ДРЖАВНА
РЕВИЗОРСКА
ИНСТИТУЦИЈА

ИЗВЕШТАЈ
О РЕВИЗИЈИ СВРСИСХОДНОСТИ ПОСЛОВАЊА

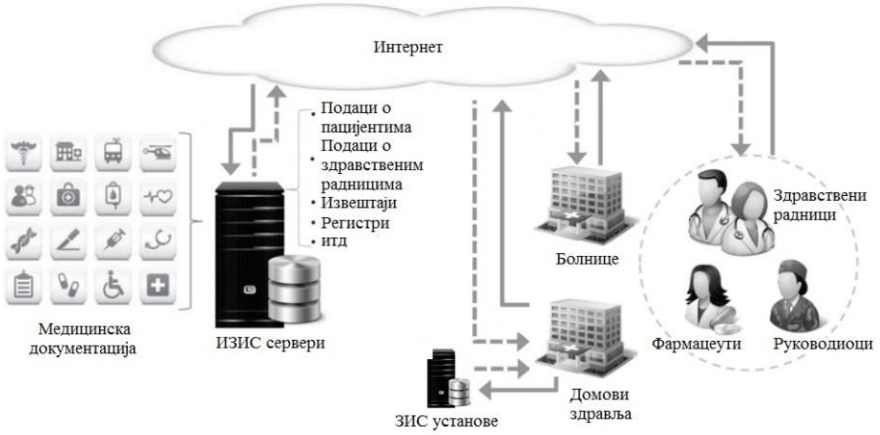
Информациона безбедност у здравственим информационим системима

Број: 400- 734/2020-03/20
Београд, 10. фебруар 2021. године

ПОТРЕБНО ЈЕ ДА МИНИСТАРСТВО ЗДРАВЉА, ИНСТИТУТ ЗА ЈАВНО ЗДРАВЉЕ СРБИЈЕ „ ДР МИЛАН ЈОВАНОВИЋ БАТУТ“ И ПОКРАЈИНСКИ СЕКРЕТАРИЈАТ ЗА ЗДРАВСТВО ВОЈВОДИНЕ УНАПРЕДЕ МЕРЕ ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ ШТО ЋЕ ДОПРИНЕТИ ВЕЋОЈ ПОУЗДАНОСТИ ЗДРАВСТВЕНИХ ИНФОРМАЦИОНИХ СИСТЕМА У РЕПУБЛИЦИ СРБИЈИ.

Интегрисани здравствени информациони систем ИЗИС уведен је у употребу у току 2016. године, и чини га здравствено-статистички део и здравствени информациони системи које користе здравствене установе, као што су Heliant, NexTZUS, ZIPsoft итд.

Базе података у овим системима садрже осетљиве личне податке, што изискује примену одређених мера заштите. У претходним ревизијама здравствених информационих система, утврђено је да постоје проблеми везани за информациону безбедност у више области: приступ бази података од стране пружаоца услуга; начин пријаве осигураника у систем, управљање резервним копијама, континуитет пословања у случају нежељених догађаја, неадекватна ИТ организациона структура, застарела опрема итд.



Потребно је унапредити **управљање** информационим системима, пре свега кроз усвајање и примену стратешких докумената и пратећих финансијских планова који треба да обезбеде стабилно функционисање и развој ових система, затим успостављање јасно дефинисане организационе структуре и јасно дефинисање и примену одговарајућих правила и процедура и ефективно управљање ИТ ризицима.

За поуздано функционисање свих компоненти ИЗИС-а (дакле и свих појединачних система у установама), неопходно је усвајање и имплементација планова за **континуитет пословања** у ванредним околностима, чији саставни део чини и управљање резервним копијама података у складу са законским обавезама и спроводити периодично тестирање тих планова.

Обезбеђивање доступности, поверљивости и интегритета података јесу кључни циљеви ИЗИС-а, зато је потребно предузети мере како би ови циљеви били постигнути. То подразумева одговарајућу организацију **ИТ безбедности**, усвајање правила и процедура у овој области, уређење процеса уговарања пружања услуга, и успостављање поузданог система уноса података и руковања излазним подацима.

Препоруке

Државна ревизорска институција је након спроведене ревизије субјектима ревизије између осталих дала следеће препоруке:

Министарству здравља:

- да предузме активности у смислу припреме предлога Стратегије развоја и организације интегрисаног здравственог информационог система и Акционог плана за примену Стартегије и да приликом припреме финансијских планова осигура стабилно финансирање циљева из Акционог плана за примену Стратегије
- да уреди услове за функционисање, управљање ризиком и безбедношћу информационих система, укључујући и континуитет пословања

Институту „Батут“

- да уреди процес обраде података од стране пружаоца услуга у здравственим информационим системима на законом прописан начин, што подразумева обавезну примену мера заштите података, и може укључити процес сертификације и издавања посебног или општег писменог овлашћења другим обрађивачима

Покрајинском секретаријату за здравство Војводине

- да приликом припреме финансијских планова осигура стабилно финансирање циљева из Акционог плана за примену Стратегије кроз детаљно планирање средстава за развој, набавку и одржавање информационих система у области здравства

Садржај

Скраћенице и термини

Табела број 1: Најчешће коришћене скраћенице у извештају

Пун назив	Скраћеница
Интегрисани здравствени информациони систем	ИЗИС
Институт за јавно здравље Србије "Др Милан Јовановић Батут"	Институт „Батут“
Покрајински секретаријат за здравство Војводине	Покрајински секретаријат
Републички фонд за здравствено осигурање	РФЗО
Аутономна Покрајина Војводина	АП Војводина
Информационе технологије	ИТ
Информациони систем	ИС
Информационо-комуникациони систем	ИКТ систем
Клинички центар	КЦ
Општа регулатива о заштити података о личности "General Data Protection Regulation"	ГДПР
Државна ревизорска институција	ДРИ

I Резиме и препоруке

Државна ревизорска институција је спровела ревизију сврсисходности „Информациона безбедност у здравственим информационим системима“.

Интегрисани здравствени информациони систем у даљем тексту ИЗИС је сложени информациони систем који чине здравствено-статистички систем, информациони системи организација здравственог осигурања и здравствени информациони системи здравствених установа, приватне праксе и других правних лица. У претходним годинама, у процесу вршења ревизије установљено је да код здравствених установа постоје проблеми везани за информациону безбедност у више области. Ови проблеми се односе на приступ базама података (поред запослених у здравственим установама, приступ је омогућен и пружаоцима услуга), управљање резервним копијама података, приступ подацима осигураника (поред употребе електронских здравствених књижица, приступ основним подацима је био омогућен и уношењем само једног идентификационог податка (ЈМБГ), континуитет пословања у случају нежељених догађаја, неадекватну организациону ИТ структуру, итд

Циљ ревизије је да се оцени у којој мери су примењене мере у здравственим информационим системима у Републици Србији испуниле неопходне циљеве када је у питању информациона безбедност.

Како су оснивачи здравствених установа Министарство здравља Републике Србије и Покрајински секретаријат за здравство у даљем тексту Покрајински секретаријат, и у њиховој је надлежности инвестиционо улагање када су у питању информациони системи, и како је Институт за јавно здравље Србије „Батут“ у даљем тексту Институт „Батут“ руковалац подацима у Интегрисаном здравственом информационом систему, ревизијом су као субјекти одабрани како би се препоруке могле свеобухватно и системски имплементирати. Узорковањем је одређен и један број здравствених установа које су нам у току ревизији биле извори информација.

У току ревизије су спроведене две анкете, обављен је већи број интервјуа, анализирано преко 1100 докумената, и коришћени су јавно доступни подаци, и подаци из извештаја ревизорских тимова ДРИ из претходних година.

Након спроведене ревизије утврдили смо:

Потребно је да Министарство здравља, Институт „Батут“ и Покрајински секретаријат за здравство унапреде мере информационе безбедности што ће допринети већој поузданости здравствених информационих система у Републици Србији.

Наведено заснивамо на закључцима и налазима који су изложени у наставку текста:

1. Постојећи системи ИТ управљања у здравству нису у потпуности омогућили испуњење пословних циљева, тачније пуну имплементацију Интегрисаног здравственог информационог система, процену ИТ ризика и успостављање адекватне организационе ИТ структуре

Не постоји стратешко планирање ни на републичком нивоу, јер Влада Републике Србије иако јој је то била и законска обавеза није усвојила Стратегију развоја и организације Интегрисаног здравственог информационог система, ни на нивоу сваке здравствене установе, које је неопходно имајући у виду константну потребу одржавања и модернизације информационих система (што подразумева хардвер, софтвер, организацију, едукацију, правила и процедуре итд). *(Препорука број 1)*

Због непостојања стратешког планирања, Министарство здравља, Покрајински секретаријат и здравствене установе нису обезбедиле стабилно финансирање здравствених информационих система самим тим ни развој и одржавање тих система, што може за последицу имати застарелу опрему и недовољан број серверских рачунара, застареле па самим тим и небезбедне оперативне системе, непотребно увећане трошкове за набавку апликативног софтвера, отежану израду финансијских планова када је у питању ИТ и на републичком нивоу и на нивоу сваке установе, недовољан број запослених на ИТ пословима и непостојање неопходних обука. *(Препоруке број 2 и 5)*

Организациона ИТ структура није успостављена на начин да је омогућена подела дужности и одговорности, као и испуњење законских обавеза. нити су усвојена правила и процедуре у вези управљања ИТ операцијама, што онемогућава или отежава контролу ових послова од стране руководства или континуитет обављања послова у случају замене запослених на ИТ пословима. У здравственим установама у којима су усвојене неке од неопходних процедура у овој области, оне нису довољно детаљне и свеобухватне. *(Препорука број 3)*

Управљање ИТ ризицима, Министарство здравља и Институт „Батут“, као и здравствене установе које смо обухватили анкетом нису успоставили иако је ово и законска обавеза, пре свега због непознавања ове проблематике, недовољно обученог ИТ кадра без искуства у овој области, а што за последицу може имати стварање непотребно великих трошкова у случају настанка нежељеног догађаја, а који се могао спречити или велике нефинансијске губитке (на пример података) због неблаговременог предузимања мера. *(Препоруке број 3 и 6)*

ИТ управљање је област која обухвата стратешко планирање, стабилно финансирање које прати акциони план за спровођење стратегије, одговарајућу ИТ организациону структуру, усвојене и примењене процедуре за ИТ послове, и управљање ИТ ризицима. Као што се из напред наведених налаза може закључити, потребно је унапређење у овој области на свим нивоима.

2. Ефективно управљање континуитетом пословања у случају ванредних околности у Интегрисаном здравственом информационом систему није у потпуности успостављено, што за последицу може имати нефункционисање делова система у дужем временском периоду

Институт „Батут“ и Министарство здравља, као и већина анкетираних здравствених установа нису усвојили ни имплементирали правила и процедуре за континуитет пословања иако је то и законска обавеза, што може за последицу имати нефункционисање система у неодређено дугом временском периоду, па самим тим и отежано пружање услуга здравственим осигураницима. *(Препорука број 3)*

Због недостатка потребне опреме, неадекватне ИТ организационе структуре и непостојања планова и процедура, Институт „Батут“, Министарство здравља и анкетиране здравствене установе нису успоставиле континуитет пословања у ванредним околностима – тј. опоравак од катастрофе, иако им је то била законска обавеза, што за последицу може имати нефункционисање информационог система у дужем временском периоду. *(Препорука број 3)*

Управљањем резервним копијама података из здравствених информационих система се не документује, зато што здравствене установе нису усвојиле одговарајуће процедуре, што су биле обавезне по закону, што отежава или онемогућава контролу овог процеса. *(Препорука број 3)*

Тестирање планова за континуитет пословања и опоравак од катастрофе Министарство здравља и Институт „Батут“, као и здравствене установе које смо

обухватили анкетом и које имају усвојене ове планове, не врше зато што немају довољно ресурса за то - пре свега запослених са довољно знања и искуства, иако је верификација тих планова обавеза свих оператора ИКТ система од посебног значаја, а што за последицу може имати нефункционални систем у току и након ванредне ситуације у дужем временском периоду. *(Препорука број 3)*

План континуитета пословања је шири оквир који дефинише кораке које треба предузети у случају нежељеног догађаја. Иако је чест случај да се посебно усвоји и план опоравка од катастрофе, он може бити и део плана континуитета. У склопу оба плана, управљање резервним копијама је обавезни и главни део тих планова, као и тестирање планова, и у склопу тога враћања података из резервних копија. Већина здравствених установа, као и Институт „Батут“ немају усвојене ове планове, а и код здравствених установа које су их усвојиле, они су непотпуни, недовољно детаљни и практично неприменљиви.

3. Здравствене установе нису усвојиле и примениле свеобухватне мере заштите информационих система, а Министарство здравља и Институт „Батут“ нису успоставили управљање информационом безбедношћу Интегрисаног здравственог информационог система и контролу примене мера заштите као приоритет, што је неопходно како би била осигурана поверљивост, доступност и поузданост података о личном здрављу грађана.

Организација ИТ безбедности у интегрисаном здравственом информационом систему није успостављена на адекватан начин, иако је то законска обавеза Министарства здравља, Института „Батут“ и здравствених установа, што за последицу има већи степен рањивости овог система па самим тим и осетљивих података здравствених осигураника. Нису организоване/спроведене обуке запослених на овим пословима, нису све здравствене установе усвојиле акт о информационој безбедности, нису ни Министарство здравља ни Института „Батут“ ни здравствене установе усвојиле политике и процедуре које се односе на информациону безбедност, није успостављена одговарајућа организациона ИТ структура, нису ни субјекти ревизије ни све здравствене установе одредиле одговорно лице за обавештавање о инцидентима. *(Препорука број 3)*

Није уређен однос са пружаоцима услуга када је у питању заштита података у здравственим информационим системима, нити је и поред тога што у већини уговора са пружаоцима услуга постоји део који се односи на поверљивост података, успостављен механизам за контролу да ли пружалац услуга ту обавезу поштује, што за последицу може имати одавање осетљивих података здравствених осигураника. *(Препоруке број 4 и 7)*

Није успостављен процес одобравања и укидања приступа продукционом систему на задовољавајући начин, због тога што нису усвојене процедуре које уређују овај процес и није успостављена контрола тог процеса, иако је то законска обавеза, што за последицу може имати угрожену безбедност података здравствених осигураника. *(Препорука број 3)*

Начин пријаве осигураника у систем није успостављен на једнообразан и максимално безбедан начин у свим здравственим установама, па постоји могућност да се од стране корисника система оствари увид у личне податке осигураника и у случајевима када он није присутан, идентификован на други начин или када то уопште није потребно. Не постоје успостављене и примењене процедуре које уређују безбедност свих излазних података, што за последицу може имати нарушавање поверљивости података. *(Препорука број 3)*

Успостављање мера које се односе на информациону безбедност, а обавезно на организацију ИТ безбедности, усвајање и примену процедуре и политике у овој области, јасно уређен процес уговарања услуга када је у питању заштита података, успостављање механизама контроле свих ових послова треба бити приоритет у наредном периоду када је у питању Интегрисани здравствени информациони систем.

Државна ревизорска институција, након спроведене ревизије „Информациона безбедност у здравственим информационим системима“, даје следеће препоруке:

Министарству здравља да:

1. Предузме активности у смислу припреме предлога Стратегије развоја и организације интегрисаног здравственог информационог система и Акционог плана за примену, које ће између осталог обухватити и прибављање мишљења Института за јавно здравље Србије „Др Милан Јовановић Батут“ и других организација и установа у области здравства, и иницира усвајање Стратегије и Акционог плана за њену примену (приоритет 2[1]);

2. Приликом припреме финансијских планова осигура стабилно финансирање циљева из Акционог плана за примену Стратегије кроз детаљно планирање средстава за развој, набавку и одржавање информационих система у области здравства (приоритет 3[2]);

3. Предузме активности у смислу припреме и доношења подзаконског акта којим ће ближе уредити услове за функционисање, управљање ризиком и безбедношћу интегрисаног здравственог информационог система, укључујући континуитет пословања у ванредним околностима, начин пријаве осигураника и заштиту излазних података, уз прибављање мишљења Института за јавно здравље Србије „Др Милан Јовановић Батут“ и других организација и установа у области здравства (приоритет 2);

4. Предузме активности у смислу припреме и одређивања ближе садржине података, укључујући и податке о личности, који се воде у електронском медицинском досијеу, начин и поступак преузимања података, као и друга питања од значаја за успостављање и коришћење података, уз прибављено мишљење Института за јавно здравље Србије „Др Милан Јовановић Батут“ и других организација и установа у области здравства (приоритет 2).

Покрајинском секретаријату за здравство да:

5. Приликом припреме финансијских планова осигура стабилно финансирање циљева из Акционог плана за примену Стратегије кроз детаљно планирање средстава за развој, набавку и одржавање информационих система у области здравства (приоритет 3);

Институту за јавно здравље Србије „Др Милан Јовановић Батут“ да:

6. Успостави одговарајуће техничке, организационе и кадровске мере за обраду података у ИЗИС-у, и да успостави механизам за праћење примене тих мера (приоритет 2);

[1] ПРИОРИТЕТ 2 - Несврсисходности које је могуће отклонити у року до годину дана
[2] ПРИОРИТЕТ 3 - Несврсисходности које је могуће отклонити у року од једне до три године

7. Уреди процес обраде података од стране пружаоца услуга у здравственим информационим системима на законом прописан начин, што подразумева обавезну примену мера заштите података, и може укључити процес сертификације и издавања посебног или општег писменог овлашћења другим обрађивачима (приоритет 2).

Генерални државни ревизор

_____

Др Душко Пејовић
Државна ревизорска институција
Макензијева 41
11000 Београд, Србија
10. фебруар 2021. године

II Увод

Државна ревизорска институција спровела је ревизију сврсисходности на тему „Информациона безбедност у здравственим информационим системима“. Ревизија је спроведена у складу са Законом о Државној ревизорској институцији[3], Пословником Државне ревизорске институције[4] и Програмом ревизије Државне ревизорске институције за 2020. године. Поступци ревизије су спроведени у периоду од јуна до новембра 2020. године.

Ревизија је обављена на начин и према поступцима утврђеним Оквиром професионалних стандарда Међународне организације врховних ревизорских институција (INTOSAI), Кодексом професионалне етике државних ревизора и принципима Међународних стандарда врховних ревизорских институција (ISSAI).

1. Проблем

ИЗИС је уведен у употребу 2016. године. Здравствене установе у претходном периоду су користиле, а и данас користе здравствене информационе системе, као што су Heliant, NexTZUS, ZIPsoft итд. на нивоу појединачне здравствене установе.

Базе података у овим системима садрже поред личних података, податке о болестима, терапијама, процесу лечења, лековима итд. што представља осетљиве личне податке и изискују примену одређених мера заштите. Проблематику заштите података осигураника уређује више законских прописа, а посебно Закон о здравственој документацији и евиденцијама у области рада, Закон о заштити података о личности, Закон о тајности података и Закон о информационој безбедности (који уређује обавезне мере заштите, које треба примењивати са циљем очувања интегритета, поверљивости и расположивости података).

У претходном периоду, у процесу вршења ревизије здравствених информационих система, установљено је да су постојали проблеми везани за информациону безбедност у више области.

Приступ бази података	• Поред запослених у здравственој установи, приступ системима и базама података имају и пружаоци услуга одржавања система, а треба имати у виду да те базе садрже јако осетљиве податке о сваком осигуранику.
Начин пријаве осигураника и приступ картону осигураника	• Решење које се примењује је такво да се подацима осигураника може приступити само на основу једног податка (ЈМБГ осигураника), без идентификационе електронске здравствене картице или ЛБО осигураника, што у пракси значи чак и без његовог присуства или чак и знања.
Приступ резервним копијама и њихово чување	• Иако се у свим ревидираним субјектима чувају резервне копије, тај процес није уређен на истоветан, формализован, контролисан па самим тим и безбедан начин.
Континуитет пословања у случају нежељених догађаја	• Како се сви прегледи и лечења заказују употребом информационих система, неопходно је обезбедити функционисање система увек, а то значи и у случају нежељених догађаја.

Илустрација 1. *Раније установљени проблеми везани за информациону безбедност у здравственим установама*

[3] „Службени гласник РС“, бр. 101/2005, 54/2007, 36/2010 и 44/2018-др.закон
[4] „Службени гласник РС“, број 9/2009

2. Циљ ревизије

Циљ ревизије је да се оцени у којој мери су примењене мере у здравственим информационим системима у Републици Србији испуниле неопходне циљеве када је у питању информациона безбедност.

Изабрана тема је повезана са Циљем 1 из Стратешког плана ДРИ за период 2019-2023, да ће ДРИ одговорити на тренутне и хитне изазове у раду корисника јавних средстава, односно потциљем 1.7: Здравство (Функционална буџетска категорија 700): ДРИ ће својим радом допринети унапређењу здравствене заштите грађана. Осим тога, може се наћи веза и са циљем 2 Утврдити проблеме и предложити решења за међусекторске проблеме на свим нивоима, ради унапређивања одговорности и транспарентности, односно у оквиру тога Потциљ 2.5: Унапредити јавно управљање и коришћење информационих технологија (ИТ)[5].

ИТ системи су од кључног значаја за пословање у оквиру јавног сектора и активности постају све скупље, сложеније и као и степен осетљивости података које оне садрже. Осим тога, иницијативе е-управе у Србији имају за циљ унапређење коришћења ИТ и интернета широм јавне управе да би се обезбедиле информације грађанима и привредним друштвима. ДРИ је кроз своје ревизије ранијих година утврдила да неки субјекти ревизије нису предузели неопходне мере у области безбедности ИТ система - укључујући и право на приступ подацима и поверљивост података. Нису спровели неопходне процене ризика, нити су усвојили стратегије које регулишу развој ИТ технологија. Ово неадекватно планирање ИТ развоја довело је до кашњења у реализацији пројеката укључујући и нови интегрисани пословни ИТ систем и резултирало је у додатним трошковима[6].

Циљ ДРИ је и да се помогне да се унапреди способност ИТ система да сви јавни програми постану ефикаснији, а да се при томе штите кључно пословање и осетљиве информације.

3. Ревизорска питања

Како бисмо остварили циљ ревизије, усмерили смо се на прибављање одговора на следећа ревизијска питања:

1. У којој мери су успостављени системи управљања здравственим информационим системима омогућили испуњење пословних циљева, успостављање јасно дефинисане организационе структуре и управљање ризицима?

- Да ли организација има ИТ Стратегију или сличан стратешки документ којим се планирају дугорочни и краткорочни циљеви развоја информационог система, а који је усвојио највиши орган управљања?
- Да ли су предузете потребне активности у циљу осигурања стабилног финансирања развоја и одржавања информационог система, а у складу са донетим плановима/ИТ стратегијом?
- Да ли је организација одобрила и користи одговарајућа правила и процедуре за управљане ИТ операцијама?
- Да ли је успостављено управљање ИТ ризицима, што подразумева њихову идентификацију и спровођење плана за умањење ризика?

[5] Стратешки план Државне ревизорске институције за период 2019-2023. *http://www.dri.rs/upload/documents/Opsti_dokumenti/DRI%20Strateski%20plan%202018-2023.pdf*

[6] Стратешки план Државне ревизорске институције за период 2019-2023. *http://www.dri.rs/upload/documents/Opsti_dokumenti/DRI%20Strateski%20plan%202018-2023.pdf*

2. Да ли је успостављен ефективан оквир за континуитет пословања у случају ванредних околности?

- Да ли постоје имплементирана правила и процедуре за континуитет пословања?
- Да ли постоји имплементиран план за континуитет пословања у ванредним околностима (план опоравка од катастрофе)?
- Да ли се резевне копије чувају у складу са донетим правилима и процедурама, на документован и безбедан начин?
- Да ли се врши документовано перидично тестирање плана за континуитет пословања и плана за опоравак од катастрофе?

3. Да ли успостављене мере безбедности података у здравственим информационим система обезбеђују доступност, поверљивост и интегритет?

- Да ли субјекат ревизије има јасну организацију ИТ безбедности и да ли су безбедносне улоге и одговорности дефинисане у вези са правилима и процедурама за безбедност информација?
- Да ли постоји механизам којим се осигурава да је пружалац услуге усвојио услове за заштиту и безбедност података и да ли их спроводи?
- Да ли организација има јасна и ефикасна правила и процедуре контроле физичког и логичког приступа и да ли је процес давања и укидања контроле приступа запосленима и пружаоцима услуга сигуран и ефективан?
- Да ли је адекватно управљање изворним документима, прикупљањем података и уносом и да ли су излазне информације правилно заштићене?

Питања која смо формулисали се односе на три најризичније области, на осонву процене ризика коју смо спровели на бази доступних тј. прикупљених података у предстудији, али и на основу сазнања из претходних година до којих је ДРИ дошла у склопу других обављених ревизија.

Прво питање се односи на ИТ управљање. Адекватно ИТ управљање је неопходно како би се управљало целим системом, тачније свим његовим компонентама почевши од идентификације захтева, одобрења, набавке, развоја, одржавања, безбедоносне политке и контроле рада апликације. И посебно важно, питање које прожима цео информациони систем и његов „животни век“ – процена ризика, проблем и питање које смо идентификовали код (скоро) свих установа и субјеката ревизије.

Друго питање се односи на континуитет пословања и опоравак од катастрофе (како се то дефинише у ИТ пракси, ИТ приручнику, итд.), тј. на континуитет пословања у ванредним околностима (како се то дефинише у Закону о информационој безбедности, тј. Уредби о ближем уређењу мера заштите ИКТ система од посебног значаја). Ризик у овој области је велики у великој већини установа које немају усвојене планове и процедуре, резервну локацију, резервне сервере а ни потребно знање за ове послове. У пракси, ослањају се на пружаоце услуга, што је опет недовољно обзиром на непостојање потребног хардвера. У склопу овог питања, анализираћемо и начин на који се израђују и чувају резервне копије. Наравно, сва ова питања се односе и на централни здравствени информациони систем.

Треће питање се односи на правила, процедуре и њихову примену када су у питању безбедност података, физичка безбедност сервера, управљање и контролу логичког приступа и безбедност улазних и излазних података на корисничким рачунарима. Безбедност података, а у овом случају се ради о осетљивим подацима које третира Закон о заштити података о личности, Закон о заштити права пацијената, Закон о информационој безбедности и други закони, је уствари кључно питање ове ревизије, због чега се и анализирају сва остала питања.

4. Обим и ограничења ревизије

Ревизијом смо обухватили активности Министарства, Института „Батут“ и Покрајинског секретаријата у периоду од 2017. до 2019. године, а због праћења тренда су обухваћени и неки подаци из 2020. године.

Предмет испитивања су биле области:

1) ИТ управљање - може се сматрати целокупним оквиром који води ИТ операције у организацији како би се обезбедило да организација задовољава потребе пословања у садашњости и да укључује планове за будуће потребе и развој. Основна улога ИТ управљања је да обезбеди: да ИТ систем одговара пословним потребама; да планира будуће промене на систему; да обезбеди неопходан ниво интерних контрола; да има одговарајућу организациону структуру и прецизно дефинисане описе послова запослених на ИТ пословима; и да ли примењује неопходне политике и процедуре који се односе на ИТ систем[7];

2) План континуитета пословања (BCP[8]) и План опоравка од катастрофе (DRP[9]). BCP је процес који организација користи за планирање и тестирање опоравка својих пословних процеса након поремећаја. Такође описује како ће организација наставити да функционише у неповољним условима који могу настати (на пример, природне или друге несреће). Планирање опоравка од катастрофе (DRP) је процес планирања и тестирања за опоравак инфраструктуре ИТ након природне или друге несреће. То је подскуп планирања континуитета пословања. BCP се примењује на организационе пословне функције док DRP на ИТ ресурсе који подржавају пословне функције.[10]

3) Информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица[11]

У поступку ревизије није испитивано да ли: (1) финансијски извештаји субјеката ревизије објективно и истинито приказују њихово финансијско стање, резултате пословања и новчане токове, у складу са прихваћеним рачуноводственим начелима и стандардима; (2) су финансијске трансакције и одлуке у вези са примањима, приходима, расходима и издацима извршене у складу са законом и другим прописима и за планиране сврхе.

