ДРЖАВНА
РЕВИЗОРСКА
ИНСТИТУЦИЈА

ИЗВЕШТАЈ
О РЕВИЗИЈИ СВРСИСХОДНОСТИ ПОСЛОВАЊА
Информациони системи у правосуђу

Број: 400-1033/2022-03/10
Београд, 10. јануар 2023. године

НЕОПХОДНО ЈЕ ДА МИНИСТАРСТВО ПРАВДЕ УНАПРЕДИ УПРАВЉАЊЕ, ОБЕЗБЕДИ ВИШИ НИВО ПОУЗДАНОСТИ ИНФОРМАЦИОНИХ СИСТЕМА И ОМОГУЋИ ГРАЂАНИМА КОРИШЋЕЊЕ ДОДАТНИХ ЕЛЕКТРОНСКИХ УСЛУГА

Правосудни информациони систем (ПИС) је прави пример тога како дигитализација може довести до ефикаснијег рада и значајних уштеда. Како процењује Министарство правде, уштеда од почетка примене је већа од седам милијарди динара. Ипак, поред нових функционалности неопходно је усавршавати и све друге компоненте информационих система. Проблеми који су идентификовани у досадашњем периоду коришћења информационих система у правосуђу су: застарели рачунари и небезбедни оперативни системи, информациона безбедност није на неопходном нивоу јер није организационо и нормативно уређена, није обезбеђен континуитет пословања у ванредним околностима и у случају раскида сарадње са пружаоцима услуга, пружалац услуге има приступ продукционој бази, обрада података о личности није уређена тако да су јасно разграничене улоге Министарства правде, судова и пружалаца услуга.

Управљање информационим системима АВП, СИПРЕС, САПС и ПИС потребно је уредити тако да се омогући равноправно коришћење папирних и електронских докумената и на тај начин додатно повећа ефикасност система, омогуће додатне још значајније уштеде и грађанима пруже нове е-услуге, процедурама уреде послови који се односе на овај систем и финансијским плановима омогући замена старих и небезбедних рачунара и оперативних система.

Систем **информационе безбедности** је неопходно унапредити применом додатних неопходних мера заштите које обухватају усвајање и примену аката и процедура које се односе на ову област, одговарајућу ИТ организациону структуру, управљање континуитетом пословања и управљање ИТ ризицима.

Потребно је унапредити механизам **сарадње са пружаоцима услуга** одговарајућим процедурама које треба да уреде мере заштите система, и омогуће контролу примене тих мера. Такође, обраду података о личности треба уредити на јасан начин, заснован на примени законских одредби

Препоруке

Државна ревизорска институција је након спроведене ревизије Министарству правде, између осталих, дала следеће препоруке:

- да приликом будућег развоја и одржавања информационих система омогући равноправно коришћење папирне и електронске документације,
- да приликом припреме финансијских планова осигура стабилно финансирање циљева који обухватају одрживи развој, набавку и одржавање свих компоненти информационих система (хардвер, софтвер, људске ресурсе, стручну обуку),
- да усвоји и имплементира правила и процедуре за безбедност података када је у питању сарадња са пружаоцима услуга, што подразумева обавезну примену мера заштите података, и успостављање механизма за праћење примене тих мера,
- да успостави континуитет пословања у ванредним околностима тако да обезбеди функционисање система у ванредним ситуацијама и у случају прекида сарадње са пружаоцима услуга, а што подразумева неопходан хардвер, апликативни софтвер, изворни код, стручно знање, базе података, управљање резервним копијама података, и процес тестирања планова континуитета пословања,
- да изради и судовима упути одговарајућа упутства у циљу успостављања мера информационе безбедности, управљања ИТ ризицима, усвајања и имплементирања процедура за безбедност података када је у питању сарадња са пружаоцима.

Садржај

Скраћенице и термини

Табела број 1: Најчешће коришћене скраћенице у извештају

Пун назив	Скраћеница
Информациони системи у правосуђу	ИСП
Аутоматско вођење предмета	АВП
Правосудни информациони системи	ПИС
Стандардизована Апликација Правосуђа Србије	САПС
СИстем ПРЕкршајних Судова	СИПРЕС
Министарство правде	МП
Информациони систем	ИС
Информационо-комуникациони систем	ИКТ систем
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 „Информациони системи у правосуђу“.

У области правосуђа у Републици Србији, у употреби је више од 20 информационих система, који се користе за вођење предмета, размену података, увид у податке итд. Користе се у основним, вишим и апелационим судовима, прекршајним и привредним судовима, основним, вишим и апелационим јавним тужилаштвима, итд.

Систем АВП (Аутоматско Вођење Предмета) представља децентрализован систем који је развијен још 2006. године који користе основни и виши судови (осим Вишег суда у Сремској Митровици), а од 2008. године и привредни судови. Централизовани информациони систем САПС (Стандардна АПликација Судова) је у употреби у Вишем суду у Сремској Митровици, апелационим судовима у Београду, Новом Саду, Нишу и Крагујевцу, Управном суду и Врховном касационом суду. Такође, централизовани информациони систем СИПРЕС (СИстем ПРЕкршајних Судова) је од 2012. године у употреби у прекршајним судовима. ПИС (Правосудни Информациони Систем) је систем који корисницима омогућује приступ подацима из различитих државних регистара, такође је у питању централизовани информациони систем. Поред ових система (који су предмет ове ревизије), у употреби су и други информациони системи, као што су еТабла, еСуд, Регистар неплаћених казни, база опортунитета, ПроНеп, еЗИО, Лурис итд.

