УНИВЕРЗИТЕТ У БЕОГРАДУ

ФАКУЛТЕТ БЕЗБЕДНОСТИ

ЗАШТИТА ЛИЧНИХ ПОДАТАКА У ИНФОРМАЦИОНИМ СИСТЕМИМА ЗДРАВСТВЕНИХ УСТАНОВА

СПЕЦИЈАЛИСТИЧКИ РАД

МЕНТОР:
Проф. др Ненад Путник

КОМЕНТОР:
Проф. др Слађана Бабић

КАНДИДАТ:
Маја Миленковић

Београд, 2018.

САДРЖАЈ

УВОД

Прецизност података од виталног је значаја за здравствене установе и сваки податак у овој области захтева евидентирање. Ово је неопходно како би здравствено стање сваког пацијента било објективно праћено и да би лекар, било које праксе, имао увид у стање пацијента, обављене интервенције и терапије које је до тог тренутка пацијент користио. Да бисмо дошли до тих података неопходно је да се сви подаци који могу да се прибаве током процеса лечења евидентирају и обраде, како би касније били лако доступни и могли да дају жељене информације на основу којих могу да се доносе одлуке пресудне по даље лечење и коначно, што је и сврха професије, спашавање живота и животних функција пацијента. Прикупљање и чување овако великих количина података је практично немогуће без савремених информационих технологија. У ту сврху потребно је применити одређене стандарде информационих технологија како би била могућа размена и упоређивање података, механизми интероперабилности између система и системи заштите података.

„Кроз стратешка документа, Здравље за све у трећем миленијуму Светске здравствене организације, Стратегија развоја информационо комуникационих технологија у здравству и Акциони план европске комисије, 2004. године постављени су стратешки и оперативни циљеви и предвиђене активности на Европском простору у циљу дугорочног ефикасног решавања изазова са којим су се суочили здравствени системи" (Опачић, 2018).

Како лични подаци, представљају веома осетљиву и поверљиву информацију, од велике је важности начин прикупљања информација као и адекватно ИТ решење за заштиту података. С обзиром на то да је 25.5.2018. године ступила на снагу Општа уредба о заштити података о личности (*GDPR - General Data Protection Regulation*), ова ИТ решења морају се ускладити са одређеним стандардима које *GDPR* подразумева. У суштини, *GDPR* се фокусира на обраду података, њихово чување и усклађивање у складу са Законом.

Обрадом података сматра се свака радња предузета у вези са подацима као што су: прикупљање, бележење, преписивање, умножавање, копирање, преношење, претраживање, разврставање, похрањивање, раздвајање, укрштање, обједињавање, уподобљавање, мењање, обезбеђивање, коришћење, стављање на увид, откривање,

објављивање, ширење, снимање, организовање, чување, прилагођавање, откривање путем преноса или на други начин чињење доступним, прикривање, измештање и на други начин чињење недоступним, као и спровођење других радњи у вези са наведеним подацима, без обзира на то да ли се врши аутоматски, полуаутоматски или на други начин. Такође је важно и ко прикупља и обрађује податке, као и ко, и из ког разлога, има приступ подацима, као што је веома битан и степен обучености ових радника и добро познавање процедура и Закона. У спроведеном истраживању обрађена је ова тематика и њена примена у тренутном систему здравствених установа (ЗУ), а дати су и конкрктни предлози за унапређење заштите личних података у информационим системима здравствених установа.

1. МЕСТО И УЛОГА ЗДРАВСТВЕНИХ УСТАНОВА У СИСТЕМУ ЗАШТИТЕ КРИТИЧНИХ ИНФРАСТРУКТУРА

Потреба динамичког, проактивног и стратешког приступа нарочито је неопходна у процесу планирања заштите критичне инфраструктуре у условима различитих типова кризних и ванредних ситуација. Пре него што је појам „критична инфраструктура" постао предмет интересовања у бројним анализама које су се односиле на тероризам и унутрашњу безбедност, појам „инфраструктура" осамдесетих година био је референтна тачка креатора јавне политике и безбедности (Јаковљевић, Гачић, 2012).

Порастом опасности од тероризма, у савременим теоријским анализама, али и у пракси, све је присутнији израз критична инфраструктура. Непосредно након терористичких напада од септембра 2001. године, критична инфраструктура постала је битан и суштински део националне безбедности, а њена заштита представља један од приоритета сваке државе, као и сваке засебне организације у склопу државе.

Као пример наводи се неколико дефиниција критичне инфраструктуре, које су заступљене као модели у неким од наведених држава (Шкеро, Атељевић 2015).

У Сједињеним Америчким Државама (САД) критична инфраструктура у основи се односи на широк опсег различитих средстава и имовине који су неопходни за свакодневно функционисање друштвених, економских, политичких

и културних система. Сваки прекид у елементима критичне инфраструктуре оцењен је као озбиљна претња за правилно функционисање ових система и може довести до оштећења имовине, људских жртава и значајних економских губитака.

У Аустралији је дефиниција за израз критична инфраструктура одређена прецизније и подразумева: физичке објекте, ланце снабдевања, информационе технологије и комуникационе мреже, које би, ако се униште или на дуже време онеспособе, могле значајно утицати на друштвено или економско благостање нације, или би утицале на способност државе да одржи националну одбрану и обезбеди националну сигурност.

Према стратегији Европске уније, критична инфраструктура представља имовину, систем или његов део који се налази на територији земље чланице, а који је неопходан за одржавање кључних друштвених функција, здравства, безбедности, сигурности, економског или социјалног благостања, а чије би ометање или уништење имало значајан утицај на земљу чланицу. Европска критична инфраструктура – ЕКИ, подразумева критичну инфраструктуру лоцирану на територији земље чланице, чије би ометање или уништење имало значајан утицај на бар две земље чланице. Значај поремећаја у функционисању елемената критичне инфраструктуре треба да се процени на основу критеријума међузависности. То подразумева ефекте настале као резултат међусекторске зависности од других типова инфраструктуре (Шкеро, 2008).

У пракси, дефинисање оквира критичне инфраструктуре у многим земљама је различито и зависи од разних специфичности, почевши од политичких прилика до географских локација.

Србија је учинила значајне напоре у стварању интегрисаног система заштите и спасавања, који би на адекватан начин одговорио у условима угрожавања критичних националних ресурса.

Законом о ванредним ситуацијама, који је усвојен 2009. године, држава се определила да Министарство унутрашњих послова буде надлежно за израду процене угрожености од елементарних непогода и других несрећа, те је доставља Влади на усвајање. Аутономне покрајине, јединице локалне самоуправе, министарства и други органи и организације израђују процену угрожености у делу

који се односи на њихов делокруг и достављају је Министарству унутрашњих послова.

Здравствене установе имају значајно место у изради плана стратегије за заштиту критичне инфраструктуре. У случају да дође до неке ванредне ситуације (нпр. терористички напад или земљотрес) која за последицу има велики број жртава (повреде, епидемије, рањавања, тровања итд.), од великог је значаја капацитет здравствених установа да прихвате и збрину унесрећене. Од огромног је значаја добро развијен информационо комуникациони здравствени систем који би олакшао сакупљање, селектовање, чување, прослеђивање и заштиту осетљивих личних и здравствених података, како у мирнодопским, тако и у ванредним ситуацијама (Опачић, 2018).

Као што је већ напоменуто, савремена медицина захтева евидентирање велике количине података.

Како бисмо дошли до свих тих података неопходно је да се евидентирају сви подаци који могу да се прибаве током процеса лечења, како би касније били лако доступни и могли да пруже жељене информације на основу којих могу да се доносе одлуке. Прикупљање и чување овако великих количина података је немогуће без савремених информационих технологија, чије основе представљају стандарди који морају да се примене како би била могућа размена и упоређивање података, механизми интероперабилности између система и система заштите података.

Здравствене организације уводе и развијају различите облике информационих система и система електронске медицинске документације. Медицинска документација садржи осетљиве личне податке који су потребни медицинском и немедицинском особљу (из различитих организација) са циљем што бољег сагледавања здравственог стања, а самим тим и што бољег, квалитетнијег и ефикаснијег доношења дијагностичких и терапијских одлука. Осетљиви подаци који се тичу пацијената могу бити злоупотребљени (различити подаци који се тичу здравственог стања одређеног лица – пацијента могу доћи у посед неовлашћених физичких или правних лица или се злоупотребити са циљем уцене дотичног лица, итд.).

То нас доводи у незавидан положај, са једне стране постоји потреба ограничења приступа подацима из електронске документације пацијената, док са

друге стране ти исти подаци морају бити доступни готово свим службама ангажованим у здравственим установама, па чак и неким ванздравственим (Костић, 2007).

Мултиорганизациона транспарентност (функција рачунара чије извршавање корисник готово не примећује, нпр. слање факса), легални и етички аспекти и одговорности намећу сложене изазове не само у погледу технолошке архитектуре медицинских информационих система. При томе, технолошка архитектура мора бити усклађена са етичким и правним стандардима који често нису у сагласности са техничко-технолошким могућностима. Генерички механизми заштите треба да омогуће дефинисање стандарда и политике коришћења личних медицинских информација који ће бити технолошки скалабилни (*скалабилност* је пожељно својство производа, мреже или система које означава могућност раста без мењања основних особина или функција). Тиме се постиже максимална искоришћеност технолошког развоја уз смањену опасност од појаве пропуста у систему заштите које могу довести до злоупотребе. Саставни део набавке или сопственог развоја тих система је и процес обезбеђивања заштите информација, као и процеса дефинисања начина да се смање ризици и предвиде, односно спрече негативне последице које могу настати услед недовољне заштите информација.

2. БЕЗБЕДНОСНЕ ПРЕТЊЕ ИНФОРМАЦИОНО-КОМУНИКАЦИОНИМ СИСТЕМИМА

Појам информација значи знање, упутство, или обавештење у зависности од тога у које сврхе се користи. Информација указује на поруку која садржи чињенице – податке из којих се могу извести закључци. Она може бити говорна, писана, штампана или електронски записана (Протић, 2013).

Са становишта савремених информационих технологија, квалитет информационо-комуникационих система одређује на који начин ће подаци бити креирани, обрађивани, складиштени и преношени, као и како ће бити обезбеђена њихова заштита и уништавање.

Информационо-комуникациони системи представљају скуп метода, поступака и ресурса уобличених тако да би се лакше дошло до неког циља.

Информациони систем дефинише интегрисани систем који обухвата људске и технолошке ресурсе за обезбеђивање информација за подршку функционисања организације. Основни циљ сваког информационог система је омогућавање прикупљања података и њихово приказивање на најбољи начин.

Информациона безбедност представља сваку активност која обезбеђују заштиту информација са циљем да буде омогућен континуитет у раду и смањен, на најмању могућу меру, утицај ризика и претњи по информациони систем.

Информациона безбедност подразумева заштиту поверљивости, интегритета и доступности података од неовлашћеног приступа, промене или уништења уз примену контролних механизама који треба да буду унапред одређени, уграђени, надгледани, проверавани и побољшавани у реалном времену.

Постоје многобројне дефиниције безбедности података зависно од нивоа потребе. На нивоу државе штите се национални интереси у информационој сфери, који су одређени скупом личних, пословних и државних интереса. Како се безбедност података обезбеђује заштитом, може се дефинисати и као заштићеност података од случајних или намерних активности који могу нанети неприхватљиву и немерљиву штету бази података организације.

Безбедност информационо-комуникационих технолошких система је објективна мера стања ризика или безбедности поузданог и неометаног функционисања система у односу на самог себе и своје окружење. Систем се сматра безбедним ако је заштићен од свих фактора ризика. Безбедност система заштите најближе одговара значењу енгл. термина *Security assurance* (гарантована безбедност).

У пракси се безбедност информација најчешће манифестује у безбедносном раду без отказивања информационог система, интернета, малициозних програма, прислушкивања, те у безбедној комуникацији и заштитом приватности. Безбедност информација је процес, континуираног одржавања заштите информација и потребно га је планирати, имплементирати, извршавати, одржавати и побољшавати кроз успостављени систем за управљање заштитом информација – *ISMS* (*Information security management system*).

Највећи проблем је недостатак свести руководећег менаџмента о потреби процене ризика, који често имплементира технологије заштите без процене ризика, као и крајњих корисника, који недовољно схватају потребу контроле и последице утицаја ризика на дневне активности.

Информационо-комуникациони системи су критични сегменти људског друштва у 21. веку. Посебан проблем јесте што се због убрзаног развоја информационо-комуникационе технологије и незаустављивог раста њене примене у свим сферама друштвеног живота увећава његова рањивост и изложеност врло озбиљним потенцијалним опасностима (Вулетић, 2016).

Савремени безбедносни изазови, који се јављају у областима политике, економије, финансија, енергетике, екологије, религије, културе, информатике и других области друштвеног живота, намећу потребу укључивања већег броја државних и друштвених организација у послове којима се осигурава национална безбедност. Поред повећања броја организација које се баве питањима националне безбедности, постоји потреба да се на безбедносне изазове и претње одговори на јединствен и усклађен начин (Недељковић, 2015).

Друштвена зависност од информационо-комуникационих система увећава последице напада, као и падова дотичних система.

Под информационо-комуникационим системом подразумева се сваки уређај или група међусобно повезаних уређаја, којима се врши аутоматска обрада података или било којих других функција.

Напад је претња која је извршена и, ако је успешан, доводи до компромитовања рачунарског система, односно, нарушава његову безбедност. Сваки систем има своје слабе тачке. Комплекснији системи имају потенцијално већу могућност рањивости и пропуста. Напад у суштини представља експлоатисање горе поменутих рањивости и пропуста, а састоји се од намерних корака које предузима нападач да би се постигао одређени циљ.

Незгоде представљају широк спектар случајно искрслих и потенцијално штетних радњи и догађаја, као што су нпр. природне, техничке и друге непогоде.

Падови система су могући штетни догађаји проузроковани мањкавостима у систему или спољним елементима од којих систем зависи. Падови система су

узроковани грешкама у изради софтвера, састављању хардвера, људским грешкама и сл.

Напади на рачунарске системе се могу класификовати према више критеријума.

Према пореклу напада деле се на:

- Унутрашњи напад, реализован од стране нападача унутар система – инсајдера који имају могућност приступа ресурсима, али их користе на начин на који нису овлашћени.
- Спољашњи напад, реализован је од стране нападача изван система.

Према последицама по системске ресурсе, напад може бити:

- Активни напад, тј. покушај да се промене системски ресурси или да се утиче на њихове операције.
- Пасивни напад је покушај да се неовлашћено приступи подацима у систему, али без утицаја на системске ресурсе (преузимање, надгледање преноса података, прислушкивање и сл., нпр. *sniffing*).

У пракси је чест случај да нежељени догађаји са аспекта безбедности у информационо-комуникационим системима представљају комбинацију различитих врста напада. Врсте напада су: *DDoS, Phishing, Botnet, Spam, Social Engineering, Sniffing, Spoting i Malware.*

Напад ускраћивањем услуга (*Denial of service*) је тип напада који покушава да спречи легитимне кориснике да приступе мрежним услугама. То се остварује преоптерећењем мрежних сервиса или прекомерном конекцијом, што узрокује пад конекције или сервера. Инфраструктура међусобно спојених система и мрежа, састоји се од ограничених ресурса. *DDoS* алати су намењени да пошаљу велики број захтева циљаном серверу (обично *e-mail, web* или *ftp server*), са циљем да преплаве ресурсе сервера и учине га неупотребљивим. Напад ускраћивањем услуга је организован тако да омета или потпуно обуставља нормално функционисање *web* сајта, сервера или других мрежних ресурса. Један од најчешћих начина је једноставно преплављивање сервера слањем превеликог броја захтева. То онемогућава нормално функционисање сервера и веб странице ће се отварати

много спорије, а у неким случајевима може довести до потпуног обарања сервера (проузроковати пад свих база података и сајтова на серверу).

Сваки систем који је спојен на интернет и који је опремљен мрежним услугама базираним на *TCP* (енгл. *Transmission Control Protocol*) протоколу потенцијална је жртва напада (Кларић, 2008).

Током *DDoS* напада, одређени сервер или мрежа прима захтеве из компромитованих система. Услед претераног слања захтева сервер успорава и постаје бескористан, све док напад траје (Благојевић, 2018).

Најчешћи *DDoS* напади су:

- *Volumetric Attack*
- *Application Level Attack*

Када у нападу учествује *Volumetric Attack*, циљани веб сајт или мрежа добијају велику количину захтева са ботнет-а и инфицираних зомби система. Ту спадају:

- *Connection flood*
- *TCP SYN flood* (ресет напади)
- *ICMP/UDP flood*

И они углавном циљају трећи и четврти ниво, односно *Network Layer* и *Transport Layer*. Овакви модели напада искоришћавају инфициране системе да створе велики проток саобраћаја. Системи се дистрибуирају географски и то са протоком који прелази чак 10ТБ/с. Овакви напади временом напредују и постају све сложенији.

Најранији облик *DDoS* напада, свакако представља *SYN flood* који се појавио 1996. године и експлоатише слабости у *TCP* (*Transmission Control Protocol*). Остали напади експлоатишу слабости у оперативним системима и апликацијама, што доводи до недоступности мрежних услуга или чак до пада сервера. Многи алати су развијени за извршење таквих напада и постали су слободно доступни на интернету (*Bonk, LAND, Smurf, Snork, Teardrop*). *TCP* напади су још увек најпопуларнији облик *DDoS* напада. Разлог је што остали типови напада, као што је употреба (потрошња) целокупног простора на хард диску, модификовање табеле рутирања

на рутеру и сл., прво захтевају упад на мрежу, што може да представља проблем за потенцијалног нападача, ако је систем добро заштићен.

Постоје три основна начина извршавања *DDoS* напада:

- Потрошња свих ресурса као што је пропусни опсег, што онемогућава легитимни саобраћај, *SYN flooding attacks* – велики број захтева да се отвори *TCP* конекција, тј. велики број отворених конекција, смурф напади – велики број пакета усмерених ка мрежи;
- Уништење или оштећење конфигурационих информација (нпр. рутера);
- Физичка оштећења компоненти мреже да би се спречио приступ услугама (рачунара, рутера, станица за напајање електричном енергијом...)

Класични *DDoS* напади су један на један напади у којима моћан хост генерише саобраћај који затрпава конекцију циљаног хоста што омета овлашћена лица да приступе мрежним услугама. Први пут су се појавили 1999. године, а масовни *DdoS* напади, почели су 2000. године, када су оборени популарни сервери, као што је *Amazon, CNN, eBay, YAHOO* и др. Најбољи начин за одбрану од таквих напада је промена конфигурација рутера код провајдера интернет услуга.

DDoS напади користе велики број рачунара заражених црвима или тројанцима, да реализују једновремени напад на циљани систем за веома кратко време. Даљински контролисани заражени рачунар назива се „Зомби". Рачунари зомбији могу, рецимо, послати на хиљаде мејлова изазивајући прекид услуга на е-маил серверу.

DDoS напад који се догодио у Естонији 2007. године био је највећи напад икада виђен. У том нападу било је укључено више различитих бот мрежа. Свака је имала више десетина хиљада зомбија. Често се у информатичким круговима догађаји у Естонији називају „Први рат на мрежи" (*Web War I*).

Последњи и највећи досадашњи *ransomware* напад у свету, отпочео је 12.5.2017. године. Нови *ransomware* је направио пометњу широм света. Погођен је *NAS* (Национални здравствени систем Велике Британије), болнице, као и организације повезане са њима, те је завладао потпуни хаос.

Забележено је више од 145.000 напада у 74 земље, а највећи број у Русији. Поред Велике Британије и Русије, тешко су погођене Турска, Казахстан, Индонезија, Вијетнам, Јапан, Шпанија, Немачка, Украјина и Филипини. Кривац за ове нападе је *v2.0 WCRY ransomware* који је познат и под називима *Wannacry, Wannacryptor ransomware*. *Ransomware* користи *NSA exploit* који је доспео у јавност захваљујући хакерској групи *The Shadow Brokers*. Има на десетине хиљада жртава широм света укључујући и руско Министарство унутрашњих послова, кинески универзитет, мађарску телекомуникациону компанију, делове америчке Федекс корпорације итд.

Нападнуте болнице у Великој Британији морале су да врате пацијенте кућама и да откажу све заказане прегледе, јер је *ransomware* онеспособио читав рачунарски систем државног здравственог система.

Не постоји безбедносно решење које ће некоме пружити стопроцентну заштиту од постојећих и нових, све комплекснијих претњи или како би Џејмс Скот рекао: „Не постоји сребрни метак за сајбер безбедност, слојевита одбрана је једина одржива одбрана."