Ограничења ове ревизије су:

- Ситуација услед вируса COVID-19 у току целе 2020.-те године и посебно ангажовања и надлежности Министарства здравља, Института „Батут“, Покрајинског секретаријата, и здравствених установа у време и након окончања ванредног стања, и у време након тога у борби за сузбијање вируса, дошло је до продужења рока ревизије због отежаног прикупљања документације;
- Доношење закључака на бази анализе ограниченог броја здравствених установа и
- Немогућност генерализовања налаза, односно закључака ревизије.

[7] WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions
[8] BCP (енгл. Business continuity Planning) Планирање континуитета пословања
[9] DRP (енгл. Disaster Recovery Planning) Планирање опоравка од катастрофе
[10] WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions
[11] Члан 7. став 3. Закона о информационој безбедности

5. Методологија у поступку рада

Да бисмо одговорили на ревизорска питања, анализирали смо законску и подзаконску регулативу, користили стручну литературу (WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions[12]), као и све податке добијене од субјеката ревизије и извора информација - здравствених установа. Анализирали смо податке и информације за период од 2017. до 2019. године.

У вези са информационом безбедношћу здравствених информационих система анализиране су области ИТ управљање, планирање континуитета пословања (BCP), планирање опоравка од катастрофе (DRP) и информациона безбедност.

У циљу потврђивања информација из документације и прикупљања података који нису доступни у документима, обавили смо интервјуе и послали анкете и упитнике корисницима информационог система здравствених установа.

Детаљнији опис коришћене методологије дат је у Прилогу 1

[12] INTOSAI Радна група за ИТ ревизију

III Опис предмета ревизије

ИЗИС је уведен у употребу у току 2016. године, је централни електронски систем, који повезује здравствене информационе системе здравствених установа, у коме се чувају и обрађују сви медицински и здравствени подаци пацијената[13], подаци здравствених радника и сарадника, подаци здравствених установа, здравствене интервенције и услуге извршене у здравственим установама, подаци електронских упута и електронских рецепата, подаци о заказивању за специјалистичке прегледе, дијагностичке процедуре и хируршке интервенције.

1. Законодавни и институционални оквир

Законодавни оквир

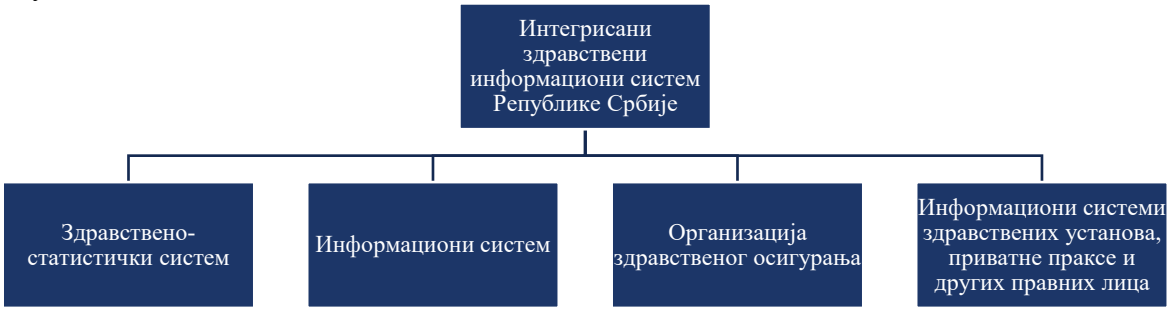
Закон о здравственој заштити[14], у члану 55, прописује је да се ради планирања и ефикасног управљања системом здравствене заштите, као и прикупљања и обраде података у вези са здравственим стањем становништва и функционисањем система здравствене заштите, односно прикупљања и обраде здравствених информација, организује и развија интегрисани здравствени информациони систем у Републици Србији.

Истим чланом, прописано је да се сврха обраде података, садржај здравствених информација, приступ подацима о пацијенту из електронског медицинског досијеа, руковаоци подацима и друга питања од значаја за заштиту података о личности, уређују се у складу са законом којим се уређује здравствена документација и евиденције у области здравства.

Закон у истом члану прописује да стратегију развоја и организације интегрисаног здравственог информационог система, доноси Влада.

Део III Закона о здравственој документацији и евиденцијама у области здравства[15] уређује Интегрисани здравствени информациони систем.

Чланом 44. наведеног закона прописано је да се Интегрисани здравствени информациони систем Републике Србије организује 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.

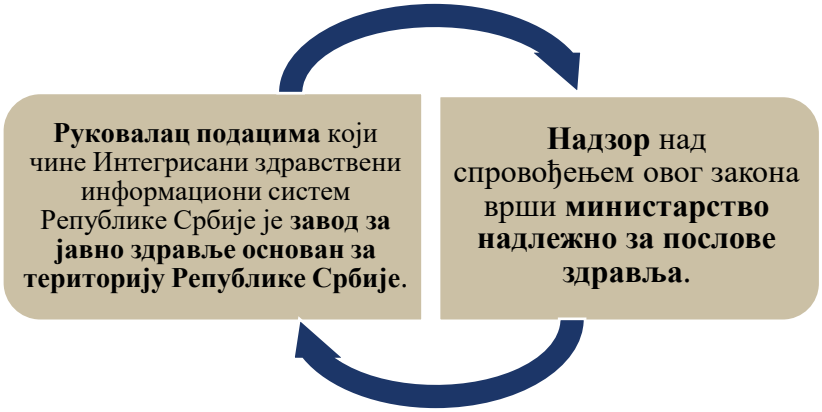


Илустрација 2. *Системи који чине ИЗИС у складу са чланом 44. став 2. Закона о здравственој документацији и евиденцијама у области здравства*

[13] Медицински подаци бележе бригу о пацијенту, а здравствени подаци поред медицинског податка садржи и податак у којој здравственој установи је пружена услуга пацијенту.
[14] „Службени гласник РС“, број 25/2019
[15] „Службени гласник РС“, бр. 123/2014, 106/2015, 105/2017 и 25/2019 - др. закон

Чланом 45. истог закона прописано је да су здравствена установа, приватна пракса и друго правно лице које води здравствену документацију и евиденцију, дужни су да успоставе информациони систем, који представља свеобухватни скуп технолошке инфраструктуре (мрежних, софтверских и хардверских компонената), организације, људи и поступака за прикупљање, смештање, обраду, чување, пренос, приказивање и коришћење података и информација.

Истим чланом[16] прописано је да ближе услове за функционисање, управљање ризиком и безбедношћу информационог система, јединствене методолошке принципе и стандарде и друге услове од значаја за функционисање овог система прописује министар уз прибављено мишљење завода за јавно здравље основаног за територију Републике Србије и организације обавезног здравственог осигурања.



Илустрација 3. *Одредбе Закона о здравственој документацији и евиденцијама у области здравства (члан 44. став 4 и члан 52.).*

Завод за јавно здравље основан за територију Републике Србије дужан је да о свакој повреди безбедности података система обухваћених чланом 44. став 5. Закона о здравственој документацији и евиденцијама о области здравства, обавести лице, односно лица на која се ти подаци односе, министарство надлежно за послове здравља и Повереника за информације од јавног значаја и заштиту података о личности.

Закон о информационој безбедности[17] у делу II Безбедност ИКТ система од посебног значаја (чланови 6. – 13.), уређује који су то ИКТ системи од посебног значаја; мере заштите ИКТ система од посебног значаја; акт о безбедности ИКТ система од посебног значаја; поверавање активности у вези са ИКТ системом од посебног значаја трећим лицима; обавештавање надлежног органа о инцидентима.

Члан 6. став 1. тачка 3) подтачка (13) наведеног закона, прописује да су ИКТ системи од посебног значаја системи који се користе у обављању делатности од општег интереса у области здравствене заштите.

Истим чланом у ставу 2. прописано је да Влада, на предлог министарства надлежног за послове информационе безбедности, утврђује листу послова и делатности из става 1. тачка 3) овог члана. Уредбом о утврђивању листе делатности у областима у којима се обављају делатности од општег интереса и у којима се користе информационо-комуникациони системи од посебног значаја[18], утврђена је Листа

[16] Члан 45. став 3. Закона о здравственој документацији и евиденцијама у области здравства
[17] „Службени гласник РС“, бр. 6/2016 и 94/2017
[18] „Службени гласник РС“, број 94/2019

делатности у областима у којима се обављају делатности од општег интереса и у којим а се користе ИКТ системи од посебног значаја. Тачка 3. односи се на област Здравства и као делатност је наведена здравствена заштита, у смислу закона којим се уређује здравствена заштита- здравствена делатност коју обављају здравствене установе и друга правна лица која обављају здравствену делатност.

Законом о правима пацијената уређена су права пацијената приликом коришћења здравствене заштите, начин остваривања и начин заштите тих права, као и друга питања у вези са правима и дужностима пацијената.[19]

Овим законом уређено је и право на заштиту физичких лица у вези са обрадом података о личности коју врше надлежни органи у сврхе спречавања, истраге и откривања кривичних дела, гоњења учинилаца кривичних дела или извршења кривичних санкција, укључујући спречавање и заштиту од претњи јавној и националној безбедности, као и слободни проток таквих података.

Закон о заштити података о личности уређује се право на заштиту физичких лица у вези са обрадом података о личности и слободни проток таквих података, начела обраде, права лица на које се подаци односе, обавезе руковалаца и обрађивача података о личности, кодекс поступања, пренос података о личности у друге државе и међународне организације, надзор над спровођењем овог закона, правна средства, одговорност и казне у случају повреде права физичких лица у вези са обрадом података о личности, као и посебни случајеви обраде.[20]

Члан 17. закона уређује обраду посебних врста података о личности, те је између осталог дефинисано да је забрањена обрада података о здравственом стању физичког лица, као и у којим случајевима је обрада допуштена, ако је неопходна у сврху превентивне медицине или медицине рада, ради процене радне способности запослених, медицинске дијагностике, пружања услуга здравствене или социјалне заштите, односно управљања здравственим или социјалним системима, на основу закона или на основу уговора са здравственим радником, ако се обрада врши од стране или под надзором здравственог радника или другог лица које има обавезу чувања професионалне тајне прописане законом или професионалним правилима; уколико је обрада неопходна у циљу остваривања јавног интереса у области јавног здравља, као што је заштита од озбиљних прекограничних претњи здрављу становништва или обезбеђивање високих стандарда квалитета и сигурности здравствене заштите и лекова или медицинских средстава, на основу закона који обезбеђује одговарајуће и посебне мере заштите права и слобода лица на које се подаци односе, посебно у погледу чувања професионалне тајне.

Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја ближе се уређују мере заштите информационо-комуникационих система од посебног значаја.[21]

Уредбом о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја, ближе се уређује садржај акта о безбедности информационо-комуникационих система од посебног значаја.[22]

[19] „Службени гласник РС“, бр. 45/2013 и 25/2019 - др. закон
[20] „Службени гласник РС“, број 87/2018
[21] „Службени гласник РС“, број 94/2016
[22] „Службени гласник РС“, број 94/2016

Уредбом о програму рада, развоја и организацији интегрисаног здравственог информационог система - "е-Здравље" утврђује се Програм рада, развоја и организација интегрисаног здравственог информационог система "е-Здравље"[23]

На основу ове уредбе донет је Правилник[24] о ближој садржини технолошких и функционалних захтева за успостављање интегрисаног здравственог информационог система, којим се прописује ближа садржина технолошких и функционалних захтева за успостављање интегрисаног здравственог информационог система

На основу Закона о здравственој документацији и евиденцији у области рада, донет је Правилник о обрасцима и садржају образаца за вођење здравствене документације, евиденција, извештаја, регистара и електронског медицинског досијеа[25], којим прописани обрасци и садржај образаца за вођење основне здравствене документације и помоћних средстава за вођење евиденција у области здравствене заштите, садржај регистара и електронског здравственог досијеа, као и садржај извештаја, осим за области које су уређене прописима из те области: (а) заразних болести (укључујући и болничке инфекције) и обавезне имунизације; (б) трансфузиолошке делатности, трансплантације и биомедицински потпомогнуте оплодње, лекова и медицинских средстава; (в) повреда на раду и професионалних обољења. Такође, овај правилник не садржи ни извештаје о умрлим лицима.

Институционални оквир

Завод за јавно здравље основан за територију Републике Србије је у складу са законом о здравственој документацији и евиденцијама у области здравства, руковалац подацима који чине Интегрисани здравствени информациони систем Републике Србије.

Министарство здравља обавља послове државне управе који се односе на: систем здравствене заштите; систем обавезног здравственог осигурања, других облика здравственог осигурања и доприноса за здравствено осигурање; ближе уређивање права из здравственог осигурања; учествовање у припреми и спровођењу међународних споразума о обавезном социјалном осигурању; стварање услова за приступ и реализацију пројеката из делокруга тог министарства који се финансирају из средстава претприступних фондова Европске уније, донација и других облика развојне помоћи; садржај здравствене заштите, очување и унапређење здравља грађана и праћење здравственог стања и здравствених потреба становништва; организацију здравствене заштите; стручно усавршавање и специјализацију здравствених радника; здравствену инспекцију; организацију надзора над стручним радом здравствене службе; обезбеђивање здравствене заштите из јавних прихода; здравствену заштиту странаца; евиденције у области здравства; услове за узимање и пресађивање делова људског тела; производњу и промет лекова, медицинских средстава и помоћних лековитих средстава и инспекцијске послове у тим областима; производњу и промет опојних дрога и прекурсора недозвољених дрога; ископавање и преношење умрлих лица у земљи, преношење умрлих лица из иностранства у земљу и из земље у иностранство; санитарну инспекцију; здравствени и санитарни надзор у области заштите становништва од заразних и незаразних болести, здравствене исправности животних намирница и предмета опште употребе у производњи и промету, јавног снабдевања становништва хигијенски исправном водом за пиће и

[23] „Службени гласник РС“, број 55/2009
[24] „Службени гласник РС“, број 95/2009
[25] „Службени гласник РС“, бр. 109/2016 и 20/2019

другим областима одређеним законом; контролу санитарно-хигијенског стања објеката под санитарним надзором и средстава јавног саобраћаја; санитарни надзор над лицима која су законом стављена под здравствени надзор, као и надзор над постројењима, уређајима и опремом која се користи ради обављања делатности под санитарним надзором; утврђивање санитарно-хигијенских и здравствених услова објеката под санитарним надзором у поступцима изградње или реконструкције и редовну контролу над тим објектима; санитарни надзор на државној граници, као и друге послове одређене законом.[26]

Општи интерес у здравственој заштити у Републици Србији обухвата и изградњу и опремање здравствених установа у државној својини чији је оснивач Република, које обухвата: инвестиционо улагање, инвестиционо - текуће одржавање просторија, медицинске и немедицинске опреме и превозних средстава, односно врши набавку медицинске и друге опреме неопходне за рад здравствених установа и превозних средстава, обезбеђивање средстава, односно набавку опреме за развој интегрисаног здравственог информационог система, као и обезбеђивање средстава за друге обавезе одређене законом и актом о оснивању.[27]

Покрајински секретаријат за здравство Војводине (у даљем тексту: Покрајински секретаријат) обавља послове покрајинске управе у области здравства. Такође прати и помаже рад здравствених установа чији су оснивачи органи АП Војводине[28].

АП Војводина преко својих органа, у складу са законима којима се уређује систем у области здравства, обавља послове:

1) друштвену бригу за здравље на нивоу АП Војводине која обухвата мере за обезбеђивање и спровођење здравствене заштите од интереса за грађане на територији АП Војводине;

2) доноси посебне програме здравствене заштите за поједине категорије становништва, односно врсте болести које су специфичне за АП Војводину а за које није донет посебан програм здравствене заштите на републичком нивоу, у складу са својим могућностима, и утврђује цене појединачних услуга, односно програма;

3) оснива здравствене установе на територији АП Војводине у складу са Планом мреже здравствених установа који доноси Влада, и то: општу болницу, специјалну болницу, клинику, институт, клинички центар, завод за јавно здравље, завод за трансфузију крви и завод за антирабичну заштиту;

4) оснива завод за јавно здравље за територију АП Војводине који координира и прати стручни рад завода за јавно здравље и других здравствених установа које обављају хигијенско-епидемиолошку и социјално-медицинску делатност на територији АП Војводине, предлаже дугорочне мере здравствене заштите са приоритетима и методолошки руководи њиховим спровођењем на територији АП Војводине, предлаже заводу за јавно здравље основаном за територију Републике Србије потребне мере у елементарним и другим већим непогодама и несрећама и врши њихово спровођење у сарадњи са другим установама;

5) оснива завод за трансфузију крви за територију АП Војводине, који обавља делатност у складу са законом којим се уређује трансфузиолошка делатност;

6) даје предлог за утврђивање Плана мреже здравствених установа који доноси Влада за здравствене установе на територији АП Војводине;

[26] члан 15. Закона о министарствима („Службени гласник РС“, бр. 44/2014, 14/2015, 54/2015, 96/2015 - др. закон и 62/2017)
[27] члан 17, тачка 24. Закона о здравственој заштити
[28] члан 35. Покрајинске скупштинске одлуке о покрајинској управи

7) именује и разрешава директоре, заменике директора, чланове управног и надзорног одбора здравствених установа чији је оснивач;

8) даје сагласност на статуте здравствених установа чији је оснивач;

9) утврђује недељни распоред рада, почетак и завршетак радног времена у здравственој установи чији је оснивач;

10) утврђује недељни распоред рада, почетак и завршетак радног времена здравствених установа и приватне праксе који се налазе на територији АП Војводине за време епидемија и отклањање последица проузрокованих елементарним и другим већим непогодама и ванредним приликама, за епидемије и друге веће непогоде и ванредне прилике на територији АП Војводине;

11) даје предлог министру надлежном за послове здравља за утврђивање броја приправника у здравственим установама са седиштем на територији АП Војводине, које су здравствене установе дужне да приме за обављање приправничког стажа на годишњем нивоу;

12) даје мишљење на План развоја кадра у здравству који доноси министар надлежан за послове здравља, за установе које се налазе на територији АП Војводине;

13) даје предлог министру надлежном за послове здравља за утврђивање референтних здравствених установа за поједине области здравствене делатности на територији АП Војводине;

14) утврђује минимум процеса рада за време штрајка здравствених установа на територији АП Војводине;

15) оснива Здравствени савет Војводине као стручно и саветодавно тело које прати развој здравствене заштите и здравственог осигурања у АП Војводини и

16) оснива Етички одбор Војводине као стручно тело.

У остваривању надлежности органи АП Војводине остварују сарадњу са републичким и органима јединица локалне самоуправе[29].

АП Војводина је надлежна за вршење следећих послова здравствене и социјалне заштите:

–оснива установе социјалне заштите на територији АП Војводине у складу са законом и актом Владе;

–утврђује послове и уређује друга питања од значаја за рад покрајинског фонда за здравствено осигурање као организационе јединице републичког фонда за здравствено осигурање и уређује друга питања од покрајинског значаја у здравству, у складу са законом;

–уређује питања од покрајинског значаја у социјалној заштити породице, деце, омладине и старих, у складу са законом и

–врши друге послове прописане законом који чине њену изворну или поверену надлежност[30].

Аутономна покрајина обезбеђује средства за вршење оснивачких права над здравственим установама чији је оснивач у складу са законом и Планом мреже здравствених установа, а које обухвата закуп пословног простора и опреме, изградњу, одржавање и опремање здравствених установа, односно инвестиционо улагање, инвестиционо одржавање просторија, медицинске, немедицинске опреме, превозних средстава и опреме у области интегрисаног здравственог информационог система, изузев трошкова текућег одржавања објеката и просторија и текућег сервисирања медицинске, немедицинске опреме, превозних средстава и опреме у области

[29] члан 26. Статута Аутономне покрајине Војводине („Службени лист АП Војводине“, број 20/2014)

[30] члан 27 тачка 10. Статута Аутономне покрајине Војводине („Службени лист АП Војводине“, број 20/2014)

интегрисаног здравственог информационог система, као и друге обавезе одређене законом и актом о оснивању[31].

Како су оснивачи здравствених установа Министарство здравља Републике Србије и Покрајински секретаријат за здравство, и у њиховој је надлежности инвестиционо улагање када су у питању информациони системи, и како је Институт за јавно здравље Србије „Батут“ руковалац подацима у Интегрисаном здравственом информационом систему, ревизијом су као субјекти одабрани како би се препоруке могле свеобухватно и системски имплементирати.

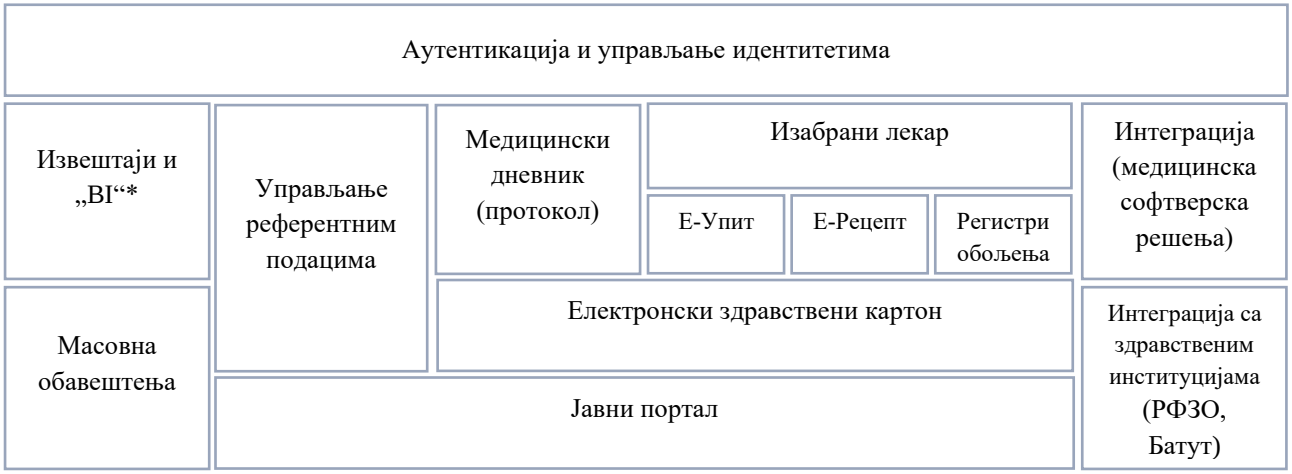
2. Интегрисани здравствени информациони систем

ИЗИС представља централни електронски систем, у коме се чувају и обрађују сви медицински и здравствени подаци пацијената, подаци здравствених радника и сарадника, подаци здравствених установа, здравствене интервенције и услуге извршене у здравственим установама, подаци електронских упута и електронских рецепата, подаци о заказивању за специјалистичке прегледе, дијагностичке процедуре и хируршке интервенције.

Циљ успостављања ИЗИС-а је да обезбеди јединство података у здравству и јединствену информационо-комуникацијску инфраструктуру за управљање збиркама података и пренос података.

Сви поступци у ИЗИС-у извршавају се на два начина:

1. Директно у систему са ауторизованом најавом корисника на порталу ИЗИС-а
2. Коришћењем дефинисаних web сервиса, уколико се користи софтверска апликација трећег произвођача, која је интегрисана са ИЗИС-ом.



*Пословна интелигенција (engl. busines intelligence)

Илустрација 4. *Мапа подсистема укључених у ИЗИС*

У складу са потребама , ИЗИС је пројектован као скуп од више модуларних целина – подсистема, који обезбеђују тражене функционалности и обухватају дефинисане процесе.

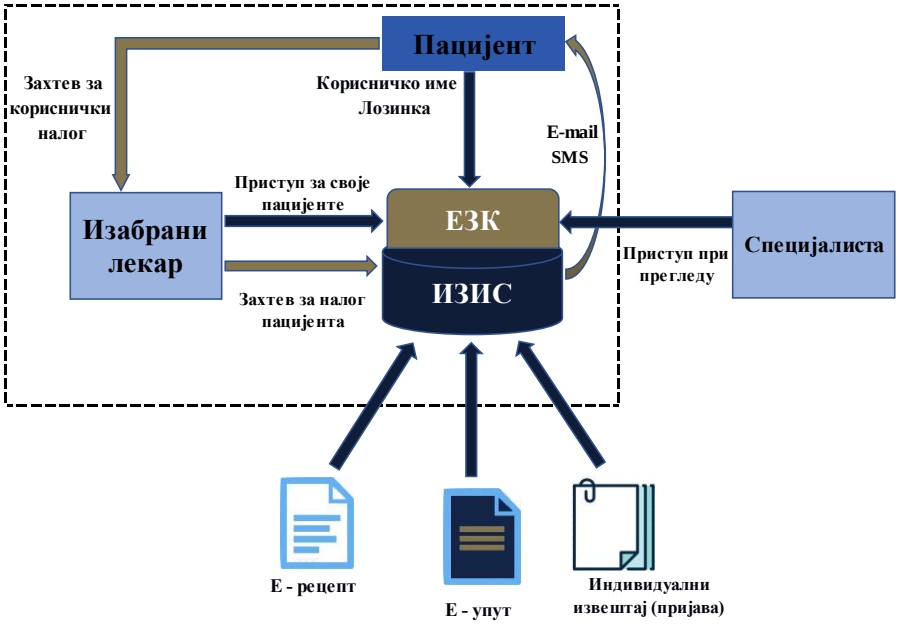
Планирани подсистеми су следећи:

- Подсистем за електронски здравствени картон
- Подсистем за медицински дневник (протокол)
- Подсистем за управљање референтним подацима

[31] члан 12. Закона о здравственој заштити („Службени гласник РС“, број 25/2019)

- Подсистем за активности изабраних лекара
- Подсистем за е - упут
- Подсистем за е - рецепт
- Подсистем за регистрацију лица оболелих од болести већег јавно-здравственог значаја
- Подсистем сервиса за интеграцију са осталим системима
- Подсистем сервиса интеграције са институцијама из области здравства
- Подсистем за извештаје и бизнис интелигенцију
- Подсистем масовног извештавања пацијената и здравствених радника
- Подсистем јавни портал
- Подсистем за управљање идентитетима

Подсистем обезбеђује интерфејс за интеграцију са постојећим локалним ИС који се користе у јавним и приватним здравственим установама.



Илустрација 5. *Функционалности ИЗИС-а*

Подсервиси е – упут и е - рецепт функционишу у оквиру апликације Мој доктор.

Илустрација 6. *Хијерархија одговорности апликације „Мој Доктор“*

Web сервиси су документовани адекватном документацијом која се налази на web порталу за подршку, на који се именовани корисници система пријављују корисничким именом и лозинком (корисници су фирме произвођачи софтвера). Интеграција се изводи имплементацијом web сервиса, разменом XML[32] документа путем HTTPS[33] конекције. Web сервиси могу бити:

1. Јавни (без аутентификације) и
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 последње активности. Саставни део ИЗИС-а је API портал[34] у коме је детаљно описан апликациони програмски интерфејс за интеграцију локалних ИС (који се користе на примарном, секундарном и терцијарном нивоу) са ИЗИС-ом.

Уговор је са Телеком Србија-Медицинска информатика склопљен у новембру 2015. године, док је имплементација иницијалног система ИЗИС завршена крајем фебруара 2016. године, када је почела и обука корисника.