Проблеми идентификовани у току предстудије и у току коришћења система у вези су са оперативним системима који су у добром броју застарели (више немају подршку што се тиче безбедоносних закрпа, самим тим су и небезбедни), затим – није обезбеђен континуитет пословања у случају раскида сарадње са пружаоцима услуга, пружаоци услуга имају потпун приступ систему и продукционој бази, обрада података о личности коју врши пружалац услуга није у потпуности успостављена на јасан, законом прописан начин, информациона безбедност није на потребном нивоу и нивоу који је законом прописан итд.

Циљ ревизије је да се оцени ефективност информационих система у правосуђу у Републици Србији.

Набавку и одржавање информационих система који се користе у правосуђу врши Министарство правде. Када су у питању централизовани информациони системи (САПС, СИПРЕС и ПИС), администрирање врше запослени у Министарству правде, док у сваком суду који користи АВП администрирање обављају запослени у том суду. Одржавање софтвера врше пружаоци услуга на основу годишњих уговора које потписују са Министарством правде. Пружаоци услуга имају приступ продукционој бази. Како би се препоруке могле имплементирати и у Министарству правде, али и у свим судовима, а како је са друге стране немогуће да сви судови буду субјекти ревизије па да им се на тај начин упуте препоруке, за субјект је одабрано Министарство правде које ће оне препоруке које се односе и на судове упутити сваком суду појединачно.

У току ревизије је спроведена анкета (упитник) која је обухватила све судове чије смо контакт податке добили од Министарства правде, анализирана је достављена документација, обављен је један број интервјуа са представницима Министарства правде, и коришћени су јавно доступни подаци. У току ревизије, судови обухваћени анкетом су били извори информација.

Након спроведене ревизије утврдили смо:

Неопходно је да Министарство правде унапреди управљање, обезбеди виши ниво поузданости информационих система и омогући грађанима коришћење додатних електронских услуга

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

1. Ефективно управљање информационим системима у правосуђу није у потпуности успостављено због недостатка финансијских средстава у буџету Министарства правде за финансирање информационих система (дакле не мисли се само на годишње одржавање софтвера, потребно је финансирати и обнављање опреме, других компоненти, набавку нових верзија софтвера, антивирусних пакета, обуку ИТ кадра итд.), зато што организација ИТ није успостављена тако да су усвојена правила и процедуре у области ИТ и да је организациона структура таква да може да одговори захтевима који обухватају сложеност послова, континуитет пословања и контролу, и што није омогућено равноправно коришћење електронских и папирних докумената.

Није обезбеђено стабилно финансирање информационих система у правосуђу због недостатка финансијских средстава, што за последицу има застареле рачунаре и застареле, самим тим и небезбедне оперативне системе, као и недовољан број запослених на ИТ пословима. Законом о уређењу судова прописано је да су, између осталог, послови правосудне управе које врши министарство надлежно за правосуђе: уређење и развој правосудног информационог система. Број запослених на ИТ пословима у суду одређује председник суда актом о унутрашњем уређењу и систематизацији радних места у суду, у складу са кадровским планом. (Препорука број 1)

Због тога што сваки суд посебно уређује ИТ послове, на нивоу целокупног система правосуђа није успостављено управљање тако да су прописане процедуре које уређују ову област и није успостављена адекватна ИТ организациона структура, што за последицу има отежану или онемогућену контролу обављања ових послова, континуитет пословања и/или пренос знања у случају раскида радног односа са запосленим који обавља те послове, или замену запосленог. Потребно је обезбедити одговарајући ниво образовања и способности лицима који управљају и користе систем, неопходно је успоставити праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу, тачније, потребно је процедурама уредити ове и друге послове како је прописано Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја. (Препорука број 2)

Због функционалних недостатака у садашњим софтверским решењима и потребе за изменом одговарајућих закона, није омогућено равноправно коришћење папирних и електронских докумената, у складу са Законом о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању, што за последицу има смањену ефикасност система и то – како у случају финансијских средстава која се троше због папирне доставе, тако и када је у питању време потребно за штампу, паковање, слање и доставу. (Препорука број 3)

2. Министарство правде и судови нису успоставили управљање информационом безбедношћу информационих система у правосуђу на свеобухватан начин јер нису усвојене и примењене мере заштите које обухватају управљање ИТ ризицима, организациону ИТ структуру и усвајање и примену одговарајућих правила и процедура у области информационе безбедности и управљање процесом континуитета пословања, што је неопходно како би била осигурана поузданост система.