Код ИТ безбедности постоје два основна проблема. Први је стални раст броја и комплексности сајбер претњи, који је објективан проблем и на њега се не може много утицати. Други проблем, на који може да се утиче, су грешке и погрешно перципирање ситуације. Компаније праве грешке када су у питању неке једноставне операције, а које чине компанију рањивом на различите нападе.

Иако не постоји једно решење или приступ за потпуну заштиту, постоје једноставне ствари које је потребно урадити да би се повећао ниво безбедности и да би се обезбедили услови за одбрану од нарастајућих претњи.

Претња која стиже у виду *dropper* тројанца који има две компоненте:

Компонента која покушава да експлоатише *SMB Ethernal Blue* рањивост других рачунара – *ransomware wanna crypt*.

Уколико успешно успостави конекцију, претња не наставља даље да инфицира систем *ransomware*-ом, или да се шири у друге системе. Једноставно, претња престаје да се извршава, а уколико не успе, наставиће са криптовањем и ширењем.

Другим речима, блокирање овог домена на заштитном зиду је врло лоша идеја, јер ће само изазвати даље ширење *ransomware* и даље криптовање фајлова. *Ransomware* такође проверава да ли се користи прокси (сервер посредник) или не, те ако види да се налази иза проксија, наставља са радом, не проверавајући постојање наведеног домена.

Wanna cry ransomware је заустављен „*kill switch*" механизмом. Проблем представљају отпорност и стална мутација овог сајбер паразита.

Како се заштити?

Корисници оперативног система *Windows* треба да примене следеће мере:

- Ажурирање (*update*) W*indows*-а. Кључно је инсталирање *MC 17010 patch.*
- *Install patch AB 2871997*
- Ажурирање антивируса
- Блокирање долазног садржаја *TCP port 445*
- Обезбедити да се све шифре за локалне администраторске налоге на рачунарима у мрежи разликују
- Направити резервну копију података (*back up*) са рачунара и сервера и сачувати на спољним меморијским јединицама све релевантне фајлове.
- Иако није доказано да се шири путем електронске поште, важно је обавестити све који раде са рачунарима да не отварају линкове унутар порука приспелих електронском поштом од непознатих пошиљалаца, посебно ако су у питању архивирани фајлови (*.zip, .rar*), извршни (*.com, .exe*) или фајлови са екстензијом (*.jz.*).

3. БЕЗБЕДНОСТ И ЗАШТИТА

Информациона безбедност подразумева скуп техничких, логистичких, нормативних и административних решења и процедура које се предузимају са циљем да се подаци заштите од неовлашћеног увида, отуђења или уништења, као и ради заштите функционалности самог информационог система (Милосављевић, 2010).

Термини безбедност информација или информациона безбедност примарно подразумевају безбедност информација и података ИКТС, а секундарно безбедност објеката рачунарског система (РС) и рачунарске мреже (РМ), чиме се посредно штите информације. Овакав приступ инплицира да је крајњи циљ безбедности и заштите – заштита информација и података, која се директно или индиректно постиже заштитом информационе имовине. Информациона имовина у *ISO/IEC 27001* обухвата информације, хардвер, софтвер и људске ресурсе.

Мисија, тј. циљеви система заштите информација је да одржањем ИКТС-а (информационо-компјутерског технолошког система) на прихватљивом нивоу ризика обезбеди поузданост рада пословног ИКТС-а и повећа ефективност пословног процеса. Примарни циљеви заштитите су заштита информационе имовине организације. Ови циљеви се најчешће наводе као довољан скуп релативно независних циљева заштите у релевантним стандардима заштите (*ISO/IEC 27001*, *NIST*). У неким стандардима и компонентама заштите, наводе се и циљеви заштите контролисане одговорности (*Accountability*), непорецивости, аутентификације и гарантоване безбедности (*Security Assurance*).

Циљеви заштите су међусобно зависни. На пример, циљ заштите интегритета обухвата заштиту непорецивости и аутентификацију, а циљ заштите расположивости – контролисану одговорност, која зависи од механизма за обезбеђивање непорецивости. Гарантовану безбедност обезбеђују сва три примарна безбедносна циља заједно.

Безбедносни захтев за расположивост информација и сервиса обезбеђује овлашћеним корисницима поуздан рад и расположивост података и информација система, сервиса и апликација, по указаној потреби. Овај циљ штити систем од намерног или случајног кашњења података, одбијања сервиса или испоруке података (*DDoS*) и од неовлашћене употребе система и информација и често је најважнији безбедносни циљ.

Безбедносни захтеви за заштиту интегритета, укључујући и заштиту интегритета података и информација (складишних, процесираних и преношених), конфигурације (РС и РМ и интегритета сесије) имају за циљ да спрече откривање неовлашћеним лицима ускладиштених, процесираних и преношених поверљивих или приватних информација.

Захтев за контролисану одговорност ентитета и појединаца у организацији, има за циљ да се акције сваког ентитета и појединца могу пратити по једнозначно регистрованим траговима. Сервис за остваривање овог циља захтева се у саопштењу политике заштите и директно укључује нормативни оквир, одвраћање нападача, издају грешака, детекцију и спречавање упада и опоравка система.

Наведени безбедносни циљеви су међусобно зависни и ретко се може остварити један, без утицаја других. Циљ заштите поверљивости зависи од заштите интегритета, зато што нема смисла очекивати да инфомација није откривена, уколико је нарушен интегритет система. Циљ заштите интегритета зависи од заштите поверљивости, зато што је врло вероватно да је механизам заштите интегритета заобиђен и интегритет инфомације нарушен, ако је нарушена њена поверљивост (нпр. лозинка администратора). Свако смањивање овог скупа циљева захтева одговарајућу апроксимацију и разумевање ове међузависности.

Са циљем гарантоване безбедности у међузависној вези су сви циљеви заштите. Када пројектује систем заштите, пројектант успоставља граничну вредност гарантоване безбедности као циљ којем се тежи и који се постиже испуњавањем захтева у сваком од преостала четири циља, у складу са процедурама и стандардима добре праксе заштите. Такође, истиче чињеницу да се за гарантовану безбедност неког система морају испунити пројектовани функционални захтеви за техничку поузданост система (вероватноћу или средње време рада без отказа система), али и спречити нежељени процеси и стећи поверење у систем заштите (Мандић, Путник, Милошевић, 2017).

Проблем рањивости информационе инфраструктуре подстакао је расправе о адекватним безбедносним политикама и, уопште, адекватним политикама заштите сајбер простора .

Током 2006. године, Европски парламент упутио је препоруку Савету Европе и европском Савету за заштиту критичних инфраструктура. У оквиру препоруке садржани су и следећи ставови:

„Критичне инфраструктуре у Европској унији постале су високо повезане и међусобно зависне, што их чини посебно рањивим на поремећаје и уништење. Услед тога, постоји потреба да се сачини Европски програм за заштиту критичне инфраструктуре (*European Programme for Critical Infrastructure Protection* –

EPCIP), који би био финансиран од стране држава чланица, и/или власника инфраструктура и оператера."

На Светском самиту о информационом друштву донета је Декларација о принципима (2003), у којој је наглашена потреба за развијањем концепта сајбер безбедности.

У одељку Декларације, посвећеном изградњи поверења и безбедности у коришћењу ИКТ, наводи се:

„Јачање поверења, укључујући безбедност информација и мреже, аутентичност, приватност и заштиту корисника, неопходно је за развој информационог друштва и стварање поверења између корисника ИКТ. Потребно је промовисати, развијати и имплементирати глобалну културу сајбер безбедности кроз сарадњу свих доносилаца одлука и међународних експертских тела. Овај напор би требало да буде подржан кроз повећање међународне сарадње. У оквиру глобалне културе сајбер безбедности важно је повећати безбедност и осигурати заштиту података и приватности, паралелно са повећањем могућности и приступа и трговине. Такође, морају се узети у обзир и степен социјалног и економског развоја сваке земље и поштовати развојно оријентисани аспекти информационог друштва."

Многе здравствене организације, од државног нивоа до нивоа примарне здравствене заштите, развијају и уводе разне облике информационих система и система електронске медицинске документације (електронски картони пацијента, енг. *Electronic Patient Record EPR*). Саставни део набавке или сопственог развоја тих система је и процес обезбеђивања заштите информација, као и процес дефинисања начина да се смање ризици и спрече негативне последице које могу настати услед неадекватне заштите података. Приватност података се односи на жељу појединца да контролише публиковање (јавно изношење) личних здравствених и других информација. Поверљивост се односи на информације – у овом контексту, на могућност појединца да контролише начин на који пружалац здравствене услуге (организација или појединац) користи личне информације, као и даље ширење тих информација (издавање другим појединцима или организацијама). Заштита омогућава осигурање приватности и поверљивости кроз избор стратегија, процедура и механизама заштите.

Информациона безбедност се дефинише као скуп техничких и административних процедура установљених са циљем да се подаци заштите од неовлашћеног или ненамерног увида и отуђења или уништења, као и ради заштите функционалности самог информационог система.

3.1. ЦИЉЕВИ ЗАШТИТЕ ПОДАТАКА И ИНФОРМАЦИЈА

„Безбедносне претње информационом друштву разноврсне су и специфичне по томе што су превасходно усмерене на злонамерно дестабилизовање информационих система. Онемогућавање нормалног функционисања информационих система у друштву које је од њих постало зависно може имати врло озбиљне последице на све сфере друштвеног живота. Последице могу бити чак и фаталне уколико се угрозе поједине инфраструктуре, као што су, нпр. системи за контролу копненог и ваздушног саобраћаја, хидроцентрала, нуклеарних електрана, безбедносних и здравствених служби или, пак, за дистрибуцију електричне енергије" (Путник, Бошковић, 2013).

Напредак умрежавања информационих система проширио је, у односу на концепт информационе безбедности, листу својстава информација пред које се постављају безбедносни захтеви тј. циљеви. Са становишта информационог обезбеђења значајно је задовољавање следећих својстава информационих система: приватност или поверљивост (енгл. *privacy, confidentiality*), интегритет (енгл. *integrity*) и расположивост (енгл. *availability*). Њима се понекад додају још два: аутентичност (енгл. *authentication*) и неопозивост (енгл. *nonrepudiation*).

Циљ приватности је да дозволи приступ информацији искључиво ауторизованим лицима или програмима. Поверљивост података може бити везана за разлоге националне безбедности (нпр. информације о наоружању), индустријске безбедности (нпр. пројекти неког новог производа) или личне приватности корисника (нпр. у здравству одређена обољења).

Интегритет је циљ који тежи да осигура податке и ресурсе који њима управљају (хардвер и софтвер) тако да могу бити модификовани или уништени само уз посебну и претходно дефинисану ауторизацију .

Циљ расположивости се састоји у томе да подаци буду у сваком тренутку доступни ауторизованим корисницима. Другачије речено, систем који даје такве услуге треба да функционише само када се то од њега захтева и то у ограниченом и унапред одређеном времену.

Са гледишта информационе безбедности, расположивост представља способност заштите од штетног догађаја или способност бекапа система у случају када се нежељени догађај већ десио. Расположивост савремених информационих система, који су у стању непрекидне активности, неопходна је како за нормално извршавање активности информационог друштва тако и за безбедност људских живота (нпр. напајање електричном енергијом аутоматизованих уређаја у интензивним негама и операционим салама у здравственим установама, од којих директно зависе животи пацијената).

„Аутентичност је мера безбедности која има за циљ да одреди вредност и валидност преноса, поруке или онога ко је шаље. Овом мером се контролише и ауторизација корисника да прими специфичне категорије информација" (Путник, 2012).

Неопозивост је мера безбедности чији је циљ да осигура ток комуникације. Овом мером безбедности се постиже да пошиљалац информације има доказ о њеној испоруци, али и да прималац информације има податак о идентитету пошиљаоца. То има за циљ да ниједан од учесника у преносу не може негирати извршену трансакцију.

Степен важности наведених својства информација варира у зависности од контекста у којем се размена информација врши (Костић, 2004).

Ови циљеви се у медицинској информатици посебно фокусирају на специфичне аспекте:

- доступност која обезбеђује тачну и ажурну информацију, свакоме коме је потребна и на месту на којем је потребна,
- урачунљивост помаже да су корисници одговорни за свој приступ и коришћење информација по принципу потреба и права да одређену информацију знају,

- дефиниција периметра омогућава да систем контролише границе поверљивог приступа и физички и логички,
- приступ базиран на улогама омогућава приступ корисника само оним информацијама које су важне за њихов посао чиме се ограничава и спречава искушење да неко неовлашћен приступи информацијама које су ван граница његових легитимних потреба,
- свеобухватност и контрола обезбеђују да власник електронске документације (организација, лекар, медицинско и парамедицинско особље укључено у процес пружања здравствене услуге), ИТ особље и пацијенти могу да разумеју и имају ефективну контролу над прикладним аспектима поверљивости и приступа информацијама.

Заштита података и једноставност, лак приступ су често супротстављени захтеви: поједностављење приступа може угрозити сигурност података ако софтверска апликација није пажљиво и адекватно пројектована и инплементирана, док превише рогобатни механизми заштите најчешће нарушавају ергометрију апликације са становишта корисника. Велики део лаика, али и информатичких професионалаца, нажалост, не уважавају комплексност заштите информација чак и када разумеју њен значај.

3.2. ПРАВНА РЕГУЛАТИВА У ОБЛАСТИ ЗАШТИТЕ ЛИЧНИХ ПОДАТАКА У ЗДРАВСТВЕНИМ УСТАНОВАМА У РЕПУБЛИЦИ СРБИЈИ

Права везана за здравље спадају у основни корпус људских права. Пацијент се налази у центру здравственог система, његова права штити Устав, а посебну пажњу придају им различите области грађанског, радног, па и кривичног права.

Права пацијента се тичу свих – болесних и оних који на било који начин долазе у контакт са здравственим системом, очекујући адекватно пружање медицинске услуге. Због специфичног положаја лица које долази у здравствену установу, јер му је угрожено здравље, права која му стоје на располагању су од кључне важности за његову сигурност и поверење према онима који му ту заштиту пружају. Управо зато, креатори закона морају познавати деликатност материје која

се односи на права пацијената и са посебном пажњом дефинисати сваку одредбу која ће уређивати и штитити права у области здравствене заштите.

Након представљања Нацрта закона о заштити права пацијената, широке јавне расправе која је након тога отворена, низа примедби и сугестија које су упутиле институције, невладин сектор и независна тела, постојала је нада да ће у скупштинску процедуру бити упућен акт који ће на јасан и свеобухватан начин пружити адекватну заштиту пацијентима. Међутим, Нацрт је постао Предлог са незнатно измењеним текстом, остављајући низ правних празнина које ће, уколико буде изгласан, изазвати велике проблеме у пракси управо онима које треба да штити.

Поред недовољно прецизираног начина остварења утврђених права, неадекватног уређивања механизама заштите и изостављања из текста Закона дефинисања процедуре по приговору пацијената, посебан проблем представља начин на који је уређено право на поверљивост података о здравственом стању пацијента.

Чланом 16 Закона о заштити података о личности прописано је да подаци који се односе на здравствено стање спадају у групу нарочито осетљивих података. У складу са тим, приступ подацима из медицинске документације и право њихове обраде мора бити омогућено само у складу са правилима о професионалној поверљивости и заштити личних података.

Многобројна истраживања и проблеми са којима се сусрећемо у свакодневној комуникацији са грађанима показују да запослени у здравственим установама нису обучени да поступају са подацима и нису свесни значаја њихове заштите, тако да се често дешава да податке о здравственом стању својих пацијената достављају својим колегама који не учествују у непосредном лечењу пацијента. Такође, углавном не дозвољавају пацијентима увид у медицинску документацију, нити издају копију на њихов захтев. С друге стране, пацијенти постају свесни својих права само у случајевима када посумњају у адекватно вођење медицинске документације, у смислу тачности података који се уносе, и у случајевима када чланови породице умрлог пацијента посумњају у лекарску грешку и суоче се са проблемом немогућности да остваре увид у медицински картон преминулог пацијента.

Како би се спречиле повреде основних људских права, поред прецизних и адекватних законских норми које уважавају комплексност и осетљивост материје коју уређују, кључно је обезбедити јаке механизме заштите.

Основна примена Закона о здравственој документацији и евиденцији („Службени гласник РС”, бр. 123 од 10. новембра 2014., члан 44 став 1) је уређење здравствене документације и евиденције, начина и поступака вођења здравствене документације од стране лица овлашћених за те послове. Затим, уређује уписивање података, рокове за достављање и обраду података, начин располагања подацима из медицинске документације пацијената, обезбеђивање квалитета, заштите и чување података.

Овај Закон обухвата и обавезне мере система безбедности којима се штите подаци које поседују здравствене установе.

Надзор над спровођењем овог Закона врши Министарство здравља. Казнене одредбе су у распону од 50.000 до 2.000.000 РСД за прекршаје који се односе на невалидне збирне извештаје, нетачност података, непоштовање процедура и све друге радње које имају за последицу било шта што доводи у питање сигурност здравствене документације.

Најбитнија информација за све оснивaче, менаџере и друга одговорна лица у приватној пракси и здравственим установама је да по члану 59 Закона све организације у области здравства уствари имају дуг рок, од чак 18 месеци, да ускладе своје правне акте, организацију и рад са одредбама овог Закона, а најкасније до 2020. године. Другим речима, постоји довољно времена да се уради све што нови Закон прописује.

Ова информација је битна и зато што су се на тржишту појавиле бројне агенције које нуде услуге обуке или услуге усклађивања ситуације са захтевима Закона.

Приликом доношења овог Закона, држава је имала у виду чињеницу да је у претходном периоду дошло до интензивног развоја здравствених и информационо-комуникационих технологија, и да се јавила потреба да се на јединствен начин уреди област здравствене документације и евиденција. Највећи део промена се доноси да би се у систему јавног здравства примениле савремене технологије и

технике, да би се створили предуслови да се здравствена документација и евиденције воде на јединствен начин и да би се применили стандарди Европске уније. Без обзира на намеру да се првенствено постигну циљеви у области јавног здравства, Закон ипак производи значајна дејства у области приватног здравства и односи се на мање организације.

Ово су неке од најбитнијих одредби Закона на основу којих се може лакше оријентисати:

Члан 11 – Дефинишу се три основне групе здравствене документације и евиденција и то:

- медицинска документација и евиденције о пружању здравствених услуга и здравственом стању пацијената и становништва,
- здравствена документација и евиденције за праћење фактора ризика из животне средине,
- здравствена документација и евиденције о кадровима, опреми, простору, лековима и медицинским средствима и информационо-комуникационим технологијама.

Члан 12 – Медицинска документација и евиденције о пружању здравствених услуга деле се на основну медицинску документацију и помоћна средства за вођење евиденције (картони, протоколи, отпуснице, евиденције и др).

Члан 13 – Дефинише се шта се уписује од података о пацијенту, а шта о здравственом стању и услугама.

Чланови од 14 до 25 – Регулише се место вођења и који тачно подаци се воде/уписују за специфичне категорије осигураника.

Члан 26 – Дефинисана је садржина здравствене документације и евиденције за праћење фактора ризика из животне средине.

Члан 27 – Прописује основну документацију о ресурсима у здравственим установама и приватној пракси, односно о кадровима, опреми, лековима и медицинским средствима и информационо-комуникационим технологијама.

Члан 28 – Предвиђа се обавеза приватне праксе да извештава надлежни завод, односно институт за јавно здравље.

Такође је предвиђено и постојање:

- Индивидуалног извештаја, пријава, пријава промене и одјава (садржина документа предвиђена чланом 29 Закона);
- Збирног извештаја (садржина документа предвиђена чланом 30 Закона).

Члан 33 – Детаљно даје списак осталих образаца за вођење и располагање (рецепти, упутнице, налази и др).

Члан 34 – Предвиђен је рок за слање индивидуалних извештаја из члана 28 (најкасније до 10. у месецу за претходни месец, а у случају збирних кварталних извештаја рок је најкасније до 15. у месецу – првом месецу који следи након краја квартала (април, јул, октобар, јануар).

Чланови од 37 до 41 – Предвиђају начин вођења, располагања и рокове чувања документације и евиденције. При томе је предвиђено да се евиденција води писмено или електронски. У одредбама се наводи да уколико се евиденција води електронски, а нису испуњени сви услови за то, постоји обавеза штампања и чувања папирне евиденције. С обзиром на то да се прецизни услови не дефинишу, Закон у овом делу остаје недоречен. Битно је да се дефинише обавеза да се документација и евиденције које се воде у електронском облику морају потписивати квалификованим електронским потписом, па се може претпоставити да ће ово бити основ за исправно вођење евиденција у електронском облику.