Сарадња са софтверским кућама (у циљу интеграције система) – домаћим произвођачима ИС у здравственом систему Републике Србије започета је јануару 2016. године.

[32] XML је стандардни скуп правила за дефинисање формата података у електронској форми. XML је скраћеница за Extensible Markup Language, односно прошириви (мета) језик за означавање (енгл. markup) текстуалних докумената.
[33] HTTPS (енгл. Hypertext Transfer Protocol Secure) је комбинација Hypertext Transfer Protocol-а са SSL/TSL протоколом да би се обезбедила енкрипција и сигурна идентификација сервера.
[34] веза (обично web место) између добављача API-ја (производи API-ја.

Илустрација 7. *Динамика интеграција система здравствених установа у ИЗИС*

У Институту „Батут“ је тренутно у функцији неколико информационих система (база података) које администрирају запослени у Центру за информатику и биостатистику:

1. Индивидуални извештај о стационарним пацијентима, породиљама и пацијентима на рехабилитацији (извештај о хоспитализацији)

Систем је успостављен 2014. године у циљу формирања јединствене базе података извештаја о хоспитализацији.

2. Индивидуални извештај о умрлима (Потврда о смрти)

Овај систем је успостављен 2006. године у циљу формирања јединствене базе о умрлима за Републику Србију.

3. Индивидуални извештај о рођењима (Пријава рођења)

Систем је успостављен 2006. године у циљу формирања јединствене базе података.

4. Индивидуални извештај о прекидима трудноће (Пријава прекида трудноће)

Систем је успостављен 2006. године у циљу формирања јединствене базе података о побачајима за Републику Србију.

5. Пријава сумње на злостављање и/или занемаривање деце

Овај систем је успостављен 2013. године у циљу формирања јединствене базе података о сумњи на злостављање и занемаривање деце у Републици Србији.

6. Регистар здравствених установа, организационе структуре и кадрова у здравственом систему Републике Србије

Систем је успостављен 2020. године у циљу формирања јединствене базе података о запосленима у здравственом систему Републике Србије.

7. Регистар медицинске опреме од националног значаја

Овај систем је успостављен 2012. године у циљу формирања јединствене базе података о медицинској опреми од националног значаја.

8. Регистар особа оболелих од шећерне болести

Систем је успостављен у циљу формирања јединствене базе података о особама оболелих од шећерне болести.

9. Регистар деце са сметњама у развоју

Овај систем је успостављен у циљу формирања јединствене базе података деце са сметњама у развоју.

10. Информациони систем за формирање база података из збирних извештаја

У току је процес редефинисања методологије прикупљања података из збирних извештаја у папирној форми које достављају институти/заводи за јавно здравље

11. Информациони систем за микробиолошке лабораторије

Овај систем је успостављен 2003. године у циљу формирања базе података за микробиолошке услуге које се врше у Институту Батут.

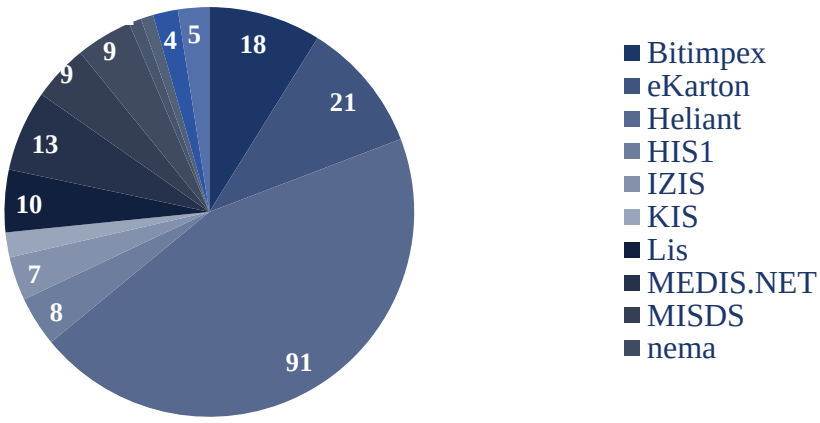
3. Здравствени информациони системи здравствених установа

Здравствене установе обављају здравствену делатност на примарном, секундарном и терцијарном нивоу.

- На примарном нивоу су здравствене установе где грађани могу да оду без упута. Најважнија здравствена установа на примарном нивоу је Дом здравља (158), а у дому здравља се налазе изабрани лекари.
- На секундарном нивоу су болнице (40+37), које пружају амбулантно лечење и/или болничко лечење. Уколико Дом здравља није у могућност да пружи одговарајућу здравствену заштиту, изабрани лекар упућује пацијенте на секундарни ниво.
- На терцијарном нивоу су Клинички центри (4), Клинике (6), Институти (16) и Клиничко-болнички центри (4). Када здравствени проблем пацијента превазилази техничке услове болнице, или је потребно стручно мишљење највишег нивоа здравствене заштите, пацијент се упућује на терцијарни ниво.

Све здравствене установе поред обавезног ИЗИС-а имају ИС које су набавили преко јавних набавки.

Најзаступљенији ИС-и у самим здравственим установама су: Heliant, BitImpeks, eKarton, Medis.Net i HIS- болнички информациони систем.



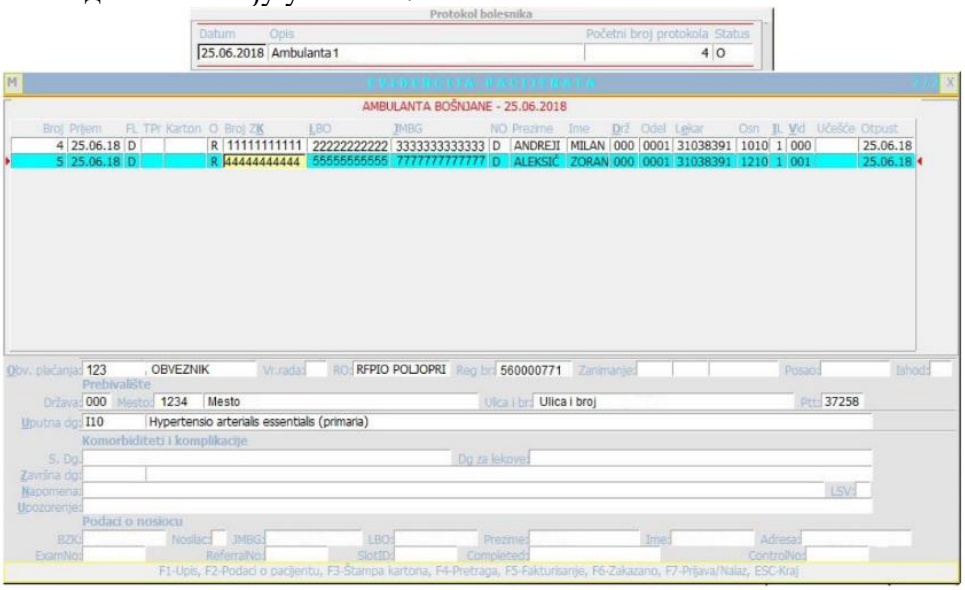
Илустрација 8. *Заступљеност ИТ система у здравственим установама*

Илустрација 9. *Апликација Heliant*

Heliant је ИС који подржава интеракције између пацијената и здравствених установа, унутар саме здравствене установе, и између здравствене установе и РФЗО.

Основне карактеристике:

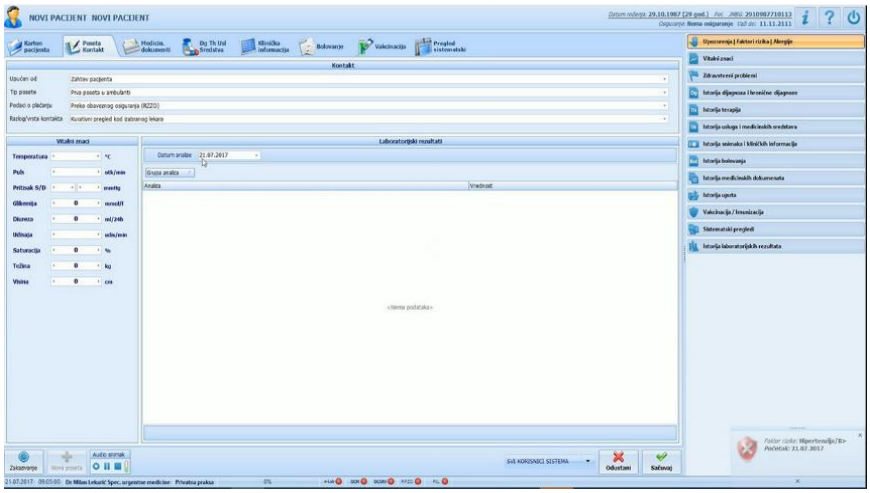
- Вишеслојна архитектура са централизованом базом података;
- Може се имплементирати у свим здравственим установама независно од степена здравствене заштите;
- Размена података између установа.



Илустрација 10. *Апликација NextZUS - BitImpeks*

BitImpeks (NextZUS) је ИС софтвер пројектован да подржава послове пријема и отпуста болесника на стационарно и амбулантно лечење, и да омогући да се:

- Подаци уносе само једном и то на месту њиховог првог појављивања и у тренутку кад се радни процеси одвијају;
- Подаци буду одмах доступни за даљу обраду свим овлашћеним лицима која их користе, као и самом стручном особљу за различите врсте стручних извештаја и анализа.

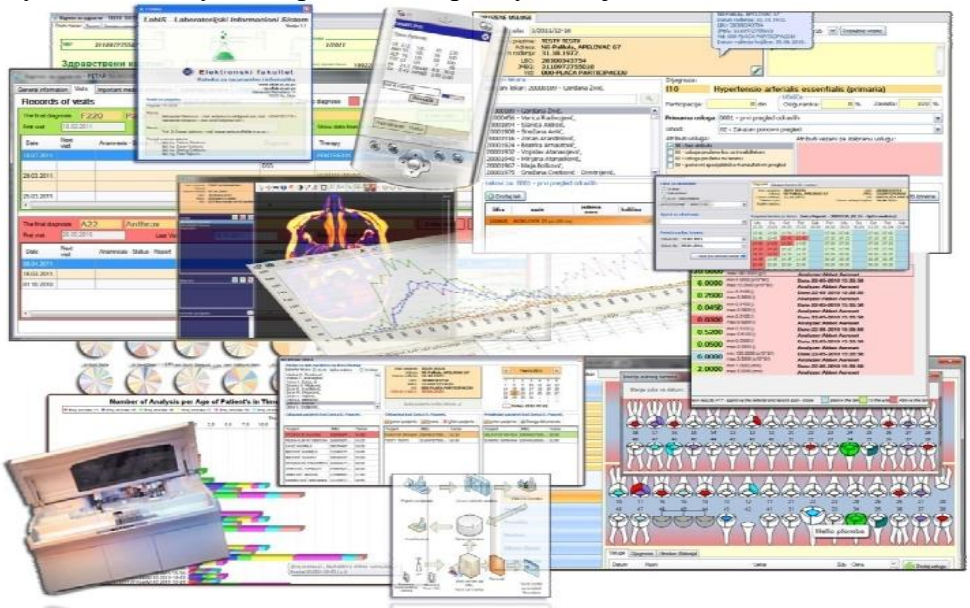


Илустрација 11. *еКартон- ZIPSoft*

еКартон је ЗИС који омогућава креирање картона пацијента, заказивање и евидентирање посете пацијента лекару издавање упута и других медицинских докумената.

Основне карактеристике:

- Штампа рецепата;
- Попуњавање и штампање свих медицинских докумената;
- Евиденције боловања;
- Преглед медицинских снимака са ултразвука, рендгена;
- Чување истих у електронском картону пацијента.

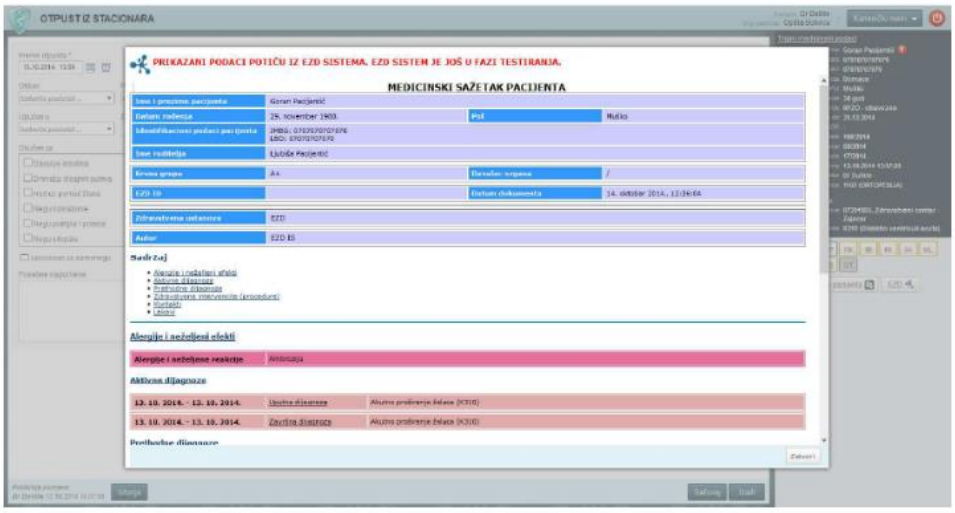


Илустрација 12. *Medis.NET*

Medis.NET је информативни систем за здравствену заштиту дизајниран да омогући следеће процесе:

- Интеграција свих одељења;
- Подаци се убацују само једном и постају доступни свуда;
- Једноставност - Medis.NET прати свакодневну рутину у рад хитне помоћи;
- Прилагођавање - систем се прилагођава у зависности од тога пријављени корисник или изабрани пацијент;
- Краткорочни рок за обуку особља;

- Извештавање на више нивоа.



Илустрација 13. *HIS- Comtrade*

HIS (енгл. Hospital Information System) је болнички ИС тако да пружа скуп елемената који омогућавају унапређење радног процеса на великој већини радних места здравствених радника и омогућава да корисници добију функционалну целину која ће подићи квалитет пословања болница на виши ниво.

Основне карактеристике:

- Лако се прати потрошња лекова и материјала;
- Смањује се обим документације која се води на папиру и задржава се само оно што је прописано законом;
- Скраћује се време прикупљања информација потребних за доношење важних одлука;
- Скраћује се време које здравствени радници троше на административне послове, што им омогућава да више времена посвете стручном медицинском раду.

IV Закључци

У овом поглављу износимо закључке до којих смо дошли спроводећи ревизију сврсисходности на тему Информациона безбедност у здравственим информационим системима, код три субјекта ревизије:

1. Министарство здравља, Београд
2. Институт за јавно здравље Србије „Др Милан Јовановић Батут“, Београд и
3. Покрајински секретаријат за здравство Војводине, Нови Сад.

Донети закључци представљају одговоре на постављена ревизијска питања, дефинисана у делу извештаја II Увод – 2. Циљ ревизије. Закључци су донети на основу утврђених налаза – сваки закључак је изведен на основу припадајућих налаза.

ЗАКЉУЧАК 1: Постојећи системи ИТ управљања у здравству нису у потпуности омогућили испуњење пословних циљева, тачније пуну имплементацију Интегрисаног здравственог информационог система, процену ИТ ризика и успостављање адекватне организационе ИТ структуре

Ревизорски тимови Државне ревизорске институције који су у претходним годинама радили ревизије финансијских извештаја и правилности пословања здравствених установа уочили су проблеме који постоје у функционисању здравствених информационих система, а који су се између осталог огледали у застарелој опреми и софтверу, а услед недостатка планирања адекватног буџета за ИТ системе. Старе верзије оперативних система које се више не ажурирају од стране произвођача представљају својеврстан безбедносни ризик када су у питању могући хакерски напади, што за последицу може, у најгорем случају имати губитак или крађу осетљивих података пацијената-осигураника.

Такође, у једном броју здравствених установа, примећено је да опис послова и одговорности запослених, када су у питању управљање, развој и одржавање ИС, није у складу са природом, обимом и сложеношћу пословања.

Иако је то и законска обавеза, у једном броју здравствених установа установљено је да не постоје усвојена правила и процедуре које се односе на ИТ послове, а такође не постоји ни управљање ИТ ризицима.

Имајући у виду све ове уочене проблеме, неправилности и ризике, у овој ревизији између осталог наш циљ је био да у оквиру првог ревизорског питања утврдимо у којој мери су успостављени системи управљања здравственим информационим системима омогућили испуњење пословних циљева, успостављање јасно дефинисане организационе структуре и управљање ризицима.

Како би одговорили на ово питање, разматрали смо да ли су усвојена стратешка документа у овој области, као и да ли је обезбеђено стабилно финансирање одржавања и развоја информационих система у складу са стратешким документима. Анализирали смо и да ли су усвојена и да ли се примењују правила и процедуре у вези управљања ИТ операцијама, као и да ли је организациона ИТ структура успостављена на начин да је омогућена подела дужности и одговорности, као и испуњење законских обавеза. Разматрали смо и да ли је успостављено управљање ИТ ризицима, што подразумева њихову идентификацију и доношење и спровођење плана за умањење ових ризика.

Наш закључак заснивамо на следећим налазима:

Налаз 1.1: Не постоји стратешко планирање развоја и одржавања Интегрисаног здравственог информационог система, иако је то и законска обавеза Владе Републике Србије, што је довело до неправовременог и несвеобухватног развоја и одржавања здравствених информационих система

Циљ је био да испитамо да ли су донета и да ли се примењују стратешка документа која се односе на ИЗИС. Законом о здравственој документацији и евиденцијама у области здравства[35] прописано је да ИЗИС чине здравствено-статистички систем, информациони систем организација здравственог осигурања и информациони системи здравствених установа, приватне праксе и других правних лица.

Дакле, стратешко планирање обухвата планирање на републичком нивоу и планирање на нивоу сваке здравствене установе, с обзиром да установе набављају и користе здравствене информационе системе за обављање послова из свог делокруга, а који се разликују по модулима, функционалностима, броју корисника, итд.

Зашто је за информациони систем важно стратешко планирање?

ИТ стратегија је у основи документ који се усваја на највишем нивоу (републичком нивоу, покрајинском нивоу, нивоу јавног предузећа, нивоу установе итд.)

Усвајању ИТ стратегије претходе кораци који обухватају:

– анализу тренутног стања (инфраструктуре, опреме, софтвера, кадрова итд.),

– анализу проблема који су се јављали у току употребе тренутног информационог система

– анализу законских и подзаконских аката који се односе на ИТ системе а који су ступили на снагу након доношења претходне стратегије

– пословне циљеве (који могу обухватати како опште циљеве тако и пословне циљеве до којих се долази анализом захтева тзв. „stakeholder“- а, тј. свих корисника – заинтересованих страна информационих система),

– успостављање приоритета и

– израда предлога стратегије.

Недостатак ИТ стратегије (или неадекватна, застарела стратегија) или недостатак ИТ планирања доводи до ограничења у нормалном функционисању и развоју ИТ система, њихове неусаглашености са важним пословним процесима, недостатака ИТ ресурса или неефикасног коришћења постојећих ресурса (хардвер, софтвер и стручно особље које је или треба бити ангажовано, добро обучено, добро организовано и мотивисано за ефикасан и квалитетан рад).

Шта је у ревизији установљено?

СТРАТЕШКО ПЛАНИРАЊЕ НА РЕПУБЛИЧКОМ НИВОУ

Законом о здравственој заштити прописано је да Стратегију развоја и организације интегрисаног здравственог информационог система, доноси Влада.

[35] „Службени гласник РС“, бр. 123/14, 106/15, 105/17 и 25/19 - др. закон - члан 44, став 2

Влада Републике Србије није донела Стратегију развоја и организације Интегрисаног здравственог информационог система.

Неки од циљева употребе информационих система у здравству дефинисани су Стратегијом развоја информационог друштва у Републици Србији до 2020. године[36]:

Примена ИКТ у систему здравствене заштите

Основна улога информационих и комуникационих технологија у систему здравствене заштите је подршка извођењу делатности система здравствене заштите. Здравствени информациони систем такође треба да обезбеди подршку реформе система здравствене заштите.

Принципи које примена информационо-комуникационих технологија у здравству мора да задовољи јесу:

– очување приватности и поверљивости личних здравствених података;
– ефикасност и употребљивост здравственог информационог система;
– промоција оптималне употребе здравствених података;
– висок квалитет здравствених информација.

Употребом информационих и комуникационих технологија у здравству требало би омогућити неометано и квалитетно функционисање свих делова система здравствене заштите кроз:

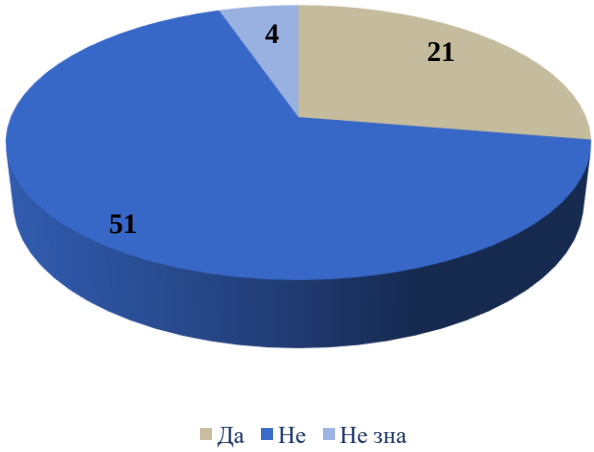
– аутоматизацију и смањење трошкова свих административних поступака и процеса који прате основне делатности система здравствене заштите;
– благовремен прихват података и подршку могућим изменама и проширењима делатности;
– сигурну и ефикасну размену информација између свих учесника здравственог система у циљу подизања доступности и квалитета здравствене заштите;
– е-Здравље - ИКТ у служби активног учешћа грађана у бризи о сопственом здрављу, пре свега у смислу потпуне информисаности и одређене слободе избора, степена одлучивања и утицаја на сопствени третман, као и учешћа у превенцији;
– формирање електронске базе знања здравственог сектора;
– размену информација од значаја за обављање научно истраживачке делатности, као и обављање перманентног образовања медицинског особља;
– здравствене информације које ће да помогну здравственим радницима у доношењу клиничких одлука, укључујући и водиче добре праксе, базе знања и стручну литературу;
– употребу података у циљу подршке функцијама јавног здравља, планирању, надгледању и оцени здравствених услуга, укључујући управљање и планирање кадровима, финансирању и алокацији ресурса, праћењу квалитета здравствених услуга, и праћењу рационалног трошења средстава;
– употребу података у циљу подршке развоју и примени одлука у циљу свеобухватне здравствене заштите појединаца, група са посебним потребама и целе популације;
– употребу података у циљу помоћи здравственим истраживањима;
– информације о стању здравља и здравственим детерминантама, заснованим на доказима и
– лакше испуњавање међународних обавеза кроз усвајање европских стандарда и иницијатива.

[36] „Службени гласник РС“, број 51/2010

Развој примене ИКТ у систему здравствене заштите уређен је и Уредбом о Програму рада, развоја и организацији интегрисаног здравственог информационог система "е-Здравље"[37] .

СТРАТЕШКО ПЛАНИРАЊЕ НА НИВОУ ЗДРАВСТВЕНЕ УСТАНОВЕ

У току спровођења ревизије, прикупили смо податке од здравствених установа који се односе на стратешко планирање у вези информационих система. Од укупног броја анкетираних здравствених установа, прикупили смо одговоре од њих 76. Од тог броја, стратешки документ који се односи на ИТ системе је донела 21 здравствена установа. Међутим, само 12 здравствених установа је доставило тражени документ.



Илустрација 14. *Да ли здравствене установе имају стратешки план*

Анализом достављених докумената, утврдили смо:

- Један документ нема податке ко је и када усвојио тај документ, нити је оверен потписом и печатом.
- Три документа се уопште не баве питањима везаним за ИТ, ради се наиме о стратешким документима који уређују друга питања.
- Седам стратешких докумената који се односе на садашњи период коришћења ИТ система (дакле углавном су у питању четворогодишњи или петогодишњи периоди од најраније 2015-те до 2024-те године) обухватају углавном средњорочне циљеве који се најчешће односе на набавку опреме, и у појединим случајевима, у кратким цртама неко софтверско решење. Нису дефинисана питања која смо обухватили овом ревизијом.
- У једном случају достављени стратешки документ (не односи се само на ИТ већ на све циљеве) садржи елементе који су приказани у „SWOT„ анализи (наведене су предности, слабости, могућности, претње), наведени су стратешки циљеви / приоритети, и тај документ је праћен одговарајућим оперативним планом. У том плану као два циља се наводе:
  1. Унапређење и кастомизација постојећег информационог система и
  2. Примена мера информационе безбедности кроз имплементацију Правилника о ИТ безбедности.

[37] „Службени гласник РС“, број 55/2009

Како показује анкета, велики број здравствених установа уопште нема стратешко ИТ планирање (72% анкетираних), а код оног малог броја установа које има неки стратешки документ у овој области, показало се да су те стратегије или планови непотпуни, и као такви неупотребљиви када се гледа развој целокупног информационог система, са свим компонентама.

Дакле, може се закључити да није препозната важност стратешког планирања информационих система у здравству, што већ за последицу између осталог има нередовну и недовољну замену застарелих рачунара, сервера, оперативних система итд. Такође, сва остала питања која су анализирана у извештају и наведени проблеми су углавном последица неблаговременог и несвеобухватног планирања када су у питању ИТ системи.

Шта су последице, или шта могу бити последице?

Најпре застарела опрема, било да је реч о серверским рачунарима, или рачунарима које користе корисници система. Процес замене опреме треба да подразумева планирање колико се и којих рачунара годишње мења. Застарели рачунари су небезбедни, пре свега због немогућности покретања нових верзија оперативних система код којих постоји неопходан ниво безбедности размене података. Упозоравајуће звуче подаци да се још увек користе рачунари са Windows XP системима, сервери старији од 10 година, непостојање резервних рачунара и сервера. Треба имати у виду и престанак развоја Windows 7 система, што посебно брине имајући у виду безбедносне „закрпе“ система које се више не ажурирају.

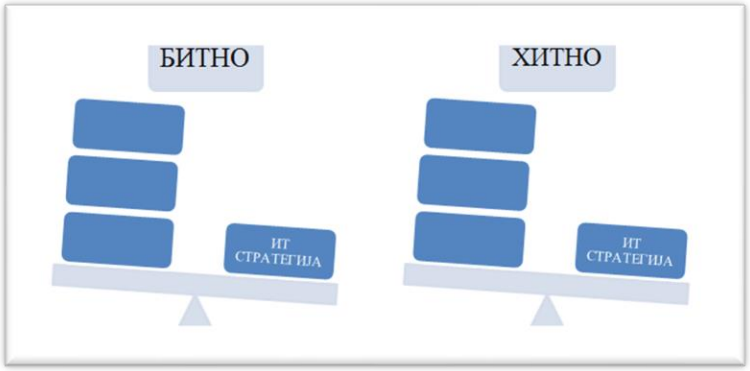
Непотребни увећани трошкови набавке и развоја апликативног софтвера, јер се у пракси дешавало да се са једног концепта ЗИС-а прешло на други, или са једног модула на други. Такође, у ревизији су представници Министарства здравља истакли да је план да се сви здравствени системи које користе установе виртуелизују, што је потпуно другачије решење у односу на садашње клијент-сервер решење. Тако се може десити да неке установе набаве нове сервере и да се за то потроше значајна средства, а на се након тога испоставо да им ти сервери неће бити потребни.