Организација ИТ безбедности у правосуђу, због недостатка довољно стручног знања и недостатка кадровских капацитета, није успостављена тако да обухвата примену адекватних докумената која уређују ову област – акт о информационој безбедности, управљање инцидентима, приступ систему и примену других мера заштите ИКТ система, и адекватну организациону структуру ИТ безбедности, што за последицу има већи степен рањивости информационог система. (Препоруке број 4 и 5)

Министарство правде и судови у Србији, због тога што не располажу потребним ресурсима, нису у потпуности успоставили мере које обезбеђују континуитет пословања у ванредним околностима и у случају прекида сарадње са пружаоцем услуга за последицу може имати нефункционисање информационог система у дужем временском периоду. (Препоруке број 6 и 7)

Министарство правде и судови у Србији, због непознавања ове проблематике, недовољно искуства и обученог ИТ кадра, нису успоставили управљање ИТ ризицима, 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. Нарочито када се документација налази у електронском облику. (Препоруке број 8 и 9)

3. Није успостављен ефективан механизам сарадње Министарства правде и судова са пружаоцима услуге, зато што нису усвојена и имплементирана правила и процедуре када је у питању ова област, пружаоци услуга имају приступ продукционим базама и процес обраде података о личности није уређен на начин прописан законом.

Због недовољно стручног кадра и знања, Министарство правде и судови у Србији нису усвојили и имлементирали правила и процедуре које се односе на безбедност података када је у питању сарадња са пружаоцима услуга. Поред тога што у уговорима са пружаоцима услуга постоји део који се односи на поверљивост података, није успостављен механизам за контролу којим се утврђује да ли пружалац услуга поштује обавезе у вези са поверљивошћу података па је нижи и степен поузданости система. Пружаоци услуга имају приступ продукционим базама. Законом о информационој безбедности и Уредбом о ближем уређењу мера заштите информационо-комуникационих система прописана је обавеза обезбеђивања механизма који одржава уговорени ниво. (Препоруке број 10 и 11)

Министарству правде препоручујемо да уреди процес обраде података када је у питању сарадња са пружаоцима услуга на начин који јасно разграничава улоге Министарства, судова и пружалаца услуга када је у питању обрада података о личности. (Препорука број 12)

Државна ревизорска институција, након спроведене ревизије „Информациони системи у правосуђу, даје следеће препоруке:

Министарству правде да:

1. приликом припреме финансијских планова осигура стабилно финансирање циљева који обухватају одрживи развој, набавку и одржавање свих компоненти информационих система (хардвер, софтвер, људске ресурсе, стручну обуку). (приоритет 2[1]);
2. изради и судовима упути одговарајућа упутства у циљу успостављања организационе ИТ структуре и процедура које ће дефинисати послове који се односе на ИТ и обезбедити континуитет обављања послова у случају замене запослених на ИТ пословима. (приоритет 2);
3. приликом будућег развоја и одржавања информационих система омогући равноправно коришћење папирне и електронске документације. (приоритет 2);
4. успостави мере информационе безбедности које обухватају усвајање и имплементацију аката која уређују ову област – акт о информационој безбедности, управљање инцидентима, приступ систему , и адекватну организациону структуру ИТ безбедности, како би биле примењене све неопходне мере безбедности и заштите података у информационим системима у правосуђу (приоритет 2);
5. изради и судовима упути одговарајућа упутства у циљу успостављања мера информационе безбедности које обухватају усвајање и имплементацију аката која уређују ову област – акт о информационој безбедности, управљање инцидентима, приступ систему , и адекватну организациону структуру ИТ безбедности, како би биле примењене све неопходне мере безбедности и заштите података у информационим системима у правосуђу (приоритет 2);
6. изради и судовима упути одговарајућа упутства у циљу успостављања континуитета пословања у ванредним околностима тако да обезбеде функционисање система у ванредним ситуацијама и у случају прекида сарадње са пружаоцима услуга, а што подразумева неопходан хардвер, апликативни софтвер, изворни код, стручно знање, базе података, управљање резервним копијама података, и процес тестирања планова континуитета пословања. (приоритет 2);
7. успостави континуитет пословања у ванредним околностима тако да обезбеди функционисање система у ванредним ситуацијама и у случају прекида сарадње са пружаоцима услуга, а што подразумева неопходан хардвер, апликативни софтвер, изворни код, стручно знање, базе података, управљање резервним копијама података, и процес тестирања планова континуитета пословања. (приоритет 2);
8. изради и судовима упути одговарајућа упутства у циљу успостављања управљања ИТ ризицима, што подразумева евидентирање, класификацију,

[1] ПРИОРИТЕТ 2 – Несврсисходности које је могуће отклонити у року до годину дана

анализу ИТ ризика и дефинисање стратегије за смањивање/отклањање ризика. (приоритет 2);

9. успостави управљање ИТ ризицима, што подразумева евидентирање, анализу, класификацију ИТ ризика и дефинисање стратегије за смањивање/отклањање ризика. (приоритет 2);
10. да изради и судовима упути одговарајућа упутства у циљу усвајања и имплементирања правила и процедура за безбедност података када је у питању сарадња са пружаоцима услуга, што подразумева обавезну примену мера заштите података, и успостављање механизма за праћење примене тих мера. (приоритет 2);
11. усвоји и имплементира правила и процедуре за безбедност података када је у питању сарадња са пружаоцима услуга, што подразумева обавезну примену мера заштите података, и успостављање механизма за праћење примене тих мера. (приоритет 2);
12. уреди процес обраде података када је у питању сарадња са пружаоцима услуга на начин који јасно разграничава улоге Министарства, судова и пружалаца услуга када је у питању обрада података о личности. (приоритет 2);