Члан 45 – Предвиђа да здравствене установе и приватна пракса имају обавезу да успоставе информациони систем, који представља свеобухватни скуп технолошке инфраструктуре (мрежних, софтверских и хардверских елемената), као и организационе процесе који ће подржати примену тог информационог система (људи и поступци за прикупљање, смештање, обраду, чување, пренос, приказивање и коришћење података и информација). Овим чланом се дефинише читав сет функционалности и елемената које информациони систем мора да има у односу на сложеност организације и процеса. Ближи услови за функционисање, принципи и стандарди ближе су одређени подзаконским актима.

Чланови од 46 до 49 – Предвиђају постојање „електронског медицинског досијеа" и „електронског медицинског картона". Ово су унифициране електронске евиденције, које садрже широк сет података о сваком кориснику медицинске

заштите. Суштински ове одредбе дефинишу креирање свеобухватног електронског регистра сваког грађанина, који ће бити на располагању надлежним здравственим радницима. Пацијент ће морати да да писану изјаву уколико не буде желео да буде регистрован на овакав начин.

Чланови од 54 до 57 – Предвиђене су казнене одредбе у случајевима непоштовања законских одредби.

Члан 58 – Предвиђа рок од 24 месеца за доношење прописа за спровођење овог закона од стране министра.

4. ИНТЕГРИСАНИ ЗДРАВСТВЕНИ ИНФОРМАЦИОНИ СИСТЕМ (ИЗИС)

Интегрисани здравствени информациони систем (ИЗИС) Републике Србије организује се и развија ради планирања и ефикасног управљања системом здравствене заштите, системом здравственог осигурања, као и ради прикупљања и обраде података у вези са здравственим стањем становништва, финансирањем здравствене заштите и функционисањем здравствене службе.

ИЗИС представља централни електронски систем, у коме се чувају и обрађују сви медицински и здравствени подаци о:

- пацијентима,
- здравственим радницима и сарадницима,
- здравственим установама,
- здравственим интервенцијама и услугама извршеним у ЗУ,
- електронским упутима и електронским рецептима,
- заказивању за специјалистичке прегледе, дијагностичке процедуре и хирушке интервенције.

Интегрисани здравствени информациони систем Републике Србије чине: здравствено-статистички систем, информациони систем организација здравственог осигурања и информациони системи здравствених установа, приватне праксе и других правних лица (извор: Мој доктор, презентација Министарстава здравља).

Поуздана и правовремена информација је темељ у доношењу одлука у целом здравственом систему и од суштинског значаја за развој и спровођење политике здравственог система, његове правне регулативе, истраживања у здравству, за развој људских ресурса у здравству, али и здравственог образовања, додатних тренинга и едукације, за пружање услуга, као и за само финансирање целокупног здравственог система.

Дакле, здравствени информациони систем обезбеђује темеље за доношење одлука и има четири кључне функције: генерисање, сакупљање, анализу и синтезу, као и комуникацију и коришћење.

Увођењем ИЗИС-а омогућено је лакше и боље планирање у области здравствене заштите. Применом система повећава се квалитет услуга пацијентима, транспарентност информација, благовремено извештавање пацијената и шире јавности, обезбеђује се објективан став према пацијентима и побољшава приступ здравственим установама, смањењем времена чекања на третман.

Типови упута

За даља упућивања, у систему постоји 5 типова упута:

1. Упут са термином
2. Упут без термина (упут изван термина)
3. Приоритетни упут
4. Хитни упут
5. Контрола (са термином)

1. Упут са термином

При креирању упута са термином лекар специјалиста обавезно бира установу у коју упућује пацијента, специјалност ресурса и ресурс према коме се упућује пацијент. Пацијент се упућује у тачно изабрани ресурс у установи. Након избора свих података приказује се први слободни термин. Уколико пацијенту не одговара први слободни термин, лекар у договору са пацијентом бира неки други слободан термин, који је дефинисан и одобрен. Уколико има потребе, лекар може креирати и више упута при прегледу, потребно је да за сваки упут понови поступак креирања упута.

Напомена: Упут са термином пацијенту обезбеђује тачан сат и датум прегледа код тачно утврђеног специјалисте, односно за тачно утврђени апарат.

2. Упут без термина

При креирању упута без термина обавезно се бира установа и специјалност ка којима се пацијент упућује. Упут без термина траје 30 дана. У том року пацијент има право да добије медицински третман од стране лекара специјалисте у установи у коју је упућен. За пацијенте без термина је предвиђен период у току дана за прегледе како се не би нарушио ред прегледа пацијената са термином.

Напомена: Прегледи са упутом без термина не смеју нарушити ред прегледа пацијената са одређеним термином.

3. Приоритетни упут

Уколико здравствено стање пацијента захтева хитни преглед од стране специјалисте или дијагностички преглед, лекар специјалиста током прегледа може креирати приоритетни упут. Приоритетни упут се креира избором установе и специјалности и исти може бити реализован у систему у току наредних 24 сата.

Напомена: Лекар који креира приоритетни упут је одговоран за унете податке (дијагноза, налаз и сл.) и исти потврђује да је здравствено стање пацијента заиста хитно.

4. Хитни упут

Уколико пацијент због здравственог стања долази на преглед код лекара специјалисте у ургентни центар или амбуланту без упута, лекар специјалиста креира хитни упут. Упут се креира уносом ЈМБГ или ЛБО пацијента коме се пружа здравствена услуга.

Напомена: Сви пацијенти без електронски креираног упута морају бити означени на овај начин како би могли бити евидентирани у систему. У вези са тим, у транзиционом периоду до преласка на потпуно централизован начин рада, мораће се користити ова врста упута и када по природи стања пацијент није „Хитан”.

5. Контрола (са термином)

Лекар при прегледу пацијента са хроничним обољењем, у систему креира упут са термином за поновни преглед. Лекар може заказати поновни преглед само у сопственом календару активности и при томе не мора да има већ креирано време за пријем пацијента.

На овај начин, пацијент лакше долази до неопходне медицинске неге, односно не мора да иде код изабраног лекара како би заказао поновни преглед.

4.1. ЗАШТИТА ИЗИС-а

Дата центар формиран је по препорукама *Cloud Security* Alliance – Cloud Controls Matrix (*CCM*), која укључује 16 стандарда као нпр. *ISO 27001*, *COBIT, PCI, HIPAA* і *FedRAMP*.

Системи заштите (*Unified Threat Management - UTM*):

- *Firewall with 4Gb/s throughput*;
- *IPS with 4Gb/s throughput*;
- *IPSec VPN* концентратор.

Мрежна инфраструктура се заснива на *Cisco* (*Nexus*) і *HP*- технологији (*VirtualConnect*, односно *FlexFabric*). Заштита ради на нивоу *Firewall*-а, где је сваки корисник мрежно изолован и налази се у посебном *VLAN*-у. Поред заштите на нивоу *Firewall*-а постоји и *Intrusion Prevention System – IPS* заштита као и *Distributed Denial of Service – DDoS* заштита.

У систему се креирају различите улоге како би сваки корисник у систему имао приступ тачно одређеним функционалностима, тачно одређеним подацима и дозволу за обављање одређеног типа радње у зависности од радних задатака које обавља.

Сваком кориснику у систему се додељује бар једна улога у систему. Доделом улога, сваки корисник кад се најави у систем, има персонализован поглед и дозвољен му је приступ само оним функционалностима дефинисаним према додељеним улогама.

У систему је имплементирана једносмерна криптографска функција коришћењем *hash* и *salt* за чување лозинки корисника да би се спречило пробијање (нежељено откривање) лозинки.

За већу безбедност, лозинка представља комбинацију од најмање 8 алфанумеричких карактера, најмање једног великог слова и специјалног знака.

У систему је омогућено постављање временског ограничења трајања лозинке. Све лозинке корисника у систему се памте и није дозвољено коришћење једне те исте лозинке више пута.

Сваки корисник аутоматски се одјављује у систему након 15 минута неактивности.

Подсистем сервиса за интеграцију са осталим системима обезбеђује интерфејс за интеграцију са постојећим локалним информационим системима који се користе у јавним и приватним здравственим установама. *Web* сервиси су документовани адекватном документацијом која се налази на *web* порталу за подршку, на који ће се именовани корисници система најављивати корисничким именом и лозинком (корисници су фирме произвођачи софтвера).

Интеграција се изводи имплементацијом *web* сервиса, разменом *XML* документа путем *HTTPS* конекције.

Web сервиси могу бити:

1. Јавни (без аутентификације)
2. Заштићени (аутентификација на нивоу корисника)

Заштићени сервиси су доступни само аутентификованим корисницима. Аутентификација ради на принципу корисничког имена и лозинке добијене од ИЗИС-а и добијањем сесијског токена са временом истицања од једног сата после задње активности.

Саставни део ИЗИС-а је *API* портал у коме је детаљно описан апликациони програмски интерфејс за интеграцију локалних ИС (који се користе на примарном, секундарном и терцијарном нивоу) са ИЗИС-ом.

4.2. ПРЕДЛОЗИ ЗА УНАПРЕЂЕЊЕ ИЗИС-а

Поуздана информација је темељ у доношењу одлука у целом здравственом систему и од непроцењивог је значаја за развој и спровођење политике здравственог система, његове правне регулативе, истраживања у здравству, за развој људских ресурса у здравству, здравственог образовања, додатних едукација, као и за финансирање целокупног здравственог система (извор: Удружење информатичара у здравству Србије, 2014).

„Информатизација у здравству је почела још 80-их година прошлог века, када су поједине установе набавиле прве рачунаре, али прва организованија информатизација почиње тек 2003. године кроз пројекте Министарства здравља. Развој здравства Србије, *DILS*, Развој здравства Србије - додатно финансирање *IPA 2008* и *EU IHIS*" (Ђокић, 2012).

Као што смо напоменули више пута, ИЗИС је назив електронског система преко којег лекари заказују пацијентима преглед код специјалисте. Циљ система је да се пацијенти растерете и да не морају сатима да зову клинике ради заказивања термина. Ипак, лекари опште медицине се жале: систем ИЗИС одбија да закаже код појединих специјалиста, што пацијенте оставља без валидног упута.

Након више од деценије, намећу се следећа питања: Докле се стигло са информатизацијом у здравству и са развојем ИЗИС Србије? Шта је до сада урађено? Шта је преостало да се уради? Који су проблеми? Које су потребе? Шта је потребно да се уради како би се информатизација здравственог система убрзала тј. унапредила и тако почела да даје резултате који су од користи за пацијента, установу и државу?

Да би се добили одговори на ова питања у периоду од марта до маја 2014. године, спроведена је опсежна анализа. У истраживању је учествовало 272 од 384 (70,8%) здравствених установа које су у плану информационе мреже здравствених установа. Циљ анализе је био да се кроз одговоре и препоруке понуди и стручна подршка процесима брже и квалитетније информатизације и развоја ИЗИС Србије, а све са циљем подршке унапређењу, ефикасности и квалитету лечења пацијената, рационалности у пружању здравствених услуга и испуњавања захтева процеса придруживања ЕУ.

„Општи закључак је био да се ИЗИС Србије налази на степену развоја који захтева значајна унапређења у погледу организације, квалификованог кадра, инфраструктуре, опреме, софтвера и прописа" (Ђокић, 2012).

Комплетном анализом искустава, примедби и предлога анкетираних установа, као и анализом правних оквира, издвојен је низ препорука које су заокружене закључком:

Потребно је да се унутар Министарства здравља формира сектор Дата Центар ИСИС Србије (сада постојећи), већ предвиђен акционим планом за реализацију стратегије развоја информационог друштва (2013-2014.), који би био одговоран директно Министру здравља.

Дата Центар је, према тадашњим плановима, требало да буде састављен од тима информатички стручних, стално запослених кадрова, а тада су му планиране следеће улоге:

Део сектора би учествовао у обезбеђивању свих потребних информација намењених Министарству здравља, здравственим и јавно-здравственим установама, здравственим радницима, грађанима, пацијентима, привреди и фондовима здравственог осигурања, као и осталим националним здравственим системима, другим Министарствима и осталим државним институцијама, као и процесима који проистичу из обавеза у погледу придруживања ЕУ;

Други део сектора би био одговоран за планирање, праћење и контролу развоја и унапређења ИЗИС Србије. Његова би улога била да учествује у пословима координације (планирање, вођење, праћење и контрола реализације) информатичких пројеката којима би се, из донација ЕУ, кредита или буџета, обезбедила средства за:

- Изградњу недостајућих или унапређење постојећих рачунарских мрежа, као и набавку рачунарско-комуникационе опреме потребне за безбедан и сигуран рад у свим здравственим установама;
- Регулисање питања лиценци, односно легализације употребе комерцијалних софтвера и спровођење детаљне обуке информатичара;

- Увођење недостајућих и унапређење уведених информационих система, као и за дигитализацију уређаја и интеграцију свих система унутар здравствених установа;
- Спровођење свих мера у погледу безбедности система података, уз обезбеђење услова за одрживост функционисања система;
- Опремање Дата Центра Србије;
- Едукацију постојећег информационог кадра;
- Информатичку едукацију за менаџмент здравствених установа.

Неопходне су измене постојећих правних аката којима би се законски уредило постојање надлежности, одговорности, али и употреба и старање о информационим системима, опреми, подацима и документима у дигиталном формату, које би се усагласле са Законом о здравственој документацији и евиденцијама у области здравства.

Израда недостајућих правних аката би дефинисала:

- Задужења и одговорност за обезбеђивање адекватних просторно-техничко-технолошких услова;
- Питање чувања, безбедности и власништва над подацима, стандардима приступа, коришћења и обраде података;
- Услове и квалификације за рад на информатичким пословима у здравственим установама;
- Изворе потребних средстава за даљу информатизацију свих нивоа у здравственом систему, као и за редовно одржавање и унапређивање уведених информационих система;
- Предлагање нових правних аката.

Потребно је израдити:

- Стратегију *e*-здравље која ће бити у складу са препорукама *WHO* и *EU*;
- Нови акциони план за реализацију стратегије развоја информационог друштва, јер је стари за период од 2013. до 2016. године;
- Правни документ који у потпуности дефинише дужности и одговорности информатичке подршке у свим деловима и сегментима у

оквиру Закона о јавном здрављу, а посебно о интерресорном прикупљању, аналитици, извештавању и предузимању мера по питању заштите животне средине.

- Измене и осавремењивање постојећих правних аката.

Потребно је изменити:

- Правилник о ближој садржини технолошких и функционалних захтева за успостављање Интегрисаног здравственог информационог система;
- Правилник о условима и начину унутрашње организације здравствених установа;
- Правилник о условима обављања здравствене делатности у здравственим установама и другим облицима здравствене службе;
- Правилник о специјализацијама и ужим специјализацијама здравствених радника и здравствених сарадника;
- Уредбу о коефицијентима за обрачун и исплату плата запослених у јавним службама, те да се уведу радна места информатичара у здравственим установама.
- Пружање информатичке подршке свим осталим активностима Министарства здравља и успостављање сталне сарадње са Удружењем информатичара у здравству Србије.

Здравствени информациони систем има четири кључне функције: генерисање, сакупљање и анализу и синтезу, као и комуникацију и коришћење. ИЗИС прикупља податке из здравственог сектора, анализира податке и обезбеђује њихов свеукупни квалитет, релевантност, правовременост и претвара податке у информације потребне за доношење одлука.

Поред тога што је од суштинског значаја за мониторинг и евалуацију ИЗИС такође служи и за шире циљеве, као што су пружање могућности раног упозоравања, подршка пацијентима (корисницима здравствених услуга), помагање менаџерима здравствених установа, омогућава планирање, подршку и подстицање истраживања, указујући на здравствено стање и анализу трендова, подржавање глобалног извештавања и подршка у комуникацији између различитих корисника. Информација је од мале вредности ако није доступна у форматима који

задовољавају потребе више корисника, креатора политике, планера, менаџера здравствених услуга, разних заједница и појединаца.

Обзиром да ИЗИС има више корисника и широк спектар намена, његова улога се може дефинисати и као подршка у стварању информација које могу да помогну доносиоцима одлука на свим нивоима здравственог система да идентификују проблеме и потребе, омогућавајући доношење одлука заснованих на доказима. Стога се по Светској здравственој организацији подаци из различитих извора користе за више циљева који су на више нивоа здравствене заштите:

1. Подаци на нивоу пацијента и његових потреба за здравственом заштитом и лечењем, као основа за клиничко одлучивање. Проблеми могу настати када услед лоших или слабо координисаних подсистема преоптерећени здравствени радници морају да уносе пуно података, или исте податке у више подсистема);
2. Подаци на нивоу здравствене установе – подаци из извештаја пословања установе, тј. управљачких извештаја (нпр. евиденције о набавкама лекова), који омогућавају здравственим менаџерима да управљају ресурсима (праћење стања залиха, потреба и усмеравање одлука о набавкама);
3. Подаци о популационом нивоу су од суштинског значаја за јавно здравље, доношења одлука, генерисање информација о корисницима услуга, као и о онима који их не користе. Подаци морају бити високог квалитета, морају да се односе на све установе (јавне и приватне) и да буду репрезентативни за становништво у целини.
4. Надзор над јавним здрављем спаја информације настале из података установа и заједнице са фокусом на дефинисању проблема у пружању основе за правовремено деловање (хитност, епидемије, болести...)

После 2000. године информатизација у здравству долази под окриље Министарства здравља и почиње да се спроводи захваљујући његовим пројектима, али и кроз самостално ангажовање здравствених установа. Пројекти који су били под окриљем Министарства здравља су:

Развој здравства Србије, који је трајао од 2003. до 2012. године, финансиран је из кредита Светске банке са 23.480.000 УСД. Део средстава био је намењен за

информатизацију четири опште болнице (Краљево, Ваљево, Зрењанин и Врање) и израду Централног информационог система (ЦИС) – портала за централизовано прикупљање и коришћење ресурсних података и објављивање шифарника који се користе у здравственом систему Републике Србије.

Развој здравства Србије – додатно финансирање (*SERBIA HEALTH Additional Financing*), почео је 2009. године и такође је финансиран из кредита Светске банке са 13.500.000 УСД. Помоћу њега су направљени и добијени болнички информациони системи (БИС) у још 14 здравствених установа (ГАК КЦ Србије, Клиника за хирургију КЦ Србије, КБЦ „Др Драгиша Мишовић" – Дедиње, итд.).

Светска банка је са 46.400.000 УСД финансирала пружање унапређених услуга на локалном нивоу – Delivery of Improved Local Services Project (DILS) у периоду од 2008. до 2014. године.

IPA 2008. који је финансиран из Донације ЕУ у вредности од 7.500.000 евра.

EU HIS, почео је 2012. године и финансиран је из донације ЕУ у вредности од 2.500.000 евра. Пројектом је потпомогнут развој електронског здравственог досијеа и увођење БИС-а у 19 здравствених установа.

Познато је да је најскупљи информациони систем онај који је делимично и непотпуно искоришћен, јер су уложена средства недовољно искоришћена. Да би се урадила ситуациона анализа спроведено је истраживање и анализирани су правни оквири за развој ИЗИС Србије. Истраживање је спроведено у периоду од марта до маја 2014. године у свим здравственим установама у Србији. Рађено је по методу дескриптивне опсервационе студије (*Cross sectional study*).

Имајући у виду да је циљ истраживања анализа стања и потреба у информационој структури у здравственим установама, креирана је анкета сачињена од питања која су се односила на:

1. Основне информације о установи;
2. Организацију и кадровске ресурсе;
3. Садашње стање ИТ опреме и потребу за унапређењем:
   - Серверских соба;
   - Рачунарских мрежа;

- Хардвера;
- Системског софтвера;
- Апликативног софтвера;

4. Потребе у погледу одрживости система.

4.3. АНАЛИЗА СТАЊА ИКТ ОПРЕМЕ И ПОТРЕБА ЗДРАВСТВЕНИХ УСТАНОВА

Од 272 установе, 160 (15,8%) се изјаснило да има серверску собу. Анализа је показала да електро-проводни под (антистатички под), као један од техничких предуслова које по стандардима мора да задовољи серверска соба, имају само 43 установе, али да га од тога 4 установе немају у свим серверским собама. Преосталих 117 установа уопште немају електро-проводни под. Климатизацију, укључујући и сплит системе има 126 установа, а 33 чак ни немају сплит систем, док једна установа није дала одговор. Заштиту сервера од прекида у напајању струјом (УПС) нема 30 установа.

Дакле од 272 установе, 112 нема серверску собу, а од преосталих 160 чак 136 има потребу за унапређењем исте. Потребно је истаћи да је 129 установа ту потребу исказало, а 7 установа није, иако нема довољно простора, антистатички под или климатизацију. Преостале 24 установе су задовољиле ових неколико критеријума.