Немогућност свеобухватног дефинисања најважнијих функционалности система, дефинисања које треба да укључи више „заинтересованих“ страна, који се иначе не консултују када се набавља софтвер, тако да је израда стратегије идеална прилика да се чују њихови ставови и разлози како нешто треба решити. У непосредној прошлости смо били сведоци ад хок израде појединих апликативних решења, од којих се брзо одустајало и прелазило на развој другачијих решења са истим циљем.

Отежана израда финансијских планова је логична последица недостатка стратешког планирања. Немогуће је планирати средства без анализе колико новца и за које потребе треба.

Неадекватна ИТ структура – на оба нивоа, и на централном и на нивоу установе. И то и када је у питању број запослених на овим пословима, и њихов стручни ниво знања. Јер, када се не зна како ће се системи развијати, не може се знати ни колико запослених треба, нити шта од стручног знања они треба да поседују. То отежава и планирање одговарајућих обука. У току ревизије је установљено да обуке тако рећи не постоје, што утиче и на ниво мотивисаности ИТ кадра, области која се убедљиво најбрже развија и за коју је неопходно константно усавршавање.

Другим речима, успостављање ИТ стратешког планирања је хитно и битно.



Илустрација 15. *Битност ИТ стратешког планирања*

Препоручујемо Министарству здравља да предузме активности у смислу припреме предлога Стратегије развоја и организације интегрисаног здравственог информационог система и Акционог плана за примену, које ће између осталог обухватити и прибављање мишљења Института за јавно здравље Републике Србије „Др Милан Јовановић Батут“ и других организација и установа у области здравства, и иницира усвајање Стратегије и Акционог плана за њену примену.

Налаз 1.2: Министарство здравља, Покрајински секретаријат за здравство Војводине и здравствене установе, због непостојања стратешког планирања, нису обезбедиле стабилно финансирање здравствених информационих система самим тим ни развој и одржавање тих система, што за последицу има застареле рачунаре и сервере, застареле па самим тим и небезбедне оперативне системе, непостојање обука за запослене и недовољан број ИТ стручњака

Зашто је неопходно стабилно, континуирано финансирање информационих система?

Законом о здравственој документацији и евиденцијама у области здравства, у члану 4, став 1. тачка 10. прописано је да је „Информациони систем“ свеобухватни скуп технолошке инфраструктуре (мрежне, софтверске и хардверске компоненте), организације, људи и поступака за прикупљање, смештање, обраду, чување, пренос, приказивање и коришћење података и информација.

Дакле, финансирање једног информационог система, у најширем смислу, обухвата набавку и одржавање хардвера (рачунара, сервера, штампача, мрежне опреме и других уређаја), набавку и развој софтвера (најчешће набавку оперативних система, док се у случају апликативног софтвера ради и о набавци, али и о набавци и развоју софтвера, када су у питању специфични послови), одржавање база података и чување резервних копија, људске ресурсе, и у неким случајевима израду одговарајућих правних аката којима се рад тог система уређује.

За неке делове ИС неопходно је издвојити одговарајућа средства, на пример када је у питању куповина сервера, рачунара, штампача (хардвер), или куповина оперативних система, или апликативног софтвера (софтвер) итд.

Не постоје прописи који дефинишу када је, тачније након ког временског периода коришћења потребна замена рачунара новим.

Правилником о номенклатури нематеријалних улагања[38], годишња стопа амортизације за ставку „Електронски рачунари и остала опрема за обраду података“

[38] „Службени лист СРЈ“, бр. 17/97 и 24/2000

износи 20%. То практично значи да је књиговодствена вредност рачунара после 5 година коришћења 0 динара. Другачије речено, сматра се да су рачунари након 5 година 100% амортизовани.

Век употребе рачунара је обрнуто пропорционалан његовој поузданости и то и у хардверском и у софтверском смислу и то треба имати у виду приликом планирања средстава за набавку новог хардвера.

У зависности од капацитета субјекта, код неких делова система је могуће остварити неку уштеду – поправка рачунара, израда апликације, резервних копија, правних аката итд. Исто важи и када је у питању обука запослених на ИТ пословима и стручно усавршавање. У ретким случајевима је могуће организовати интерну обуку за неке послове (када постоје запослени који могу и знају да спроведу обуку, и када има ко да похађа обуку – у случајевима када је број запослених на ИТ пословима 1-2, то је немогуће).

У овој ревизији је анализирано финансирање ИЗИС-а (како је то између осталог прописано у Закону о здравственој документацији и евиденцијама у области здравства, у члану 44, став 2. да Интегрисани здравствени информациони систем Републике Србије из става 1. овог члана чине: здравствено-статистички систем, информациони систем организација здравственог осигурања и информациони системи здравствених установа, приватне праксе и других правних лица.) и на централном нивоу, дакле на нивоу оснивача здравствених установа, и истовремено субјеката ревизије у овом случају, и на нивоу здравствених установа.

Шта је у ревизији установљено?

ФИНАНСИРАЊЕ ИЗИС-А - РЕПУБЛИЧКИ НИВО (МИНИСТАРСТВО ЗДРАВЉА И ПОКРАЈИНСКИ СЕКРЕТАРИЈАТ)

Обавеза Министарства да финансира здравствене установе када је у питању развој ИЗИС-а, прописана је чланом 17. став 1. тачка 24. Закона о здравственој заштити:

Општи интерес у здравственој заштити у Републици Србији обухвата и изградњу и опремање здравствених установа у државној својини чији је оснивач Република, које обухвата: инвестиционо улагање, инвестиционо - текуће одржавање просторија, медицинске и немедицинске опреме и превозних средстава, односно врши набавку медицинске и друге опреме неопходне за рад здравствених установа и превозних средстава, обезбеђивање средстава, односно набавку опреме за развој интегрисаног здравственог информационог система, као и обезбеђивање средстава за друге обавезе одређене законом и актом о оснивању.

Такође, када је у питању Покрајински секретаријат, обавеза инвестиционог финансирања здравствених установа чији је оснивач Аутономна Покрајина Војводина је прописана истим законом:

Аутономна покрајина обезбеђује средства за вршење оснивачких права над здравственим установама чији је оснивач у складу са законом и Планом мреже здравствених установа, а које обухвата закуп пословног простора и опреме, изградњу, одржавање и опремање здравствених установа, односно инвестиционо улагање, инвестиционо одржавање просторија, медицинске, немедицинске опреме, превозних средстава и опреме у области интегрисаног здравственог информационог система, изузев трошкова текућег одржавања објеката и просторија и текућег сервисирања медицинске, немедицинске опреме, превозних средстава и опреме у области

интегрисаног здравственог информационог система, као и друге обавезе одређене законом и актом о оснивању[39].

Планирана средстава за Министарство здравља за пројекте „Информатизација здравственог система у јединствени информациони систем“ и „Други пројекат развоја здравства за посматрани период била је:

Планирана средства су приказана у табели

у динарима

Раздео	Програмска активност/ Пројекат	Економска класификација	ОПИС	Укупна средства	Година
25	4001		**Информатизација здравственог система у јединствени информациони систем**	**360.000.000**	2017
25		423	Услуге по уговору	50.000.000	2017
25		512	Машине и опрема	30.000.000	2017
25		515	Нематеријална имовина	280.000.000	2017
25	4007		**Развој здравства 2**	**138.000.000**	2017
25		413	Накнаде у натури	150.000	2017
25		415	Накнаде трошкова за запослене	900.000	2017
25		421	Стални трошкови	1.800.000	2017
25		422	Трошкови путовања	1.700.000	2017
25		423	Услуге по уговору	102.600.000	2017
25		425	Текуће поправке и одржавање	2.000.000	2017
25		426	Материјал	2.400.000	2017
25		465	Остале дотације и трансфери	1.300.000	2017
25		482	Порези, обавезне таксе и казне и пенали	150.000	2017
25		511	Зграде и грађевински објекти	12.000.000	2017
25		512	Машине и опрема	12.000.000	2017
25		515	Нематеријална имовина	1.000.000	2017
27	4001		**Информатизација здравственог система у јединствени информациони систем**	**600.000.000**	2018
27		423	Услуге по уговору	214.000.000	2018
27		512	Машине и опрема	60.000.000	2018
27		515	Нематеријална имовина	326.000.000	2018
27	4007		**Развој здравства 2**	**976.910.000**	2018
27		413	Накнаде у натури	150.000	2018
27		415	Накнаде трошкова за запослене	900.000	2018
27		421	Стални трошкови	3.900.000	2018
27		422	Трошкови путовања	11.200.000	2018
27		423	Услуге по уговору	230.000.000	2018
27		425	Текуће поправке и одржавање	2.500.000	2018
27		426	Материјал	21.575.000	2018
27		465	Остале дотације и трансфери	68.700.000	2018
27		482	Порези, обавезне таксе, казне, пенали и камате	150.000	2018
27		511	Зграде и грађевински објекти	106.875.000	2018
27		512	Машине и опрема	447.460.000	2018
27		515	Нематеријална имовина	83.500.000	2018

[39] члан 12. Закона о здравственој заштити („Службени гласник РС“, број 25/2019)

у динарима

Раздео	Програмска активност/ Пројекат	Економска класификација	ОПИС	Укупна средства	Година
27	4001		**Информатизација здравственог система у јединствени информациони систем**	**710.000.000**	2019
27		423	Услуге по уговору	185.369.000	2019
27		512	Машине и опрема	34.631.000	2019
27		515	Нематеријална имовина	490.000.000	2019
27	4007		**Развој здравства 2**	**332.550.000**	2019
27		413	Накнаде у натури	150.000	2019
27		415	Накнаде трошкова за запослене	200.000	2019
27		421	Стални трошкови	2.300.000	2019
27		422	Трошкови путовања	5.100.000	2019
27		423	Услуге по уговору	256.800.000	2019
27		425	Текуће поправке и одржавање	1.250.000	2019
27		426	Материјал	4.100.000	2019
27		444	Пратећи трошкови задуживања	500.000	2019
27		465	Остале дотације и трансфери	51.000.000	2019
27		482	Порези, обавезне таксе, казне, пенали и камате	150.000	2019
27		512	Машине и опрема	10.000.000	2019
27		515	Нематеријална имовина	1.000.000	2019
27	4009		**Развој здравства 2 - додатно финансирање**	**612.310.000**	2019
27		415	Накнаде трошкова за запослене	50.000	2019
27		421	Стални трошкови	600.000	2019
27		422	Трошкови путовања	2.110.000	2019
27		423	Услуге по уговору	51.100.000	2019
27		425	Текуће поправке и одржавање	250.000	2019
27		426	Материјал	1.350.000	2019
27		444	Пратећи трошкови задуживања	300.000	2019
27		482	Порези, обавезне таксе, казне, пенали и камате	150.000	2019
27		511	Зграде и грађевински објекти	69.100.000	2019
27		512	Машине и опрема	479.300.000	2019
27		515	Нематеријална имовина	8.000.000	2019
			УКУПНО ЗА ОБА ПРОЈЕКТА 2017-2019. ГОДИНЕ	**3.729.770.000**	

Илустрација 16. *Планирана средства за период 2017. – 2019. године*

У посматраном трогодишњем периоду, за машине и опрему планирано је укупно 124.631 хиљаду динара, за потребе информатизације здравственог система у јединствени информациони систем.

У склопу пројекта „Други пројекат развоја здравства Србије“, за машине и опрему је планирано 948.760 хиљада динара. Пројекат се састоји из четири компоненте, и ни у једној није експлицитно предвиђено издвајање средстава за набавку рачунарске опреме.

Министарство здравља је у 2019. години и 2020. години, за здравствене установе набавило рачунарску опрему и то: укупно 295 радних станица, са оперативним

системом Windows 10 Professional, као и 295 монитора, тастатура и мишева. Структура набављене опреме је следећа:

Редни број	Здравствена установа за коју је извршена набавка	Година у којој је набављена опрема		Број*
		2019	2020	
1	Домови здравља	51	135	186
2	Здравствени центри	90		90
3	Клиничко болнички центар	19		19
4	**Укупно**	**160**	**135**	**295**

* свака јединица набављене опреме обухвата једну радну станицу, оперативни систем Windows 10 Professional, монитор, тастатуру и миш.

Илустрација 17. *Рачунарска опрема коју је за здравствене установе набавило Министарство здравља у 2019. и 2020. године*

Сву опрему набављену у 2019. години, Министарство је доделило здравственим установама на Косову и Метохији.

У периоду обухваћеним ревизијом, Институт „Батут“ није добио финансијска средства за набавку нове рачунарске опреме, или занављање постојеће.

ФИНАНСИРАЊЕ ИЗИС-А – ЗДРАВСТВЕНЕ УСТАНОВЕ

Здравствене установе из сопствених средстава финансирају здравствене информационе системе када је у питању текуће одржавање, али део средстава се издваја и за инвестиционо улагање, које је апсолутно недовољно имајући у виду број рачунара и корисника система, али и остале компоненте хардверског дела, нарочито серверских рачунара.

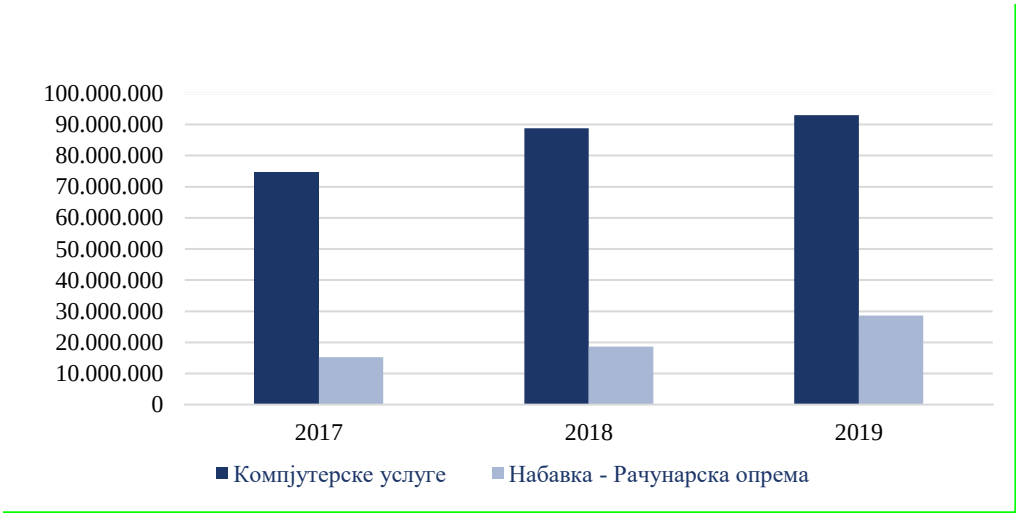
Анализом прикупљених података у току ревизије, утврђено је да у просеку, за набавку рачунара се из сопствених прихода здравствених установа издваја између 20 и 30 процената, преостали део буџета за ИТ обухвата плаћање компјутерских услуга и текућег одржавања.

У посматраном периоду ревизије, збирни подаци за анкетиране здравствене установе које су доставиле податке (33), су приказани табеларно и графички.

у динарима

Редни број	Година	Компјутерске услуге	Текуће поправке и одржавање опреме	Набавка - Рачунарска опрема
1	2017	74.695.055	6.093.097	15.292.398
2	2018	88.782.355	10.395.568	18.648.520
3	2019	92.993.297	11.769.076	28.582.651

Илустрација 18. *Финансирање ИЗИС-а од стране здравствених установа*



Илустрација 19. *Однос улагања у рачунарску опрему и давања за компјутерске услуге*

Када је у питању број корисника система у посматраним здравственим установама, он износи 13.690, односно у просеку 428 по здравственој установи.

У посматраном периоду, за набавку рачунарске опреме ове 33 здравствене установе су укупно издвојиле 62.523.569 динара, односно у просеку, једна здравствена установа у току једне године 631.552 динара.

Укупно су ове здравствене установе, за све три године, издвојиле за компјутерске услуге 256.470.706 динара, односно просечно једна установа за једну годину 2.590.613 динара издваја за компјутерске услуге.

За текуће поправке и одржавање опреме, анкетиране установе су за посматрани период од 3 године издвојиле 28.257.741 динара. Просечно, једна здравствена установа за једну годину је издвојила 285.432 динара.

Шта су последице, или шта могу бити последице?

Као што показује анализа, није успостављено стабилно финансирање ИЗИС-а. У највећем делу се то односи на рачунаре и опрему, и то ствара ризик да у случају кварова неће функционисати сви делови система, ово се нарочито односи на сервере на којима је покренут апликативни софтвер. Што се тиче Storage[40] сервера, ризик у случају квара ових уређаја је мањи него у претходном случају, из разлога што се израђују и чувају резервне копије података.

Када су у питању здравствени информациони системи, здравствене установе плаћају услугу коришћења и одржавања овог софтвера из сопствених прихода, што представља највећи део укупних средстава која се издвајају за ИТ. Преостали део новца се издваја за набавку рачунара и опреме, иако је то недовољан износ и у појединим случајевима за израду процедура за управљање ИТ.

Из наведених података се може закључити да једна здравствена установа у просеку годишње може набавити 10-12 нових рачунара, под условом да се у току те године не набавља ништа друго од рачунарске опреме (штампачи, мрежни уређаји и слично). То је главни разлог зашто су рачунари (и остала опрема, оперативни системи итд) у једној мери застарели и као такви представљају ризик за функционисање система – делимично или у целини.

[40] Сервер који се користи за складиштење података

Због обавеза да финансирају софтвер, рачунаре и опрему, јавља се проблем недостатка средстава, којим би здравствене установе финансирале стручно усавршавање ИТ кадра, што ствара ризик да запослени неће имати довољно знања у будућности да управљају новим оперативним системима и новим софтвером.

На крају, а не мање важно, недостатак средстава у неким установама доводи до тога да се не набавља неопходан антивирусни софтвер, већ се користе рањивије, бесплатне верзије, па су самим тим већи и безбедносни ризици.

Имајући у виду да је дигитализација један од приоритета Владе Републике Србије, као и област здравства, усвајањем Стратегије којој ће претходити одговарајуће анализе, створили би се услови да се сва ова питања и проблеми везани за финансирање системски уреде.

Препоручујемо Министарству здравља и Покрајинском секретаријату да приликом припреме финансијских планова осигура стабилно финансирање циљева из Акционог плана за примену Стратегије кроз детаљно планирање средстава за развој, набавку и одржавање информационих система у области здравства.

Налаз 1.3: Министарство здравља, Институт за јавно здравље Србије „Др Милан Јовановић Батут“ и здравствене установе нису усвојиле процедуре за управљање ИТ пословима, иако су то и законски били у обавези, што онемогућава или отежава контролу ових послова од стране руководства или континуитет обављања послова у случају замене запослених на ИТ пословима

Зашто су важне процедуре за ИТ послове?

Процедуре детаљно уређују обављање ИТ послова, што са једне стране пружа могућност за контролу квалитета рада на тим пословима, а са друге стране омогућава да у случајевима кадровских промена, новозапослена лица могу веома брзо и лако наставити са свим пословима, што би у случају да процедура нема било скоро немогуће, или немогуће у неком краћем временском периоду.

Зато је неопходно да процедуре буду довољно детаљне, да поред описа процеса садрже и податке ко ради на којој активности (не у смислу имена него у смислу одређеног радног места).

Мере заштите ИКТ система се односе између осталог на: успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система; обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност; заштиту од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система; идентификовање информационих добара и одређивање одговорности за њихову заштиту; класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком.[41]

Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја је дефинисано успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система од посебног значаја.

У том смислу, успостављају се неке од следећих процедура:

- Процедура развоја и одржавања ИС;
- Процедура за ажурирање информационог система;

[41] Члан 7 Закон о информационој безбедности („Службени гласник РС“, бр. 6/2016 и 94/2017)

– Процедура за пријављивање и отклањање застоја у раду информационог система
– Процедура о инсталацији и конфигурацији система
– Процедура о коришћењу мобилних уређаја;
– Процедура за поступање, обраду, складиштење и пренос података
– Процедура за администрирање Web сајта.

Процедуре које на адекватан начин уређују неки процес садрже следеће елементе:
– Дефиниција саме процедуре;
– Предмет процедуре - утврђује активности, носиоце активности;
– Подручје примене – где се примењује;
– Одговорност - одговорна лица;
– Опис поступка;
– Референтни документи – процедура је у вези са документима,
– Правни основ;
– Дијаграм тока – пожељно је да има дијаграм тока.

Шта је у ревизији установљено?

ИНСТИТУТ „БАТУТ“ И МИНИСТАРСТВО ЗДРАВЉА

Институт „Батут“ је 1. августа 2017. године усвојио Правилник о безбедности информационо-комуникационог система Института за јавно здравље Србије „др. Милан Јовановић Батут“, који обухвата области дефинисане наведеном Уредбом.

Међутим, Институт „Батут“ није успоставио и процедуре у складу са наведеном Уредбом (чланом 2. наведене уредбе је дефинисано да Оператор ИКТ система успоставља процедуре ради праћења активности, ревизије и надзора у оквиру управљања информационом безбедношћу).

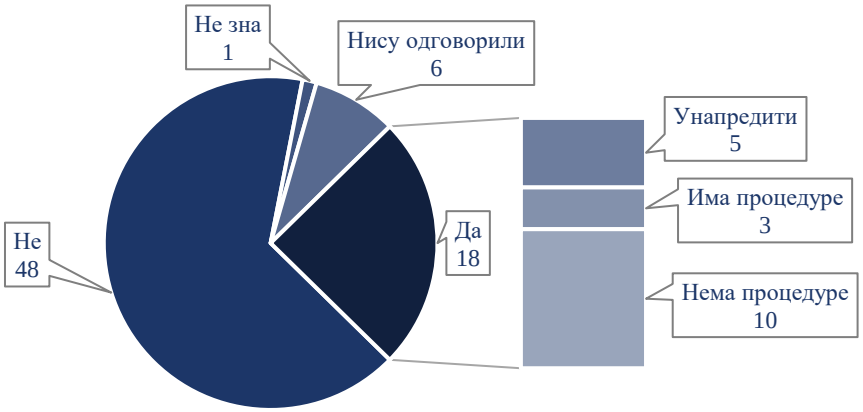
Министарство здравља није усвојило акт о безбедности ИКТ система, и није успоставило процедуре у складу са наведеном Уредбом.

ЗДРАВСТВЕНЕ УСТАНОВЕ

У току ревизије, у вези процедура и политика у ИТ, од укупног броја анкетираних здравствених установа, прикупили смо одговоре од њих 67. Од тог броја процедуре које се односе на управљање ИТ системима је донело 19 здравствених установа.

Анализом достављених докумената (19 установа), утврдили смо:
– Једна здравствена установа се у анкети изјаснила да има усвојене процедуре које се односе на ИТ управљање, али је анализом достављеног документа установљено да се тај документ уопште не односи на ИТ послове.
– Три здравствене установе имају већину дефинисаних процедура и политика пословања који се односе на ИТ.
– Десет здравствених установа има једну или две процедуре и то су Процедура о вршењу надзора над сигурносним обавезама из уговора пружаоца услуга и Правилник о заштити података личности.
– Пет здравствених установа имају дефинисан одређени број процедура који се односе на ИТ, али је потребно дефинисати још неке.

– Пример добре праксе је Институт за онкологију и радиологију Србије као и Институт за ортопедско-хируршке болести „Бањица“ које имају дефинисане кључне процедуре.



Илустрација 20. *Да ли здравствене установе имају процедуре за управљање ИТ системима*

Шта су последице, или шта могу бити последице?

Чест је случај да процедуре за управљање ИТ система „формално“ постоје, да су усвојене, али да су непотпуне, недовољно детаљне, и да не постоје докази (било каква евиденција) да се примењују.

Укупно гледано, може се закључити да у ИЗИС систему не постоје усвојене и имплементиране процедуре које уређују ИТ послове. Самим тим, није могуће успоставити одговарајући систем контроле, или „преношења знања“ што је неопходно у случајевима кадровских замена на овим пословима. Последице се огледају и у повећаном степену ризика по функционисање информационог система којим управља установа, или Институт „Батут“ или Министарство здравља.

Препоручујемо Министарству здравља да предузме активности у смислу припреме и доношења подзаконског акта којим ће ближе уредити услове за функционисање, управљање ризиком и безбедношћу интегрисаног здравственог информационог система, укључујући континуитет пословања у ванредним околностима, начин пријаве осигураника и заштиту излазних података, уз прибављање мишљења Института за јавно здравље Србије „Др Милан Јовановић Батут“ и других организација и установа у области здравства.

Препоручујемо Институту „Батут“ да успостави одговарајуће техничке, организационе и кадровске мере за обраду података у ИЗИС-у, и да успостави механизам за праћење примене тих мера.

Налаз 1.4: Министарство здравља и Институт за јавно здравље Србије „Др Милан Јовановић Батут“, као и установе које смо обухватили анкетом, нису успоставили управљање ИТ ризицима, иако је ово и законска обавеза, пре свега због непознавања ове проблематике, недовољно искуства и обученог ИТ кадра, а што за последицу може имати стварање непотребно великих трошкова у случају настанка нежељеног догађаја, а који се могао спречити, или великих нефинансијских губитака (података на пример) због неблаговременог предузимања мера

Зашто је важна процена ИТ ризика?

Једно од начела Закона о информационој безбедности је управо процена ИТ ризика. Сва питања разматрана у овој ревизији у основи имају процену одређених ризика (континуитет пословања, приступ подацима од стране пружаоца услуга, организација ИТ безбедности итд.). Када су у питању ИТ ризици, у пракси се примењује тзв. 3Д приступ (претња, рањивост, последица) или 2Д приступ (вероватноћа, утицај). Сама класификација ризика се најчешће врши према утицају, а кораци који обично следе обухватају анализу ризика (вероватноћа појављивања сваког ризика понаособ и процена утицаја), дефинисање стратегије за смањивање/отклањање ризика, а крајњи циљ је да се дође до поузданог информационог система код кога су ризици добро процењени тако да функционише у потпуности а са најмањим утрошком ресурса.

У Уредби о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, у члану 2 прописано је да 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.

Иако се напред наведени члан Уредбе односи на све операторе ИКТ система, па самим тим и на здравствене установе које су набавиле и користе здравствене информационе системе, када су у питању здравствене установе, чланом 45. Закона о здравственој документацији и евиденцијама у области здравства, прописано је да су здравствена установа, приватна пракса и друго правно лице, дужни да успоставе информациони систем, који представља свеобухватни скуп технолошке инфраструктуре (мрежних, софтверских и хардверских компонената), организације, људи и поступака за прикупљање, смештање, обраду, чување, пренос, приказивање и коришћење података и информација. Осим тога, у истом члану, став 2. тачка 6, прописано је да у складу са природом, обимом и сложеношћу делатности ИС мора да успостави процес управљања ризиком и безбедношћу информационог система.

Шта је у ревизији установљено?

