆENICE**

IZIS – integrisani zdravstveni informacioni sistem
ISO – engl. International Organization for Standardization
IEC – engl. International Electrotechnical Commission
GDPR – engl. The EU General Data Protection Regulation
BIH - Bosna i Hercegovina
RS - Republika Srpska
JMBG – jedinstveni matični broj građanina
DNK – engl. Deoxyribonucleic acid
IT – informacione tehnologije
IP ADRESA – engl. Internet Protocol address
CD – engl. Compact Disc
DVD – engl. Digital Video Disc
USB – engl. Universial Serial Bus
E-MAIL – engl. Electronic mail
ISMS – engl. Information Security Management System
BS – engl. British Standards
BAS – bosanskohercegovački standard
PDCA – engl. Plan Do Check Act
SOA - engl. State of Applicability
CIA – engl. Confidentiality, Integrity, Availability
IKT – informaciono-komunikacione tehnologije
EU – Evropska unija
FZO - Fond zdravstvenog osiguranja
IDDEEA – Agencija za identifikacione dokumente, evidenciju i razmjenu podataka Bosne i Hercegovine
MUP – Ministarstvo unutrašnjih poslova
ASKVA - Agencija za sertifikaciju, akreditaciju i unapređenje kvaliteta zdravstvene zaštite Republike Srpske
KSZ – konsultativno-specijalistička zdravstvena zaštita
EMR – engl. Electronic Medical Record
EHR – engl. Electronic Health Record
SGT OBRAZAC – sigurnosno – tehnički obrazac

**PRILOZI**

**LITERATURA**


Agencija za zaštitu ličnih podataka u Bosni i Hercegovini, 2006, *Zakon o zaštiti ličnih podataka Bosne i Hercegovine* http://azlp.ba/propisi/default.aspx?id=1331&langTag=bs-BA

Agencija za zaštitu ličnih podataka u Bosni i Hercegovini, 2011, *Zakon o izmjenama i dopunama zakona o zaštiti ličnih podataka* http://azlp.ba/propisi/Default.aspx?id=5&langTag=hr-HR&template_id=149&pageIndex=1

Agencija za zaštitu ličnih podataka u Bosni i Hercegovini, *Šta je opšta uredba o zaštiti podataka (GDPR)*, datum pristupa 01.08.2023, http://azlp.ba/GDPR_Menu/Sta_je_GDPR/default.aspx?id=2373&langTag=bsBA&template_id=149&pageIndex=1

Banković, Miroljub, 2008, Menadžment informacionih sistema, Viša tehnička škola strukovnih studija, Kragujevac https://vts.edu.rs/wp-content/uploads/2017/05/Informacioni_menadzment.pdf

Bijelić, Drago, 2015, *Vodič kroz standardizaciju, pitanja i odgovori*, Republički zavod za standardizaciju i metrologiju, Banja Luka https://rzsm.org/images/stories/RZSM/Odabrani-sadrzaj/Vodic_kroz_standardizaciju-januar_2015.pdf

Bjelajac Đ. Željko, Vesić Lj. Slavimir, 2020, "Bezbednost informacionih sistema", Pravo-teorija i praksa, str. 63-76 https://scindeks-clanci.ceon.rs/data/pdf/0352-3713/2020/0352-37132002063B.pdf

Borojević, Nebojša i Krstan Borojević, 2017,"Transparentnost informacija u bolničkom sektoru u Republici Srpskoj", Naučno-stručni časopis SVAROG, str. 201-221 https://svarog.nubl.org/wp-content/uploads/2022/01/TRANSPARENTNOST-INFORMACIJA-U-BOLNICKOM-SEKTORU-U-REPUBLICI-SRPSKOJ.pdf

Božić, Velibor, 2012, "Upravljanje informacijskom sigurnošću u zdravstvu", Medix, broj 101/102, str. 254-263 http://www.kardio.hr/wp-content/uploads/2014/02/Medix_107-108_219-228.pdf

Coming, *Informaciona bezbednost – Pretnje za koje se moramo pripremiti*, datum pristupa: 01.09.2023. https://coming.rs/business-and-it/business-and-it-broj-4/informaciona-bezbednost-pretnje-za-koje-se-moramo-pripremiti/

Donatas, Mažeika and Rimantas Butleris, 2020, „MBSEsec: Model-Based Systems Engineering Method for Creating Secure Systems", Applied Siences, str. 1-18 https://www.mdpi.com/2076-3417/10/7/2574#

Fond zdravstvenog osiguranja Republike Srpske, 2018, *Politika bezbjednosti integrisanog zdravstvenog informacionog sistema Republike Srpske* https://www.zdravstvo-srpske.org/files/dokumenti/Politika-bezbjednosti-IZISa.pdf