У примедбама које се односе на серверске собе, анкетиране установе су навеле да серверске собе треба изместити јер се налазе у неадекватним просторијама, као што су:

- библиотека,
- крај ходника,
- фотокопирница,
- архива,
- шалтери или ординације,
- просторија за медицинске интервенције,
- телефонска централа,
- канцеларија од 9 м^2 са још 5 запослених,
- сала за састанке,

- просторија за одлагање урина са столом за замену уринарних катетера код пацијената,
- канцеларија књиговодства,
- лекарска соба,
- архива рачуноводства,
- канцеларија за административне службенике,
- канцеларија за информатичаре.

Поред обезбеђивања серверске собе, њеног проширења или измештања, комплетне адаптације или реконструкције у складу са стандардима, неке анкетиране установе су имале захтев да им се обезбеди само:

- антистатички под,
- климатизација,
- преспојни орман или постоље (енг. *Rack*),
- рек серверски,
- уређаји за беспрекидно напајање ел. енергијом (УПС-еви),
- звучна изолација сервер собе,
- заштита од сунчеве светлости,
- да се заштити од могућег проблема са канализационим цевима које пролазе кроз сервер собу,
- безбеднија врата,
- противпожарни и противпоплавни системи,
- видео надзори и сигурносне браве,
- системи за аутоматску контролу микро климе,
- резервни клима уређај,
- агрегат,
- замена батерија за УПС-ове који су добијени у *DILS* пројекту
- спуштени плафон,
- систем за контролу приступа сервер соби.

Неке анкетиране установе су имале потребе да се:

- електроинсталације прилагоде стандардима за сервер собе, како би се омогућило стабилно напајање,

- замене стари дрвени прозори ПВЦ прозорима ради боље изолације простора.

Серверска соба представља централну компоненту без чијег је постојања, на овом степену развоја, тешко замислити један озбиљан информациони систем здравствене установе.

Спора информатизација здравствених установа је допринела да рачунарска опрема застари пре него што је добила своју пуну употребну функцију. Правно недефинисана надлежност је учинила да је одржавање и набављање рачунарске опреме добра воља управе здравстевене установе. Неке установе које су у пројектима Министарства, сматрају да је то у надлежности Министарства, док друге сматрају да је то у надлежности РФЗО-а, јер се по њиховом мишљењу информациони системи највише користе у РФЗО. Стање у установама које нису у пројектима Министарства је још горе, јер оне наручују рачунаре тек када на тржишту нема делова за поправку старих.

Узимајући у обзир постојеће стање опреме, сервери највише недостају специјалним болницама, клиникама, институтима и заводима за јавно здравство, радне станице недостају клиничким центрима и клиничко-болничким центрима, док су се потребе за штампачима највише исказале у клиничко-болничким центрима и клиникама.

Примедбе које су испитиване здравствене установе исказале, а које се односе на хардвер најчешће говоре о:

- застарелој опреми,
- потребној реконструкцији, осавремењивању, унапређењу мрежне инфраструктуре или постављању мреже,
- недостатку мрежне опреме,
- потребној обуци за програмирање и одржавање мрежне опреме,
- потребној мрежној инфраструктури која ће повезати удаљене делове установе који се налазе у руралним деловима Србије,
- добијеним штампачима из *DILS*-а који не могу да штампају рецепте,
- добијеном опремом из *DILS*-а која је инсталирана, али нико није обучен да је користи;

- потребним скенерима за дигитализацију папирне документације;
- штампачима који користе скупе тонере;
- потребе за ИТ буџетом.

Примери добијени анкетом:

Питање лиценци за комерцијалне софтвере који су у примени је нерешено. Иако закон о ауторским и сродним правима постоји, многе наше здравствене установе још увек користе нелиценциране „пиратске" софтвере. На најкритичнијим местима, користи се бесплатан антивирусни програм који не задовољава основе безбедности персоналног рачунара, а камоли рачунарских система.

Сервери који се користе за електронски здравствени картон раде под *Linux* оперативним системом, а на пример финансијско књиговодствени програм ради на нелиценцираном *Windows* оперативном систему. Што се радних станица тиче, у плану је комплетан прелазак на бесплатна решења, као што су *Ubuntu OS, Open office* и сл. Ситуација је слична и у погледу антивирус заштите, користе се бесплатна решења. Серверске базе се бекапују, али не и све радне станице.

Закључак: од 272 испитане установе ниједна установа нема комплетно уведене и интегрисане информационе системе који су јој потребни у подржавању процеса свакодневног рада.

„Он (информациони систем) не постоји" – једина је примедба из једне од установа!?

Да би се уведени информациони системи могли користити, неопходно је да се одржавају и унапређују. Одржавање треба да иде у правцу примене нових технологија и осавремењивања већ уведених система.

Закључак ИЗИС-а је да „Основни разлог за развој интегрисаног здравственог система Србије не треба да лежи у захтевима ЕУ, него у потреби да се унапреди здравствени систем Србије, јер је то систем у коме се сви ми лечимо и који остављамо нашим поколењима, која ће враћати милионске кредите уложене у реформу здравственог система" (извор: Удружење информатичара у здравству Србије, 2014).

5. ИНФОРМАЦИОНО-КОМУНИКАЦИОНИ СИСТЕМИ У ЗДРАВСТВЕНИМ УСТАНОВАМА

Према Закону о заштити података о личности („Сл. гласник РС” бр . 97/2008, 104/2009 и Закон 68/2012 – одлука УС 107/2012) који се односи на услове прикупљања и обраде података о личности, правна лица и заштиту права лица чији се подаци прикупљају и обрађују, под заштиту овог Закона подлежу: заштита података о личности, поступак пред надлежним органом за заштиту података о личности, обезбеђење података, евиденција, изношење података из Републике Србије и надзор над извршењем Закона.

Последњих година уочљиво је ангажовање Владе Републике Србије на унапређењу и побољшању функционисања информационо-комуникационих система, изради Плана о инфраструктури, као и заштити информација од посебног значаја.

Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, која је донета 17.11.2016. године, ближе се уређују мере заштите информационо-комуникационих система од посебног значаја.

У овој Уредби се потенцира имплементација организационе структуре, где ће бити јасно дефинисане улоге као и одговорности запослених у систему у којем се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система од посебног значаја.

Оператор ИКТ система од посебног значаја је дужан да, у оквиру организационе структуре, у складу са природом, обимом и сложеношћу пословања утврди послове и одговорности запослених у циљу управљања информационом безбедношћу.

Оператор ИКТ система утврђује, у оквиру организационе структуре, послове и одговорности запослених за заштиту информационих добара, односно средстава и имовине, за надзор над пословним процесима од значаја за информациону безбедност, за управљање ризицима у области информационе безбедности, као и за послове предвиђене процедурама у области информационе безбедности.

Подела одговорности запослених треба да се изврши тако да се онемогући неовлашћена или ненамерна измена, оштећење или злоупотреба средстава, односно информационих добара од стране оператора ИКТ система, као и да се онемогући приступ, измена или коришћење средстава без овлашћења и без евиденције о томе.

Оператор ИКТ система успоставља процедуре ради праћења активности, ревизије и надзора у оквиру управљања информационом безбедношћу.

Приликом коришћења мобилних уређаја мора да се обезбеди заштита података од интереса за оператора ИКТ система и смање ризици коришћења мобилних уређаја у незаштићеним окружењима (јавним местима, мрежама са непознатом или недовољном заштитом и слично), при чему оператор ИКТ система узима у обзир следеће:

1. Евиденцију мобилних уређаја;
2. Мере физичке заштите мобилних уређаја (од уништења, оштећења, губитка или неовлашћеног приступа уређајима и подацима од интереса за оператора ИКТ система);
3. Ограничења за инсталацију и ажурирање софтвера;
4. Инсталацију адекватних софтвера за мобилне уређаје и њихово редовно ажурирање;
5. Ограничење коришћења услуга информационог друштва које би угрозиле информациону безбедност ИКТ система;
6. Контроле приступа мобилном уређају и подацима на њему;
7. Криптографске технике;
8. Заштиту од вируса и других злонамерних софтвера;
9. Даљинско управљање мобилним уређајем у случају инцидента, од стране овлашћеног лица оператора ИКТ система, путем којег је могуће да се изврши неповратно брисање података и онемогућавање даљег коришћења уређаја;
10. Успостављање и одржавање резервне копије (*Backup*) података;
11. Омогућавање безбедног коришћења интернет сервиса и апликација.

Лица која користе ИКТ систем, односно управљају ИКТ системом, морају бити оспособљена за посао који раде и разумети своју одговорност.

Оператор ИКТ система је дужан да, уговором или другим актом, обавеже запослене и по другим основама ангажована лица да након престанка или промене радног ангажовања не откривају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система. Дужности и обавезе, које остају важеће и после престанка ангажовања, треба да буду садржане у условима уговора са запосленим, односно по другом основу ангажованим лицем.

Оператор ИКТ система је дужан да идентификује и класификује информациона добра, односно средства и имовину, путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИКТ систему, изврши попис информационих добара, односно средстава и имовине и успостави, одржава и редовно ажурира њихову евиденцију.

Оператор ИКТ система је дужан да класификацију врши према степену осетљивости и критичности, узимајући у обзир могуће последице нарушавања поверљивости, интегритета и расположивости добара, да доследно примењује ту класификацију, као и да, у складу с тим, обезбеди адекватан ниво заштите ових добара.

За свако информационо добро, односно средство и имовину, потребно је одредити задужено лице за њихову заштиту.

Класификовање података мора се сачинити тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из Закона о информационој безбедности.

Оператор ИКТ система одређује шему класификације података према којој се подаци класификују узимајући у обзир осетљивост, важност података, штету која може да настане услед неовлашћеног откривања, измене или брисања података и примењује прописе који уређују питања заштите података (тајни подаци, пословна тајна, подаци о личности и сл.).

Оператор ИКТ система је у обавези да дефинише одговарајући скуп процедура за поступање, обраду, складиштење и преношење података

Приликом дефинисања процедура и поступања са носачима података, треба предвидети неповратно брисање података, у случају када су истекли рокови за њихово чување и када они више нису потребни, поступак одобравања изношења

носача података из просторија оператора ИКТ система, чување носача података на безбедном месту, коришћење криптографских техника за заштиту података када је то предвиђено прописима, односно у другим случајевима када је таква врста заштите потребна, обезбеђивање сигурног преноса података на нови носач података, чување резервних копија на одвојеним носачима података и друге мере и поступке за заштиту носача података.

Оператор ИКТ система треба да предвиди процедуре за безбедно расходовање и уништавање носача података када више нису потребни, а које треба да на минимум сведу ризик од приступа подацима од стране неовлашћених лица.

Носачи података треба да буду заштићени од неовлашћеног приступа, злоупотребе или оштећења приликом транспорта, обезбеђивањем поузданог транспорта и поузданих особа које преносе носаче података и обезбеђивањем адекватне амбалаже у циљу физичке заштите приликом транспорта.

Оператор ИКТ система одређује за које податке, у складу са шемом класификације података, треба водити евиденцију о коришћењу носача података и предузетим поступцима у вези са заштитом података и носача података.

5.1. ОГРАНИЧЕЊЕ ПРИСТУПА ПОДАЦИМА И СРЕДСТВИМА ЗА ОБРАДУ ПОДАТАКА

Ограничење приступа подацима и средствима за обраду података подразумева дефинисање прецизних правила приступа, тако што се дефинише ко има право чему да приступи и која су ограничења приступа, а водећи рачуна о специфичностима података и опреме и одговорностима и радним задужењима лица која приступају подацима и опреми (Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја http://www.ratel.rs/).

Ограничење приступа подразумева хардверско, односно софтверско ограничење приступа подацима и средствима за обраду података, укључујући и физичко ограничење. Ограничење приступа врши се у складу са класификацијом података из члана 7 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја.

Оператор ИКТ система треба да обезбеди приступ мрежи и мрежним услугама само лицима која имају овлашћења за коришћење, да одобрава овлашћени и спречава неовлашћени приступ ИКТ систему и услугама које систем пружа.

Ради заштите тајности, аутентичности и интегритета података, оператор ИКТ система треба да размотри коришћење одговарајућих мера криптозаштите, узимајући у обзир осетљивост информација које треба да се штите, пословне процесе који се спроводе, ниво захтеване заштите, имплементацију примењених криптографских техника и управљање криптографским кључевима.

Управљање криптографским кључевима обухвата њихов целокупан животни циклус, укључујући генерисање, складиштење, архивирање, преузимање, расподелу, повлачење и уништавање кључева.

Оператор ИКТ система треба да посебно води рачуна о заштити средстава криптозаштите од свих облика компромитације.

У циљу физичке заштите објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему оператор ИКТ система мора да води рачуна о постављању средстава на безбедна места, елиминише непотребан приступ у простор у коме се налазе, врши редовне провере заштићености средстава од крађа, пожара, електромагнетних зрачења и других претњи и прати услове околине (температуру, влажност и др.) који би могли негативно да утичу на рад средстава.

Средства треба да буду заштићена у случају поремећаја у дистрибуцији електричне енергије, телекомуникационих капацитета, воде, гаса, вентилације обезбеђивањем алтернативних решења која омогућују наставак рада ИКТ система.

Измештање имовине ИКТ система може да се врши само уз претходно одобрење овлашћеног лица, уз примену безбедносних механизама, узимајући у обзир различите ризике приликом рада изван просторија организације.

Заштита од губитка података постиже се редовном израдом резервних копија података, софтвера и система путем одговарајућих средстава за израду резервних копија.

Оператор ИКТ система дефинише време чувања и заштите резервних копија, обим и учесталост резервних копија, безбедно место чувања резервних

копија, обезбеђује физичку заштиту резервних копија и заштиту од спољашњих утицаја, проверава носаче података како би се осигурало њихово исправно функционисање и поузданост у складу са планом израде резервних копија.

Оператор ИКТ система врши израду резервних копија које треба да обухвате све системске информације, апликације и податке који су неопходни за опоравак целокупног система у случају наступања последица изазваних ванредним околностима чува податке о догађајима који могу бити од значаја за безбедност система и брине се о заштити података у комуникационим мрежама, укључујући уређаје и водове.

Захтеви за информациону безбедност морају да се испуне у свим фазама животног циклуса ИКТ система односно делова система, што подразумева фазу пројектовања ИКТ система, успостављања новог или мењање постојећег ИКТ система, односно делова система, и набавку производа потребних за његово функционисање.

Успостављање новог ИКТ система, односно мењање постојећег, обухвата спровођење процедуре документовања, дефинисања захтева за информациону безбедност, проверу испуњености захтева, контролисање и управљање поступка увођења новог, односно мењања постојећег ИКТ система.

Захтеви за информациону безбедност морају да се испуне и када се врши пренос информација путем јавних комуникационих мрежа и користе апликативне услуге преко њих.

Приликом поверавања активности у вези са ИКТ системом трећим лицима, потребно је да оператор ИКТ система надгледа и прати активности развоја ИКТ система.

У погледу заштите података који се користе за потребе тестирања ИКТ система, односно делова система, оператор ИКТ система је у обавези да одреди одговорно лице за обавештавање надлежних органа о инцидентима у систему који могу да имају значајан утицај на нарушавање информационе безбедности. Оператор треба да дефинише и примењује процедуре које треба да обезбеде процесе за идентификацију, прикупљање и чување информација које могу да послуже као доказ ради покретања дисциплинског, прекршајног или кривичног

поступка, у оквиру редовних процедура за одржавање информационе безбедности или доношењем посебних процедура.

Оператор ИКТ система треба да успостави, документује, имплементира и одржава процесе, процедуре и контроле да би осигурао захтевани ниво континуитета пословања током ванредне ситуације.

Оператор ИКТ система треба да верификује успостављене и имплементиране контроле континуитета пословања у редовним условима рада, како би оне биле важеће и ефективне током ванредне ситуације.

Оператор ИКТ система треба да идентификује захтеве за доступност ИКТ система. Редундантне компоненте треба размотрити онда када се доступност не може гарантовати коришћењем постојећих архитектура система (Редунданција је дуплирање критичних компоненти система са циљем повећања поузданости).

5.2. ОПИС СТАЊА У ОБЛАСТИ ЗАШТИТЕ ЛИЧНИХ ПОДАТАКА У ЗДРАВСТВЕНИМ УСТАНОВАМА

Методологија процеса који се односе на заштиту личних информација у медицинским информационим системима, представља комплексан скуп стратегија које обухватају анализу система, контролу ризика и контролу процеса (Костић, 2004).

Основних шест корака у процесу развоја методологије заштите личних информација у информационим системима здравствених установа су: идентификација информатичких ресурса којима је потребна заштита; опис тј. приказивање архитектуре информационог система који се имплементира; идентификација опасности по информације; рангирање опасности у односу на потенцијалну штету која може да настане; дизајнирање предлога за решења која треба да умање хазарде и евентуалне последице; спецификација спроведених препорука.

Избор адекватне стратегије заштите представља проналажење равнотеже између нивоа и обима заштите, потенцијалних ризика и цене последица у случају настанка штете.

Здравствене установе су упознате са последицама до којих могу да доведу активности злоупотребе поверљивости информација, а са тим у вези постоји обавеза и потреба за безбедношћу и заштитом личних информација у процесу пружања здравствених услуга.

„Информација је податак са одређеним значењем, који има употребну вредност, односно сазнање које се може пренети у било којем облику (писано, аудио, видео , електронском или било којем другом).

Појам безбедности информација не односи се искључиво на техничке мере заштите (лозинке, заштита компјутерских програма, права приступа и сл.), већ подразумева и административне (безбедносне политике, правилнике, процедуре и слично), као и физичке мере заштите (видео надзор, заштита просторија, физичка контрола приступа и слично)" (Милосављевић, 2010).

Инфомациона безбедност постала је један од кључних фактора развоја друштва уопште, због чега се укључују бројни стандарди који су се показали најбоље у пракси, у безбедном управљању информацијама.

Сврха оваквог приступа информацијама је да обезбеди и заштити информације и имовину од што већег броја претњи, било унутрашњих или спољашњих, случајних или намерних, а кроз увођење – имплементацију, извршавање, надзирање, одржавање, побољшавање, односно, надоградњу и измене у складу са технолошким напретком система безбедности информација.

Када нека организација примени методолошки процес на одређени пројекат заштите разматрајући све организационе, пројектне и тимске промене, мала је вероватноћа да ће се потпуно подударити са било којом познатом методологијом за развој ИКТС-а. Зато су потребне сталне измене, надоградње и комбинације различитих методологија.

5.3. АРХИТЕКТУРА ИНФОРМАЦИОНИХ СИСТЕМА У ЗДРАВСТВЕНИМ УСТАНОВАМА

Информациони систем увек се појављује у контексту ширег система, односно његове архитектуре. Размена информација, њихова видљивост и

коришћење у спољашњим, тј. екстерним системима има значајну улогу у побољшању ефикасности свих пословних процеса. Са порастом потребе за што већом применом информационих система, све већим захтевима за разменом информација између различитих система и корисника, расте и ризик злоупотреба или губитка информација.

„Архитектура информационог система представља план остварења визије будуће функционалности система кроз спровођење потребних набавки, што укључује и сопствени развој и имплементације и елемената система" (Костић, 2004).

Процес набавке се спроводи кроз процедуру финансијског одлучивања у оквиру ресурса којима се располаже. Треба имати у виду да се обезбеде потребна технолошка и техничка средства (рачунари који су дефицитарни у здравственим установама) и комуникациона средства, али и особље које је едуковано да та средства примени на ефикасан начин.

„Неадекватна средства или нестручна употреба представљају највећи фактор ризика за функционалност система и безбедност података" (Ђокић, 2012).

До великих оштећења најчешће долази управо због потпуног одсуства свести о безбедности и импровизованог решења. Из тог разлога је веома битно професионално дизајнирање информационих система, поштовање основа планирања и спровођење механизама заштите информација.

Да би се смањио број хаварија и побољшала ефикасност информационих система, као и безбедност личних информација, уведени су међународни и европски стандарди (*ISO:IEC; ITU; SPS*). Стандардизацијом се постиже виши квалитет са доста нижим трошковима, као и безбедност лица и пословања. Да би систем функционисао предуслов је усаглашеност стандарда са прописаним процедурама.

„У Закону о стандардизацији Републике Србије (члан 3) стандард се дефинише као јавни доступан документ, утврђен консензусом и донет од признатог тела, у којем се за општу и вишекратну употребу утврђују правила, захтеви, карактеристике, упутства, препоруке или смернице за активности или њихове

резултате, ради постизања оптималног нивоа уређености у одређеној области у односу на постојеће или могуће проблеме" (Кековић, Савић и сарадници, 2011).