ПРОЦЕНА ИТ РИЗИКА – МИНИСТАРСТВО ЗДРАВЉА И ИНСТИТУТ „БАТУТ“

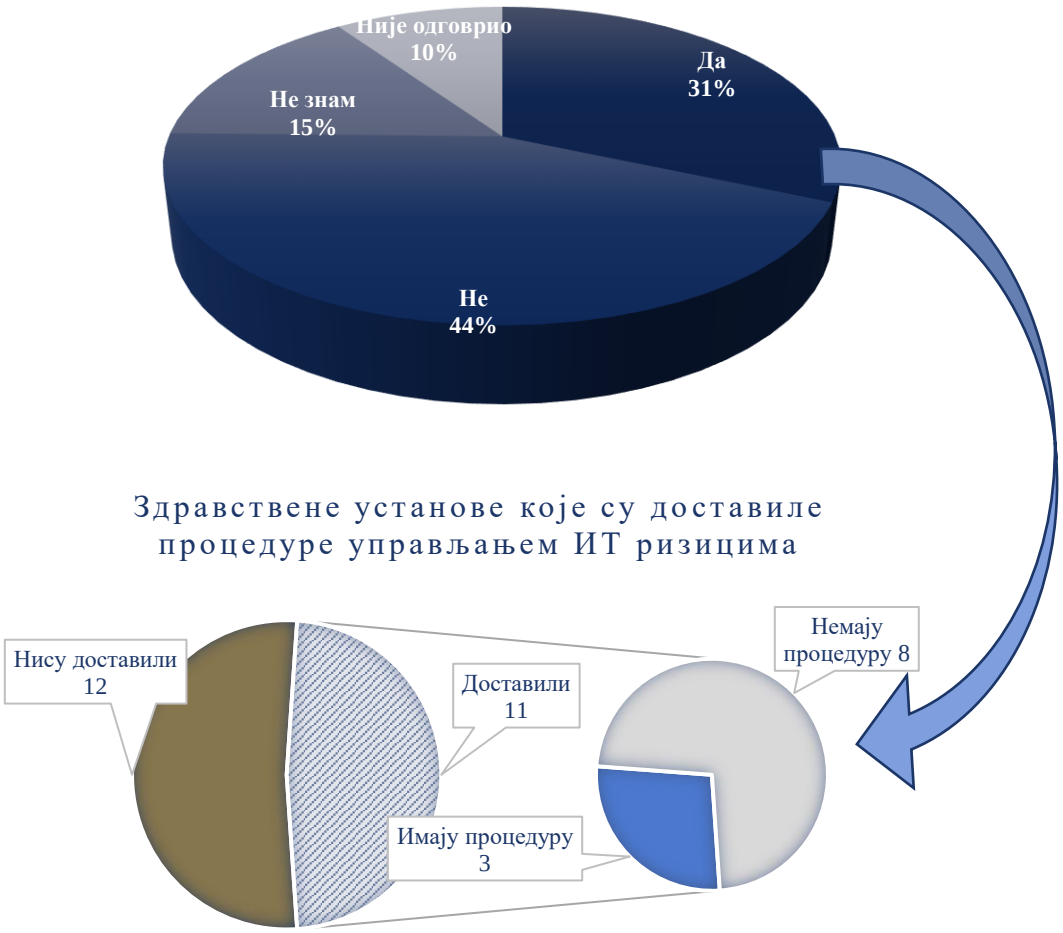
Министарство здравља и Институт „Батут“ који управљају неким од компоненти ИЗИС-а, нису успоставили управљање ИТ ризика за ИС којима управљају.

ПРОЦЕНА ИТ РИЗИКА – ЗДРАВСТВЕНЕ УСТАНОВЕ

Процес управљања ризиком је законска обавеза свих у ИЗИС-у. Међутим, већина здравствених установа овај процес није успоставила уопште, а и оне које су одговориле да јесу и доставиле неки документ који то поткрепљује, то у ствари нису учиниле, јер достављена документација не садржи идентификоване ИТ ризике, нити мере за њихову умањење. Разлози зашто је то тако леже у неспроведеним обукама запослених на ИТ пословима па самим тим и недовољном знању када су ови послови у питању, недовољној активности одговорних лица у здравственим установама итд.

На постављено питање да ли је успостављено управљање ИТ ризицима, што подразумева њихову идентификацију и спровођење плана за умањење ризика, од укупног броја анкетираних, одговор смо добили од 66 здравствених установа. 23 здравствене установе су се изјасниле да је проценом ризика обухваћена и процена ИТ ризика. Међутим, само 11 здравствених установа је доставило документ са проценом ИТ ризика.

На следећем графикону је приказана структура одговора:



Илустрација 21. *Да ли су у систему управљања ризицима обухваћени и ИТ ризици?*

Анализом достављених докумената, утврдили смо:

- Три од 11 здравствених установа имају акт о процени ИТ ризика и то КЦ Војводине, Институт за лечење и рехабилитацију „Нишка Бања“ и Дом здравља „Др Милорад Мика Павловић“ Инђија. Само је КЦ Војводине описао како управља ИТ ризиком.
- Осталих осам здравствених установа које су нам доставиле процедуру за управљање ризицима у пословању здравствених установа односе се на процену ризика које носи радно место информатичар.

Шта су последице, или шта могу бити последице?

Основно што треба знати: немогуће је успоставити ефикасан систем без процене ризика, тачније без успостављеног процеса управљања ризиком.

Разлози зашто је то тако су управо последице које могу настати или које су већ настале у информационим системима, а које стварају губитке, финансијске или нефинансијске природе (података на пример), који се добром проценом ризика могу избећи.

Другим речима, уколико се жели поуздан, али истовремено и ефикасан систем, без процене ризика то се не може постићи. На пример, могуће је све елементе система дуплирати, и тако постићи скоро 100% поуздан систем. Али због цене дуплирања, такав систем се не може сматрати ефикасним, јер се можда исти циљ (поузданост) може постићи и са мање улагања.

Последице невршења процене ризика у здравственим информационим системима се могу најпре огледати у губитку неких услуга у одређеном временском периоду, или привременом или трајном губитку података (у електронској форми) о пацијентима.

Препоручујемо Министарству здравља да предузме активности у смислу припреме и доношења подзаконског акта којим ће ближе уредити услове за функционисање, управљање ризиком и безбедношћу информационог система, укључујући континуитет пословања у ванредним околностима, начин пријаве осигураника и заштиту излазних података, уз прибављање мишљења Института за јавно здравље Србије „Др Милан Јовановић Батут“ и других организација и установа у области здравства.

ЗАКЉУЧАК 2: Ефективно управљање континуитетом пословања у случају ванредних околности у Интегрисаном здравстеном информационом систему није у потпуности успостављено, што за последицу може имати нефункционисање делова система у дужем временском периоду

Ризик у области управљања континуитета пословања је велики. Већина здравствених установа нема усвојене планове и процедуре, немају обезбеђену резервну локацију, као ни резервне сервере. Осим тога, често не поседују ни потребно знање за ове послове. У пракси се ослањају на пружаоце услуга, што је опет недовољно с обзиром на непостојање потребног хардвера.

Законом о информационој безбедности уређени су критеријуми мере заштите од безбедносних ризика у информационо-комуникационим системима (ИКТ). Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима. Здравствене установе су обавезне да донесу мере заштите ИКТ система, које се односе на превенцију и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и

претњама као и мере које обезбеђују континуитет обављања посла у ванредним околностима.

Уредбом о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја, ближе се уређује садржај акта о безбедности информационо-комуникационих система од посебног значаја.

Уредбом о утврђивању листе делатности у областима у којима се обављају делатности од општег интереса и у којима се користе информационо-комуникациони системи од посебног значаја се утврђује Листа делатности у областима у којима се обављају делатности од општег интереса и у којима се користе информационо-комуникациони системи.

Здравствене установе као и Министарство здравља и Институт „Батут“ су дужни да имају план континуитета пословања и план опоравка активности у случају ванредних околности. Сам план треба да садржи одређене смернице, процедуре и правила како треба да се поступа услед нежељених догађаја. У случају да дође до нежељеног догађаја здравствене установе треба да имају и резервне копије.

Више је разлога зашто смо у ревизији разматрали питања везана за континуитет пословања у ванредним околностима. Треба истаћи да овај термин „континуитет пословања у ванредним околностима“ у ширем смислу подразумева више подобласти: континуитет пословања, чување резервних копија и опоравак система у случају ванредних околности (у терминологији другачије речено – опоравак од катастрофе (disaster recovery - DR).

Први разлог је што су ревизорски тимови у ревизијама здравствених установа у претходним годинама уочили проблеме у овој области, пре свега када је у питању континуитет пословања у случају нежељених догађаја, јер већина ревидираних здравствених установа није имала овај план ни усвојен, ни наравно имплементиран и тестиран. Разлога за ово је више: неинформисаност, недостатак хардверске опреме, резервне локације, па и кадровских капацитета.

Други проблем који је уочен у претходним годинама се тицао начина на који се управљало резервним копијама. Није било дефинисано како се резервне копије чувају, ко има право приступа резервним копијама али је у скоро свим случајевима установљено да се установе у овој области ослањају искључиво на пружаоце услуга, и да немају капацитет да саме успоставе континуитет пословања користећи резервне копије.

Трећи разлог је да је управљање овим процесима и законска обавеза, која треба да буде уређена и одговарајућим процедурама, а што није био случај.

Имајући у виду све ове уочене проблеме, неправилности и ризике, али и законске обавезе у овој ревизији између осталог наш циљ је био да у оквиру другог ревизорског питања утврдимо да ли је у ИЗИС-у успостављен ефективан оквир за континуитет пословања у случају ванредних околности?

Како би одговорили на ово питање, разматрали смо да ли постоје имплементирана правила и процедуре за континуитет пословања, да ли постоји имплементиран план за континуитет пословања у ванредним околностима (план опоравка од катастрофе), да ли се резервне копије чувају у складу са донетим правилима и процедурама, на документован и безбедан начин и да ли се врши документовано периодично тестирање плана за континуитет пословања и плана за опоравак од катастрофе.

Наш закључак заснивамо на следећим налазима:

Налаз 2.1: У систему Интегрисани здравствени информациони систем, нису усвојена ни имплементирана правила и процедуре за континуитет пословања код већине анкетираних установа, као ни на нивоу субјеката ревизије, Института за јавно здравље Србије „Др Милан Јовановић Батут“ и Министарства здравља, због недостатка довољно стручног знања и недостатка кадровских капацитета, иако је то и законска обавеза, а што може за последицу имати нефункционисање система у неодређеном временском периоду, па самим тим и отежано пружање услуга здравственим осигураницима

Шта је процес континуитета пословања и зашто је важан?

Циљ је био да анализирамо да ли су донета правила и процедуре која уређују континуитет пословања, и да ли, ако су донета, тај процес уређују на адекватан начин – што значи да ли су свеобухватна, детаљна и на крају да ли је тај процес успостављен у пракси.

Законом о информационој безбедности, у члану 7., који прецизира мере заштите ИКТ система од посебног значаја, је између осталог прописано да оператор ИКТ система од посебног значаја одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система. Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима. Тачком 28. наведеног закона прописано је да се мере заштите ИКТ система односе на мере које обезбеђују континуитет обављања посла у ванредним околностима.

Влада Републике Србије је обавезе оператора ИКТ система детаљније уредила Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја. Члан 29. наведене Уредбе уређује мере које обезбеђују континуитет обављања посла у ванредним околностима и то:

– Оператор ИКТ система треба да предвиди мере којима се обезбеђује обављање послова у ванредним околностима, а које подразумевају одржавање информационе безбедности на задовољавајућем нивоу, дефинисање одговорности, планова, поступака у случају ванредних догађаја и процедура за опоравак ИКТ система, 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.

Како ИЗИС обухвата системе и апликације и на републичком нивоу и на нивоу здравствене установе, обзиром да установе набављају и користе здравствене информационе системе за обављање послова из свог делокруга, наведене законске обавезе се односе на све системе, па је анализа обухватила Институт „Батут“, Министарство здравља и здравствене установе.

Напретком ИТ, нивоа знања у тој области расте код све већег броја грађана, па и оних недобронамерних (хакери), повећава се ризик и могућност да поред проблема

изазваних кваровима, или незнањем, информациони системи постану и предмет хакерских, сајбер напада.

У таквим случајевима, дакле када се у неком делу система појави проблем, управо план континуитета пословања омогућује установи да настави са функционисањем, да смањи ризик од настанка веће штете као што је на пример губитак података, нефункционисање у дужем временском периоду и слично.

Да би то било тако, потребно је да постоје планови како да систем, што подразумева и информациони систем, функционише и у случају неког непредвиђеног и нежељеног догађаја.

Чест је случај да се подразумева да план континуитета пословања (Business Continuity Plan - BCP) и план опоравка од катастрофе (Disaster Recovery Plan - DRP) чине два дела једног свеобухватног плана. Међутим, то не мора бити тако.

Процес опоравка од катастрофе пре свега обухвата ситуације када су технички проблеми у питању, кварови, хаварије, итд.

План континуитета пословања обухвата у принципу организационе мере, када се мора некако обезбедити функционисање кључних процеса. Наравно, опоравак од катастрофе може бити део плана континуитета пословања.

Овде треба напоменути да процена ризика, о којој је било речи у претходном делу извештаја, олакшава израду овог плана, јер садржи све потенцијалне ризике по функционисање система, процену могућих штетних последица и омогућава израду плана за максимално умањење штете.

Шта је у ревизији установљено?

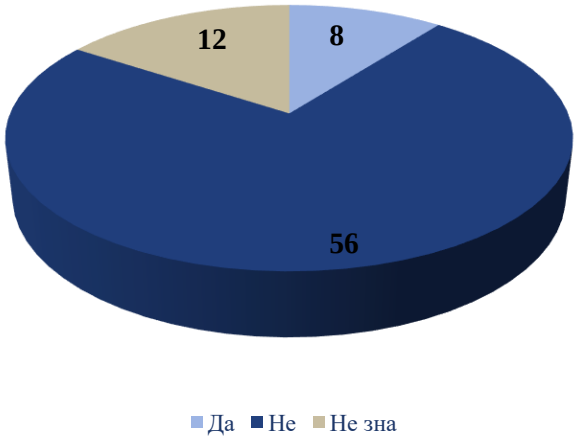
КОНТИНУИТЕТ ПОСЛОВАЊА КОД СУБЈЕКАТА РЕВИЗИЈЕ

Министарство и Институт „Батут“ немају донет план континуитета пословања, па самим тим ни одговарајућа правила и процедуре.

Није документован разлог, нити је неусвајање ових докумената на било који начин објашњено на одржаним састанцима.

КОНТИНУИТЕТ ПОСЛОВАЊА НА НИВОУ ЗДРАВСТВЕНЕ УСТАНОВЕ

У току спровођења ревизије, прикупили смо податке од здравствених установа који се односе на континуитет пословања. Како је приказано у Прилогу 1, од укупног броја анкетираних здравствених установа, прикупили смо одговоре од њих 76. Од тог броја планове, правила или процедуре за континуитет пословања је донело 8 здравствених установа. Међутим, само 7 здравствених установа је доставило тражена документа.



Илустрација 22. *Да ли постоји план континуитета пословања (BCP)*

Анализом достављених докумената, утврдили смо да су пет здравствених установа донеле планове континуитета пословања, који обухватају детаљну анализу претњи, могућа сценарија и коју активност је потребно предузети уколико се догоди неки нежељени догађај који узрокује прекид континуитета пословања. Ближе је дефинисано шта се дешава у следећим случајевима, односно могућа сценарија:

1. Нестанак електричне енергије
2. Прекид интернет конекције
3. Поплаве
4. Пожар
5. Квар на серверима и комуникационој опреми
6. Провала и крађа у просторијама Службе информатике
7. Упад преко интернета и рачунарске опреме
8. Тероризам
9. Епидемија или пандемија и
10. Земљотрес.

Три здравствене установе су доставиле документа која се уопште не баве питањима континуитета пословања и не представљају планове континуитета пословања, већ је реч о документима која уређују друга питања – општи планови рада здравствених установа.

Шта су последице, или шта могу бити последице?

Процес управљања континуитетом пословања није успостављен на нивоу целог ИЗИС-а, иако је то и законска обавеза свих здравствених установа и Института „Батут“ и Министарства здравља. Чак и у оним здравственим установама где су донете процедуре, оне нису свеобухватне и детаљне. Поред планирања и усвајања процедура, проблем је недостатак ресурса: финансијских средстава, опреме, кадрова. Здравствене установе су уговорима са пружаоцима услуга дефинисале континуитет у случају софтверских проблема, али све остало није обавеза пружаоца услуга, већ здравствених установа.

У системима као што је здравствени, веома је важно да све функционише увек, да грађани могу да имају поверење у здравствени систем да ће им најбоља могућа здравствена заштита бити пружена увек, и свуда, на целој територији Републике Србије. Међутим, уколико се планови и процедуре за континуитет пословања не успоставе у целом систему ИЗИС, последице се могу огледати у (привременом)

губитку или прекиду у протоку података, немогућности пружања неке услуге у одређеном временском периоду итд.

У случају честих прекида у функционисању може доћи до нарушавања поверења грађана у здравствени систем.

Препоручујемо Министарству здравља да предузме активности у смислу припреме и доношења подзаконског акта којим ће ближе уредити услове за функционисање, управљање ризиком и безбедношћу интегрисаног здравственог информационог система, укључујући континуитет пословања у ванредним околностима, начин пријаве осигураника и заштиту излазних података, уз прибављање мишљења Института за јавно здравље Србије „Др Милан Јовановић Батут“ и других организација и установа у области здравства.

Налаз 2.2: Институт за јавно здравље Србије „Др Милан Јовановић Батут“, Министарство здравља и анкетиране здравствене установе због недостатка потребне опреме, адекватног ИТ кадра и недовољно стручног знања нису обезбедиле ефективан план континуитета пословања у ванредним околностима – план опоравка од катастрофе, иако им је то била законска обавеза, што за последицу може имати нефункционисање информационог система у дужем временском периоду

Шта је план опоравка од катастрофе и зашто је важан?

План опоравка од катастрофе се успоставља за реаговање установе након неког инцидента, најчешће након неког квара на уређајима, физичког оштећења или квара услед пожара, поплаве и сличних догађаја, трајнијег губитка напајања.

Основни циљ плана је што је могуће брже ставити у функцију основне делове система након неког нежељеног догађаја, хаварије.

Мере и активности дефинисане планом зависе од препознатих ризика, и њихов приоритет зависи од важности појединих процеса, података, трошкова итд.

Нестанак електричне енергије, нарочито у дужем периоду, поплава, земљотрес, пожар, па чак и крађа или намерно оштећење опреме су догађаји које се не могу предвидети, а који могу систем или део система оштетити у толиком проценту да је онемогућено његово функционисање. Ово се чак може односити и на саму зграду у којој се систем налази.

План опоравка од катастрофе, када су ови ризици у питању, садржи мере које су усмерене на опремање и употребу секундарне (резервне) локације у оваквим случајевима. Та локација се успоставља на удаљености која треба да обезбеди њено функционисање у случају неких од наведених догађаја (наравно, у зависности од природе послова, њиховог обима и важности, величине система итд). На резервној локацији се поставља неопходна опрема за функционисање система: електрично напајање, мрежна инфраструктура, секундарни сервери – апликативни и за складиштење података итд.

Такође, план треба да садржи прецизно дефинисане процедуре у случајевима када је потребно прећи на употребу секундарног система, и дефинисано време опоравка појединих функционалности.

На крају, не мање важно, план треба да дефинише и начин и период тестирања секундарне локације, тј. процедура за опоравак од катастрофе.

Шта је у ревизији установљено?

ОПОРАВАК ОД КАТАСТРОФЕ МИНИСТАРСТВО ЗДРАВЉА И ИНСТИТУТ „БАТУТ“

Министарство здравља и Институт „Батут“ немају донет план опоравка од катастрофе.

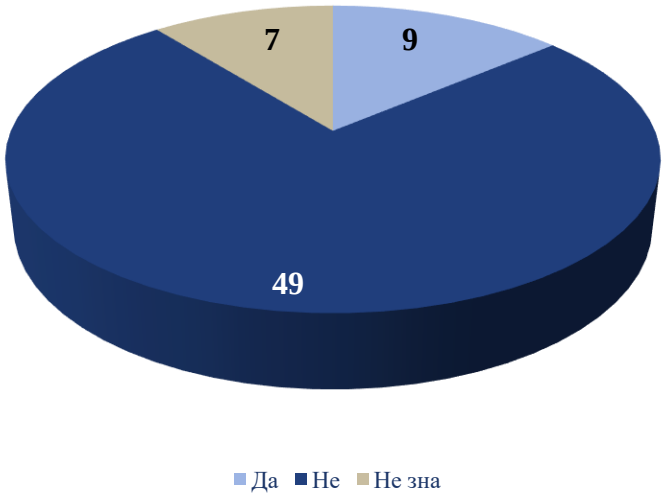
Није документован разлог, нити је неусвајање ових докумената на било који начин објашњено на одржаним састанцима.

ОПОРАВАК ОД КАТАСТРОФЕ – ЗДРАВСТВЕНЕ УСТАНОВЕ

У току спровођења ревизије, прикупили смо податке од здравствених установа који се односе на опоравак од катастрофе (хаварије). Од укупног броја анкетираних здравствених установа прикупили смо одговоре од њих 65. Чак 49 здравствених установа је одговорило да нема усвојен план опоравка од катастрофе, док је девет здравствених установа навело да је донело план опоравка од катастрофе. Међутим, само седам здравствених установа је доставило тражена документа.

Анализом достављених докумената, утврдили смо да од седам здравствених установа које су доставиле тражени план опоравка активности у случају хаварије, једна здравствена установа није доставила захтевани план, већ упутство за рад одсека за здравствено информациони систем, у коме се не предвиђају активности у случају да је потребан опоравак од катастрофе у случају ванредних околности.

Три здравствене установе су у плану опоравка од катастрофе навеле да постоје резервне локације са којих се могу преузети резервне копије уколико дође до хаварија. Једна здравствена установа није планом опоравка активности у случају хаварије предвидела резервне локације.



Илустрација 23. *Да ли је, у склопу управљања континуитетом пословања, усвојен план опоравка активности у случају хаварије (DRP)*

Шта су последице, или шта могу бити последице?

Континуитет пословања је могуће успоставити само у случају исправног хардверског дела система. То подразумева апликативни сервер и сервер за складиштење података, али и мрежну опрему, напајање струјом итд. У случају отказа неког од ових делова, немогуће је успоставити функционисање система, без обзира на остале мере предвиђене планом континуитета и постојањем резервних копија података.

Последица је нефункционисање система у често дужем временском периоду. Како већина анкетираних установа нема усвојен план опоравка од катастрофе, нити је уговором пренела ове обавезе на пружаоца услуга, нити располаже резервном опремом (серверима пре свега), ризик да у случају већег квара установа неће у дужем временском периоду моћи да пружа неке од услуга грађанима је велики.

Препоручујемо Министарству здравља да предузме активности у смислу припреме и доношења подзаконског акта којим ће ближе уредити услове за функционисање, управљање ризиком и безбедношћу интегрисаног здравственог информационог система, укључујући континуитет пословања у ванредним околностима, начин пријаве осигураника и заштиту излазних података, уз прибављање мишљења Института за јавно здравље Србије „Др Милан Јовановић Батут“ и других организација и установа у области здравства.

Налаз 2.3: Резервним копијама података из здравствених информационих система се не управља на документован начин, зато што здравствене установе нису усвојиле одговарајуће процедуре, што су биле обавезе по закону, што отежава или онемогућава контролу овог процеса

Зашто је важно (и обавезно) уредити процес управљања резервним копијама?

Законом о информационој безбедности, у члану 7, који прецизира мере заштите ИКТ система од посебног значаја прописано је и да Оператор ИКТ система од посебног значаја одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система. Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима. Тачком 16. наведеног члана прописано је да се мере заштите ИКТ система односе на заштиту од губитка података.

Влада Републике Србије је обавезе оператора ИКТ система детаљније уредила Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја. Члан 17. Уредбе уређује заштиту од губитака података и то на следећи начин:

– 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.

Израда резервних копија података представља основну сигурносну компоненту плана континуитета пословања, па самим тим и информационе безбедности здравствених информационих система.

Политике, правила и процедуре које уређују ову област могу да садрже информације о томе које податке је потребно backup[42], да ли ће се тај процес одвијати аутоматски или ручно, који ће се уређаји у ту сврху користити, где ће копије бити чуване, ко је задужен за тај процес, како ће копије бити означене, како се и колико често тестирају копије итд.

Шта је у ревизији установљено?

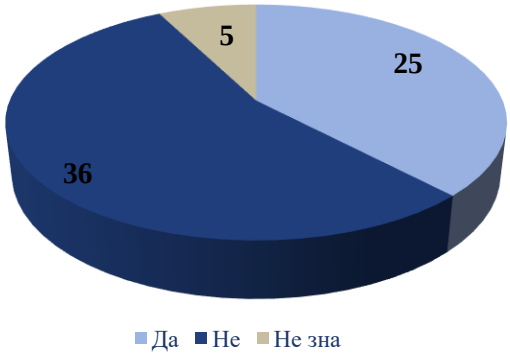
УПРАВЉАЊЕ РЕЗЕРВНИМ КОПИЈАМА МИНИСТАРСТВО ЗДРАВЉА И ИНСТИТУТ „БАТУТ“

Министарство здравља и Институт „Батут“ нису усвојили правила и процедуре за израду резервних копија.

У Институту „Батут“, резервне копије података се израђују на дневном нивоу, на недељном се експортују на два екстерна хард диска. Један хард диск се чува у Институту „Батуту“, а други се односи на другу удаљену локацију. Ниједан хард диск није криптован, јер већина податкака су збирни подаци зато сматрају да није велики ризик, па се подаци не криптују. Нису усвојене писане процедуре за бекаповање и чување података.

УПРАВЉАЊЕ РЕЗЕРВНИМ КОПИЈАМА – ЗДРАВСТВЕНЕ УСТАНОВЕ

У току спровођења ревизије, прикупили смо податке од здравствених установа који се односе на процедуре за управљање резервним копијама, и да ли се копије чувају на безбедним локацијама. Од свих анкетираних здравствених установа прикупили смо одговоре од њих 66. Од тог броја, 25 здравствених установа је навело да се резервне копије складиште на безбедним локацијама ван здравствених установа.



Илустрација 24. *Да ли су резервне копије смештене у безбедан простор за одлагање ван објекта*

Шта су последице, или шта могу бити последице?

Процес израде резервних копија се у скоро свим здравственим установама одвија аутоматски, при чему се копија података чува на примарној локацији, а један број установа резервну копију (екстерни хард диск) чува на другој (удаљеној) локацији.

[42] backup – израда резервне копије

Међутим, у току ревизије смо установили да се у појединим случајевима резервне копије носе кући (као најбезбеднијем месту по оцени запослених који то раде), што носи ризик да тај диск буде украден, изгубљен и да подаци буду евентуално компромитовани.

Како су истакли поједини запослени у неким здравственим установа, резервне копије се у једном броју случајева налазе и на рачунарима код пружаоца услуга. У уговорима који су достављени у току ревизије то није регулисано.

Препоручујемо Министарству здравља да предузме активности у смислу припреме и доношења подзаконског акта којим ће ближе уредити услове за функционисање, управљање ризиком и безбедношћу интегрисаног здравственог информационог система, укључујући континуитет пословања у ванредним околностима, начин пријаве осигураника и заштиту излазних података, уз прибављање мишљења Института за јавно здравље Србије „Др Милан Јовановић Батут“ и других организација и установа у области здравства.

Налаз 2.4: Министарство здравља и Институт за јавно здравље Србије „Др Милан Јовановић „Батут“, као и здравствене установе које смо обухватили анкетом, не врше тестирање планова за континуитет и опоравак од катастрофе, зато што немају довољно ресурса за то - пре свега запослених са довољно знања и искуства, иако је верификација тих планова обавеза свих оператора ИКТ система од посебног значаја, а што за последицу може имати нефункционални систем у току и након ванредне ситуације у дужем временском периоду

Зашто треба периодично тестирати планове за континуитет пословања и опоравак од катастрофе?

Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, у члану 29. уређује мере које обезбеђују континуитет обављања посла у ванредним околностима и то:

– Оператор ИКТ система треба да предвиди мере којима се обезбеђује обављање послова у ванредним околностима, а које подразумевају одржавање информационе безбедности на задовољавајућем нивоу, дефинисање одговорности, планова, поступака у случају ванредних догађаја и процедура за опоравак ИКТ система, 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.