Генерални државни ревизор

_____

Др Душко Пејовић
Државна ревизорска институција
Макензијева 41
11000 Београд, Србија
10. јануар 2023. године

II Увод

Државна ревизорска институција спровела је ревизију сврсисходности на тему „Информациони системи у правосуђу“. Ревизија је спроведена у складу са Законом о Државној ревизорској институцији[2], Пословником Државне ревизорске институције[3] и Програмом ревизије Државне ревизорске институције за 2022. годину. Поступци ревизије су спроведени у периоду од маја до октобра 2022. 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

Циљ успостављања информационих система у правосуђу јесте ефикаснији рад правосудних органа, како у смислу уштеде у времену, тј. утрошених радних сати запослених у правосуђу за обављање својих послова, тако и у смислу финансијске уштеде.

Министарство правде је у претходном периоду, управо препознајући важност дигитализације, омогућило привреди и грађанима коришћење електронских услуга на порталима еУправа и еПравосуђе. Поред тога, донета је и Стратегија развоја ИКТ у правосуђу 2022–2027 године и, како је Министарство навело, у току је рад на више пројеката када је у питању примена информационих технологија у правосуђу.

На Порталу еУправе:

Грађани:

- Издавање уверења о вођењу кривичног поступка (КУ) (издаје суд)

Привреда:

- Издавање уверења о вођењу кривичног поступка (КУ) (издаје суд)
- Издавање уверења из Казнене евиденције правних лица (КЕПЛ)

[2] „Службени гласник РС“, бр. 101/05, 54/07, 36/10 и 44/18-др.закон
[3] „Службени гласник РС“, број 9/09

На Порталу правосуђа:

- Токови предмета у судовима и токови код јавног извршитеља https://portal.sud.rs/cr/tok-predmeta
- Регистар неплаћених казни и новчаних износа https://rnk.sipres.sud.rs/?lang=cyrl
- Електронско плаћање судских такси: https://etakse.sud.rs/
- Електронско вођење Управног спора https://etakse.sud.rs/
- Електронска Аукција https://eaukcija.sud.rs
- Електронска огласна табла https://etabla.sud.rs/
- База судске праксе https://sudskapraksa.sud.rs/sudska-praksa

Иако је успостављен један број услуга и олакшан и убрзан рад судова, али и других (као што су на пример јавни извршитељи), потребно је у наредном периоду систем унапредити тако да буде у складу са оним што је основна интенција дигитализације, а то је да се електронски документ може равноправно користити као и папирни, да се судовима могу подносити докази, дописи, поднесци итд. у електронском облику, да се електронским сертификатима могу потписивати пресуде, али и потврдити пријем итд. Са друге стране, управљање овим системом треба да обухвати све оне мере прописане у циљу успостављања адекватног нивоа информационе безбедности, што је дефинисано Законом о информационој безбедности, Законом о заштити података о личности итд., а што сада није случај.

У претходном периоду, установљено је да су постојали проблеми у вези са информационом безбедношћу у више области:

• Судови у Србији у једном броју користе застареле рачунаре на којима се користе застарели оперативни системи и антивирусна заштита.

• Није обезбеђен континуитет пословања у ванредним ситуацијама и у случају раскида уговора са пружаоцима услуга и у том случају био би отежан процес даљег одржавања и развоја система, због недостатка стручног кадра и скоро сигурних проблема са миграцијом база података.

• Пружалац услуге има приступ системима и продукционим базама података, без механизма који подразумева претходно одобрење и евидентирање разлога приступа.

• ИТ послови нису уређени одговарајућим процедурама, нарочито у области информационе безбедности, нити је обезбеђена неопходна ИТ организациона структура.

• Обрада података о личности коју врши пружалац услуга није у потпуности успостављена на јасан, законом прописан начин јер је суд руковалац, а у овом случају имајући у виду да имају увид у податке пружалац услуге обрађивач, а да руковалац и обрађивач нису потписали уговор и дефинисали обавезе, јер је Министарство правде набавило све системе и потписало уговоре.

2. Циљ ревизије

Циљ ревизије би био да се оцени ефективност информационих система у правосуђу.

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 1.3: Јавни ред и безбедност, област – Судови: ДРИ ће својим радом утврдити проблеме у наменској и сврсисходној реализацији средстава намењених за јавни ред и безбедност и предложити решења како би позитивно утицала на остваривање циљева и задатака из ове функције. У оквиру функционалне буџетске категорије 3 груписани су општи циљеви и задаци државе везани за јавни ред и безбедност. У буџетима на централном и локалном нивоу исказани су расходи и издаци за ову област, независно од организација које спроводе ову функцију. Области у овој функцији су: услуге полиције, услуге противпожарне заштите, судови, затвори, јавни ред и безбедност, истраживање и развој и јавни ред и безбедност некласификована на другом месту. На централном нивоу државе средства се одобравају Министарству унутрашњих послова (60%), судовима и тужилаштвима (27%) и осталима 13%. ДРИ ће вршити ревизију субјеката из ових области. Такође, 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)*. 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. Рад ДРИ ће помоћи да се унапреди способност ИТ система да сви јавни програми постану ефикаснији, а да се при томе штите кључно пословање и осетљиве информације.