Стандардизацију можемо применити:

- за конфигурацију софтвера,
- обележавање фолдера и докумената,
- за конфигурацију електронских докумената (изгледа, формата, записа података, итд.).

Ништа мање битна за развој организације је обука запослених у циљу стицања нових знања и напредовања. Едукација би требало да се обавља на свим хијерархијским нивоима. Један од најбитнијих фактора је ангажовање адекватних и специјализованих едукатора.

Приликом спровођења едукације могу се јавити неки од следећих проблема: лош избор едукатора, неодговарајућа старосна доб запослених који се едукују, неусклађени термини одржавања обуке. Све ове проблеме могуће је ефикасно решити постављањем стандарда за едукацију.

5.4. ПРОЦЕНА РИЗИКА У ЗДРАВСТВЕНИМ УСТАНОВАМА

„Ризик је могућност да дође до материјалне или нематеријалне штете услед губитка информација. До штете могу довести људске грешке, намерне акције, као и технички или природни фактори" (Костић, 2004).

Прво се врши идентификација опасности по пословни процес, пословне циљеве и ресурсе организације. Након тога се спроводи истраживање ризика, што доводи до прављења планова за умањење ризика који могу имати најштетније последице. Овакав процес идентификације ризика и развој планова за њихово отклањање, дефинише се као управљање ризиком.

Здавствене установе не сагледавају све потенцијалне ризике и не формулишу целокупну и свеобухватну стратегију контроле ризика. Много је ажурнији свеобухватни приступ, чак и са основним механизмима заштите, у односу на парцијални са скупим механизмом.

Најделотворнији резултати су добијени употребом методологије *OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation),* која омогућава истраживање организационих и технолошких аспеката ради синтезе и добијања реалне слике о стању информационе безбедности. „*OCTAVE* омогућава да интерни тим идентификује факторе ризика за најкритичније објекте ИКТС и изгради план заштите за ублажавање тих фактора ризика" (Костић, 2004).

OCTAVE методологија се састоји из следећих фаза:

1. Идентификације и дефинисања опасности за ресурсе – Овде се анализирају организациона својства система. Истражују се основни информатички захтеви по сегментима организације, опасности по кључне информационе ресурсе, безбедносне мере које су потребне, тренутно примењене мере, као и организационе слабости и рањивости (организациона рањивост).

2. Идентификације слабости у инфраструктури – У овој фази се анализирају информатичка искуства. Кључне компоненте инфраструктуре (сервери, мреже, радне станице, екстерне комуникације, софтвери, оперативни системи, базе података...) се анализирају ради проналажења слабости и недостатака (технолошка рањивост) које могу довести до угрожености безбедности информационог система.

3. Развој сигурносне стратегије и плана – У овој фази се анализирају сви запажени ризици. Информације сакупљене у организационој и технолошкој процени анализирају се са аспекта идентификације ризика и процењује се значај сваког. На основу добијених резултата развијају се стратегија заштите и планови за избегавање појединих опасности у складу са значајем појединих ризика.

Процес увођења система заштите у стадијум оперативног рада може се разликовати, али је генерички ток, глобално посматрајући, веома сличан.

Процес имплементације система заштите одвија се у четири фазе:

1. Фаза припреме - утврђивање обима пројекта и избор тима;
2. Фаза идентификације - детектовање безбедносних фактора ризика;
3. Фаза ревизије - препоруке за измене система заштите;

4. Фаза прилагођавања - интеграција система заштите у складу са налозима ревизије.

Сваки процес имплементације система заштите састоји се од следећих обавезних компоненти:

- обуке запослених,
- надзора,
- контроле и ревизије усаглашености система,
- инсистирања на обавези спровођења политике заштите.

Обука запослених укључује детаљно упознавање свих запослених са политиком и процедурама заштите. Људски фактор је кључан за заштиту информација.

„Контрола усаглашености мери степен усаглашености имплементираног и усаглашеног система заштите са политиком, стандардима и законима заштите" (Ђокић, 2014).

Запослени у менаџменту организују, обезбеђују и одговорни су за контролу опште усаглашености политике заштите са нормативима и стандардима, као и за реализацију процеса који намећу политику заштите. Мониторинг (праћење) запослених је најлакши начин да се надгледа нормативна усаглашеност политике и процедура, али није у складу са Законом о заштити запослених. Послодавац је у обавези да обавести запослене да су сви подаци под сталним надзором.

Интерни надзор, контрола и техничка ревизија система заштите играју кључну улогу у заштити информационих система и олакшавају екстерну ревизију. „Препоруке стандарда заштите (*ISO/ IEC 27001*) су да се најмање једном годишње процењује ризик, а на основу те процене прави план за интерни надзор, контролу и ревизију" (Грубов, Милосављевић, 2010).

Препоручују се рутинске вежбе и симулације инцидента, чиме се истиче значај надзора, контроле и ревизије информационих система, обезбеђују приоритети заштите и управљање инцидентима.

Спољна ревизија се мора извршити у безбедном окружењу и атмосфери поверења уз обавезно присуство интерног ревизора и одобрење главног менаџера.

У извештају о ревизији треба обухватити одговоре на питања као што су:

- Заштићеност системских и апликативних програма;
- Ажурност и усаглашеност политике и других докумената заштите;
- Адекватност и прихватљивост мануелног/аутоматизованог система ревизије;
- Формат извештаја о ревизији;
- Свест о потреби, итд.

Ревизорски извештај је значајна информација за реинжењеринг и отклањање слабих тачака система заштите.

5.5. ФОРМУЛИСАЊЕ БЕЗБЕДНОСНЕ ПОЛИТИКЕ У ОБЛАСТИ ИКТ ЗДРАВСТВЕНЕ УСТАНОВЕ

Сврха имплементације информационих безбедносних система је да обезбеди сигурно пословање, заштиту поверљивих информација без обзира на њихов облик, као и подизање задовољства корисника квалитетом пружених услуга. „Циљ безбедности информација је да се обезбеди и заштити информациона имовина организације од свих унутрашњих и спољашњих, намерних или случајних, претњи кроз успостављање, имплементацију, примену, праћење, преиспитивање, одржавање *ISMS*, као дела интегрисаног менаџмент система, а у складу са захтевима *ISO/IFC 27001*" (извор: Управа за безбедност, 2017).

Ова политика представља оквир за успостављање циљева безбедности информација и гарантује:

1. Непрекидно побољшање пословања уз примену савремених информационих решења;
2. Заштиту информација;
3. Омогућава несметан приступ информацијама које су потребне за пружање услуга;
4. Спречава неовлашћен приступ информацијама, редовну заштиту истих, софтвера и мрежне инфраструктуре;
5. Очување интегритета информација кроз контролу приступа;

6. Континуирано стручно усавршавање и оспособљавање запослених;

7. Праћење, документовање и анализу инцидената и атака на информациону безбедност;

8. Употребу криптографских техника (обавезна врста заштите информација којима се приступа са удаљених локација);

9. Усаглашеност са законским, регулаторним и уговорним обавезама.

6. МОГУЋНОСТ УНАПРЕЂЕЊА ЗАШТИТЕ ЛИЧНИХ ПОДАТАКА У ЗДРАВСТВЕНИМ УСТАНОВАМА

Под механизмом заштите информационих система подразумева се низ организационих и технолошких мера, које се примењују у циљу смањења ризика и отклањања потенцијалних узрока ризика и хазарда. Веома је битно, због сконцентрисаности информација и њиховог обима и значаја, јасно дефинисати правила и обезбедити највиши ниво заштите, поготово када је реч о корпоративним информационо-комуникационим системима, у шта свакако спада и систем ЗУ.

Информације, информациони системи и мреже, представљају битну имовину која има материјалну и употребну вредност за сваког појединца и организацију.

”Информације и информационе инфраструктуре могу бити од пресудног значаја за конкурентност правних субјеката и све аспекте њиховог пословања” (Путник, Милошевић, 2016).

Нужно је да руководство установе или компаније, у нашем случају Министарство здравља, сачини политику безбедности информационо-комуникационих ресурса и њихових корисника, која би се заснивала на „холистичком приступу” и да у обзир узме различите аспекте заштите са нарочитим освртом на примену модела вишеслојне заштите (Путник, Гаврић, 2012).

У питању је принцип проактивног деловања који обухвата следеће аспекте:

- логичко-технички,
- физички,

- кадровски,
- организациони,
- нормативни.

Сви корисници (физичка и правна лица) суочавају се са великим бројем безбедносних претњи у сајбер простору (преварама, саботажама, шпијунажама, вандализмима, крађама итд.)

„Механизми заштите су организационе и технолошке мере које се предузимају у циљу смањења ризика и отклањања узрока ризика. Веома често се безразложно сматра да су технолошки механизми заштите сами по себи довољни одбрамбени механизми. Велики проценат штете настаје као последица злоупотребе информација, а не губитка или оштећења, што је последица антропогеног фактора, због непрофесионалне примене технолошких механизама заштите или због организационих пропуста" (Мандић, Путник, Милошевић, 2017).

Ова правна регулатива, на нивоу највишег менаџмента, веома је битна, с обзиром на то да је у мају 2018. на снагу ступила Општа уредба о заштити података о личности (*General Data Protection Regulation – GDPR*) која је донета још 2016. године са адаптационим периодом од пуне две године. Међутим, период прилагођавања је прошао, а на основу истраживања које је почетком године спровела компанија Веритас – свега 2% испитаника је заиста прилагодило свој начин пословања GDPR-у, упркос томе што се 31% изјаснило да је у потпуности применило регулативу.

Једна од битнијих новина коју нам доноси одредба GDPR је и тзв. „право на заборав" (*right to be forgotten*) које постојеће право на брисање података прилагођава стварности интернета у којима се наши подаци константно објављују и деле. Слично је и са правом на преносивост података, које подразумева да ће компаније које се баве аналитиком личних података својим корисницима на захтев морати да доставе све податке о њима у машински читљивом формату, како би ти подаци могли да се користе и за друге услуге. Ово уједно значи да су компаније у поседу личних података, као и до сада, дужне да своје кориснике обавесте о начинима на које њихове податке користе, да им омогуће увид у податке, доставе копију, или измене нетачне податке.

С обзиром на све правне и репутационе ризике за компаније које се баве обрадом података о личности, именовање лица за заштиту података о личности (*data officer*) би свакако био мудар потез. Именовање оваквог лица по GDPR-у постоји за државне органе, али и за компаније које се баве масовним праћењем грађана или обрадом нарочито осетљивих података у великом обиму. Лице које се бави заштитом података о личности треба да сачини попис, категоризацију и кодирање свих информација о корисницима које се дефинишу као њихови лични подаци – било која комбинација личних чињеница која скупа посматрано тачно одређује једног појединца. То су, између осталог, име и презиме, подаци о локацији, физички, физиолошки, генетски, ментални, економски, социјални, културни и други фактори.

Незаштићеност података запослених и бивших запослених је још један од проблема са којима се суочавају здравствене установе.

Поред тога, појединцима од којих се информације прикупљају даје се право да увек и у сваком тренутку знају ко и у какве сврхе сакупља њихове личне податке, као и да захтевају да се ти подаци избришу из базе података у којој се налазе.

Додатно повећање права власника информација обезбеђено је и проценом утицаја коју прикупљање и обрађивање података има на права и слободе појединца, као и обавештавање надлежних власти и власника информације уколико дође до било какве угрожености или неадекватне употребе података (у року од 72 часа). Како би се осигурали да ће све наведене ставке бити испоштоване, законодавци су одредили и постојање независног државног органа у свакој земљи чланици који ће водити рачуна о пријавама из ове области, а чији ће рад координисати европски орган – *Article 29 Working Party (WП29)*. Па ипак, контрола процеса третирања података није остала само на нивоу државе или наднационалне заједнице. Kako смо напоменули, према GDPR -у, организације/компаније ће морати да имају *Data Protection Officer* (*DPA*), тачније запосленог експерта или спољашњег сарадника који ће контролисати третирање података.

Његово постојање није повезано са бројем запослених у фирми, већ са количином података који се обрађују, те ће стога све компаније које редовно и систематски прате податке у великој размери, као и оне које то чине са подацима

осетљивих категорија (здравствене, религиозне, расне и сл.) морати да приме још једног запосленог.

Свакако, један од основних предуслова адекватне заштите података је правни оквир који организацији даје овлашћења и обавезе у погледу заштите поверљивих информација, као и њихово бесправно коришћење од стране неовлашћених лица (Мандић, Путник, Милошевић, 2017).

Овај правни оквир представљају прописи од стране државе, на челу са Уставом и правним регулативама, у које од маја 2018. године улази и *GDPR*.

Битно је разумети да се заштита података о личности не може постићи само доношењем правних аката, односно пуким усаглашавањем са прописима. Зато *GDPR* прописује да се морају имплементирати одговарајуће техничке и организационе мере за заштиту података у складу са сврхом, обимом, природом и контекстом обраде података. То значи да у сваком конкретном случају треба проценити које су мере неопходне попут интерних систематизација, ангажовања организационих стручњака, набавке посебне опреме, коришћења сигурних мрежа за пренос података, а потом је неопходно да се те мере имплементирају.

Уставом РС, члан 52, гарантован је и слободан приступ информацијама од јавног значаја, док се ставом 2 истог члана утврђује право на приступ информацијама у поседу државних органа и организација којима су поверена јавна овлашћења у складу са законом.

Законом о здравственој документацији и евиденцијама у области здравства ("Сл. гласник РС", бр. 123/2014, 106/2015 и 105/2017) уређује се здравствена документација и евиденције, врсте и садржина здравствене документације и евиденција, начин и поступак вођења, лица овлашћена за вођење здравствене документације и унос података, рокови за достављање и обраду података, начин располагања подацима из медицинске документације пацијената која се користи за обраду података, обезбеђивање квалитета, заштите и чувања података, као и друга питања од значаја за вођење здравствене документације и евиденција.

Имајући у виду чињеницу да је у претходном периоду дошло до интензивног развоја здравствених и информационо-комуникационих технологија, као и потребу да се на јединствен начин уреди област здравствене документације и евиденција,

израђен је нови Закон о здравственој документацији и евиденцијама, како би се на адекватнији и рационалнији начин пратило здравствено стање и здравствене потребе становништва. Разлози за доношење новог Закона условљени су, с једне стране, унапређењем планирања и ефикасног управљања системом здравствене заштите, као и прикупљања и обраде података у вези са здравственим стањем становништва и функционисањем здравствене службе, са циљем рационалног коришћења свих расположивих ресурса у систему здравствене заштите (кадар, опрема и простор, лекови и медицинска средства, информационо-комуникационе технологије) и с друге стране, увођењем информационо-комуникационих технологија у праксу спровођења здравствене заштите становништва рационализује се приступ здравственој заштити, како са аспекта пацијента, тако и са аспекта здравственог радника. Наведеним Законом утврђује се и основ за функционисање интегрисаног здравственог информационог система.

Приликом јавних разматрања заштите приватности од стране носилаца државне власти и других заинтересованих субјеката, потпуно је занемарен аспект заштите података о личности у специфичним областима, као што су здравство и пословање уопште. Подаци из упоредне праксе показују да на том плану постоје бројне опасности, али и (пословне, развојне) могућности.

Упоредна пракса, а посебно инсистирање кључних институција ЕУ на сталном усавршавању правних прописа који се односе на заштиту приватности, указује да право представља темељни инструмент за остваривање такве заштите. То је и становиште Европске комисије.

Али не било какво право, већ оно које задовољава одређене стандарде. У савременим условима управљање подацима јесте управљање људима. Појединац се у односу према држави (друштву уопште) све више одређује скуповима података. Тешко је пренагласити потребу за прецизним законским регулисањем заштите личне приватности, односно заштите података о личности.

Многе здравствене организације, од државног нивоа до нивоа примарне здравствене заштите, развијају и уводе разне облике информационих система и система електронске медицинске документације (електронски картони пацијента – ЕКП). Саставни део набавке или сопственог развоја тих система је и процес обезбеђивања заштите података, као и процес дефинисања начина да се смање

ризици и предупреде негативне последице које могу настати услед неадекватне заштите. Приватност података се односи на жељу појединца да контролише публиковање (јавно изношење) личних здравствених и других података. Поверљивост се односи на могућност појединца да контролише начин на који пружалац здравствене услуге (организација или појединац) користи личне податке, као и њихово даље дељење (давање другим појединцима или организацијама). Заштита омогућава осигурање приватности и поверљивости кроз избор стратегија, процедура и механизама заштите. „Информатичка безбедност се дефинише као скуп техничких и административних процедура установљених са циљем да се подаци заштите од неовлашћеног или ненаменског увида и отуђења, измене или уништења као и ради заштите функционалности самог информационог система" (*Gostin*, 1993).

Посебни циљеви у напору да се обезбеди сигурност односно пружи заштита информацијама (Делетић В. и М. 2010) су:

- Очување интегритета података;
- Једноставност приступа подацима од стране легитимних корисника;
- Осигурање приватности личних података као и њиховог прикладног коришћења.

Ови циљеви се у медицинској информатици посебно фокусирају на специфичне аспекте:

- Доступност која обезбеђује тачну и ажурну информацију свакоме коме је потребна и на месту на којем је потребна.
- Урачунљивост помаже да су корисници одговорни за њихов приступ и коришћење информација по принципу потреба и права да одређену информацију знају.
- Дефиниција периметра омогућава да систем контролише границе поверљивог приступа и физички и логички.
- Приступ базиран на улогама омогућава приступ корисника само оним информацијама које су важне за њихов посао, чиме се ограничава и спречава искушење да неко неовлашћено приступи информацијама које су ван граница његових легитимних потреба.

Свеобухватност и контрола обезбеђују да власници електронске медицинске документације (организација, лекар, медицинско и парамедицинско особље укључено у процес пружања здравствене услуге), ИТ особље и пацијенти могу да разумеју и имају ефективну контролу над прикладним аспектима поверљивости и приступу подацима.

Заштита података и једноставан, лак приступ су често супротстављени захтеви: поједностављење приступа може угрозити сигурност података ако софтверска апликација није пажљиво и адекватно пројектована и имплементирана. С друге стране, превише компликовани механизми заштите најчешће нарушавају ергономију апликације са становишта корисника. Велики део лаика, али и информатичких професионалаца, нажалост, не респектују комплексност заштите података чак и када разумеју њен значај.

6.1. ЕЛЕКТРОНСКИ ЗДРАВСТВЕНИ КАРТОН – ЕЗК

У Србији релативно велики број здравствених установа већ развија различите моделе електронског здравственог картона. Оно што се издваја као неопходно из досадашњих искустава је консензус, свима прихватљиво решење, око тога шта ће сваки електронски здравствени картон морати да садржи, као и развој техничких стандарда који ће електронски здравствени картон учинити лако доступним и безбедним.

Опште је прихваћено и у пракси доказано да се, самим преласком са администрације засноване на папиру на компјутерску обраду података, постиже најмање троструки пораст ефикасности и огромне материјалне уштеде у било којој сфери модерног пословања.

По новом систему, већ по пријављивању пацијента на пријемном шалтеру, његови подаци се прослеђују на рачунар лекара, који у сваком тренутку има пред собом дневни списак и распоред прегледа. Нови приступ који доноси информациони систем није заснован само на употреби рачунара, већ су, сходно савременим препорукама ЕУ, створени тимови лекар – медицинска сестра. Тако нпр. док лекар интервјуише и прегледа пацијента, медицинска сестра уноси опште податке, а док лекар преписује терапију или упуте за даље специјалистичке

прегледе, сестра припрема пацијента за додатне радње у оквиру прегледа, нпр. ЕКГ или ултразвук. Симултано се користи исти рачунар и на овај начин се само једном евидентирају потребни подаци од стране лекара и медицинске сестре у тиму, и то на месту где се одвија сам преглед. Овако унети подаци су после тога лако доступни статистичкој служби и рачуноводству, који са много мање обраде могу да их прослеђују вишим инстанцама.

Оваквим приступом се пацијентима скраћује чекање и шетање од шалтера до шалтера и побољшава се квалитет здравствене услуге која им се пружа. Примена електронског здравственог картона не мења трајање прегледа, већ мења однос у корист ефективног времена које лекар посвећује свом пацијенту.

e-Health – (е-здравље или е-здравство) апликација за вођење електронског картона и електронско фактурисање урађена је од стране програмера са Електротехничког факултета из Београда. Замишљена је тако да временом треба да покрије све потребе примарног здравства у погледу електронске обраде података о пацијентима. Ова апликација даје могућност контроле рада на свим нивоима и у сваком кораку обраде података о осигуранику. Поред тога, *e-Health* значајно убрзава и олакшава рад, како докторима запосленим у примарној здравственој заштити, тако и осталом медицинском особљу, али и Републичком Заводу за здравствено осигурање (РЗЗО) који кроз ову апликацију има могућност детаљног праћења и контроле рада домова здравља (Родић, 2012).