Fond zdravstvenog osiguranja Republike Srpske, 2019, *Pravilnik o izgledu i sadržaju identifikacione elektronske kartice zdravstvenog radnika*, Službeni glasnik Republike Srpske broj 99/2019 https://www.zdravstvo-srpske.org/files/dokumenti/Pravilnik-o-izgledu-obliku-sadrzaju_el-kartice-zdravst_radnika.pdf

Fond zdravstvenog osiguranja Republike Srpske, 2021, *Tehnički preduslovi za integraciju sa IZIS-om* https://www.zdravstvo-srpske.org/files/dokumenti/Tehnicki_preduslovi_integracije_sa_IZISom_v1.1-1.pdf

Fond zdravstvenog osiguranja Republike Srpske, 2018, *Uputstvo o funkcionisanju, upravljanju rizikom i bezbjednošću integrisanog zdravstvenog informacionog sistema*, Službeni glasnik Republike Srpske broj 98/2018 https://www.zdravstvo-srpske.org/files/dokumenti/Uputstvo-o-funkc-upravlj-rizicima-i-bez-IZISa-konacna-verzija.pdf

Fond zdravstvenog osiguranja Republike Srpske, 2022, *Uputstvo o procedurama i postupcima omogućavanja pristupa, prenosa i razmjene podataka unutar IZIS-a*, Službeni glasnik Republike Srpske broj 25/2022 https://www.zdravstvo-srpske.org/files/dokumenti/2022-025_uputstvo.pdf

Fond zdravstvenog osiguranja Republike Srpske, 2018, *Uputstvo za delegiranu administraciju integrisanog zdravstvenog informacionog sistema Republike Srpske*, Službeni glasnik Republike Srpske broj 65/2018 https://www.zdravstvo-srpske.org/files/dokumenti/SL_Gl_065_2018-Uputstvo-o-delegiranoj-administraciji.pdf

Fond zdravstvenog osiguranja Republike Srpske, 2017, *Uredba o integrisanom zdravstvenom informacionom sistemu*, Službeni glasnik Republike Srpske broj 30/2017 https://www.zdravstvo-srpske.org/files/dokumenti/SL_30_2017_Uredba_o_IZISu.pdf

Fond zdravstvenog osiguranja Republike Srpske, 2022, *U toku je integracija privatnih ustanova u IZIS*, datum pristupa: 17.07.2023. https://www.zdravstvo-srpske.org/novosti/pocela-integracija-privatnih-ustanova-u-izis.html

Gemserv, 2019, *ISO/IEC 27001 and the General Data Protection Regulation (GDPR): How the ISO/IEC 27001 framework supports GDPR compliance*, London https://gemserv.com/wp-content/uploads/2019/09/ISO-IEC-27001-and-GDPR-v1.0.pdf

Hamidović, Haris, 2020, *Tehničke i organizacione mjere zaštite ličnih podataka*, Repro-Karić d.o.o, Sarajevo

Hrvatska akademska i istraživačka mreža, *Sigurnosna politika CCERT-PUBDOC-2009-05-265*
https://www.cert.hr/wp-content/uploads/2009/05/CCERT-PUBDOC-2009-05-265.pdf

Institut za standardizaciju Bosne i Hercegovine, *Sistemi upravljanja sigurnošću informacija*, datum pristupa 15.06.2023.
https://isbih.gov.ba/p/sistemi-upravljanja-sigurnoscu-informacija

International Organization for Standardization. 2013. Information security, cybersecurity and privacy protection — Information security management systems — Requirements., ISO/IEC 27001:2013.

ISO/IEC 27001:2022, *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements (third edition)*, datum pristupa: 24.08.2023
https://www.iso27001security.com/html/27001.html

Itpedia, Smjernice za sobu za IT opremu (MER, SER i DER), datum pristupa: 01.09.2023.
https://bs.itpedia.nl/2019/05/15/de-it-equipment-room-mer-ser-en-der/

Kaspreska, Natalija , Ašmanov Igor, 2021, *Digitalna higijena*, Riznica +, Beograd

Kiber, *Šta je Malware?*, datum pristupa: 01.09.2023.
https://kiber.ba/2023/02/09/sta-je-malware/

Kokić, Momčilo i Tasevski Petar, Primena standarda ISO/IEC 27001 kao faktora konkurentske prednosti organizacija, Infoteh – Jahorina, 2016, str. 485-490, vol 15.
https://infoteh.etf.ues.rs.ba/zbornik/2016/radovi/RSS-1/RSS-1-6.pdf

Košutić, Dejan, *What is ISO 27001? A quick and easy explanation*, datum pristupa: 17.07.2023.
https://advisera.com/27001academy/what-is-iso-27001