3. Ревизијска питања

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

1. У којој мери је успостављено ефективно управљање информационим системима у правосуђу?
   1) Да ли је МП успоставило оквир за управљање информационим системом у смислу планирања, финансирања, успостављања неопходне организационе структуре и процедура које уређују ове послове и континуиране обуке?
   2) Да ли МП спроводи обуке у вези са управљањем и коришћењем информационих система и како управља хардверским ресурсима?

3) Да ли МП прикупља и анализира проблеме корисника, да ли је успостављена хелп-деск услуга, да ли се и како прикупљају, анализирају, одобравају и имплементирају захтеви за измене система?
4) Да ли је организација одобрила и користи одговарајућа правила и процедуре за управљане ИТ операцијама?
5) Да ли су неопходне информације доступне свим (потенцијалним) корисницима у информационом систему?

2. У којој мери успостављене мере информационе безбедности обезбеђују поузданост информационих система у правосуђу?
   1) Да ли постоје имплементирана правила и процедуре за информациону безбедност?
   2) Да ли је и на који начин у МП, судовима и тужилаштвима успостављена организација ИТ безбедности?
   3) На који начин су успостављене мере физичке заштите и контроле логичког приступа системима?
   4) На који начин се управља континуитетом пословања у ванредним околностима?
   5) На који начин се спроводи управљање ИТ ризицима?
   6) На који начин се у системима управља инцидентима?

3. У којој мери је успостављен механизам сарадње са пружаоцима услуга испунио све неопходне циљеве, укључујући и поузданост података?
   1) Да ли постоје правила и процедуре које се односе на безбедност података када су у питању уговори са пружаоцима услуга?
   2) Да ли постоји механизам којим се осигурава да је пружалац услуге усвојио услове за заштиту и безбедност података и да ли их спроводи?
   3) На који начин МП прати реализацију извршења уговора?

Како је циљ ревизије да се оцени ефективност информационих система у правосуђу у Србији, формулисали смо три питања која се односе на три најризичније области, по нашој оцени и процени ризика коју смо спровели на бази доступних тј. прикупљених података у досадашњем периоду рада на предстудији.

Прво питање се односи на ИТ управљање. Адекватно ИТ управљање је неопходно како би се управљало целим системом, тачније свим његовим компонентама почевши од планирања, израде и усвајања стратегије, акционог плана за примену стратегије, измене закона у складу са стратегијом итд., адекватног финансирања система, што подразумева претходно урађене анализе и усклађеност са акционим плановима за спровођење стратегије, затим јасно дефинисану организацију и правила и процедуре за ИТ послове, као и редовно спроведене ИТ обуке, управљање изменама система, што обухвата идентификације захтева, одобрења, имплементације измена, такође и управљање системом, што се у овом случају посебно односи на хардверски део – рачунаре и интернет. Такође, предмет ревизије у овом делу обухватиће и начин на који ИТ запослени управљају ИТ операцијама. На крају, потребно је спровести и

анализу којом се утврђује да ли су подаци које генерише систем доступни свима којима треба да буду доступни, и само њима.

Друго питање се односи на информациону безбедност, укључујући и континуитет пословања и у склопу тога управљање резервним копијама. Ризици у овој области се односе на усвајање и имплементацију планова и процедура које уређују ова питања, а што је и законска обавеза свих оператера ИКТ система од посебног значаја, успостављање одговарајуће организационе ИТ структуре, примену неопходних мера заштите система, како физичке заштите, тако и контроле логичког приступа и редовну контролу примене тих мера, успостављање континуитета пословања у ширем смислу, што подразумева и одговарајући план опоравка 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) и управљање резервним копијама, а што сада није случај. Безбедност података, а у овом случају се ради о осетљивим подацима, које третира Закон о заштити података и други закони, важно је питање ове ревизије, због чега се и анализирају сва остала питања. Управљање ИТ ризицима је такође потребно уредити на одговарајући начин, а што обавезно треба да обухвати идентификацију свих ИТ ризика, њихову оцену и доношење плана/стратегије за умањење или уклањање тих ризика, а то је и законска обавеза. Као последње питање у овој области, које се такође односи на законску обавезу, јесте управљање и пријављивање ИТ инцидената.

Треће питање се односи на успостављање ефективног механизма сарадње са пружаоцима услуга. Као и у случају претходна два питања, најпре се анализирају правила и процедуре које се односе на сарадњу са пружаоцима услуга, а посебно када је у питању ИТ безбедност, тј. заштита података. Такође, потребно је анализирати механизам за контролу спровођења уговора, нарочито у погледу поверљивости. У том смислу потребно је анализирати обавезе субјекта и судова у вези са Законом о заштити података о личности.

4. Обим и ограничења ревизије

Ревизијом смо обухватили активности Министарства у периоду од 2019. до 2021. године.