Функционисање саме апликације је замишљено тако да на једној страни имамо базу података која служи да складишти жељене податке, да те податке организује по табелама, и да их затим једноставно и брзо достави клијенту који их потражује. На једној страни постоји сервер на којем се налази база података (где се чувају подаци) а на другој страни се налази клијент (који тражи податке од сервера). Комуникација између клијента и сервера се одвија *SQL* језиком.

Кориснички интерфејс *e-Health*-а је врло једноставан и углавном је заснован на одабиру жељених опција међу понуђеним у оквиру падајућих менија. Претрагу по осигураницима је могуће брзо и прецизно вршити по различитим критеријумима, од имена и презимена, преко ЈМБГ-а и места до ЛБО-а и броја здравствене књижице. Из програма је могуће добити различите врсте извештаја неопходних здравственим радницима у циљу израде периодичних прегледа рада на

нивоу установе. Сама чињеница да се одабир жељених опција врши преко падајућих менија, доводи до тога де је унос података укуцавањем са тастатуре минималан (изузев дела анамнеза и налаз), што своди могућност прављења грешака на минималну меру.

Електронски картон је део апликације који је намењен раду доктора са пацијентом, за унос података о посети пацијента здравственој установи, односно анамнези и налазу, дијагнози као и прописаној терапији. Он даје могућност брзог и једноставног прегледа претходних посета пацијента, као и штампања прописане терапије односно рецепата, што само по себи додатно олакшава и аутоматизује поступак обраде података о пацијенту, посебно имајући у виду да постоји могућност очитавања броја здравствене књижице и рецепта помоћу читача бар кода и аутоматског проналажења пацијента и штампања одговарајућег рецепта.

Електронска фактура обухвата рад осталог медицинског особља, односно медицинских сестара са пацијентима, тј. унос података о пруженим услугама, коришћеном медицинском и санитетском материјалу, ампулираним терапијама, итд. Она у генерисаном облику пружа све потребне податке РЗЗО о раду установе примарне здравствене заштите у периоду за који се генерише, као и податке о висини финансијских средстава које та установа потражује од Завода.

Иначе, програм даје могућност потпуне индивидуализације и праћења рада сваког појединачног корисника програма, задавањем личних корисничких шифара. На тај начин је у потпуности омогућен увид у рад медицинског особља, доктора у примарној здравственој заштити са једне стране, броја рецепата који они издају, броја пацијената и остварених прегледа у одређеном периоду по лекару, као и осталог медицинског особља, а са друге стране, у број пружених услуга и утрошеног санитетског и медицинског материјала по осигуранику. Уношење нових података (о лековима, лекарима, ценама материјала и услуга), задатих од стране РЗЗО-а у програм врши се учитавањем шифарника које медицинске установе у примарној здравственој заштити добијају од филијала РЗЗО. У том смислу постоје одређене потешкоће, које се посебно односе на шифарник лекова и неслагање постојећег шифарника прописаног од стране РЗЗО-а и позитивне листе лекова које лекари у примарној здравственој заштити имају могућност да препишу својим пацијентима.

Електронска медицинска документација (електронски картони) садржи осетљиве личне информације које могу бити лако злоупотребљене. Са друге стране, широк приступ електронском картону пацијента од стране медицинских и других професионалаца који треба да пруже медицинску услугу пацијенту је предуслов за успешно лечење. Тако, са једне стране постоји потреба ограничења приступа подацима из електронског картона пацијента, док са друге постоји интерес пацијента да што више стручњака (из, по правилу, различитих организација) има увид у његов електронски картон у циљу што бољег сагледавања медицинског статуса и тиме што квалитетнијег и ефикаснијег доношење дијагностичких и терапијских одлука (Смиљанић, 2018).

Мултиорганизациона транспарентност, легални и етички аспекти и одговорност, намећу сложене изазове не само у погледу технолошке архитектуре медицинских информационих система. При томе, технолошка архитектура мора бити усклађена са етичким и правним стандардима који често нису у сагласности са техничко-технолошким могућностима. Генерички механизми заштите треба да омогуће дефинисање стандарда и политике коришћења личних медицинских информација који ће бити технолошки скалабилни. Тиме се постиже максимално искоришћење технолошког развоја уз смањену опасност од појаве пропуста у систему заштите које могу довести до злоупотреба.

Збир података из основне медицинске документације и подаци које се воде у здравствено-статистичком систему и информационим системима организација здравственог осигурања чувају се у централном систему. ЕЗК представља само „*read only*” (само за читање) преглед, што значи да приступањем ЕЗК-у није дозвољено мењање података који се у њему налазе. Приступ подацима мора бити у непосредној вези са остваривањем здравствене заштите пацијената, односно може се вршити непосредно пре пружања здравствене заштите. У систему се води детаљна евиденција за сваки приступ пацијента ЕЗК-у.

Подаци у ЕЗК су подељени у групе података:

1. Лични подаци;
2. Лекови – сви преписани и подигнути рецепти подељени у две групе (хронична и акутна обољења);
3. Алергије – листа свих евидетираних алергија пацејента;

4. Болести од већег јавно-здравственог значаја;
5. Специјалистички прегледи – листа свих прегледа код лекара специјалиста;
6. Болничко лечење – листа пријема у болнице;
7. Дијагностика – листа снимања на апаратима са извештајима;
8. Хируршке интервенције – листа заказаних и извршених хируршких интервенција (извор: ИЗИС Републике Србије www.kombeg.org.rs, 2016).

6.2. МЕТОДОЛОГИЈА ЗАШТИТЕ ЛИЧНИХ ПОДАТАКА И РЕСУРСА У ЗДРАВСТВЕНИМ УСТАНОВАМА

Методологија за развој заштите личних информација у медицинским информационим системима се састоји од шест основних корака (Делетић, В. и М.):

1. Идентификација информатичких ресурса који захтевају заштиту;
2. Дескрипција архитектуре информационог система који се имплементира;
3. Идентификација опасности по информације у склопу планиране архитектуре;
4. Рангирање опасности по значају и потенцијалној штети;
5. Дизајнирање решења која треба да смање ризике и последице;
6. Спецификација имплементационих препорука.

Пре саме примене мера обезбеђења информација, потребно је идентификовати оне које је потребно штитити. Превише широка заштита која чува и информације које нису критичне изискује непотребне ресурсе, компликује увођење система заштите и често умањује укупне перформансе система. Веома је важно наћи оптималан однос између критичног скупа информација и расположивих ресурса.

Медицински информациони системи који садрже личне информације морају примењивати посебне мере опреза и заштите, како би се спречиле могуће злоупотребе које могу угрозити законска и људска права на приватност.

Информациони систем, или апликација, увек се појављује у контексту ширег система, односно његове архитектуре. Размена података, њихово ширење и коришћење у спољашњим системима има значајну улогу у повећању ефикасности свих пословних процеса. Због потребе за што широм интеграцијом информационих система и апликација, све већим захтевима за слободном разменом информација и повезивањем са другим изворима података, расте и ризик од злоупотребе или оштећења информација.

Архитектура информационог система представља план остварења будуће функционалности система кроз спровођење потребних набавки (укључујући и сопствени развој) и имплементације компоненти и елемената система. Процес набавке се спроводи кроз процедуру инвестиционог одлучивања која треба да обезбеди потребну технологију (технику – хардвер, софтвер и комуникације, а и људе који су способни да та средства на најефикаснији начин примене).

Неадекватна средства и нестручна употреба представљају највећи фактор ризика за функционалност система и безбедност података. Најчешће штете настају као последица потпуног одсуства свести о постојању нестручног приступа или импровизованих решења.

Професионално дизајнирање архитектуре и њено стриктно поштовање је у основи планирања и спровођења механизама заштите.

Ризик је могућност да дође до материјалне или нематеријалне штете услед непланиране измене или губитка података због људске грешке или намерне акције, као и техничких или природних фактора.

Први корак у контроли ризика је разумевање шта је то ризично по пословни процес, пословне циљеве или ресурсе организације. Након тога, спроводи се свеобухватно истраживање ризика што доводи до идентификације ризика. После тога врши се израда планова за умањење ризика, који могу имати најштетније последице (одређивање приоритета).

Најчешће, здравствене организације не сагледавају све потенцијалне ризике и не формулишу целовиту и свеобухватну стратегију контроле ризика.

Једна од методологија евалуације ризика (*OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation*) омогућава истраживање организационих

и технолошких аспеката ради синтезе свеобухватне слике потреба информатичке безбедности. Основне фазе *OCTAVE* методологије обухватају (Делетић, В. и М.):

1. Изградња профила опасности за ресурсе – Овде се оцењују организациона својства система. Истражују се основни информатички захтеви по стручним сегментима организације, опасности по кључне информационе ресурсе, безбедносне мере које су потребне, тренутно примењене мере као и организационе слабости и рањивости.
2. Проналажење слабости у инфраструктури – Кључне компоненте инфраструктуре (сервери, радне станице, мрежа, екстерне комуникације, оперативни системи, базе података итд.) се истражују ради проналажења технолошких слабости које могу довести до непланираних активности на нивоу информационог система.
3. Развој сигуроносне стратегије и плана – У овој фази се анализирају сви уочени ризици. Информације се анализирају да би се проценио значај сваког ризика на укупне интересе организације. Истовремено се развија стратегија заштите и планови за избегавање појединих опасности. Механизми заштите су организационе и технолошке мере које се предузимају ради смањења ризика и отклањања узрока ризика. Врло често се, неправилно, сматра да су технолошки механизми заштите сами по себи довољни одбрамбени механизам. Већина штета које настају као последица злоупотребе података су последица људског фактора, због непрофесионалне примене технолошких механизама заштите или због организационих пропуста.
4. Организациони механизми заштите подразумевају планирање правила и процедура које се односе како на ИТ особље у свакодневном администрирању система, тако и на корисничку политику, тј. правила и права у коришћењу информација. Технолошки механизми треба да обезбеде поуздану и контролисану функцију свих компоненти система. Примери технолошких механизама заштите (технологија заштите) су: антивирусни програми (апликација), *RAID* контролер (уређај), *Firewall* (сервис), Смарт-картица (медијум), *PKI* (стандард), *SSL* (мрежни протокол) итд.

У склопу функционалности система се онда обезбеђују и потребни механизми за примену и спровођење организационих механизама заштите.

Спровођење организационе заштите информација базира се на планској уградњи потребних функционалности система, која гарантује доследно испуњење свих дизајнираних функционалности и поуздану заштиту.

Генеричке функционалности се могу реализовати, различитим технолошким механизмима, тј. решењима. Генеричке функционалности су веома стабилне и не мењају се радикално са променом технологије. Стратегија заштите базирана на генеричким механизмима не захтева сталне измене и ревизије процедура (организационих механизама) услед напретка технологије, већ технолошки напредак само стабилно подиже ниво и ефикасност заштите. У пракси највећи проблем и енергију захтева увођење процедура, односно привикавање корисника на доследно спровођење политике употребе система и располагања подацима. Технику и технологију је лакше мењати, него људске навике.

Већина савремених ИКТ инфраструктурних компоненти (*OS, DBMS,* мрежни уређаји итд.) обезбеђују генеричке заштитне функционалности. Сама генеричка функционалност не подразумева и стварну ефективну заштиту коју конкретна компонента омогућава. Лаички и непрофесионални приступ ствара илузију заштите, док се у стварности појављује висок фактор ризика од „упада" управо кроз „сигурну" компоненту.

6.3. ФИЗИЧКО-ТЕХНИЧКА СФЕРА ЗАШТИТЕ

„Техничка заштита представља скуп радњи којима се непосредно или посредно штите људи и њихова имовина, а изводи се техничким средствима, уређајима и системима техничке заштите којима је основна намена спречавање противправних радњи усмерених према штићеним лицима или имовини, као што су: противправно деловање, противпрепадно деловање, противдиверзионо и противсаботажно деловање" (Правилник о начину вршења послова техничке заштите и коришћења техничких средстава „Службени гласник РС", бр. 19 од 20. фебруара 2015, 71 од 21. јула 2017).

Суштина механизма деловања система техничке заштите је у забрани неконтролисаног приступа неком предмету, простору или објекту заштите. Овакав вид заштите, неопходан је за све врсте здравствених установа. Ово је јако битно и

због чувања просторија у којима је омогућен приступ ИТ секторима, а управо због заштите поверљивих података.

Техничка заштита врши се употребом техничких средстава и уређаја за спречавање противправних радњи према лицима, имовини или пословању, а са циљем заштите од:

- недозвољеног приступа у објекте и просторе,
- изношења и неовлашћеног коришћења штићених предмета,
- уношења оружја, експлозивних и других опасних предмета и материја,
- провале, диверзије и насилног напада на објекат или простор,
- неовлашћеног приступа информацијама и документацији, итд.

Техничка средства и уређаји који су повезани образују систем техничке заштите.

„Системи техничке заштите имају првенствени задатак да открију опасну појаву, прецизирају место њеног настанка, обезбеде контролу исправног рада сигурносне опреме, дају одговарајућу сигнализацију, омогуће пренос аларма на даљину, делимично утичу на отклањање опасне појаве и створе услове одговарајућој служби обезбеђења да ефикасно интервенише" (Закон о приватном обезбеђењу, „Сл. гласник РС", бр. 104/2013 и 42/2015).

Активности техничке заштите односе се на: детекцију извора опасности, одређивање потребног нивоа заштите, анализу тренутног нивоа заштите, процену ризика, пројектовање система заштите, избор опреме, монтирање система заштите и његово редовно одржавање.

Техничка заштита се састоји од механичке и електронске. Механичку заштиту чине средства која не користе електричну енергију као извор напајања. Електронским средствима је за рад неопходна електрична енергија.

У електронске системе заштите убрајају се:

- алармни системи,
- видео обезбеђење и системи за контролу приступа,
- системи електронских средстава надзора робе (сензори, зујалице и сл.),

- системи за контролу обиласка објекта од стране службеника обезбеђења,
- електронски системи за заштиту од индустријске шпијунаже,
- интегрисани системи електронске заштите,
- уређаји за уништавање докумената, оптичких и магнетних медија (Центар за обуку – Криминолошка академија, Београд 2015, фонд испитних питања 9-10 Prirucnik-za-montazu-i-odrzavanje-sistema.pdf).

Алармни системи имају функцију детекције и алармирања неовлашћеног уласка у објекат.

У зависности од тренутка употребе, алармне системе делимо на противпровалне и противпрепадне.

Основна разлика између ова два система је првенствено у:

- Специфичној намени (детекција провале или разбојништва);
- Начину детекције штетног догађаја (аутоматска – активирањем сензора или магнетног контакта, или активирањем прекидача тихе дојаве);
- Начину дојаве (активирањем сирене или само прослеђивањем информације заинтересованом субјекту);
- Времену оперативног функционисања (ван радног времена или у току радног времена правног лица).

Алармни системи за заштиту од пожара

Протипожарна заштита је категорија техничке заштите намењена раном откривању и упозорењу на пожар или прекомерно повећање температуре штићеног објекта, у зависности од изабране конфигурације, омогућава и деловање на инцидент са удаљене локације до доласка патролног тима.

Детекција дима, ватре или гаса може се вршити алармним системима, где се уградњом противпожарних детектора, који се повезују на алармну централу, добијају противпожарни системи техничке заштите.

Систем затворене телевизије

Систем затворене телевизије је категорија техничке заштите намењена осматрању, снимању и одвраћању. У зависности од конфигурације, омогућава и функцију локалног, интерног или даљинског мониторинга.

Осматрање омогућава сагледавање стања над простором и у простору који се обезбеђује. Олакшава рад запосленима на пословима физичког обезбеђења и код контролних пунктова, где је неопходан преглед посетилаца пре њиховог уласка у обезбеђени простор. Неопходно је што прецизније дефинисати зону осматрања и у оквиру ње штетни догађај који се може десити, на основу кога дефинишемо процедуре које треба предузети. Снимање је категорија техничке заштите која омогућава репродукцију догађаја, што је од изузетног значаја за накнадну анализу у случају штетног догађаја. Да би функција снимања, односно анализе садржаја и снимљених материјала била употребљива, потребно је исправно функционисање целокупног система обезбеђења и активно укључивање свих запослених кроз функцију самозаштите. Неопходан је и правилан избор камера (Мандић, Путник, Милошевић, 2017). Одвраћање је функција техничког система која има првенствено психолошко дејство на лица која имају намеру да уђу у обезбеђени простор, односно у оквиру тог простора изврше одређену недозвољену радњу.

Основни делови система затворене телевизије су камере, преносни путеви, излазни монитори, уређаји за снимање и репродукцију слике.

У зависности од начина рада и технологије коју користе, системи затворене телевизије деле се на: аналогне и дигиталне.

Аналогни системи углавном се везују за старију генерацију система, где се пренос видео сигнала врши аналогно путем коаксијалног кабла. Камере се повезују на аналогне ДВР-ове, а квалитет слике се изражава бројем ТВ линија.

Дигитални системи затворене телевизије су савремени и напреднији у односу на аналогне, а видео сигнал код ових система се преноси као дигитална информација и тако не губи на кавалитету ни онда када се преноси на већем растојању.

Системи за контролу приступа

Контрола приступа и изласка је категорија техничке заштите намењена за контролисање кретања лица, возила и робе на одређеним приступним и излазним тачкама. Контрола приступа врши се преко система који се састоји од наменског хардвера и припадајућег софтвера, са базама података.

Примарна функција система за контролу приступа је регистрација уласка и изласка и идентификација свих лица која имају потребу да уђу у штићене просторе.

Системи за контролу приступа деле се на: системе са електронском шифром, системе на бази идентификационе картице и системе на бази физичких особина (лице, отисак прста, препознавање гласа, скенирање зенице ока, итд). Софтвери система евидентирају све активности у систему, упоређујући претходно унете податке са подацима на елементима за идентификацију.

Поред наведених елемената техничке заштите, веома је важан ангажман службеника лиценцираних за послове физичког обезбеђења (ФО) у складу са законским и подзаконским актима Републике Србије везаних за послове физичког обезбеђења. Запослене који раде на пословима обезбеђења информационих система треба едуковати о начину рада и потенцијалним ризицима по информационе системе и њихове елементе.

Службенике физичког обезбеђења треба обучити и направити им процедуре за случај ванредних ситуација које се могу догодити и утицати на функционисање информационих система (пожари, поплаве, поремећено електрично напајање и сл.). Запослени морају бити свесни значаја података који су производ и циљ постојања информационих система.

6.4. НОРМАТИВНА СФЕРА ЗАШТИТЕ

Нормативни оквир обезбеђује значајне функције основног слоја заштите, попут истицања значаја заштите информација на државном нивоу, концентрисања ресурса на стратешким правцима истраживања и развоја, захтева за обуку и образовање, санкционисања злоупотребе заштите, обавезивања на сертификацију и акредитацију и др. У нормативном оквиру веома битан значај имају подзаконски

правни акти (нпр. Правилници о успостављању *PKI* (*Public key infrastructure*) – тј. инфраструктуре јавног кључа дигиталног потписа итд.) и стандарди заштите.

На нивоу сваке државе углавном постоји Закон о заштити информација, који обавезује појединце и пословне системе да штите своје информације у *e*-окружењу, прописују обавезан обим заштите, од чега и како штитити приватност корисника и какве су санкције за повреде система заштите. Поред Закона о заштити информација, на нивоу државе, потребни су и доносе се бројни закони који регулишу компјутерски криминал (Закон о компјутерском криминалу, Закон о дигиталном доказу, Закон о судском вештачењу у области ИКТ, Закон о формирању ЦИРТ и ЦЕРТ тела и др.).

Глобални карактер компјутерског криминала захтева да се у развоју програма заштите информационих система у Србији разматрају усклађеност са међународним законима, регулативама и стандардима, разлике правосудних система, обавезе о чувању пословних тајни, заштита приватности и личних података.

ЕУ је усвојила Директиву о приватности и електронским комуникацијама (25.7.2002.), захтевајући од провајдера Интернет сервиса да у одређеном периоду задржавају податке на свим *e*-комуникацијама.

„Ауторска права морају бити заштићена на начин који задовољава легалне захтеве.” Поверљиве и информације о интелектуалној својини, програм заштите мора штитити на начин који задовољава минималне захтеве Закона о заштити поверљивих информација, да би се могло обезбедити законско гоњење починиоца у правосудном систему где је кривично дело извршено.