Дакле, поред обавезе да успостави континуитет пословања у случајевима ванредних ситуација, оператор ИКТ система има обавезу и да све те процесе и верификује, тј. тестира.

Шта је у ревизији установљено?

ТЕСТИРАЊЕ ПЛАНОВА ЗА КОНТИНУИТЕТ ПОСЛОВАЊА У ВАНРЕДНИМ СИТУАЦИЈАМА МИНИСТАРСТВО ЗДРАВЉА И ИНСТИТУТ „БАТУТ“

Министарство здравља, и Институт „Батут“ не врше тестирање планова за континуитет пословања.

ТЕСТИРАЊЕ ПЛАНОВА ЗА КОНТИНУИТЕТ ПОСЛОВАЊА У ВАНРЕДНИМ СИТУАЦИЈАМА – ЗДРАВСТВЕНЕ УСТАНОВЕ

У поступку ревизије, прикупили смо податке од здравствених установа који се односе на тестирање планова, односно да ли се спроводи тестирање планова. Од 67 здравствених установа које су доставиле одговор да ли спроводе тестирање планова само три здравствене установе су одговориле потврдно, две од три су и то документовале.

Илустрација 25. *Да ли се спроводи тестирање ланова*

Шта су последице, или шта могу бити последице?

Уколико се не тестирају планови за континуитет пословања и опоравак од катастрофе за последицу може имати нефункционалан систем у дужем временском периоду у току али и након ванредне ситуације. Другим речима, ИС можда неће бити доступан здравственим радницима, што може онемогућити или успорити пружање неких услуга грађанима у краћем или дужем временском периоду.

Посебно велики ризик постоји када су у питању резервне копије, и нетестирање враћања резервних копија података. Наиме, у случају да примарна локација, или примарни сервери на којима се подаци обрађују и складиште буду уништени, једини део система који се не може купити јесу подаци. Без обзира колико времена и новца ће требати да се информатичка структура поново успостави (у случају на пример тоталне штете), тај проблем је решив. Уколико међутим подаци нису сачувани, или нису сачувани на начин да се могу повратити, та штета би била ненадокнадива.

Препоручујемо Министарству здравља да предузме активности у смислу припреме и доношења подзаконског акта којим ће ближе уредити услове за функционисање, управљање ризиком и безбедношћу интегрисани здравствени информационог система, укључујући континуитет пословања у ванредним околностима, начин пријаве осигураника и заштиту излазних података, уз прибављање мишљења Института за

јавно здравље Србије „Др Милан Јовановић Батут“ и других организација и установа у области здравства.

ЗАКЉУЧАК 3: Здравствене установе обухваћене анкетом нису усвојиле и примениле свеобухватне мере заштите информационих система, а Министарство здравља и Институт за јавно здравље Републике Србије „Др Милан Јовановић Батут“ нису успоставили управљање информационом безбедношћу Интегрисаног здравственог информационог система и контролу примене мера заштите као приоритет, што је неопходно како би била осигурана поверљивост, доступност и поузданост података о личном здрављу грађана

Све више пословних процеса се обавља употребом рачунара и информационих система, системи су због тога све сложенији, па су самим тим и претње и ризици све већи. Поред одговорних лица у здравственим установама, за управљање информационом безбедношћу у информационим системима у ИЗИС-у, одговорни су и Министарство здравља и Институт „Батут“, а посебно се то односи на заштиту осетљивих података осигураника, где је поред поверљивости потребно обезбедити и доступност и поузданост тих података, како са једне стране не би дошли у посед неовлашћених лица, а са друге стране како би све здравствене услуге могле бити правовремено пружене.

Зато је информациона безбедност једно од најважнијих питања које треба уредити и дефинисати мере заштите, а основа за то је управо акт о информационој безбедности.

Поједини послови у овој области треба да су уређени одговарајућим процедурама, то је и законска обавеза, зато што акт о безбедности као општи акт обично не садржи детаљне инструкције како се неки процес спроводи, и ко је за то одговоран.

Спровођење мера је посао добро обучених, стручних ИТ кадрова. Организацијски треба да буду уређени тако да омогућавају јасну поделу дужности и одговорности, али и контролу свих тих послова.

Уколико неке послове обавља пружалац услуге, то је потребно дефинисати уговором. Између осталог обавезно је дефинисати све обавезе пружаоца услуга када је у питању информациона безбедност.

Посебна пажња се треба посветити питањима приступа систему: физичком и логичком приступу. И то најпре одговарајућим процедурама, упутствима, евиденцијама, а затим и практичном имплементацијом тих докумената и контролом.

Треба обезбедити максималну могућу заштиту података осигураника, у складу са домаћим законодавством, почевши од тренутка приступа подацима (уз употребу електронске здравствене књижице или на начин који осигурава да се подацима осигураника не приступа без знања осигураника), али и успоставити мере контроле и заштите излазних података.

Све то, у посматраном периоду ревизије 2017-2019. година, није на адекватан начин препознато од стране субјеката и установа које користе ИЗИС. Здравствене установе су на различит и несвеобухватан начин уредиле ову област, занемарујући и своје законске обавезе, док Министарство здравља и Институт „Батут“ нису предузели мере из своје надлежности да ове процесе испрате, најпре кроз редовно прикупљање података о овим питањима, а затим и предузимањем одговарајућих активности како би унапредиле информациону безбедност у установама, па тако и у ИЗИС систему у целини.

Када су у питању обавезе Министарства здравља и Института „Батут“, поред других законских обавеза, у смислу информационе безбедности, посебно треба истаћи да је Законом о здравственој документацији и евиденцијама у области здравства, у члану 45. прописано:

„Здравствена установа, приватна пракса и друго правно лице, дужни су да успоставе информациони систем, који представља свеобухватни скуп технолошке инфраструктуре (мрежних, софтверских и хардверских компонената), организације, људи и поступака за прикупљање, смештање, обраду, чување, пренос, приказивање и коришћење података и информација.

У складу са природом, обимом и сложеношћу делатности адекватан информациони систем мора да:

1) поседује функционалност, капацитете и перформансе који омогућавају пружање одговарајуће подршке пословним процесима;
2) обезбеђује благовремене и тачне информације од значаја за доношење одлука и ефикасно обављање активности;
3) буде пројектован тако да са одговарајућим контролама за валидацију података на улазу, у току процеса обраде и на излазу из тог система, може да уочи појаве нетачности и неконзистентности у подацима и информацијама. Ради успостављања и очувања интегралности информационог система потребно је обезбедити да постојећи и други системи за обраду података, као и систем извештавања буду уподобљени;
4) обезбеди одговарајућу организациону структуру са јасно утврђеном поделом послова и дужности запослених како би се омогућило адекватно функционисање и управљање информационим системом;
5) усвоји и документује одговарајућу методологију којом се утврђују сва правила везана за информациони систем;
6) успостави процес управљања ризиком и безбедношћу информационог система;
7) политиком безбедности информационог система уреди принципе, начине и процедуре постизања и одржавања адекватног нивоа безбедности система и података, као и овлашћења и одговорности везаних за коришћење ресурса информационог система.

Ближе услове за функционисање, управљање ризиком и безбедношћу информационог система, јединствене методолошке принципе и стандарде и друге услове од значаја за функционисање овог система прописује министар уз прибављено мишљење завода за јавно здравље основаног за територију Републике Србије и организације обавезног здравственог осигурања.

Треба истаћи и да је истим законом, у члану 44. прописано да се Интегрисани здравствени информациони систем Републике Србије организује 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.

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.

Интегрисани здравствени информациони систем Републике Србије обезбеђује доступност здравствених података свим учесницима у здравственом систему у складу са њиховим правима, улогама и одговорностима.

Руковалац подацима који чине Интегрисани здравствени информациони систем Републике Србије је завод за јавно здравље основан за територију Републике Србије.

Завод за јавно здравље основан за територију Републике Србије дужан је да о свакој повреди безбедности података обавести лице, односно лица на која се ти подаци односе, министарство надлежно за послове здравља и Повереника за информације од јавног значаја и заштиту података о личности.“

Зато је у овој ревизији циљ био анализа стања у овој области, са идејом да препоруке за унапређење информационе безбедности буду дате Министарству здравља и Институту Батут, како би они својим актима и својим активностима у сарадњи да свим здравственим установама дефинисали, прописали, применили и контролисали све мере које би водиле побољшању нивоа информационе безбедности у свим сегментима ИЗИС-а.

Наш закључак заснивамо на следећим налазима:

Налаз 3.1: У систему Интегрисани здравствени информациони систем, организација ИТ безбедности није успостављена на адекватан начин, иако је то законска обавеза и субјеката ревизије и здравствених установа, што за последицу има већи степен рањивости овог система па самим тим и осетљивих података здравствених осигураника

Зашто је важно успоставити организацију ИТ безбедности на адекватан, свеобухватан начин?

Главни циљ ове ревизије јесте информациона безбедност.

Организација ИТ безбедности обухвата више послова које треба уредити, у смислу успостављања управљачке и организационе структуре, обученог и стручног ИТ кадра, процене ИТ ризика, обезбеђивања континуитета пословања у случају ванредних ситуација и у склопу тога управљања резервним копијама података, усвајања и имплементације правила и процедура за све ИТ послове, уређивање обавеза пружаоца услуга у складу са законом и подзаконским актима, контроле логичког и физичког приступа систему, управљања улазним и излазним подацима итд.

Нека од ових питања су већ разматрана, о некима ће бити речи касније, а у овом делу је циљ да се изврши анализа да ли су усвојена одговарајућа документа која се односе на информациону безбедност, што је и законска обавеза свих оператора ИКТ система од посебног значаја (што у пракси значи и субјеката ревизије и здравствених установа), да ли су имплементирана и да ли је успостављена организациона ИТ структура са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу, а чији запослени су оспособљени за посао који раде и разумеју своју одговорност.

Без успостављања адекватне организације ИТ безбедности није могуће управљати подацима на начин прописан законима.

Више закона који се односе на обавезе Министарства, Покрајинског секретаријата, Института „Батут“ и здравствене установе, прописују читав низ мера које је у овом погледу потребно применити, а посебно Закон о информационој безбедности (цео закон) и пратеће уредбе и Закон о здравственој документацији и евиденцијама у области здравства (посебно чланови 44-51).

Дакле, анализа је обухватила питања усвајања адекватних докумената која уређују ову област - акта о безбедности информационог система и одговарајућих процедура, организациону структуру ИТ безбедности и примену других мера заштите ИКТ система.

Шта је у ревизији установљено?

ОРГАНИЗАЦИЈА ИТ БЕЗБЕДНОСТИ КОД ИНСТИТУТ „БАТУТ“ И МИНИСТАРСТВО ЗДРАВЉА

Министарство здравља нема донет акт о безбедности информационог система, нити одговарајуће процедуре.

Институт „Батут“ није усвојио процедуре које се односе на информациону безбедност.

Нису спровођене обуке запослених на пословима ИТ безбедности.

ОРГАНИЗАЦИЈА ИТ БЕЗБЕДНОСТИ – ЗДРАВСТВЕНЕ УСТАНОВЕ

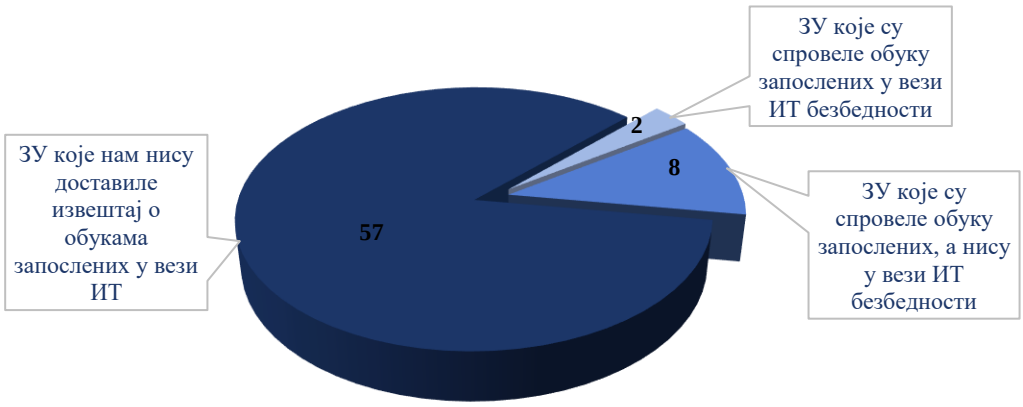
У току спровођења ревизије, установљено је да већина здравствених установа није успоставила адекватну организациону ИТ структуру, тачније структуру која омогућава јасну поделу дужности и одговорности, али и контролу свих тих послова. Такође, већина здравствених установа у посматраном периоду није спровела неопходне ИТ обуке, ни када су у питању запослени који користе систем, нити, што је важније из угла информационе безбедности, када су у питању запослени на ИТ пословима.

Иако је то законска обавеза већ три године, један број здравствених установа није усвојила акт о безбедности информационог система, као ни одговарајуће процедуре у овој области.

Такође, већина здравствених установа није одредила лице за пријаву инцидената надлежном органу, иако је и то законска обавеза, нити је успоставило управљање инцидентима.

а) **обуке запослених на ИТ пословима везане за безбедност ИТ**

У току спровођења ревизије, прикупили смо податке од здравствених установа који се односе на организацију ИТ безбедности. Од 67 здравствених установа, десет здравствених установа је доставило извештаје о одржаним обукама.



Илустрација 26. *Извештаји о спроведеним обукама запослених у вези ИТ*

Анализом тих извештаја утврђено је да само две здравствене установе су реализовале обуке на тему ИТ безбедности, док се сва остала достављена документа од стране других установа односе на теме које нису обухваћене овом ревизијом (стоматолошке услуге, радиолошки системи, апотеке, телефонска мрежа итд).

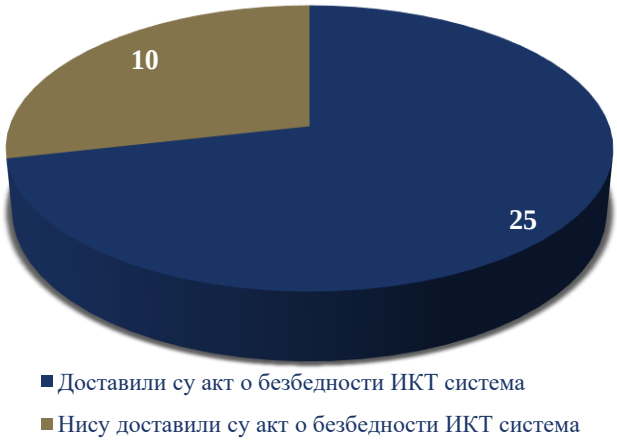
Нису организоване обуке за ИТ кадар, дакле за запослене у здравственим установама које администрирају и одржавају здравствене информационе системе, што ствара ризик да они нису у довољној мери информисани о могућим безбедносним претњама, нити довољно обучени да на њих одговоре правовременим предузимањем мера.

Од свих анкетираних здравствених установа које су доставиле документацију, када су у питању ИТ обуке, може се издвојити Институт за онкологију и радиологију Србије, који је одржао више обука са различитим ИТ темама, па се на неки начин, у мрежи здравствених установа може издвојити као пример добре праксе.

б) **Усвојен акт о информационој безбедности**

У току спровођења ревизије, прикупили смо податке од здравствених установа који се односе на питање да ли су здравствене установе донеле акт о информационој безбедности. Од 35 здравствених установа од којих смо прикупили одговоре акт о информационој безбедности донело је 25 здравствених установа и исти нам доставили.

Треба напоменути да је ово законска обавеза свих здравствених установа. Закон о информационој безбедности ступио на снагу 5. фебруара 2016. године, док су уредбе које ближе уређују примену закона донете 17. новембра 2016. године. У року од 90 дана требало је донети Акт о безбедности ИКТ система што значи да је последњи рок за то је био 17. фебруар 2017. године.



Илустрација 27. *Акт о информационој безбедности*

Анализом достављених докумената утврђено је да у посматраном периоду ревизије (2017-2019 година), две од 25 здравствених установа нису имале усвојен акт о безбедности ИКТ система. Два документа немају уписан датум и годину усвајања акта, док су остале здравствене установе, сем једног изузетка, правилнике о информационој безбедности усвојиле након 2017. године, тачније након усвајања и ступања на снагу Закона о информационој безбедности.

Што се тиче садржаја достављених докумената, у смислу свеобухватности и детаљности, као добре примере од преосталих 21 могу се издвојити свега два документа. Остали правилници у приличној мери личе један на други, прате мере предвиђене законом, али нису довољно детаљни, не дефинишу обавезе и одговорности запослених, не баве се скоро уопште континуитетом пословања, посебно имајући у виду недостатак процедура за те послове.

Поред континуитета пословања, у скоро свим достављеним правилницима недостаје детаљнија дефиниција организационе структуре са обавезама и одговорностима ИТ кадра, што отежава управљање овим пословима, али и контролу ИТ послова.

Али оно што је уочено у свим документима, то је да се не баве проценом ризика, у правилницима се ова област скоро и не спомиње, а процена ИТ ризика с једне стране не само што је можда најважније начело Закона о информационој безбедности због своје важности, већ је и основа од које се полази приликом израде свих других процедура за ИТ послове.

Другим речима, закључак је да су правилници о информационој безбедности усвојени зато што су законска обавеза, а не зато што је препозната потреба да се информациона безбедност ИКТ система уреди на свеобухватан начин, ради лакшег управљања и контроле са једне стране, и стварања услова за даљи развој информационих система, са друге стране.

Од свих анкетираних установа које су доставиле документацију, када је у питању акт о безбедности ИКТ система, могу се издвојити примери Института за онкологију и радиологију Србије, Института за лечење и рехабилитацију „Нишка Бања“, који су свеобухватнији и детаљнији у односу на друге, па се на неки начин, у мрежи здравствених установа могу издвојити као примери добре праксе.

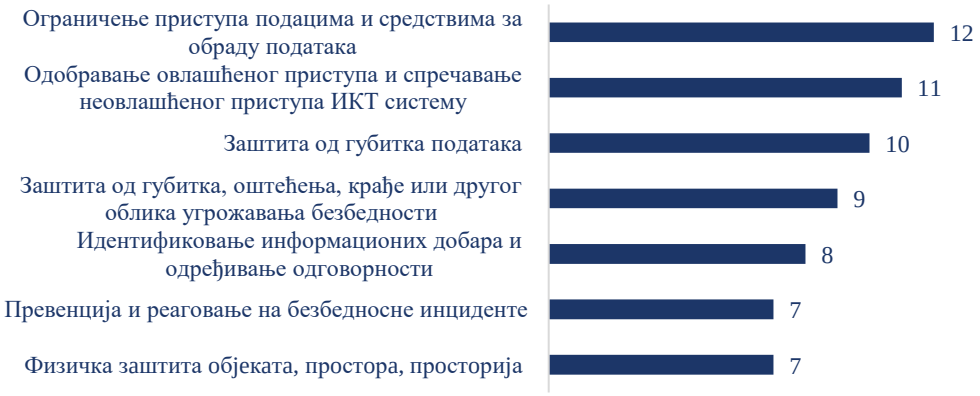
в) **Усвојене и примењене процедуре које се односе на информациону безбедност**

У току спровођења ревизије, прикупили смо податке од здравствених установа који се односе на питање да ли су здравствене установе усвојиле и примениле процедуре које се односе на информациону безбедност. Од 35 здравствених установа које су одговоре на анкету 17 здравствених установа је доставило процедуре које се односе информациону безбедност.

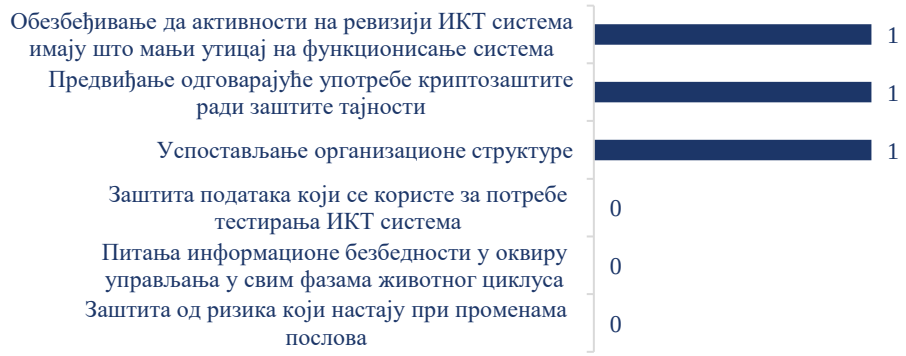
Треба напоменути да је и ово законска обавеза свих здравствених установа. У члану 45. Закона о здравственој документацији и евиденцијама у области здравства, прописано је у ставу 2. да у складу са природом, обимом и сложеношћу делатности адекватан ИС мора да:

– усвоји и документује одговарајућу методологију којом се утврђују сва правила везана за информациони систем (тачка 5),
– успостави процес управљања ризиком и безбедношћу информационог система (тачка 6);
– политиком безбедности информационог система уреди принципе, начине и процедуре постизања и одржавања адекватног нивоа безбедности система и података, као и овлашћења и одговорности везаних за коришћење ресурса информационог система (тачка 7).

Такође, већ више пута је истакнуто, обавеза усвајања процедура за ИТ безбедност је прописана и Законом о информационој безбедности.



Илустрација 28. *Процедуре које су односе на информациону безбедност код здравствених установа*



Илустрација 29. *Процедуре које су односе на информациону безбедност код здравствених установа*

Анализом достављених докумената, установили смо да су и процедуре које су усвојене недовољно детаљне и несвеобухватне и као такве не могу послужити за управљање пословима, контролу послова и трансфер знања.

г) **Успостави одговарајућу организациону структуру са јасно утврђеном поделом послова и дужности запослених**

У току спровођења ревизије, прикупили смо податке од здравствених установа који се односе на питање да ли су здравствене установе усвојиле и примениле процедуре које се односе на организациону ИТ структуру која се односи на информациону безбедност. Од 35 здравствених установа које су одговоре на анкету 27 здравствених установа је доставило изводе из правилника о систематизацији радних места на ИТ пословима.

Треба напоменути да је и ово законска обавеза свих здравствених установа. (Да подсетимо, у Уредби о ближем уређењу мера заштите ИКТ система од посебног значаја, у члану 2. који уређује успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система од посебног значаја, прописано је прописано да:

Оператор ИКТ система од посебног значаја (у даљем тексту: оператор ИКТ система) 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 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 утврђивања одговорности запослених потребно је предвидети и одговорност за обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима.

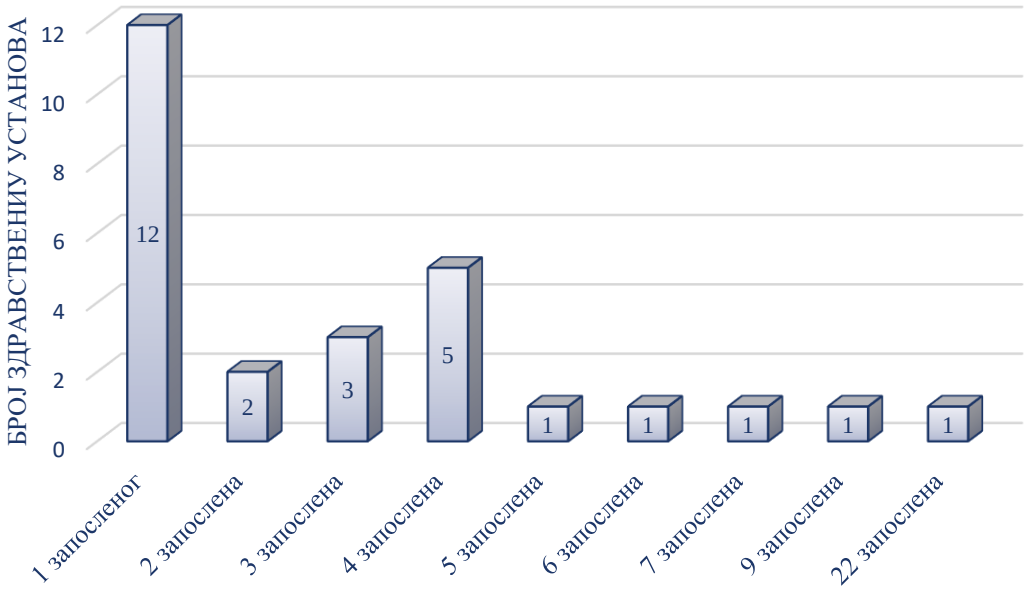
Анализом достављених података установили смо да организациона ИТ структура код скоро свих здравствених установа није успостављена на начин да омогућава јасну поделу дужности и одговорности, али и контролу свих тих послова. Овај закључак темељимо на следећим чињеницама:

У десет здравствених установа на ИТ пословима ради само један запослени, што значи да он ради све ИТ послове, без икакве могућности да се успостави контрола квалитета и законитости (не може се очекивати да контролише сам себе). Није дефинисано ко ће мењати или ко мења тог јединог запосленог у случају годишњег одмора, боловања и слично, а нарочито треба имати у виду континуитет пословања, пренос неопходног знања и слично.

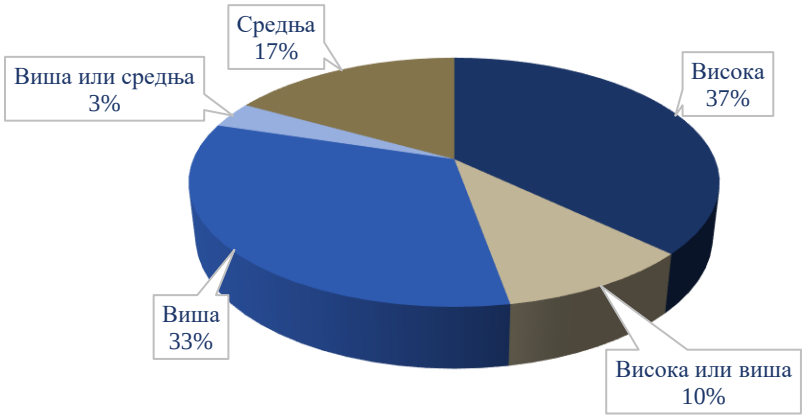
Постоје случајеви у којима су за радно место са истим називом дефинисани описи послова на различит начин, што само по себи ствара недоумицу ко је одговоран за које послове.

Описи послова код скоро свих здравствених установа које су доставиле документацију нису дефинисани тако да омогућавају са једне стране континуитет пословања у случају одсуства/замене неког запосленог, нити, са друге стране омогућавају контролу рада запослених на ИТ пословима, с обзиром да у великој већини достављених докумената не постоји уопште дефинисана контрола било ког ИТ посла.

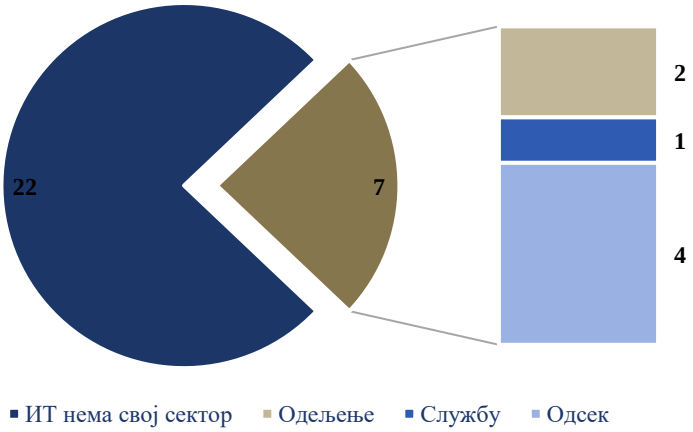
Илустрација 30. *Број систематизованих ИТ радих места у 27 здравствених установа*



Илустрација 31. *Приказ колико здравствена установа има запослених лица у ИТ*



Илустрација 32. *Заступљеност стручне спреме на месту ИТ*



Илустрација 33. *Колико здравствених установа има одељење / одсек / службу за ИТ*

д) Одређивање одговорног лица за обавештавање о инцидентима

У току спровођења ревизије, прикупили смо податке од здравствених установа који се односе на одређивање одговорног лица за обавештавање надлежних органа у инцидентима у ИКТ систему. . Од 35 здравствених установа које су одговоре на анкету 13 здравствених установа је доставило документ да су одредили одговорно лице за обавештење о инцидентима.