Предмет испитивања су биле области:

1) ИТ управљање – Зашто ова област? Зато што се може сматрати да је ИТ управљање 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 примењује неопходне политике и процедуре који се односе на ИТ систем[4];

2) 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[5];

3) Успостављање ефективног механизма сарадње са пружаоцима услуга како би се осигурало да се услуге пружају према очекивањима субјекта. Субјект ревизије треба да има процесе у циљу обезбеђивања периодичног праћења статуса пројекта, квалитета услуге и тестирања производа пре увођења у оперативно окружење. Осим тога, као део процеса праћења извршења обавеза пружаоца услуга, субјект ревизије може да врши и ревизију интерног процеса осигурања квалитета пружених услуга, како би се обезбедило да кадар пружаоца услуга прати уговорно одобрену политику и планове за све своје послове.[6]

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

5. Методологија у поступку рада

Да бисмо одговорили на ревизијска питања, анализирали смо законску и подзаконску регулативу, користили стручну литературу (WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions[7]), као и све податке добијене од субјекта ревизије и извора информација – судова. Анализирали смо податке и информације за период од 2019. до 2021. године. У вези са информационим системима АВП, САПС, СИПРЕС и ПИС, анализиране су области ИТ управљање, информациона безбедност и успостављање ефективног механизма сарадње са пружаоцима услуга.

У циљу потврђивања информација из документације и прикупљања података који нису доступни у документима, обавили смо интервјуе и послали упитнике корисницима наведених информационих система.

Детаљнији опис коришћене методологије дат је у Прилогу 1.

[4] WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions
[5] Члан 7. став 3. Закона о информационој безбедности
[6] WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions
[7] INTOSAI Радна група за ИТ ревизију

III Опис предмета ревизије

Судови користе више различитих система, издвојена су четири, од којих ПИС користе сви, док су АВП (основни судови), САПС (Апелациони судови, ВКС, Управни суд) и СИПРЕС (прекршајни судови) системи које наведени судови користе за вођење предмета.

Неким системима, или деловима система, управљају запослени ИТ стручњаци у судовима док неке системе (као што је ПИС) администрирају ИТ стручњаци у Министарству правде (МП).

Када су у питању информациони системи, предмет ревизије била би четири наведена система: АВП, САПС, СИПРЕС и ПИС.

Период обухваћен ревизијом је 2019–2021. година.

1. Законодавни и институционални оквир

Законодавни оквир

Законом о уређењу судова, у члану 70. прописано је да су између осталог послови правосудне управе које врши министарство надлежно за правосуђе: уређење и развој правосудног информационог система. Истим законом, у члану 57. прописано је да судско особље чине судијски помоћници, судијски приправници и државни службеници и намештеници запослени на административним, техничким, рачуноводственим, информационим и осталим пратећим пословима значајним за судску власт. Број судског особља одређује председник суда актом о унутрашњем уређењу и систематизацији радних места у суду, у складу са кадровским планом. Мерила за одређивање броја судског особља утврђује министар надлежан за послове правосуђа.

У члану 1. истог закона прописано је да су судови самостални и независни државни органи. Чланом 51. прописано је да Судску управу чине послови који служе вршењу судске власти, као и финансијском и материјалном пословању суда. Судска управа детаљније се уређује Судским пословником.

Чланом 52. прописано је да Председник суда руководи судском управом и одговоран је за правилан и благовремен рад суда.

Чланом 55а. прописано је да суд републичког ранга, апелациони суд и суд са 30 и више судија има управитеља суда. Председник суда поверава управитељу суда обављање материјално-финансијских и организационо-техничких послова. Послови управитеља суда се детаљније уређују Судским пословником.

У складу са Законом о информационој безбедности[8] ИКТ системи од посебног значаја су и системи који се користе у обављању делатности од општег интереса и у обављању послова у органима власти. Истим законом прописане су мере заштите ИКТ система од посебног значаја. Оператор ИКТ система од посебног значаја одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система.

Чланом 7. овог закона дефинисано је да се мере заштите ИКТ система, између осталог, односе 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.

Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја ближе се уређују мере заштите информационо-комуникационих система од посебног значаја.[9]

Чланом 2. ове уредбе уређено је успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система од посебног значаја.

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.[10]

Закон о заштити података о личности уређује 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.[11]

Члан 16. закона уређује пристанак малолетног лица у вези са коришћењем услуга информационог друштва, те је дефинисано да малолетно лице које је навршило 15 година може самостално да даје пристанак за обраду података о својој личности у

[8] „Службени гласник РС“, бр. 6/16, 94/17 и 77/19
[9] „Службени гласник РС“, број 94/16
[10] „Службени гласник РС“, број 94/16
[11] „Службени гласник РС“, број 87/18

коришћењу услуга информационог друштва. Ако се ради о малолетном лицу које није навршило 15 година, за обраду података пристанак мора дати родитељ који врши родитељско право, односно други законски заступник малолетног лица. Руковалац мора предузети разумне мере у циљу утврђивања да ли је пристанак дао родитељ који врши родитељско право, односно други законски заступник малолетног лица, узимајући у обзир доступне технологије.

Чланом 42. Закона о заштити података о личности прописано је да се мере заштите уређују 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, истим чланом прописано је 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).