У многим земљама Закон о борби против сајбер криминала је неадекватан и не покрива на исти начин међународни криминал, који се мора истраживати, доказивати и санкционисати у складу са законима и стандардизованим процедурама у свим укљученим правосудним системима.

Заштита приватности личних података у правосудним системима, није усаглашена са законима ЕУ. Препоруке да се приватност и лични подаци штите општим и техничким мерама заштите, остављају простор за импровизацију и увек су јефтиније решење за организацију, него обавезна заштита прописана законом.

6.5. ОРГАНИЗАЦИОНА И ТЕХНОЛОШКА СФЕРА ЗАШТИТЕ

Добра организација информационих система заснива се на добром управљању заштитом (*Security managment*). Управљање или менаџмент представља процес у коме се долази до неког циља коришћењем одређеног скупа ресурса. Да би процес информатичке безбедности добио на ефикасности, треба добро разумети основне принципе управљања. Руководилац или менаџер ради са или преко других запослених у организацији координирајући њихове радне активности у циљу постизања најбољих резултата организације (Икић, 2011).

Организација заштите подразумева следеће активности:

- дефинисање процеса заштите,
- дефинисање политика, стандарда процедура и упутстава,
- управљање ризицима,
- контроле,
- технологије
- документацију,
- ИТ културу,
- едукацију.

Због чињенице да је управљање заштитом оптерећено преузимањем одговорности за специјализоване програме одређени аспекти ове врсте менаџмента имају своје особености. Главне карактеристике су познате као:

- Планирање (*Planning*) – одговора на инцидент, наставка пословног процеса, опоравка од инцидента, полиса, кадрова, риск менаџмента и безбедносних програма (едукацију, тренинг и освешћивање запослених.
- Полисе (*Policy*) – су скуп организационих упутстава која захтевају одговорно понаше запослених у некој организацији. Постоји три категорије полиса и то: генералне полисе (на нивоу предузећа, полисе које се односе на специфичне проблеме и оне које се односе на специфичне системе. Полисе су важна референтна документа за унутрашњу организацију и показују намеру руководства да жели да уведе ред у област безбедности информационих система. Оне никада не смеју да буду у супротности за законом, морају бити одрживе у

судском процесу и морају да буду подржане и администриране на прави начин.

- Програми (*Programs*) – Програми подразумевају дефинисање назива и опис радних места запослених који се баве пословима заштите у предузећу. У опису послова најважнији су: планирање сигурносних решења, пројектовање, израда и примена сигурносних решења, управљање сигурносним алатима, праћење безбедносних функција и континуирано побољшање процеса.
- Заштита (*Protection*) – Функције заштите су: риск менаџмент који укључује процену и контролу ризика, механизми за заштиту, технологије и алати.
- Људи (*People*) – Постоје разни сертификати који се добијају у области заштите, али код нас за најбоље од њих још увек не постоји могућност обуке и полагања испита (нпр. за сертификат који се зове *Certified Information Systems Security Professional (CISP)* може да полаже само онај који има најмање пет година радног искуства у области информатичке безбедноси и да има широк спекта знања из различитих области.
- Управљање пројектом (*Project Management*) – односи се на све елементе програма информатичке безбедности и веома је важан за праћење процеса приликом увођења система безбедности у неку организацију.

Примери технолошких механизама заштите – технологија заштите (Костић, 2004) су:

Антивирусни програми (апликација) – Представљају први ниво заштите од вируса и тројанаца. То су софтверски пакети способни да детектују, издвоје и (или) елиминишу вирусе. Сви антивирусни програми састоје се из више целина. Један његов део „*Monitor*" је резидентан у меморији и осигурава непрестану заштиту од вируса, док други део „*Scan*" омогућава скенирање целог система.

Антивируси су данас неопходан део софтвера који свако треба да има инсталиран на свом рачунару. Ови програми укључују различите начине надгледања и заштите рачунара од малициозног кода. Најчешће се ради о заштити у реалном времену и скенирању на захтев корисника, док модерне верзије ових

програма нуде разне друге видове заштите од вируса који се шире путем Интернета. Најпознатији и најчешће коришћени антивирусни програми (извор: http://www.seminarski-diplomski.co.rs) су:

- NORTON ANTIVIRUS,
- SOPHOS ANTIVIRUS,
- MCAFFEE,
- PCCLLIN.

RAID контролер (уређај) - (*Redundant Array of Independent Disks*) је комбинација више мањих хард дискова уређених у низ, односно у поље дискова. Основне предности *RAID* контролера су побољшање перформанси, повећање капацитета и повећање поузданости у односу на појединачни диск (Ђорђевић и група аутора, 2015).

Firewall (сервис) – дозвољава или блокира токове мрежног саобраћаја који се оддијају између небезбедне (*untrusted*) зоне (нпр. интернет) и безбедне (*trusted*) зоне (нпр. приватна или корпоративна мрежа). *Firewall* треба да спречи нежељени саобраћај, блокира упаде у локалну мрежу и заштити рачунаре у њој, као стратешки најбитнија безбедносна компонента у мрежној инфраструктури (извор: ИТ клиника https://www.it-klinika.rs/blog/sta-je-firewall).

Смарт-картица (медијум) – је пластична картица, која подсећа на обичну кредитну или дебитну, а разликује се од њих јер има у себи интегрисано коло или чип, на коме се налази процесор или меморија. На чипу се на сигуран начин могу чувати одређене информације. Захваљујући интелигенцији картице, могуће је развити разноврсне сигурносне апликације у областима као што су: заштита приступа рачунару или мрежи, идентификација, мобилна телефонија, електронски новац, возачка дозвола, здравствена књижица, и сл. (Марковић, Ђорђевић 2018 – aurora.ekof.bg.ac.rs)

PKI (*Public Key Infrastructure*) – инфраструктура система са јавним кључевима представља платформу која омогућава корисницима јавних мрежа, као што је Интернет, сигурне трансакције података и новца. Сигурност се постиже шифровањем (криптовањем) података.

ИП (мрежни протокол) – протоколи представљају правила којима су дефинисани синтакса, семантика и синхронизација комуникације. Називамо их још мрежним или интернет протоколима. Постоје различити мрежни протоколи, при чему сваки има посебно место и врши своју улогу. Интернет протокол (енгл. *Internet Protocol* (IP) је протокол трећег слоја *OSI* референтног модела (слоја мреже). Садржи информације о адресирању, чиме се постиже да сваки мрежни уређај (рачунар, сервер, радна станица, интерфејс рутера) који је повезан на интернет има јединствену адресу и може се лако идентификовати у целој интернет мрежи, а исто тако садржи контролне информације које омогућују пакетима да буду прослеђени (рутирани) на основу познатих IP адреса. Овај протокол је документован у RFC 791 и представља са TCP протоколом језгро интернет протокола, TCP/IP стек протокола (енгл. *Transmission Control Protocol/Internet Protocol*). Пар који сачињавају интернет протокол IP и протокол за контролу преноса TCP је најбитнији од мрежних протокола и термин TCP/IP протокол стек означава скуп најкоришћенијих од њих (https://sr.wikipedia.org/sr/).

6.6. КАДРОВСКА СФЕРА ЗАШТИТЕ

Човек је, с једне стране, носилац заштите података и информација, док са друге стране, представља потенцијалну опасност. Кадрови омогућавају да се организациона структура покрене, да се обаве планирани задаци и достигну планирани циљеви. Претња од стране инсајдера (некога изнутра) је у све већем порасту. Инсајдер није само стално запослени радник институције, већ то може бити и бивши радник запослен у некој од кооперантских фирми који има унутрашњи приступ систему (Николић, 2010).

Запослено особље, посебно немотивисани и незадовољни радници, представљају највећу претњу. Имају свакодневни приступ осетљивим информацијама, а за злоупотребу им није потребан нарочито висок ниво образовања. Претњу представљају бивши радници компаније (отпуштени радници, или они који су прешли из једне у другу, конкурентску, компанију). Лица запослена у кооперантским компанијама (здравствене установе често користе услуге фирми задужених за хигијену и обезбеђење), такође могу представљати велики проблем за безбедност информација, јер имају приступ интерним подацима.

У спровођењу кадровске политике треба применити све расположиве мере којима би се опасност од инсајдера свела на прихватљив ниво. Те мере се односе на људске ресурсе, избор кадрова, безбедносно образовање и стручно усавршавање, а све са циљем подизања безбедносних мера заштите информација на што виши ниво.

На кључна места треба да буду постављени проверени, поуздани и стручни кадрови. Заштита података и информација од кадрова подразумева да сваки радник буде предмет пажње лица задужених за безбедност. Посебну пажњу треба усмерити на знакове који би указали на нелојалност, склоност пороцима (алкохолу, коцки и дрогама), финансијске и породичне проблеме и сл.

Заштита самих кадрова подразумева заштиту од сопствених ненамерних пропуста и грешака, а спроводи се безбедносним образовањем и безбедносном културом, као и стварањем система рада и радних услова где ће грешке бити сведене на минимум.

На основу промена у интерном и екстерном окружењу предвиђају се потребе за кадровима. Утврђивање потреба за кадровима је почетна фаза у процесу кадровања. Да би се одредио потребан број запослених и њихова квалификациона структура, пре свега треба анализирати послове и задатаке.

Анализа посла је систематски поступак утврђивања природе и садржаја посла (задатака, дужности и одговорности), услова и метода рада, као и психофизичких особина које посао захтева. Резултат процеса анализе посла је опис посла одређеног радног места, писани документ који описује које активности и задаци се обављају на конкретном радном месту. Садржи информације о опреми која се користити на том радном месту, радне услове у којима се посао обавља, потребна знања, вештине, способности и друго.

Избор кадрова је један од најзначајнијих и веома сложених фаза у процесу кадровања. Треба извршити селекцију кандидата и изабрати оне који највише одговарају постављеним захтевима за одређена радна места. Основни критеријум код избора је њихова стручност за послове и задатке које би требало да обављају (дипломе, дужина радног стажа, радно искуство и сл.).

Неопходно је да лица која су испунила предвиђене услове прођу и безбедносну проверу, која обухвата процену да ли се за неког појединца у погледу лојалности, поверљивости, поузданости и веродостојности може дати овлашћење за приступ поверљивим подацима и информацијама, а да то не представља неприхватљив ризик за безбедност информација. Безбедносну проверу је потребно спроводити и за лица која су само привремено у контакту с поверљивим информацијама. Лицима која су прошла безбедносну проверу даје се понуда за посао и када је они прихвате процес селекције је завршен.

Адаптација људи у радној околини је веома значајан психолошки проблем. Радна адаптација је активан процес, прилагођавање човека професионалним и социјално-психолошким захтевима, у коме се формирају навике и вештине, врши активно укључивање појединца у колектив и групу, добијају и продубљују постојећа знања, задовољство радом и радним местом. Истовремено веома захтевни и психички исцрпљујући процеси у појединим колективима, у којима владају лоши међуљудски односи (где не постоје емпатија, хуманост, солидарност итд.), доводе до лоше адаптације (изостанци, повреде, несигурност, избегавање одговорности, неефикасност на раду). Лоша професионална адаптација није само грешка појединца, већ колектива и целокупног менаџмента.

Код распоређивања новопримљених кадрова препоручује се постепено увођење у процесе рада по принципу од једноставних ка сложенијим, од мање важних ка значајнијим пословима. Запосленог треба детаљно упознати са организационом шемом, садржајем рада, позицијом његовог радног места у хијерархији, са надређеним и подређеним радним местима, дужностима и правима, као и са важећим мерама, процедурама и правилима заштите.

Безбедносно образовање треба да пружи довољно знања о потребама, разлозима и начинима заштите, да објасни потребе и разлоге поштовања и придржавања стандардних мера и процедура заштите и да предочи обавезе у погледу заштите.

Основе заштите података и информација (безбедносни термини, концепти, осетљивости, претње, последице) стичу се подизањем свести о потреби заштите, а надоградња се реализује кроз обуку. Подизање свести запослених о важности чувања података и информација мора бити свакодневна брига. Релативно честом

неслужбеном комуникацијом или путем семинара и информативних састанака о заштити, запосленима се предочава какве штете могу настати губитком одређених података и како се то може одразити на њих саме.

Стручно усавршавање представља напор да се побољшају радне карактеристике запослених на њиховом радном месту. Организованим стручним усавршавањем може се отклонити опасност која прети од нестручних, неспособних и неодговорних кадрова. На тај начин делује се превентивно на претње и на најбољи начин се штите осетљиве информације.

6.7. ЕДУКАТИВНА СФЕРА ЗАШТИТЕ

Социјални инжењеринг представља поступак манипулације особама, како би се извеле недозвољене акције или открили поверљиве информације, без директног покушаја упада у компанијски информациони систем. Сам појам обично подразумева прикупљање информација, покушаје превара или покушај добијања информација неопходних за приступ рачунарском систему.

Према истраживању групе аутора, постоји тврдња да је у социјалном инжењерингу најпре потребно обратити пажњу на сигнале који могу упућивати на манипулацију, као што су на пример: необични захтеви који нису у складу са процедурама, питања о поверљивим информацијама (шифре, корисничка имена), пренаглашавања о хитности случаја, итд. Да би се ово спречило, нужно је да запослени располаже знањем о процедурама, техникама и последицама које могу настати због социјалног инжењеринга. Ово је за здравствени сектор и безбедност од великог значаја, нарочито за запослене у контакт центрима за подршку корисницима система ИЗИС, јер уколико запослени не буду имали оваква сазнања и познавали методе одбране, цео систем о заштити података могао би бити угрожен, што би за последицу могло да има несразмерну безбедносну штету (Мандић, Путник, Милошевић, 2017).

Постоје многе технике и рањивости које злонамерни корисници могу искористити за пробој информационе сигурности неке организације. Једну од њих представљају и људске рањивости, које је могуће искористити преко разних метода социјалног инжењеринга. Ове методе искоришћавају људске грешке или слабости како би се остварила права приступа систему, без обзира на ниво сигурности коју је организација увела. Усредоточеност на људске особине попут поверења, жеље за

помоћи или немарности основна је предност ових напада. Такође, свака особа може постати социјални инжењер и применити неку од бројних тактика напада. Социјални инжењеринг укључује разне технике, од једноставне крађе записаних лозинки до стварања и извођења сложених сценарија. Једна од најраширенијих и најпознатијих, је извођење *Phishing* напада (пецање или мрежна крађа идентитета). Реч је о процесу преваре у којем се нападач представља као поверљива страна, како би дошао до осетљивих података жртве. Током историје изведени су разни напади социјалног инжењеринга, а неки од њих су узроковали велике губитке разним организацијама (Шкундрић, 2016).

Јако је битно да се у случају уочених инцидената примене устаљена правила и процедуре, што би запослени у контакт центрима подршке требало да имају у оквиру обуке за рад у овим службама.

Реакција на социјални инжењеринг представља одговор система на напад, а подразумева скуп одређених мера у складу са безбедносним правилима и процедурама (Мандић, Путник, Милошевић, 2017).

Према овој групи аутора, неопходно је одредити:

- реакцију запосленог након уочавања инцидента,
- начин извештавања о инциденту,
- начин реакција сектора за безбедност по пријему информације о инциденту.

Уколико запослени примети било који вид потенцијалног напада, неопходно је да се фокусира на разговор, односно престане са другим активностима које је, можда, до тада радио. Без обзира да ли је сигуран или није сигуран да може да пружи одређене информације које се тичу конкретних детаља, који су у вези са поверљивим подацима, он мора направити паузу у комуникацији како би трезвено приступио даљој комуникацији. Уколико је уочио сумњиви напад, оператер може замолити саговорника да остане на вези и позвати супервизора да се укључи у разговор, сними га, као и да затражи број телефона корисника уз молбу да ће га контактирати након прибављања неопходних информација. Уколико корисник одбија да се представи, или се представи лажно, што се може утврдити на основу броја телефона позиваоца, а преко центра за информацију о телефонским бројевима, претпоставља се да је у питању социјални инжењеринг.

Уколико се уочи социјални инжењеринг, запослени треба да дође до што више информација о саговорнику, које ће му помоћи у састављању извештаја.

Оваква радна места, као што су оператери техничке подршке ИЗИС-а, на пример, потребно је да имају непрестани надзор од стране супервизора, и сви ови разговори требало би да буду снимани. Такође је, као стимулацију личне надоградње сваког запосленог у овом сектору, препоручљиво оцењивати разговоре по методу насумичног одабира разговора и на основу оцена давати одређене бенефите запосленима. На овај начин се подиже ниво рада запослених, као и сам квалитет комуникације и професионализма, а свакако се у том случају не дозвољава да се запослени опусте и дају информације које не би требало.

ЗАКЉУЧАК

Од када је акценат стављен на терористичке нападе широм света, са великим бројем повређених, здравствене установе су добиле на значају. До тада, стицао се утисак да имају споредну важност у односу на друге области које се убрајају у критичну инфраструктуру. У Републици Србији здравствене установе имају значајно место у изради плана Стратегије за заштиту критичне инфраструктуре. У случају да дође до неке ванредне ситуације (нпр. терористички напад, земљотрес, пожар, поплаве) која за последицу има велики број жртава (тровања, рањавања, повреде, епидемије, опекотине, итд.), од великог је значаја капацитет и опремљеност ЗУ да прихвате и збрину унесрећене. Од огромног је значаја добро развијен информациони здравствени систем који би олакшао сакупљање, селектовање, прослеђивање и чување осетљивих личних и здравствених података. Функционалан информациони здравствени систем ништа мање није битан ни у мирнодопским условима.

Постоји много специфичности у креирању информационих система у оквиру здравствених установа. За разлику од стандардних система, где постоје корисници и администратори, у случају здравствених информационих система постоји много више корисника, а самим тим и велика могућност губитка или „цурења" података.

Највећи проблем је недостатак свести руководећег менаџмента о потреби процене ризика, који, у највећем броју случајева, имплементира технологије заштите без процене ризика, као и олако схватање важности података крајњих корисника. Недовољно добро увиђају потребу контроле и последице које настају губитком или злоупотребом података у здравственим установама.

Неопходно је да државни органи и запослени схвате значај заштите личних података у информационим системима здравствених установа. Безбедност података је веома битна за егзистенцију и стабилност ЗУ и комплетног друштва. На нивоу државе то је стање заштићености националних интереса у информационој сфери, одређених скупом личних, корпоративних и државних интереса. Систем се сматра безбедним ако је у највећој могућој мери заштићен од фактора ризика. Сигурност је синоним безбедности. Сигурност се, начелно, односи на субјективно осећање, а безбедност на објективно стање. Фактори ризика се могу свести на минимум, али никада уклонити у потпуности.

Интегрисани здравствени информациони систем Републике Србије (ИЗИС) је одлична новина (у теоријском смислу) која је уведена у здравствени систем, која би у многоме требало да олакша корисницима здравствене заштите, тј. пацијентима (брже заказивање прегледа, одлазак код изабраног лекара и самим тим бржу примену терапијских процедура и спречавање тежих последица по здравље). Такође, овај систем би и здравственим радницима требало да пружи одређени комфор у приступу подацима о пацијенту путем јединствене базе података и самим тим уштеди им време за прикупљање и обраду података. Оно што је најбитније, јесте да се све то обезбеди на адекватне начине како не би дошло до злоупотребе прикупљених података.

Методологија података у здравственим информационим системима, представља комплетан скуп стратегија које обухватају анализу система, контролу фактора ризика и контролу процеса прикупљања и преноса података, а од посебног значаја је избор адекватне стратегије заштите.

Значај ИЗИС-а се не односи само на мониторинг и евалуацију података, већ и на више циљеве, као што су могућности раног упозорења у вези података, подршка пацијентима (корисницима здравствених услуга), помоћ менаџерима у сагледавању броја пацијената који пролазе кроз ЗУ, броја датих услуга, потрошње

материјала, финансијског прилива и одлива, злоупотребе положаја, неправилности у раду и благовремено упозорење о губитку и цурењу података итд. Омогућује планирање, подршку и подстицање истраживања, као и подршку у комуникацији између различитих корисника, што би требало имати у виду током даљег унапређења свих електронских могућности протока података.

У условима са ограниченим финансијским средствима, што је случај у нашим ЗУ, правилно планирање безбедносне политике информационих система пре уласка у набавке опреме и софтверских решења од суштинског је значаја, не само са аспекта рационализације трошкова набавке саме ИТ опреме, већ и са аспекта смањења ризика од проблема и штета који се могу појавити у информационим системима.

Као што је напоменуто раније, ИЗИС је одлична новина у теоретском смислу, али у пракси изгледа доста другачије. У току истраживања сусрели смо се са низом потешкоћа у усклађивању података из електронског информационог система и података из папирне документације, којом су здравствени радници у буквалном смислу речи „затрпани" и преоптерећени уносом података у систем. Идентични подаци се уписују у низ папирне документације (различите листе, протоколи), а затим уносе у електронски систем, што доводи до неминовне појаве грешака и губитка података.