Илустрација 34. *Лице за обавештење надлежних органа о инцидентима у ИКТ систему*

Анализом достављених докумената утврдили смо да је:

– Шест здравствених установа доставило одлуке одређивању одговорног лица за обавештавање надлежних органа о инцидентима у ИКТ

– Шест здравствених доставило решења којим се уписује у евиденцију ИКТ система од посебног значаја о оператеру ИКТ система од посебног значаја.

– Једна здравствена установа заправо доставила одлуку којом се формира тим за заштиту података о личности.

Треба напоменути да је и ово законска обавеза здравствених установа.

Може се закључити да је мали број здравствених установа у овом погледу испунио своју законску обавезу, али да истовремено управљање инцидентима, што подразумева евидентирање и реаговање, нису препознале као активност која за циљ има заштиту информационог система.

Шта су последице, или шта могу бити последице?

Неуспостављање организационе ИТ структуре код субјеката и здравствених установа као главну последицу има то да се не спроводи контрола информационе безбедности – активности администратора, управљање резервним копијама, активности пружаоца услуга, итд. Наиме, у већини установа не постоји довољан број запослених на ИТ пословима, нити радна места која и опису послова имају и послове ИТ безбедности.

Неуспостављање процедура које се односе на ИТ безбедност с једне стране није у складу са Законом о информационој безбедности, а с друге стране онемогућава два веома важна процеса – контролу ИТ послова и трансфер знања новозапосленим на тим пословима. У једном броју здравствених установа на ИТ пословима ради један запослени. У таквим случајевима, не постоји могућност контроле рада тог једног запосленог, јер то нема ко да ради, непостојање процедура у пракси ствара ризик да у случају замене тог једног запосленог, новозапослени неће знати који процес се на који начин одвија и које су његове конкретне, па и свакодневне обавезе.

Циљ управљања инцидентима је успостављање механизама да се најпре инциденти евидентирају а затим и да се правовремено реагује. Како се инцидент може десити било где у систему, запослени који уочи настали проблем треба обавестити надлежно лице, које ће предузети даље кораке, или дати инструкције. Уколико се не врши евидентирање инцидената, и не спроводе мере како се такав инцидент не би поновио, то може као последицу имати понављање инцидената, које није морало да се деси, па самим тим и настанак додатне штете у систему (оштећење, нестанак рачунарске опреме, штете настале активирањем малициозног кода, неовлашћен приступ систему, покушаји упада у систем итд.)

Препоручујемо Министарству здравља да предузме активности у смислу припреме и доношења подзаконског акта којим ће ближе уредити услове за функционисање, управљање ризиком и безбедношћу интегрисаног здравственог информационог система, укључујући континуитет пословања у ванредним околностима, начин пријаве осигураника и заштиту излазних података, уз прибављање мишљења Института за јавно здравље Републике Србије „Др Милан Јовановић Батут“ и других организација и установа у области здравства.

Налаз 3.2: Институт за јавно здравље Србије „Др Милан Јовановић Батут“, Министарство здравља и анкетиране здравствене установе и поред тога што у уговорима са пружаоцима услуга постоји део који се односи на поверљивост података, нису успоставили механизам за контролу да ли пружалац услуга ту обавезу поштује, због недостатака кадровских капацитета, недоумица у вези законске регулативе и недовољно стручног знања, што за последицу може имати одавање осетљивих података здравствених осигураника.

Зашто су важне мере заштите информационог система у случајевима када тај систем одржава пружалац услуге ?

Када су у питању пружаоци услуга и законске обавезе здравствених установа и субјеката ревизије, треба истаћи неке од најважнијих чланова закона који уређују питања заштите информационих система и поверљивости података.

Закон о информационој безбедности, у члану 7. уређује мере заштите ИКТ система од посебног значаја и то:

Оператор ИКТ система од посебног значаја одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система. Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

Мере заштите ИКТ система се, између осталог, односе на: заштиту средстава оператора ИКТ система која су доступна пружаоцима услуга (став 3, тачка 25) и одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга (став 3, тачка 26).

С друге стране, Закон о заштити права пацијената и Закон о заштити података о личности ова питања уређују на, здравственим установама, нејасан начин:

- **Закон о правима пацијената**

Члан 21. наведеног закона уређује право на поверљивост података о здравственом стању пацијента. Ставом 1. овог члана прописани је да подаци о здравственом стању, односно подаци из медицинске документације, спадају у податке о личности и представљају нарочито осетљиве податке о личности пацијента, у складу са законом.

Ставом 2. овог члана закона, прописано је да су податке из става 1. овог члана, дужни да чувају сви здравствени радници, односно здравствени сарадници, као и друга лица запослена у здравственим установама, приватној пракси, организационој јединици високошколске установе здравствене струке која обавља здравствену делатност, другом правном лицу које обавља одређене послове из здравствене делатности у складу са законом, организацији обавезног здравственог осигурања, као и правном лицу које обавља послове добровољног здравственог осигурања, код којих је пацијент здравствено осигуран, а којима су ти подаци доступни и потребни ради остваривања законом утврђених надлежности.

Чланом 22. наведеног закона прописано је да дужности чувања података из члана 21. став 1. овог закона, надлежни здравствени радници, односно здравствени сарадници, као и друга лица запослена код послодаваца из члана 21. став 2. овог закона, могу бити ослобођени само на основу писменог пристанка пацијента, односно његовог законског заступника, или на основу одлуке суда.

- **Закон о заштити података о личности**

Чланом 17. наведеног закона уређена је обрада посебних врста података о личности. Прописано је да је забрањена обрада којом се открива расно или етничко

порекло, политичко мишљење, верско или филозофско уверење или чланство у синдикату, као и обрада генетских података, биометријских података у циљу јединствене идентификације лица, података о здравственом стању или података о сексуалном животу или сексуалној оријентацији физичког лица.

У тачки 8) прописано је да је обрада из става 1. овог члана допуштена у случају када је обрада неопходна у сврху превентивне медицине или медицине рада, ради процене радне способности запослених, медицинске дијагностике, пружања услуга здравствене или социјалне заштите, односно управљања здравственим или социјалним системима, на основу закона или на основу уговора са здравственим радником, ако се обрада врши од стране или под надзором здравственог радника или другог лица које има обавезу чувања професионалне тајне прописане законом или професионалним правилима.

Члан 42. овог закона, уређује мере заштите:

Узимајући у обзир ниво технолошких достигнућа и трошкове њихове примене, природу, обим, околности и сврху обраде, као и вероватноћу наступања ризика и ниво ризика за права и слободе физичких лица који произилазе из обраде, руковалац је приликом одређивања начина обраде, као и у току обраде, дужан да:

1) примени одговарајуће техничке, организационе и кадровске мере, као што је псеудонимизација, које имају за циљ обезбеђивање делотворне примене начела заштите података о личности, као што је смањење броја података;

2) обезбеди примену неопходних механизама заштите у току обраде, како би се испунили услови за обраду прописани овим законом и заштитила права и слободе лица на која се подаци односе (став 1).

Осим тога прописује истим чланом да је руковалац дужан да сталном применом одговарајућих техничких, организационих и кадровских мера обезбеди да се увек обрађују само они подаци о личности који су неопходни за остваривање сваке појединачне сврхе обраде. Та се обавеза примењује у односу на број прикупљених података, обим њихове обраде, рок њиховог похрањивања и њихову доступност (став 2).

Такође прописује да се овим мерама мора увек обезбедити да се без учешћа физичког лица подаци о личности не могу учинити доступним неограниченом броју физичких лица (став 3).

Издати сертификат из члана 61. овог закона руковалац може користити да предочи да се придржава обавеза из ст. 1. до 3. овог члана (став 4).

Став 4. се не примењује се на обраду коју врше надлежни органи у посебне сврхе (став 5).

Члан 45. овог закона уређује област „Обрађивач“:

Ако се обрада врши у име руковаоца, руковалац може да одреди као обрађивача само оно лице или орган власти који у потпуности гарантује примену одговарајућих техничких, организационих и кадровских мера, на начин који обезбеђује да се обрада врши у складу са одредбама овог закона и да се обезбеђује заштита права лица на које се подаци односе (став 1).

Обрађивач из става 1. овог члана може поверити обраду другом обрађивачу само ако га руковалац за то овласти на основу општег или посебног писменог овлашћења. Ако се обрада врши на основу општег овлашћења, обрађивач је дужан да информише руковаоца о намераваном избору другог обрађивача, односно замени другог обрађивача, како би руковалац имао могућност да се супротстави таквој промени (став 2).

Обрада од стране обрађивача мора бити уређена уговором или другим правно обавезујућим актом, који је закључен, односно усвојен у писменом облику, што

обухвата и електронски облик, који обавезује обрађивача према руковаоцу и који уређује предмет и трајање обраде, природу и сврху обраде, врсту података о личности и врсту лица о којима се подаци обрађују, као и права и обавезе руковаоца (став 3).

Даље је у истом члану прописано да се уговором или другим правно обавезујућим актом из става 3. овог члана прописује да је обрађивач дужан да:

1) обрађује податке о личности само на основу писмених упутстава руковаоца, укључујући и упутство у односу на преношење података о личности у друге државе или међународне организације, осим ако је обрађивач законом обавезан да обрађује податке. У том случају, обрађивач је дужан да обавести руковаоца о тој законској обавези пре започињања обраде, осим ако закон забрањује достављање тих информација због потребе заштите важног јавног интереса;

2) обезбеди да се физичко лице које је овлашћено да обрађује податке о личности обавезало на чување поверљивости података или да то лице подлеже законској обавези чувања поверљивости података;

3) предузме све потребне мере у складу са чланом 50. овог закона;

4) поштује услове за поверавање обраде другом обрађивачу из ст. 2. и 7. овог члана;

5) узимајући у обзир природу обраде, помаже руковаоцу применом одговарајућих техничких, организационих и кадровских мера, колико је то могуће, у испуњавању обавеза руковаоца у односу на захтеве за остваривање права лица на које се подаци односе из Главе III. овог закона;

6) помаже руковаоцу у испуњавању обавеза из члана 50. и чл. 52. до 55. овог закона, узимајући у обзир природу обраде и информације које су му доступне;

7) после окончања уговорених радњи обраде, а на основу одлуке руковаоца, избрише или врати руковаоцу све податке о личности и избрише све копије ових података, осим ако је законом прописана обавеза чувања података;

8) учини доступним руковаоцу све информације које су неопходне за предочавање испуњености обавеза обрађивача прописаних овим чланом, као и информације које омогућавају и доприносе контроли рада обрађивача, коју спроводи руковалац или друго лице које он за то овласти.

У случају из става 4. тачка 8) овог члана, обрађивач је дужан да без одлагања упозори руковаоца ако сматра да писмено упутство које је од њега добио није у складу са овим законом или другим законом којим се уређује заштита података о личности.

Члан 50. овог закона уређује безбедност обраде:

У складу са нивоом технолошких достигнућа и трошковима њихове примене, природом, обимом, околностима и сврхом обраде, као и вероватноћом наступања ризика и нивоом ризика за права и слободе физичких лица, руковалац и обрађивач спроводе одговарајуће техничке, организационе и кадровске мере како би достигли одговарајући ниво безбедности у односу на ризик (став 1).

У складу са ставом 2, према потреби, мере из става 1. овог члана нарочито обухватају:

1) псеудонимизацију и криптозаштиту података о личности; 2) способност обезбеђивања трајне поверљивости, интегритета, расположивости и отпорности система и услуга обраде; 3) обезбеђивање успостављања поновне расположивости и приступа подацима о личности у случају физичких или техничких инцидената у најкраћем року и 4) поступак редовног тестирања, оцењивања и процењивања делотворности техничких, организационих и кадровских мера безбедности обраде.

Приликом процењивања одговарајућег нивоа безбедности из става 1. овог члана посебно се узимају у обзир ризици обраде, а нарочито ризици од случајног или незаконитог уништења, губитка, измене, неовлашћеног откривања или приступа

подацима о личности који су пренесени, похрањени или обрађивани на други начин (став 3).

Примена одобреног кодекса поступања из члана 59. овог закона, односно издат сертификат из члана 61. овог закона, може се користити у циљу предочавања испуњености обавеза из става 1. овог члана (став 4).

Руковалац и обрађивач дужни су да предузму мере у циљу обезбеђивања да свако физичко лице које је овлашћено за приступ подацима о личности од стране руковаоца или обрађивача, обрађује ове податке само по налогу руковаоца или ако је на то обавезано законом (став 5).

Одредбе ст. 1. до 5. овог члана не примењују се на обраду коју врше надлежни органи у посебне сврхе.

Члан 61. овог закона уређује издавање сертификата:

У циљу доказивања поштовања одредби овог закона од стране руковаоца и обрађивача, а посебно узимајући у обзир потребе малих и средњих предузећа, могу се установити поступци издавања сертификата о заштити података о личности, са одговарајућим жиговима и ознакама за заштиту података (став 1).

Руковаоцу, односно обрађивачу на које се овај закон не примењује, у циљу доказивања предузимања мера заштите од стране руковаоца и обрађивача, а у оквиру преноса њихових података о личности у друге државе или међународне организације на основу члана 65. став 2. тачка 5) овог закона, може се издати сертификат, са одговарајућим жиговима и ознакама, у складу са ставом 5. овог члана, под условом да они путем уговора или другог правно обавезујућег акта прихвате примену ових мера заштите, укључујући и заштиту права лица на које се подаци односе (став 2).

Поступак издавања сертификата је добровољан и транспарентан (став 3).

Постојање издатог сертификата не може утицати на законске обавезе руковаоца и обрађивача, нити на инспекцијска и друга овлашћења Повереника из чл. 77. до 79. овог закона (став 4).

Сертификат издаје сертификационо тело из члана 62. овог закона или Повереник, на основу критеријума које прописује Повереник, у складу са овлашћењима из члана 79. став 3. овог закона (став 5).

Руковалац и обрађивач који захтевају издавање сертификата дужни су да сертификационом телу из члана 62. овог закона, односно Поверенику, ако је захтев упућен њему, омогуће приступ радњама обраде и пруже све информације о обради које су неопходне за спровођење поступка издавања сертификата (став 6).

Сертификат се издаје руковаоцу и обрађивачу на период који не може бити дужи од три године, а може се обновити ако они и даље испуњавају исте прописане услове и критеријуме за издавање сертификата (став 7).

Сертификат из става 7. овог члана се укида у случају кад сертификационо тело, односно Повереник, ако је захтев упућен њему, утврди да руковалац, односно обрађивач више не испуњава прописане критеријуме за издавање сертификата (став 8).

Повереник води и јавно објављује на својој интернет страници списак сертификационих тела и издатих сертификата, са одговарајућим жиговима и ознакама (став 10).

Одредбе ст. 1. до 9. овог члана не примењују се на обраду коју врше надлежни органи у посебне сврхе (став 10).

Шта је у ревизији установљено?

МИНИСТАРСТВО ЗДРАВЉА ИНСТИТУТ „БАТУТ“ - ОБЕЗБЕЂЕЊЕ ПОВЕРЉИВОСТИ ПОДАТАКА КОД ПРУЖАОЦА УСЛУГА

Министарство здравља није успоставило механизам контроле заштите података здравствених осигураника од стране пружаоца услуга апликативног софтвера „Мој доктор“

У Институту „Батут“ све апликације и базе података одржавају и администрирају запослени у Институту „Батут“.

ЗДРАВСТВЕНЕ УСТАНОВЕ – ОБЕЗБЕЂЕЊЕ ПОВЕРЉИВОСТИ ПОДАТАКА КОД ПРУЖАОЦА УСЛУГА

Законска обавеза јесте да свака здравствена установа прати одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга. Али, постављају се питања:

1. Како то урадити?
2. Да ли имају довољно обученог кадра за то?
3. Како је то уређено уговором?
4. Да ли постоје процедуре у којима је дефинисано како се прате и контролишу клаузуле о поверљивости у уговорима?
5. Да ли здравствене установе могу да спроведу ове мере?

а) Да ли је правилницима о систематизацији радних места предвиђено радно место које у опису послова има и праћење безбедносних клаузула у уговорима са пружаоцима услуга?

У току спровођења ревизије, прикупили смо податке од здравствених установа који се односе на питање да ли су здравствене установе успоставиле организациону ИТ структуру која се односи на информациону безбедност. Од 35 здравствених установа које су одговоре на анкету 27 здравствених установа је доставило изводе из правилника о систематизацији радних места на ИТ пословима.

Анализом достављених података добијених од анкетираних здравствених установа, утврдили смо да не постоје радна места које у опису послова има и праћење безбедносних клаузула у уговорима са пружаоцима услуга.

б) Да ли су здравствене установе усвојиле процедуре које се између осталог односе на праћење безбедносних клаузула у уговорима са пружаоцима услуга?

У току спровођења ревизије, прикупили смо податке од здравствених установа који се односе на питање да ли су здравствене установе усвојиле процедуре које се између осталог односе на праћење праћење безбедносних клаузула у уговорима са пружаоцима услуга?. Од 35 здравствених установа које су одговоре на анкету 27 здравствених установа је доставило тражене процедуре.

Анализом достављених докумената, утврдили смо да су само три здравствене установе усвојиле процедуре које се односе на одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга.

в) Да ли су здравствене установе у уговорима са пружаоцима услуга који се односе на набавку и/или одржавање здравствених информационих система предвиделе и клаузуле које се односе на поверљивост података?

У току спровођења ревизије, прикупили смо податке од здравствених установа који се односе на питање да ли су здравствене установе у уговорима са пружаоцима услуга који се односе на набавку и/или одржавање здравствених информационих система предвиделе и клаузуле које се односе на поверљивост података? Од 35 здравствених установа које су одговоре на анкету 32 здравствене установе је доставило тражене уговоре.

Анализом достављених докумената, утврдили смо да у шест случајева уговори нису садржали одредбе о поверљивости података. Само у једном случају, у уговору је предвиђен механизам за проверу активности пружаоца услуга, који се обавезао да ће, како то пише „снимати сваку сесију“, како би у случају потребе здравствена установа могла да оствари увид у активности приликом приступа.

У свим осталим случајевима у уговорима постоји део који се односи на поверљивост података, али без дефинисања икаквог механизма како то здравствена установа може да контролише. Чак постоји и један случај у којем се здравствена установа обавезује да не сме дати податке из базе без сагласности пружаоца услуга.

У једном случају, здравствена установа је навела да не дозвољава пружаоцу услуга приступ бази, јер то није у складу са законом.

Дакле, из приказаних резултата анализе се може закључити да здравствене установе нису успоставиле механизам за контролу да ли пружалац услуга ту обавезу поштује. Разлога има више. Прво, као што се може видети у питању су кадровски капацитети, и неусаглашавање правилника о систематизацији са (законским) обавезама здравствених установа. Друго, здравствене установе нису усвојиле процедуре којим треба да уреде ове активности, а пре свега начин на који ће контролисати да ли пружаоци услуга поштују ове клаузуле о поверљивости. Што се тиче уговора који су анализирани у току вршења ревизије, на основу уговора који су достављени може се закључити да одредбе о поверљивости нису саставни делови свих уговора, али и то да постоји случај да се сматра да се пружаоцима услуга уопште не сме дозволити приступ продукционој бази, тј подацима пацијената/здравствених осигураника.

У неком обиму постоји и неразумевање улоге здравствених установа у ИЗИС-у када се у питању заштита података осигураника. Наиме, у току анализе достављених докумената, уочен је и случај да је једна здравствена установа себе прогласила за руковаоца података, иако је законом уређено да је руковалац података за ИЗИС Институт „Батут“, а то се наравно односи и на све здравствене установе, у складу са дефиницијом ИЗИС-а. Са друге стране, и Институт „Батут“ је као руковалац подацима требао да преузме активнију улогу о комуникацију са здравственим установама, како би се ова питања разјаснила и дефинисала.

Шта су последице, или шта могу бити последице?

Претходних година били смо сведоци неовлашћеног изношења у јавност здравствених података пацијената, али се ни у једном случају није утврдило како су ти подаци ту доспели.

Како наводе представници установа, или ИТ запослени, разлог зашто пружалац услуге приступа продукционој бази је тај што се повремено појави потреба да се неки унети податак коригује, а то запослени у установи не знају да ураде. Такође, приступ продукционој бази је потенцијално потребан и у случају када је потребно да пружалац услуге докаже да софтвер у потпуности одговара постављеним захтевима, да раде све

функционалности, а за таква тестирања нису довољни тестни подаци, или када се тестира упис и читање података из базе, измена података и рад са резервним копијама. У овим ситуацијама, а пракса показује да је чест случај свакодневног приступа продукционим базама од стране пружаоца услуга, пружалац услуга има приступ делу или целој бази података (или резервној копији базе).

Дакле, иако се са пружаоцима услуга потписује уговор са клаузулом о поверљивости, у једном броју случајева, тачније код једног броја здравствених установа не постоји механизам контроле када и из којих разлога пружалац услуге приступа продукционој бази, и то из једноставног разлога што то нема ко да ради, јер је већ раније напоменуто да постоје установе са једним, или чак ниједним ИТ стручњаком, и који у неким случајевима нема довољно знања да то може да прати, или координира.

Ризик се делимично може умањити тако што би пружаоци услуге развој радили искључиво на тестним подацима, што би процес израде и враћања резервне копије података био искључиво у надлежности здравствене установе, и што би сваки приступ продукционом окружењу од стране пружаоца услуга био уређен процедуром која би између осталог обухватила и евидентирање захтева свих активности у том процесу.

Препоручујемо Министарству здравља да предузме активности у смислу припреме и одређивања ближе садржине података, укључујући и податке о личности, који се воде у електронском медицинском досијеу, начин и поступак преузимања података, као и друга питања од значаја за успостављање и коришћење података, уз прибављено мишљење Института за јавно здравље Србије „Др Милан Јовановић Батут“ и других организација и установа у области здравства.

Препоручујемо Институту „Батут“ да уреди процес обраде података од стране пружаоца услуга у здравственим информационим системима на законом прописан начин, што подразумева обавезну примену мера заштите података, и може укључити процес сертификације и издавања посебног или општег писменог овлашћења другим обрађивачима.

Налаз 3.3: У информационим здравственим системима није успостављен процес одобравања и укидања приступа на задовољавајући начин, због тога што нису усвојене процедуре које уређују овај процес и није успостављена контрола тог процеса, иако је то законска обавеза, што за последицу може имати угрожену безбедност података здравствених осигураника

Зашто је важно (и обавезно) уредити процес контроле физичког и логичког приступа информационом систему?

Чланом 10. Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја, у прописује одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа и то:

Оператор ИКТ система је у обавези да предвиди процедуру за одобравање и укидање овлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа, тако што предвиђа услове за одобравање и укидање овлашћеног приступа, проверу адекватности одобреног нивоа приступа и доделу јединствене идентификационе ознаке лицу којем се одобрава приступ (став 1);

Оператор ИКТ система води евиденцију о додељеним и одузетим ознакама, утврђује услове за коришћење заједничке идентификационе ознаке у случајевима када је то неопходно, дефинише начин и услове онемогућавања и уклањања јединствених

идентификационих ознака, као и услове за доделу и коришћење администраторских права (став 2);

Лицима којима се одобрава овлашћени приступ омогућује се приступ на основу података за аутентификацију (лозинке, криптографски кључеви, подаци складиштени на токенима и сл.) (став 3);

Додела и коришћење администраторских права приступа треба да буде ограничена и контролисана (став 4);

Оператор ИКТ система дужан је да обезбеди механизам за укидање права приступа у случајевима промене радног места, престанка радног односа и, по потреби, у другим случајевима (став 5).

Такође, када су у питању овлашћења и одговорности везаних за коришћење ресурса информационог система (апликације, базе података итд.), чланом 45. Закона о здравственој документацији и евиденцијама у области здравства је прописано да здравствена установа, приватна пракса и друго правно лице, дужни су да успоставе информациони систем, који представља свеобухватни скуп технолошке инфраструктуре (мрежних, софтверских и хардверских компонената), организације, људи и поступака за прикупљање, смештање, обраду, чување, пренос, приказивање и коришћење података и информација (став 1).

Став 2. тачка 5) овог члана Закона, прописује да у складу са природом, обимом и сложеношћу делатности адекватан информациони систем мора да усвоји и документује одговарајућу методологију којом се утврђују сва правила везана за информациони систем; тачком 6) је прописано да мора да успостави процес управљања ризиком и безбедношћу информационог система; док је тачком 7) прописано да мора да политиком безбедности информационог система уреди принципе, начине и процедуре постизања и одржавања адекватног нивоа безбедности система и података, као и овлашћења и одговорности везаних за коришћење ресурса информационог система.

Ставом 3. овог члана Закона је прописано да ближе услове за функционисање, управљање ризиком и безбедношћу информационог система, јединствене методолошке принципе и стандарде и друге услове од значаја за функционисање овог система прописује министар уз прибављено мишљење завода за јавно здравље основаног за територију Републике Србије и организације обавезног здравственог осигурања.

Дакле, све здравствене установе и министарство здравља и Институт „Батут“ треба да овај процес уреде поштујући управо наведене одредбе Закона. Али, то не значи само да се свим корисницима система доделе параметри приступа и улоге у систему. Потребно је и обезбедити механизам контроле тог процеса како би се у сваком тренутку могло установити да ли листа корисника одговара тренутној листи корисника система, са одговарајућим улогама.

Само на такав, свеобухватан начин управљања логичким приступом се може обезбедити неопходан степен безбедности система и података.

На сличним принципима се уређује и физички приступ, дакле обухвата одређивање лица која могу да приступе сервер собама, разлоге за то, тј. улоге тих лица, и механизам контроле тог процеса.

Шта је у ревизији установљено?

ИНСТИТУТ „БАТУТ“ И МИНИСТАРСТВО ЗДРАВЉА

Институт „Батут“ и Министарство здравља нису усвојили процедуре које се односе на логички и физички приступ.

ЗДРАВСТВЕНЕ УСТАНОВЕ

У току спровођења ревизије, прикупили смо податке од здравствених установа који се односе на питање да ли су здравствене установе усвојиле процедуре које се односе на контроле физичког и логичког приступа Од 35 здравствених установа које су одговоре на анкету 27 здравствених установа је доставило тражене процедуре.

Анализом достављених докумената, утврдили смо да су само три здравствене установе усвојиле процедуре које детаљније уређују питања контроле логичког и физичког приступа, док је још три донело процедуре у којима се у свега неколико реченица разматрају ова питања, и то више у форми циљева које је потребно остварити, а не детаљне дефиниције корака-мера које је и на који начин потребно применити.

Један број здравствених установа нема оспособљене администраторе који управљају овим процесом, већ процес додељивања и укидања права приступа обављају пружаоци услуга.

Увидом у списак примењених физичких мера заштите, али и након обиласка неких серверских просторија (тачније просторије у којима су смештени серверски рачунари), њихова физичка безбедност је такође на вишем нивоу уређена него што је то случај са већином других питања информационе безбедности ИКТ система.

Шта су последице, или шта могу бити последице?