Члан 45. овог закона прописује да 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 тако да 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).

Руковалац и обрађивач дужни су да предузму мере у циљу обезбеђивања система у којем 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).

Члан 56. став 2. тачка 1) прописује да су руковалац и обрађивач дужни да одреде лице за заштиту података о личности, ако се обрада врши од стране органа власти. Тачка 2) прописује да су руковалац и обрађивач дужни да одреде лице за заштиту података о личности ако се основне активности руковаоца или обрађивача састоје у радњама обраде које по својој природи, обиму, односно сврхама захтевају редован и систематски надзор великог броја лица на које се подаци односе.

Законом о електронском документу и електронској идентификацији, у члану 7. је прописано је да се електронском документу не може оспорити пуноважност, доказна снага, као ни писана форма само зато што је у електронском облику. Такође, у истом закону, у члану 15. је прописано да се електронско општење и електронско достављање између органа јавне власти и странака врши у складу са законом којим се уређује општи управни поступак, законом којим се уређује електронска управа и другим прописима, као и путем услуге квалификоване електронске доставе.

Закон о електронској управи као једно од начела наводи управо ефикасност управљања опремом, где прописује да је орган дужан да ефикасно управља опремом којом располаже тако да омогући њено правилно и економично коришћење.

Институционални оквир

Министарство правде обавља послове државне управе који се односе на:

- кривично законодавство и законодавство о привредним преступима и прекршајима;
- припрему закона којим се уређује право својине и друга стварна права;
- облигационе односе;
- наслеђивање;
- поступак пред судовима;
- управни спор;
- организацију и рад правосудних органа;
- правосудни испит;
- стручно усавршавање носилаца правосудних функција и правосудних професија;
- судске вештаке, преводиоце и тумаче;
- извршење кривичних санкција;

- рехабилитацију, амнестију и помиловање;
- изручењ;
- прикупљање података о извршеним кривичним делима против човечности и других добара заштићених међународним правом;
- доношење решења о предаји окривљених лица Међународном кривичном суду, а на основу правноснажних и извршних судских одлука;
- спровођење програма заштите учесника у кривичном поступку;
- адвокатуру и друге правосудне професије;
- бесплатну правну помоћ;
- судску стражу;
- статистику и аналитику рада правосудних органа и правосудних професија;
- одржавање, развој и координисање правосудног информационог система;
- међународну правну помоћ;
- управљање одузетом имовином проистеклом из кривичног дела;
- заступање Републике Србије пред Европским судом за људска права и старање о објављивању пресуда тог суда које се односе на Републику Србију и праћење њиховог извршења;
- припрему прописа о поступку пред Уставним судом и правном дејству одлука Уставног суда; припрему прописа у области борбе против корупције;
- усклађује међународну сарадњу у области борбе против корупције; припрему прописа о црквама и верским заједницама;
- регистар цркава и верских заједница;
- припрему прописа о заштити података о личности и тајности података;
- надзор над применом прописа који уређују тајност података;
- програмирање, спровођење и праћење спровођења пројеката који се финансирају из средстава претприступних фондова Европске уније, донација и других облика развојне помоћи из делокруга тог министарства;
- координацију активности осталих институција у оквиру свог делокруга у процесу програмирања, спровођења и праћења спровођења пројеката који се финансирају из средстава развојне помоћи, као и друге послове одређене законом.

Апелациони судови

Апелациони судови поступају у предметима односно надлежни су за подручја више виших судова. Седишта апелационих судова су у Београду, Новом Саду, Нишу и Крагујевцу. Апелациони суд одлучује по жалбама на одлуке основних судова, у случајевима у којима за одлучивање није надлежан виши суд, и о жалбама на одлуке виших судова.

Преглед организације Апелационих судова

- Апелациони суд у Београду
- Апелациони суд у Новом Саду
- Апелациони суд у Нишу
- Апелациони суд у Крагујевцу

Виши судови

Виши суд у првом степену суди за кривична дела за која је као главна казна предвиђена казна затвора преко десет година, суди за кривична дела: против човечности и других добара заштићених међународним правом, против Војске Србије; одавање државне тајне; одавање службене тајне; кривично дело прописано законом који уређује тајност података; позивање на насилну промену уставног уређења; изазивање националне, расне и верске мржње и нетрпељивости; повреда територијалног суверенитета; удруживање ради противуставне делатности; повреда угледа Републике Србије; повреда угледа стране државе или међународне организације; прање новца; кршење закона од стране судије, јавног тужиоца и његовог заменика; угрожавање безбедности ваздушног саобраћаја; убиство на мах; силовање; обљуба над немоћним лицем; обљуба злоупотребом положаја; отмица; трговина малолетним лицима ради усвојења; насилничко понашање на спортској приредби и јавном скупу; примање мита; злоупотреба положаја одговорног лица; злоупотреба у јавним набавкама, суди у кривичном поступку према малолетним учиниоцима кривичних дела; одлучује о молби за престанак мере безбедности или правне последице осуде за кривична дела из своје надлежности; одлучује о захтевима за рехабилитацију; одлучује о забрани растурања штампе и ширења информација средствима јавног информисања; суди у грађанскоправним споровима кад вредност предмета спора омогућује изјављивање ревизије; у споровима о ауторским и сродним правима и заштити и употреби проналазака, индустријског дизајна, модела, узорака, жигова, ознака географског порекла, топографије интегрисаних кола, односно топографије полупроводничких производа и оплемењивача биљних сорти ако није надлежан други суд; у споровима о оспоравању или утврђивању очинства и материнства; у споровима за заштиту од дискриминације и злостављања на раду; у споровима о објављивању исправке информације и одговора на информацију због повреде забране говора мржње, заштите права на приватни живот, односно права на лични запис, пропуштања објављивања информације и накнаде штете у вези са објављивањем информације; суди у споровима поводом штрајка; поводом колективних уговора ако спор није решен пред арбитражом; поводом обавезног социјалног осигурања ако није надлежан други суд; поводом матичне евиденције; поводом избора и разрешења органа правних лица ако није надлежан други суд.