Kulašin,Džemal, Faruk Unkić i Goran Dalila, 2012, "Sistem upravljanja informacijskom sigurnošću prema standardu ISO/IEC 27001", Univerzitetska hronika – časopis Univerziteta u Travniku, str. 31-38
https://casopis.fmpe.edu.ba/images/casopis/12/12-3.pdf

Majernik, Milan, Daneshjo Naqib, Chovancova Jana, Sanciova Gabriela, 2017, "Design of integrated managament systems according to the revised ISO standards", Vol.15. No. 1, str. 135-143

https://www.researchgate.net/publication/318582632_Design_of_integrated_management_systems_according_to_the_revised_iso_standards

Microsoft, *Kreiranje i korišćenje jakih lozinki*, datum pristupa: 25.08.2023. https://support.microsoft.com/sr-latn-rs/windows/kreiranje-i-kori%C5%A1%C4%87enje-jakih-lozinki-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb

Mijić, Branka, 2019, "Informacijska sigurnost u Bosni i Hercegovini", FBIM Transactions, 91–99. https://doi.org/10.12709/fbim.07.07.01.11

Mrdović, Saša, 2014, *Sigurnost računarskih sistema*, ETF UNSA, Sarajevo https://people.etf.unsa.ba/~smrdovic/publications/Sigurnost_Racunarskih_Sistema_Mrdovic.pdf

Nezavisni operator sistema u Bosni i Hercegovini (NOSBiH), *Zaštita ličnih podataka*, datum pristupa: 02.06.2023, https://www.nosbih.ba/bs/o-nama/zastita-licnih-podataka/

Ngqondi,Tembisa G., 2009, *The ISO/IEC 27002 and ISO/IEC 27799 Information Security Management Standards: A Comparative Analysis from a Healthcare Perspective* https://vital.seals.ac.za/vital/access/manager/Repository/vital:9765?site_name=GlobalView

Nikander, Jussi, Onni Menninen and Mikko Laajalahti, 2020, "Requirements for cybersecurity in agricultural communication networks", Computers and Electronics in Agriculture, Vol. 179, https://www.sciencedirect.com/science/article/pii/S0168169920314812

Pavić, Tihomir , Jelenković L. 2006, "Autentifikacija i autorizacija korisnika na jednom mjestu", Fakultet elektrotehnike i računarstva, Zagreb https://bib.irb.hr/datoteka/299708.06_ISS_1043.pdf

Richardson, Robert, 2008, *The latest results from the longest-running project of its kind*, CSI Computer Crime & Security Survey http://www.sis.pitt.edu/jjoshi/courses/IS2150/Fall10/CSIsurvey2008.pdf

Riječnik, datum pristupa: 14.06.2023. https://www.rječnik.com/Autorizacija

Službeni list Europske unije, 2016, *Opšta uredba Evropske unije o zaštiti ličnih podataka* https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32016R0679&qid=1462363761441&from=HR

Svijet kvalitete, 2013, *PDCA krug (Demingov krug)*, datum pristupa: 01.08.2023. https://www.svijet-kvalitete.com/index.php/upravljanje-kvalitetom/948-pdca-krug

Telecommunications Infrastructure Standard for Data Centers TIA-942, 2005, Telecommunications industry association, Arlington https://manuais.iessanclemente.net/images/9/9f/Tia942.pdf

The British Standards Institution (BSI). 2022. *The new ISO/IEC 27001:2022 standard*., datum pristupa 13.08.2023. https://www.bsigroup.com/en-GB/iso-27001-information-security/isoiec-27001-revision/

Urankar, Danijel, 2015, "Mjere procjene sigurnosti i zaštite poslovnog korisnika", Fakultet prometnih znanosti, Sveučilište u Zagrebu, Zagreb https://repozitorij.fpz.unizg.hr/islandora/object/fpz:161/datastream/PDF

Vlada Republike Srpske, 2022, *Zakon o zdravstvenoj zaštiti i evidencijama u oblasti zdravstva,* Službeni glasnik Republike Srpke broj 57/2022 https://www.vladars.net/sr-SP-Cyrl/Vlada/Ministarstva/MZSZ/dokumenti/Documents/SG_57-22%20Zakon%20o%20zdrav%20dok%20i%20evidenc.pdf

World Economic Forum, *Fourth Industrial Revolution*, datum pristupa: 14.07.2023, https://www.weforum.org/focus/fourth-industrial-revolution

World Health Organization, 2011, *The protection of personal data in health information systems – principles and processes for public health* https://iris.who.int/bitstream/handle/10665/341374/WHO-EURO-2021-1994-41749-57154-eng.pdf?sequence=1&isAllowed=y

Yee, Chai K. and Mohamad F. Zolkipli, 2021, "Review on Confidentiality, Integrity and Availability in Information Security", Journal of ICT in Education (JICTIE), Vol. 8. No. 2, str. 24-42 https://ejournal.upsi.edu.my/index.php/JICTIE/article/view/5203/3091