У здравственим установама у којима не постоје администратори који су задужени за додељивање и укидање права, већ тај посао обавља пружалац услуга постоји могућност неовлашћеног приступа софтверу, кроз неовлашћено креирање привременог администраторског или корисничког налога, што може довести до злоупотребе у смислу увида у приватне податке осигураника од стране за то неовлашћеног лица.

Исти ризик постоји и у случајевима када у здравственим установама постоји више администратора, а они за обављање послова управљања логичког приступа користе исти администраторски налог, тако да је немогуће утврдити ко је заиста неку операцију и извршио.

У претходним годинама било је случајева да се обелодањују подаци из здравствених картона грађана, без утврђивања начина како је и ко дошао у посед тих података.

У току вршења ревизија у претходним годинама ревизорски тимови су уочили проблеме који су се односили на логички приступ, а који су се огледали у немогућности утврђивања који администратор је креирао неки кориснички налог, или у коришћењу једног истог корисничког налога од стране више лица итд.

Препоручујемо Министарству здравља да предузме активности у смислу припреме и доношења подзаконског акта којим ће ближе уредити услове за функционисање, управљање ризиком и безбедношћу интегрисаног здравственог информационог система, укључујући континуитет пословања у ванредним околностима, начин пријаве осигураника и заштиту излазних података, уз прибављање мишљења Института за јавно здравље Србије „Др Милан Јовановић Батут“ и других организација и установа у области здравства.

Налаз 3.4: Здравствене установе нису успоставиле максималну могућу заштиту приступа подацима осигураника (уз употребу електронске здравствене књижице или на начин који осигурава да се подацима осигураника не приступа без знања осигураника), нити су успоставиле мере контроле и заштите излазних података, што за последицу може имати неовлашћен приступ или изношење здравствених података

Зашто је важно (и обавезно) уредити процес пријаве осигураника у систем, и обезбедити заштиту излазних података?

Електронске здравствене књижице (укључујући и два податка које су повезане са њом – ЛБО и број здравствене књижице) су између осталог за циљ имале и једнозначну идентификацију здравственог осигураника, што се у пракси показало да није увек случај. Процес подразумева да се осигураник приликом пријема идентификује електронском здравственом књижицом и да на тај начин буде потврђено лично присуство осигураника, што треба да осигура да ће се његовим подацима приступити само када осигураник буде лично присутан.

Када су у питању излазни подаци, важно је обезбедити да се они генеришу само у законом уређене сврхе, и да их могу видети/користити само за то овлашћене особе. Када су у питању излазни подаци, у здравствени информационим системима се поред појединачних извештаја, дијагноза итд. могу генерисати и збирни извештаји. Заштита свих тих излазних података се постиже искључиво успостављањем строгих механизама контроле који се односе на то како се и коме ти подаци могу даље дистрибуирати.

Шта је у ревизији установљено?

ЗДРАВСТВЕНЕ УСТАНОВЕ

У здравственим установама, осигураника је могуће пријавити (изабрати) уносом само једног податка (ЈМБГ), значи без здравствене књижице, па и без присуства осигураника. Како су навели представници (запослени) у здравственим установама овакав начин пријаве осигураника омогућен је делимично из разлога проблема са радом електронских читача, а делимично због брже идентификације осигураника.

Уместо очитавања књижице, претрагу и пријаву осигураника је могуће вршити уз унос само јединственог матичног броја осигураника, или чак и претрагу по имену и презимену.

УСБ портови на корисничким рачунарима у већини здравствених установа нису закључани.

Шта су последице, или шта могу бити последице?

У здравственим установама у којима је могуће осигураника унети/изабрати уносом само једног податка (ЈМБГ, или име и презиме), без електронске здравствене књижице, постоји могућност да се од стране корисника система оствари увид у личне податке осигураника и у случајевима када он није присутан, идентификован на други начин или када то уопште није потребно

Када УСБ портови нису закључани могуће је снимити не екстерну меморију све податке који се у здравственим информационим системима генеришу као фајл, што укључује и појединачне извештаје/дијагнозе и збирне извештаје.

Препоручујемо Министарству здравља да предузме активности у смислу припреме и доношења подзаконског акта којим ће ближе уредити услове за функционисање, управљање ризиком и безбедношћу интегрисаног здравственог информационог система, укључујући континуитет пословања у ванредним околностима, начин пријаве осигураника и заштиту излазних података, уз прибављање мишљења Института за јавно здравље Србије „Др Милан Јовановић Батут“ и других организација и установа у области здравства.

V Захтев за доставу одазивног извештаја

Субјекти ревизије су, на основу члана 40. став 1. Закона о Државној ревизорској институцији, дужан да поднесе Државној ревизорској институцији писани извештај о отклањању откривених несврсисходности (одазивни извештај) у року од 90 дана почев од наредног дана од дана уручења овог извештаја.

Одазивни извештај мора да садржи:

1) навођење ревизије, на коју се он односи;

2) кратак опис несврсисходности у пословању, које су откривене ревизијом;

3) приказивање мера исправљања.

Мере исправљања су мере које субјект ревизије предузима да би отклонио несврсисходности у свом пословању или мере умањење ризика од појављивања одређене несврсисходности у свом будућем пословању за чије предузимање субјект ревизије мора поднети уз одазивни извештај одговарајуће доказе.

Субјекти ревизије су обавезни да у одазивном извештају искажу мере исправљања по основу откривених несврсисходности односно свих закључака и налаза датих у Извештају о ревизији сврсисходности пословања, као и да поступи по датим препорукама осим оних који су отклоњени у току обављања ревизије и садржани у поглављу Мере предузете у поступку ревизије. За мере исправљања је дужан да уз одазивни извештај достави доказе према следећем:

1. За налазе, односно несврсисходности првог приоритета, односно које је могуће отклонити у року од 90 дана субјекти ревизије су у обавези да доставе доказе о отклањању несврсисходности односно предузимању мера исправљања;
2. За налазе, односно несврсисходности другог приоритета, односно које је могуће отклонити у року до годину дана субјекти ревизије су у обавези да доставе акциони план у којем ће описати мере и активности које ће бити предузете ради отклањања несврсисходности или смањења ризика од појављивања несврсисходности у будућем пословању као и планирани период предузимања мера и одговорно лице;
3. За налазе, односно несврсисходности трећег приоритета, односно које је могуће отклонити у року од једне до три године субјекти ревизије су у обавези да доставе акциони план у којем ће описати мере и активности које ће бити предузете ради отклањања несврсисходности или смањења ризика од појављивања несврсисходности у будућем пословању као и планирани период предузимања мера и одговорно лице.

На основу члана 40. став 2. Закона о Државној ревизорској институцији одазивни извештај је јавна исправа која је потписана и оверена печатом од стране одговорног лица субјекта ревизије.

Државна ревизорска институција ће оценити веродостојност одазивног извештаја, тј. провериће истинитости навода о мерама исправљања, предузетим од стране субјекта ревизије, подносиоца одазивног извештаја. У случају потребе извршиће се и оцена да ли су мере исправљања исказане у одазивном извештају задовољавајуће.

Сагласно члану 57. став 1. тачка 3) Закона о Државној ревизорској институцији, ако субјекат ревизије у чијем су пословању откривене несврсисходности, не подносе у прописаном року Институцији одазивни извештај, против одговорног лица субјекта ревизије поднеће се захтев за покретање прекршајног поступка.

Ако се оцени да одазивни извештај не указује да су откривене несврсисходности отклоњене на задовољавајући начин, сматра се да субјект ревизије крши обавезу доброг пословања. Ако се ради о незадовољавајућем отклањању значајне несврсисходности, сматра се да постоји тежи облик кршења обавезе доброг пословања. У овим случајевима Државна ревизорска институције је овлашћена да предузима мере сагласно члану 40. ст 7. до 13. Закона о Државној ревизорској институцији.

VI Прилог

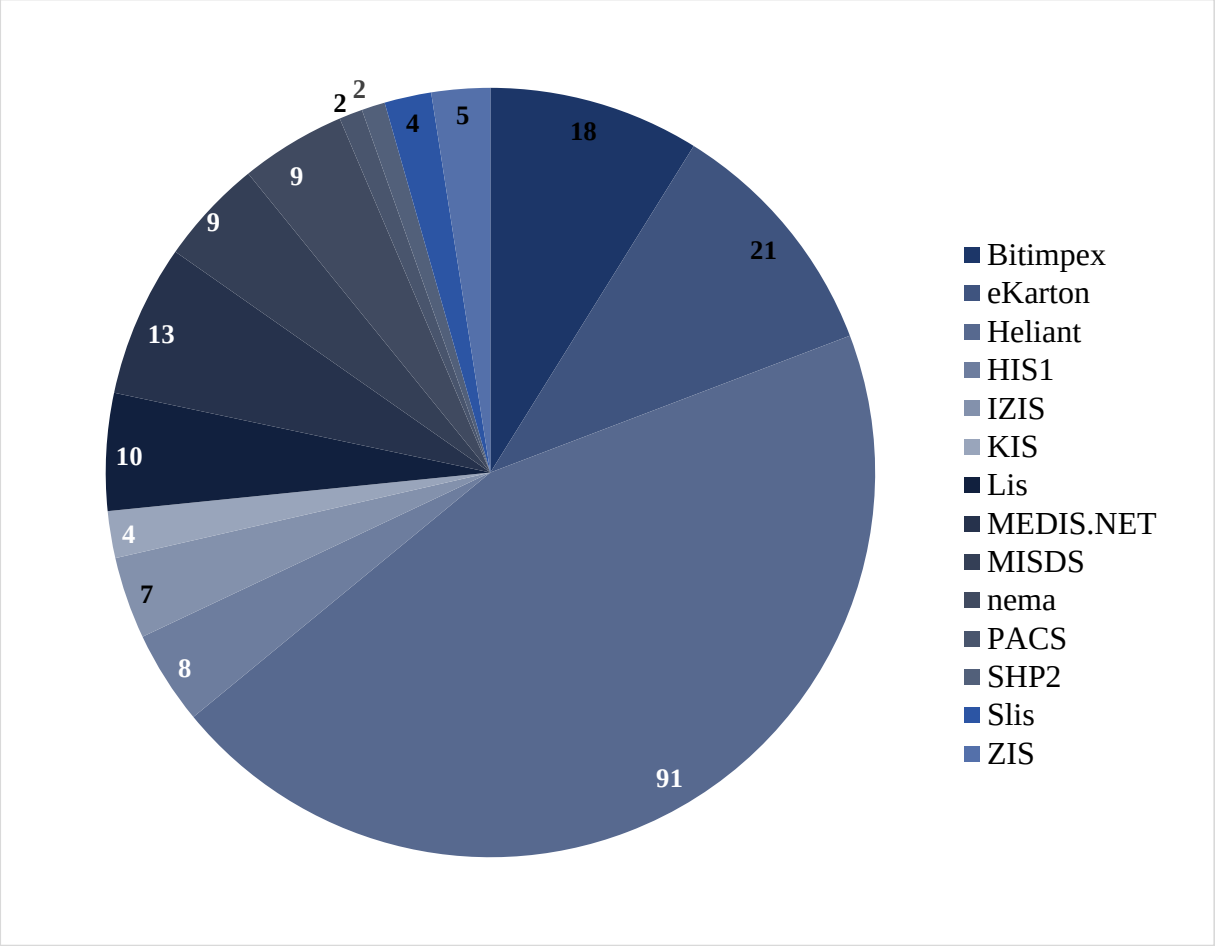
Прилог 1. Методологија у поступку рада

У току предревизије послали смо упитник на 349 здравствених установа од којих смо тражили следеће податке:

- Назив установе
- Назив здравственог информационог система
- Број запослених
- Број корисника система

На упитник је одговорило 203 здравствене установе где смо дошли до следећих информација:

- Број различитих информационих система је 25 (не рачунајући ИЗИС);
- Број корисника система је 53180.



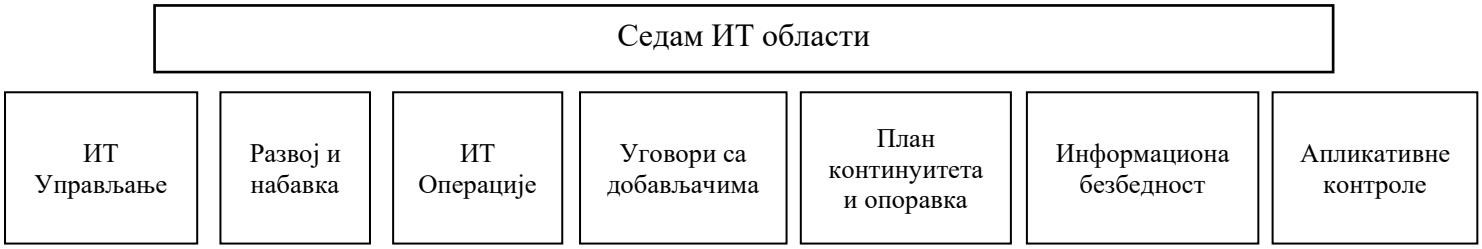
Илустрација 35. *Заступљеност ИТ система у здравственим системима*

Узорковање

Приликом формулисања ревизорских питања, првобитан одлука у фази планирања ревизије, била је да извор информација чини 82 здравствене установе. Део здравствених установа је по плану требало обићи на терену – лично и том приликом им дати упитник који је потребно да попуне, а одређеном броју здравствених установа требало је послати на имејл наведени упитник. С обзиром на новонасталу ситуацију изазвану пандемијом вируса COVID-19, нисмо успели да обиђемо све планиране здравствене установе (укупно 9), због чега је упитник за формулисање ревизорских питања упућен на укупно 73 здравствене установе (од чега део лично приликом посете здравственим установама, пре појаве пандемије вируса COVID-19, а део слањем путем имејла). У следећој фази, када смо прикупљали информације од здравствених установа, захтеве за истим смо упутили на свих 82 здравствене установе.

Критеријуми за одабир здравствених установа били су:

- географска припадност (пет региона – Војводина, Београдски регион, Шумадија и западна Србија, Источна и јужна Србија и Косово и Метохија)
- здравствени информациони систем (седам најзаступљенихјих информационих система у здравственим установама (Heliant; Bitimpex; eKarton; HIS1; MEDIS.NET; MISDS; ИЗИС)
- збирни пондер (Збирни пондер смо рачунали тако што смо сабирали пондер броја запослених са пондером броја корисника информационог система. Пондер броја корисника информационог система смо опет добили тако што смо број корисника информационог система који поседује здравствена установа делили са најмањим бројем корисника тог истог информационог система у осталим здравственим установама.



Илустрација 36. *ИТ области*

Упитник садржи питања која обухватају значајна подручја у вези са информационим системом Сва питања у упитнику подељена су у седам области и груписана у посебним табелама.

На основу прикупљених података ревизорски тим је одрадио процену ризика где је сваки члан понаособ доделио одређену оцену ризика. Сабирањем оцена закључено је да три области – ИТ управљање, Континуитет пословања, опоравак од катастрофе и управљање резервним копијама, и Информациона безбедност података у највећом мери одређују ризик када је у питању безбедност (осетљивих, здравствених) података осигураника у Републици Србији, и пружају простор да се ово питање уреди на

модернији и свеобухватнији начин. Не постоји идеално решење, али је циљ ове ревизије да се дође до бољег решења у овој области него што је то сада.

У циљу одговора на ревизорска питања, а имајући у виду законодавни и институционални оквир у периоду 2017 – 2019. године, за субјекте ревизије изабрани су:

- Министарство здравља,
- Институт за јавно здравље Србије „Др Милан Јовановић-Батут“,
- Покрајински секретаријат за здравство Војводине.

Да бисмо одговорили на ревизорска питања, анализирали смо законодавни и институционални оквир, као и:

1. За прво ревизијско питање:

- Преглед докумената да би се осигурало да су нови пословни захтеви идентификовани и анализирани у складу са правилима за управљање захтевима.
- Преглед одобрених или одбијених захтева да би се осигурало да су они у складу са прихваћеним принципима пословања.
- Интервјуисање руководства или других одговорних лица за одобравање пројеката да би се утврдило да су они узели у обзир ИТ организационе способности, вештине, ресурсе и обуку, и могућност да се користе нови алати методе или процедуре.
- Периодичан преглед белешки са састанка руководства да би се осигурало да су стратешке ИТ одлуке донете на највишем нивоу.
- Преглед ИТ стратегије или интервјуисање руководства да би се утврдили неопходни ресурси и на који начин су они утврђени и одобрени.
- Преглед организационих шема да би се утврдило да је ИТ организација успостављена на стратешком нивоу.
- Преглед ИТ организационе шеме да би се утврдило да је усклађена тако да пружа потребну подршку и у складу са законским обавезама.
- Разговори са запосленима који су одговорни за поштовање правила и процедура да би се утврдило колико често они извештавају више руководство о својим резултатима и на који начин они анонимно и независно траже податке о непоштовању.
- Разговори са руководиоцима и корисницима да би се разумело њихово виђење и став у вези са анализом правила и процедура. У случају честог мишљења: Процедуре су комплексне - питати које процедуре и на који начин би се могле поједноставити.
- Преглед историје контроле промена правила и процедура да би се утврдило да су правила ажурирана периодично или по потреби.
- Преглед механизама (електронске, физичке поште, обука, итд.) да би се осигурало да су правила дистрибуирана запосленима онда када се ажурирају или када за то постоји потреба
- Преглед политика или правила за решавање питања непоштовања правила и процедура
- Преглед плана за управљање ризицима или осталих докумената да би се осигурало да су одговорности за управљање ризицима јасно и недвосмислено додељене
- Преглед докумената да би се утврдило да ли су ИТ ризици део општег оквира за управљање ризицима и усклађености.

- Преглед белешки са састанка да би се осигурало да су нови ризици анализирани.
- Интервјуисање запослених одговорних за управљање ризицима да би се утврдило да ли је решавање ризика имало одговарајуће процене трошкова.
- Интервјуисање руководства или преглед белешки са састанака да би се утврдила да је руководство свесно и ИТ и осталих ризика, и да периодично прати њихов статус.

2. За друго ревизијско питање:

- Преглед докумената за процену да су правила и процедуре у складу са општим ИТ правилима и процедурама организације
- Преглед докумената да би се проценило да правила и процедуре узимају у обзир захтеве за континуитет пословања кроз дефинисање организационих циљева за непредвиђене ситуације.
- Преглед или интервјуисање запослених да би се утврдило колико често се правила и процедуре за континуитет пословања ажурирају уколико се промене услови.
- Преглед докумената да би се проценило да план за прављење резервних копија садржи све кључне хардвере, податке, апликативне софтвере
- Преглед докумената да би се проценило да су израђене детаљне процедуре за прављење резервних копија
- Преглед докумената да би се проценило да се план за прављење резервних копија адекватно спроводи
- Анализа евидентирања да би се проценило да је прављене резервних копија почелу у утврђеним временским оквирима и да су резервне копије задржане за назначен временски период
- Провера да је доступна права верзија резервне копије
- Преглед докумената да би се проценила адекватност локације резервне копије и начина транспорта датотека, итд., резервне копије на локацију резервне копије
- Провера да је безбедност, како логична тако и физичка, адекватна за локацију резервне копије
- Провера да се резервне копије датотека могу користити за опоравак
- Преглед докумената да би се проценило да су израђене детаље процедуре за опоравак и да садрже параметре за поновно постављање система, инсталационе закрпе, успостављајући поставку конфигурације, доступност системске документације и оперативних процедура, реинсталацију апликативних и системских софтвера, доступност најновијих резервних копија, тестирање система
- Преглед докумената да би се проценило да је ИТ кадар обучен на пољу процедура за прављење резервних копија и опоравак.
- Преглед докумената да би се проценило да ли су све релевантне ставке обухваћене тестирањем
- Преглед докумената да би се проценило да ли се реализују тестирања у одређеним временским интервалима, и благовремено
- Преглед докумената да би се проценило да су препоруке након тестирања адекватно праћене и да су план за континуитет пословања и план за опоравак након катастрофе адекватно ажурирани

- Провера да ли организација контролише да ли су сачувани број и статус датотека, апликативног софтвер и хардвера током прављења резервних копија и поступка опоравка података у спољно ангажованој агенцији
- Провера да ли организација контролише да ли су подаци, апликативни софтвер и хардвер били подвргнути променама током поступка прављења резервне копије или током опоравка након катастрофе кроз студију контролних алата о броју евиденција и величини докумената који се односе на податке и апликативни софтвер спољно ангажоване агенције
- Провера да ли организација контролише да ли је било неког кршења безбедносних правила кору проверу евиденције (физичке и логичне)
- Провера да ли организација контролише да ли је осигурано тестирање резервне копије и плана за опоравак након катастрофе код спољно ангажоване агенције
- Провера да ли је организација упозната са повезаним ризицима код могућег преузимања пружаоца услуге
- Провера да ли се организација постарала да је континуитет пословања садржан у споразум о пружању услуге

3. За треће ревизијско питање:

- У одсуству писане ИТ стратегије, интервјуи са највишим руководством, руководством средњег нивоа и запосленима да би се утврдило колико разумеју стратешку улогу безбедности информација.
- Провера да ли план ИТ безбедности идентификује: улоге и одговорности руководства и свих корисника, свест и обуку о безбедности.
- Провера извештаја о безбедносним инцидентима и докумената за праћење како би се утврдило које активности установа предузима када појединци крше безбедносна правила и процедуре.
- Провера извештаја о инцидентима да би се идентификовао број кршења безбедности информација од стране запослених или трећих лица у датом периоду, у циљу процене ефективности правила и процедура.
- Провера процедуралних мера које је установа предузела да би се ускладила са захтевима поверљивости.
- Провера да ли уговорни услови и обавезе дефинишу безбедносна ограничења и обавезе које контролишу како ће извођачи користити имовину организације и приступати информационим системима и услугама.
- Провера да ли су извођачи извршили повреде безбедности информација. Провера активности руководства у погледу таквих кршења.
- Утврђивање да ли је одговорност за ИТ безбедност формално и јасно наведена.
- Прегледање матрица улога за утврђивање одговорности за администрирање конфигурације и опсега контроле конфигурације у операцијама.
- Утврђивање да ли су се у прошлости јављали проблеми због конфигурацијских недоследности. Ако је тако, интервјуи са руководиоцима да би се проверило који су поступци примењени при променама конфигурације
- Анализа шта су примарне контроле физичке безбедности организације субјекта ревизије. Провера да ли одговарају најновијој анализи ризика.
- Прегледање локацијских и физичких мера предострожности у смислу кључних елемената ИТ инфраструктуре. Провера какве су контроле за заштиту животне средине успостављене (апарат за гашење пожара, аларм, системи за напајање, итд.)
- Утврђивање да ли су спроведене препоруке релевантних служби.

- Одабир узорка корисничких и системских налога да би се утврдило постојање јасно дефинисане улоге и/или привилегије мапиране према функцијама посла као и овлашћење власника података и руководства (тј. потписане/ писане сагласности)
- Провера процедура у циљу утврђивања колико често се прегледају различити приступи и привилегије које запослени или корисници имају у организацији.
- Интервјуи са узорком корисника и провера упутства да би се утврдило како су корисници упознати са својим одговорностима за заштиту осетљивих информација или имовине, када им се одобри приступ
- Анализа других привилегија осим лозинке, нпр. како се проверава да ли корисник заиста има довољан приступ и привилегије за тражени ресурс? (Примери укључују приступ са сигурне локације, хардверске токене или читаче отисака прстију, итд.)
- Тест ваљаности 1: Оперативна ефективност премештаја и прекида радног односа:
- Прибављање од кадровског одељења узорка премештаја запосленог и прекида радног односа и, кроз прегледање профила системских налога утврђивање да ли је приступ исправно измењен и/или укинут благовремено.
- Тест ваљаности 2: Управљање лозинком:
- Провера да ли су квалитативни захтеви за лозинке дефинисани и примењени системом за управљање мрежом и/или оперативним системима заснованим на локалним захтевима/ организационим правилима и процедурама или најбољој пракси.
- Провера приватности и безбедности поступања са излазним информацијама и процедура задржавања. Процена да ли су процедуре дефинисане тако да захтевају евидентирање потенцијалних грешака и њихово решавање пре дистрибуције извештаја.
- Провера да ли постоје документоване процедуре за обележавање осетљивих излазних информација апликација и, где је то потребно, слање осетљивих излазних информација на посебне уређаје са контролом приступа.
- Добијање документације и процена пројекта, имплементације, приступа и прегледање основе за ревизијски траг. Провера структуре основе за ревизијски траг и других докумената да би се потврдило да је основа за ревизијски траг ефективно пројектована. Испитивање ко може онемогућити или избрисати основе за ревизијски траг.

Обавили смо интервјуе са одговорним лицима Министарства здравља и Покраинског секретаријата за здравство Војводине (посебно запосленима у организационим јединицама које се баве ИТ пројектима), запосленима у институту за јавно здравље Србије „Др Милан Јовановић Батут“ као и у здравственим установама које смо посетили.

Такође, у циљу прикупљања доказа и одговора на ревизорска питања, послати су је велики број захтева за доставу одговора запосленима у здравственим установама како би одвојено посматрали како је успостављен систем код субјеката ревизије, а како код здравствених установа:

1) Да ли су донели ИТ Стратегија (или други стратешки документ који се односи на вишегодишње планирање управљања и развоја ИТ у вашој установи)
2) Да ли су донели Акт о информационој безбедности
3) Да ли су донели План континуитета пословања
4) Да ли су донели План опоравка од катастрофе (у случају ванредних околности)

5) Да ли имају извештаје од спроведеним тестирањима ових планова
6) Да ли су донели политике и процедуре које се односе на ИТ
7) Да ли су донели Акт о процени (и управљању) ИТ ризицима
8) Евиденција о изради резервних копија (дневна, месечна, итд)
9) Стратегија (план) у случајевима прекида сарадње са пружаоцем услуга
10) Стратегија (план) у случајевима прекида сарадње са пружаоцем услуга
11) Да ли имају извештаје о спроведеним обукама запослених у вези ИТ
12) Уговоре са пружаоцима услуга када су у питању здравствени информациони системи
13) Извод акта (правилника) о систематизицији радних места који се односи на ИТ
14) Извод из главне књиге/аналитичка картица који се односи на плаћања за све ИТ послове/услуге везане за здравствебни информациони систем (по врсти) и за набавку и одржавање хардвера. Потребни подаци које смо тражили односе на године 2017., 2018. И 2019.
15) Да ли су донели одлуку (решење) о одређивању одговорног лица за обавештавање надлежних органа о инцидентима у ИКТ систему
16) Евиденцију која садржи списак лица која користе информациони систем, са њиховим правима приступа, и датумима добијања односно укидања права приступа систему
17) Документацију о физичко-техничким мерама заштите просторија у којима се налазе средства и документи информационог система, као и извештаје релевантних служби (ако их је било) о периодичном тестирању примењених мера (ватрогасна служба и слично)
18) Списак докумената о сачуваним догађајима у ИТ систему (лог фајлова) који обухватају активности корисника, и догађаје у вези нарушавања информационе безбедности
19) Записнике са састанака који се односе на безбедност информационих система
20) Извештаје који се односе на обуке запослених у вези безбедности ИС (обуке екстерне/интерне/вебинари/преко мејлова)
21) Извештаје о активностима и предузетим мерама у случају нарушавања информационе безбедности (ако је таквих случајева било)
22) Ажурну листу e-mail адреса здравствених установа чији сте оснивач, или сте задужени за део послова на управљању информационим системом који те установе користе
23) Извештаје о интерним или екстерним ревизијама информационог (информационих) система које користите и/или којима управљате
24) Мере за обезбеђење сигурности података и Одлуку о одређивању лица за заштиту података о личности.