Приметили смо и велике неправилности током истраживања које имају огроман утицај на безбедност података у информационим системима ЗУ: сви запослени који уносе податке у електронски систем (потрошни материјал, услуге) имају увид у демографске податке сваког пацијента, матичне бројеве, цене услуга и потрошног материјала и комплетан износ финансијских средстава уложених у лечење сваког хоспитализованог здравственог осигураника. Затим, свака медицинска служба када се улогује користећи заједничку лозинку (отприлике десет различитих особа), има увид у комплетан потрошни материјал, услуге и цене услуга друге медицинске службе. Свако ко се улогује може несметано да промени податке у систему (обрише, измени, слика итд.). Самим тим може доћи до случајне или намерне грешке, злоупотребе података, чиме је угрожена безбедност пацијената, запослених и саме здравствене установе (финансије, углед, идеје, итд.). Због нелиценцираних софтвера и антивирус програма, као и застареле опреме, сусрели

смо се са честим падовима система, уништењем хард диска, при чему се губе унети подаци или је потребно доста времена за доступност истих.

У циљу побољшања безбедности личних података у информационим системима здравствених установа, било би корисно уважити неке од следећих препорука:

База података мора да буде јединствена, односно да садржи исте податке као и националне базе истих корисника здравствених осигураника. Грађани мењају своје личне податке (адресе, презимена), а да ти подаци нису ажурирани у националним базама, већ се по први пут појављују као измена у установама примарне здравствене заштите. На пример, компликације које и после хоспиталне опсервације остављају трајне последице (психичке и физичке) нису евидентиране у бази података, особи НН није забрањено управљање моторним возилом (лице изазива саобраћајну несрећу са леталним исходом, инвалидитетом и психолошким траумама).

Раздвајањем личних података од медицинских, направити такав механизам да нико директним приступом информационом систему у ЗУ не може да повеже здравствене податке корисника са његовим именом, односно демографским подацима.

У интересу корпоративне безбедности ЗУ треба ограничити и увести нивое заштите, а самим тим и видљивост података путем персоналних лозинки и преусмеравањем података (сервер соба – директор – управни одбор треба да имају увид у све податке, а медицинске и парамедицинске службе само у податке из свог домена посла). У свакој медицинској и немедицинској служби податке у информациони систем треба да уноси особа која је задужена и обучена за тај посао. Она мора да поседује своју персоналну лозинку и да је обавезана уговором и упозната са санкцијама које проистичу из злоупотребе података.

Било би пожељно да медицински подаци о пацијенту буду шифровани како би касније могли да се обрађују и употребљавају. Потребно је да се у све ЗУ уведу стандардни шифрарници за дефинисање обољења, процедура које особље спроводи над пацијентом, лекова који се дају, итд.

Организација функционисања здравственог система у Републици Србији није на задовољавајућем нивоу. Промене су неопходне и због потребе усклађивања домаће регулативе са европском Општом уредбом о заштити података о личности – *GDPR*, која је ступила на снагу маја 2018. године. Безбедност и заштита информација у здравственим информационим системима је веома важан аспект који треба посебно планирати и имплементирати у системе и апликације.

Неопходан је динамички, проактивни приступ самом процесу планирања заштите на свим нивоима, а нарочито у нашем „осетљивом" здравственом окружењу, у којем су запослени у контакту са веома поверљивим подацима чија злоупотреба може довести до катастрофалних последица. Будући да је наша земља у процесу придруживања ЕУ, корисно је од просперитетних држава усвојити и добру праксу. Заштита података свакако представља једну од њих.

Почетком ове деценије, државни органи су учинили доста добрих корака када је у питању безбедност и заштита података. Ти кораци су још увек ситни у односу на „трчање" које нам предстоји, како бисмо, најпре донели добре законе, а затим исте ускладили са праксом, што за нашу земљу управо и представља један од највећих проблема – пут од доношења закона до извршења. Заштита личних података одавно је један од приоритета чија се усклађеност захтева од наше земље у односу на законе ЕУ. *GDPR* ће свакако представљати један од огромних „залогаја" са којим ћемо морати да се изборимо. О концептима Приватност по дизајну и Приватност по правилу ће се тек пуно причати, јер ће имплементација информационих решења заснованих на овим принципима бити императив за велике системе који рукују подацима о личности, али и пословна прилика за компаније које се баве развојем софтвера и сличних техничких решења.

GDPR прописује да је неопходно од самог почетка дизајнирати процесе обраде података и информационе системе како би се успешно спровела начела заштите података и заштитила права лица на која се подаци односе, те да је потребно имплементирати одговарајуће мере како би се обрада вршила само над подацима о личности који су неопходни за конкретну сврху обраде, тј. да се од грађана прикупља минимум података.

То конкретно значи да ће од сада свака компанија када прави нови бизнис план или стратегију, који обухватају и руковање или прикупљање података, од

самог почетка морати да прилагођава бизнис модел стандардима у области заштите приватности.

ПРИЛОГ: МОДЕЛ ИЗВЕШТАЈА О ИСТРАЖИВАЊУ ФУНКЦИОНИСАЊА ИЗИС-а У СКЛОПУ ЕЛЕКТРОНСКО-РАЧУНАРСКОГ ЦЕНТРА (ЕРЦ-а) ЗДРАВСТВЕНЕ УСТАНОВЕ

У циљу верификације налаза и донетих закључака о проблемима функционисања ИЗИС-а спроведено је емпиријско истраживање. Ово истраживање, у форми опсервационе студије спроведено је на основу Уговора од 28.3.2018. године потписаног са здравственом установом (ЗУ) у Западнобачком управном округу о приступу подацима у корист овог истраживања (назив ЗУ и седиште нису наведени због обавезе чувања пословне тајне, али су предочени ментору), у периоду од марта до маја 2018. године. Резултати студије сажети су у форми овог Извештаја.

У току истраживања фокус је стављен на:

- Организацију рада и кадровске ресурсе;
- Хардвер и софтвер (системски и апликативни);
- Рачунарску мрежу;
- Општу инфраструктуру која има везе са ЕРЦ-ом;
- Предузете мере безбедности;
- Потребе неопходне за одрживост функционисања система.

У старијој оронулој управној згради ЗУ, на високом приземљу, налазе се две просторије (по 30 м^2) савременог изгледа и опремљености, које су додељене ЕРЦ-у. Поред два стално запослена лица, ангажовано је и једно лице по Уговору о ПП пословима, што свакако не задовољава потребе установе која има 4 физички издвојене јединице и око 400 радних станица. У склопу прве просторије којој се приступа из ходника, налази се радни простор службеника ЕРЦ-а, са радним столовима и адекватном ИТ опремом, као и мини електро-техничка радионица за оправку хардверских компоненти.

При улазу у поменуту зграду, са десне стране, налазе се врата која воде у серверску собу (30 м^2), у којој се налазе „*rack*" витрине са веома задовољавајућом хардверском опремом за тренутне потреба ЗУ. Запослени су нам у својим примедбама указали на успорене процесе јавних набавки због законских процедура (законски рокови, обарања тендера и сл.), па им опрема стиже много касније, а самим тиме није у складу са непретком ИТ-а, јер бива застарела.

Системски софтвер је базиран на *Windows 7 Professional*, који је лиценциран на *Aprox* 50% радних станица, док се на осталих 50% користи нелиценциран софтвер због недостатка буџета. Руководилац ИТ сектора је присталица коришћења *Linux* оперативног система, али одређене вансистемске апликације (попут апликација за очитавање личних докумената, здравствених књижица и сл. нису подржане у *Linux*-у).

Серверска соба поседује адекватну климатизацију, антистатички (електропроводни) под, УПС уређаје за стабилно напајање електричном енергијом. Безбедност приступа просторијама је веома квалитетно урађена, ојачаним вратима и бравама, а са спољашње стране прозори су заштићени решеткастим баријерама. Серверска соба такође поседује противпровални алармни систем.

Недостаци у серверској соби (као кључном елементу ЕРЦ-а и ИЗИС-а) су следећи:

1. Противпожарна превентивна заштита (оптички и ручни јављачи пожара) требало би да се инсталирају на постојећу ПП централу, с обзиром на то да смо у самој болничкој јединици приметили да постоји инфраструктура за постављање истих. Такође, треба набавити адекватније противпожарне апарате од постојећих;
2. Противпоплавна заштита неопходна је из разлога што кроз обе собе пролазе цеви централног грејања и неопходни су сензори присуства воде, због могућности евентуалне хаварије.
3. Електронска контрола приступа јесте пожељна, али не и неопходна због високих трошкова инсталације и одржавања. Како кључевима располажу само запослени у ЕРЦ-у, неопходно је да још један кључ буде на располагању лицу одговорном за ППЗ или службенику ФО (свакако некоме ко је лиценциран и дежура у објекту 24 часа) у случају

опасности (пожар, поплава) које могу задесити ЗУ, а самим тим и серверску собу.

4. Како би се додатно спречио неовлашћен приступ серверској соби, пожељно је што пре (иако се парцијално ради на томе на нивоу ЗУ) увести видео надзор са 2 до 4 камере (ИП или аналогне).

Приступ подацима о пацијентима је регулисан на такав начин да сваки корисник (здравствени или ванздравствени радник ЗУ) *Heliant* апликације (електронско заказивање прегледа, е-здраствена књижица и е-рецепти) има своје корисничко име и лозинку, тако да је злоупотреба података о пацијентима сведена на оптимални минимум.

Што се мреже тиче, она је базирана на *VPN L-3, 256 Kbps*, што је далеко испод потреба данашње ере комуникација (нарочито узевши у обзир 4 издвојене јединице ЗУ), а уз потребе пацијената на стационару за *WI-FI* услугом, мишљења смо да треба ревидирати Уговор са добављачем телекомуникационих услуга.

Електрична инсталација у ЕРЦ-у је реализована преко посебних напојних водова са адекватном таблом са осигурачима. Сва серверска и активна мрежна опрема напаја се преко УПС уређаја, а долазни електрични вод је спојен и на агрегат који треба да обезбеди непрекидно напајање у случајевима прекида у снабдевању/хаварија у електроенергетском систему.

Пошто су службе ЗУ распоређене у више физички одвојених објеката, повезивање објеката је урађено оптичким кабловима, док је унутрашња мрежна инсталација бакарна. Тренутни капацитет оптичких линкова је 1 *Gbps*, што задовољава потребе, док је унутрашња инсталација од 100 *Mbps* на појединим чвориштима слаба због великог протока података.

Када је у питању заштита мреже, приступ интернету је делимично централизован са *internet gateway* сервером који има *firewall* заштиту (*Linux* решење које сами одржавају), док се на удаљеним локацијама користе посебни интернет линкови који немају довољан ниво заштите, а нису у могућности да их централизују због ограниченог капацитета *VPN* линка (256 Kbps).

Антивирусна решења која се користе су углавном *Microsoft Security Essentials*, *AVG* или *Avast* у бесплатним варијантама. Централизованог антивирусног решења нема.

Још један потенцијални сигурносни проблем је недостатак доменског сервера у мрежи, већ се користи *P2P,* односно *peer to peer,* модел комуникације путем интернета, пандан клијент/сервер моделу, најчешће у употреби за дељење датотека. Разлози овог проблема су недостатак средстава за адекватно опремање хардвером и софтвером, а исто тако и недостатак ИТ стручњака који би покривали ову област функционисања система.

Због хетерогености рачунарске мреже и уређаја на њој, броја и немогућности контроле спољних веза, сматрамо да систем који функционише у ЗУ није довољно безбедан, те запослени нису у могућности да сагледају и благовремено препознају могуће спољне упаде у исти.

По речима запослених, за сада на срећу, таквих упада није било, а број ситуација заразе вирусима је минималан, пре свега због дисциплинованости корисника (недисциплиновани су санкционисани, нпр. укидањем приступа интернету и сл.). Што се тиче падова система, сервери и мрежна инфраструктура раде поуздано и ту нема проблема, док су падови система на корисничким рачунарима учестали, најчешће због дотрајалости хардвера и застарелог софтвера.

ИТ сектор у овој ЗУ нема предвиђен буџет, што свакако отежава функционисање, планирање и развој истог, те је за даље квалитетно функционисање:

- Неопходно дефинисати буџет (подразумевана и софтверска и хардверска компонента). Тренутне реалне потребе на годишњем нивоу су реда величине 6 милиона динара, а уколико се реализује планирани пројекат ПАКС система, потребна финансијска средства могу бити и до 50% већа.
- Повећати број ИТ стручњака, јер садашњи број извршилаца није у могућности да одговори свим изазовима у администрацији система. Да би били успешни у овом послу, потребно је минимум 5-7 људи стручних у адекватним областима.
- Променити организациону структуру – тренутно је постојећи ЕРЦ на нивоу одсека који припада одељењу за финансијске послове, а реално,

делокруг рада ЕРЦ-а се дотиче свих сфера функционисања установе – како рачуноводствено-финансијског, тако и правно-кадровског, а нарочито медицинског.

ЛИТЕРАТУРА

1. Благојевић, И. (2018): Како функционишу *DDoS* напади и како заштитити *WordPress* сајт од DDoS напада, https://adriahost.rs/kako-funkcionisu-ddos-napadi-i-kako-zastititi-wordpress-sajt-od-ddos-napada/
2. Веиновић, М., Јевремовић, А. (2011): Рачунарске мреже, прво издање, Универзитет Сингидунум, Београд
3. Веиновић, М., Адамовић, С. (2013): Криптологија I, прво издање, Универзитет Сингидунум, Београд
4. Винер, Н. (1973): Кибернетика и друштво – људска употреба људских бића, Нолит, Београд
5. Вулетић, Д. (2011): Одбрана од претњи у сајбер простору, Институт за стратегијско истраживање, Београд
6. Делетић, В., Делетић, М. (2010): Заштита личних информација у информационим системима, Часопис из области економије, менаџмента и информатике БизИнфо, Блаце, бр. 2/2010, стр. 161-169
7. Ђокић, Д. (2012): Модел портала за интелигентно управљање електронским документима, докторска дисертација, Универзитет у Београду, Факултет организационих наука, Београд
8. Ђокић, Д. (2006): Дигитални сертификати и њихова улога у систему размене електронских докумената, ИНФО М, 5 (18), (11-15)
9. Ђорђевић, Б., Тимоченко, В., Баштјанчић Рокас, С., Мачек, Н., Купрешанин, М. (2015): Моделовање и поређење RAID перфомански на хардверском motherboard – RAID контролеру, ИНФОТЕХ-ЈАХОРИНА, Вол. 14, стр. 731
10. Ериксен, Т. (2003): Тиранија тренутка: брзо и споро време у информационом друштву, Библиотека XX век, Београд
11. Икић, Б. (2011): Организација заштите савремених информационих система, мастер рад, Универзитет Сингидунум, Департман за последипломске студије, Београд
    https://singipedia.singidunum.ac.rs/izdanje/41856-organizacija-zastite-savremenih-informacionih-sistema

12. Јаковљевић, В., Гоцић, Ј. (2012): Заштита критичне инфраструктуре у кризним ситуацијама, Међународна научна конференција, Менаџмент 2012, Младеновац, Србија 21-24. април 2012. (280-286)
13. Јанковић, Н. (2012): ИТ контроле и управљање ризицима информационих система, ПП презентација, ИНФОТЕХ 2012., Врњачка Бања, (1-37)
14. Катић, Д. (2015): Заштита здравственог информационог система, мастер рад, Универзитет Сингидунум, Београд https://singipedia.singidunum.ac.rs/izdanje/41062-zastita-zdravstvenog-informacionog-sistema
15. Кековић, З., Савић, С., Комазец, Н., Милошевић, М., Јовановић, Д. (2011): Процена ризика у заштити лица, имовине и пословања, Центар за анализу ризика и управљање кризама, Београд
16. Кларић, И. (2008): Пенетрацијски алат за испитивање рањивости Веб послужитеља, дипломски рад, Свеучилиште Загреб, Факултет електротехнике и рачунала, новембар 2008
17. Костић, П. (2004): Заштита личних информација у медицинским информационим системима, Универзитет Сингидунум, Београд https://singipedia.singidunum.ac.rs/izdanje/40048-zastita-licnih-informacija-u-medicinskim-informacionim-sistemima
18. Латиновић, М., Рајченић, С., Марић, С. (2010): ПКИ системи, стандарди и домаће законодавство, ИНФОТЕХ-ЈАХОРИНА, Вол.9, стр.827-831
19. Lawrence O. Gostin et al. (1993): Privacy and Security of Personal Information in a New Health Care System, Journal of the American Medical Association, 270(20), Nov.24, 1993, p 2487
20. Мандић, Г. (2015): Систем обезбеђења и заштите правних лица, Универзитет у Београду, Факултет безбедности, Београд
21. Мандић, Г., Путник, Н., Милошевић, М. (2017): Заштита података и социјални инжењеринг – правни, организациони и безбедносни аспекти, Универзитет у Београду, Факултет безбедности, Београд
22. Милосављевић, М., Адамовић, С. (2014): Криптологија II, прво издање, Универзитет Сингидунум, Београд

23. Николић, Д. (2010): Нормативни аспекти заштите података и информација, Београд, https://singipedia.singidunum.ac.rs/izdanje/40154-normativni-aspekti-zastite-podataka-i-informacija
24. Опачић, М.: (2018) Медицински информациони системи, Информационе технологије у медицини, лекција 1 (1-13), bmi.mas.bg.ac.rs/fajlovi/diplomske/ITM1.pdf
25. Петровић, С. (2004): Компјутерски криминал, Војноиздавачки завод, Београд
26. Протић, Д. (2013): Информациона безбедност: стандарди и правила, Војно дело пролеће/2013, (133-149)
27. Путник, Н., Бошковић, М. (2013): Савремени безбедносни изазови – хактивизам као нови облик друштвеног конфликта, монографска студија, Факултет безбедности Београд, Култура полиса, год.X (2013), бр. 21, (115-132)
28. Путник, Н. (2009): Сајбер простор и безбедносни изазови, Универзитет у Београду, Факултет безбедности, Београд
29. Путник, Н. (2012): Кибер ратовање – нови облик савремених друштвених конфликата, докторска дисертација, Универзитет у Београду, Факултет безбедности, Београд
30. Родић, Б. (2012): Андроид апликација за *Health Care* систем, мастер рад, Универзитет Сингидунум, Београд, https://singipedia.singidunum.ac.rs/izdanje/41641-android-aplikacija-za-health-care-sistem
31. Смиљанић, Н. (2018): Електронска обрада података, статистика и администрација, Београд https://iceps.edu.rs/wp-content/uploads/2018/03/Elektronska-obrada-podataka-statistika-i-administracija-dr-Smiljanic-Nina.pdf
32. Трнинић, З. (2015): Политика безбедности информација, Управа за заједничке послове републичких органа Републике Србије, Београд
33. Шкеро, М., Атаљевић, В. (2015): Заштита критичне инфраструктуре и основни елементи усклађивања са директивом Савета Европе 2008/114/ЕС, Војно дело 3/2015 (192-207)

34. *GDPR* уредба о заштити података о личности – https://startit.rs/gdpr-dolazi-u-srbiju-sve-sto-treba-da-znate-o-novoj-regulativi-za-zastitu-podataka-o-licnosti/
35. Закон о тајности података – Указ о проглашењу, Службени гласник Републике Србије, бр.104/2009
36. Закон о обради података, Службени гласник РС, бр. 97/08 од 27.10.2008. године, 104/09 - др. Закон 68/2012- одлука УС и 107/2012)
37. Закон о приватном обезбеђењу, Службени ласник Републике Србије бр. 104/2013
38. Закон о информационој безбедности, Службени гласник Републике Србије, бр. 6/2016
39. Закон о агенцији за борбу против корупције, Службени гласник Републике Србије, бр. 97/2008, 53/2010, 66/2011-УС, 67/2013-УС и 8/2015)
40. Закон о спречавању злостављања на раду, Службени гласник Републике Србије 36/2010
41. Закон о заштити пословне тајне, Службени гласник Републике Србије 72/2011
42. Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, 05 број 110-9472/2016-1 у Београду, 17. новембра 2016
43. Закон о здравственој документацији и евиденцијама у области здравства, Службени гласник Републике Србије, бр. 123/2014
44. Закон о ауторским и сродним правима, Службени гласник Републике Србије бр. 104/2009, 99/2011 и 119/2012
45. Закон о информационој безбедности, Сл. ласник РС, бр. 6/2016
46. Стратегија развоја информационог друштва у Републици Србији до 2020. године, Службени гласник Републике Србије, бр. 5/2010