Виши суд, у другом степену, одлучује о жалбама на одлуке основних судова у случајевима предвиђеним Законом о уређењу судова.

Преглед организације Виших судова

- Виши суд у Београду
- Виши суд у Ваљеву

- Виши суд у Врању
- Виши суд у Зајечару
- Виши суд у Зрењанину
- Виши суд у Јагодини
- Виши суд у Крагујевцу
- Виши суд у Краљеву
- Виши суд у Крушевцу
- Виши суд у Лесковцу
- Виши суд у Неготину
- Виши суд у Нишу
- Виши суд у Новом Пазару
- Виши суд у Новом Саду
- Виши суд у Панчеву
- Виши суд у Пироту
- Виши суд у Пожаревцу
- Виши суд у Прокупљу
- Виши суд у Смедереву
- Виши суд у Сомбору
- Виши суд у Сремској Митровици
- Виши суд у Суботици
- Виши суд у Ужицу
- Виши суд у Чачку
- Виши суд у Шапцу

Основни судови

Основни судови су првостепени судови опште надлежности. Основни судови поступају у предметима односно надлежни су за територију града, једне или више општина. На подручјима основних судова, у појединим општинама, поступа се у судским јединицама, преко којих грађани остварују своја права у поступцима, за које су надлежни основни судови који покривају територију те општине.

Основни суд пружа грађанима правну помоћ, међународну правну помоћ ако није надлежан други суд и врши друге послове одређене законом, а према чл. 23. ст. 2 истог закона – виши суд води поступак за изручење окривљених и осуђених лица, пружа међународну правну помоћ у поступцима за кривична дела из своје надлежности, извршава кривичну пресуду иностраног суда, одлучује о признању и извршењу страних судских и арбитражних одлука ако није надлежан други суд,

одлучује о сукобу надлежности основних судова са свог подручја, обезбеђује и пружа помоћ и подршку сведоцима и оштећенима и врши друге послове одређене законом.

Преглед организације Основних судова

- Први основни суд у Београду
- Други основни суд у Београду
- Трећи основни суд у Београду
- Основни суд у Алексинцу
- Основни суд у Аранђеловцу
- Основни суд у Бачкој Паланци
- Основни суд у Бечеју
- Основни суд у Бору
- Основни суд у Брусу
- Основни суд у Бујановцу
- Основни суд у Ваљеву
- Основни суд у Великој Плани
- Основни суд у Великом Градишту
- Основни суд у Врању
- Основни суд у Врбасу
- Основни суд у Вршцу
- Основни суд у Горњем Милановцу
- Основни суд у Деспотовцу
- Основни суд у Димитровграду
- Основни суд у Зајечару
- Основни суд у Зрењанину
- Основни суд у Ивањици
- Основни суд у Јагодини
- Основни суд у Кикинди
- Основни суд у Књажевцу
- Основни суд у Косовској Митровици
- Основни суд у Крагујевцу
- Основни суд у Краљеву
- Основни суд у Крушевцу

- Основни суд у Куршумлији
- Основни суд у Лазаревцу
- Основни суд у Лебану
- Основни суд у Лесковцу
- Основни суд у Лозници
- Основни суд у Мајданпеку
- Основни суд у Мионици
- Основни суд у Младеновцу
- Основни суд у Неготину
- Основни суд у Нишу
- Основни суд у Новом Пазару
- Основни суд у Новом Саду
- Основни суд у Обреновцу
- Основни суд у Панчеву
- Основни суд у Параћину
- Основни суд у Петровцу на Млави
- Основни суд у Пироту
- Основни суд у Пожаревцу
- Основни суд у Пожеги
- Основни суд у Прибоју
- Основни суд у Пријепољу
- Основни суд у Прокупљу
- Основни суд у Рашкој
- Основни суд у Руми
- Основни суд у Сенти
- Основни суд у Сјеници
- Основни суд у Смедереву
- Основни суд у Сомбору
- Основни суд у Сремској Митровици
- Основни суд у Старој Пазови
- Основни суд у Суботици
- Основни суд у Сурдулици
- Основни суд у Трстенику

- Основни суд у Убу
- Основни суд у Ужицу
- Основни суд у Чачку
- Основни суд у Шапцу
- Основни суд у Шиду

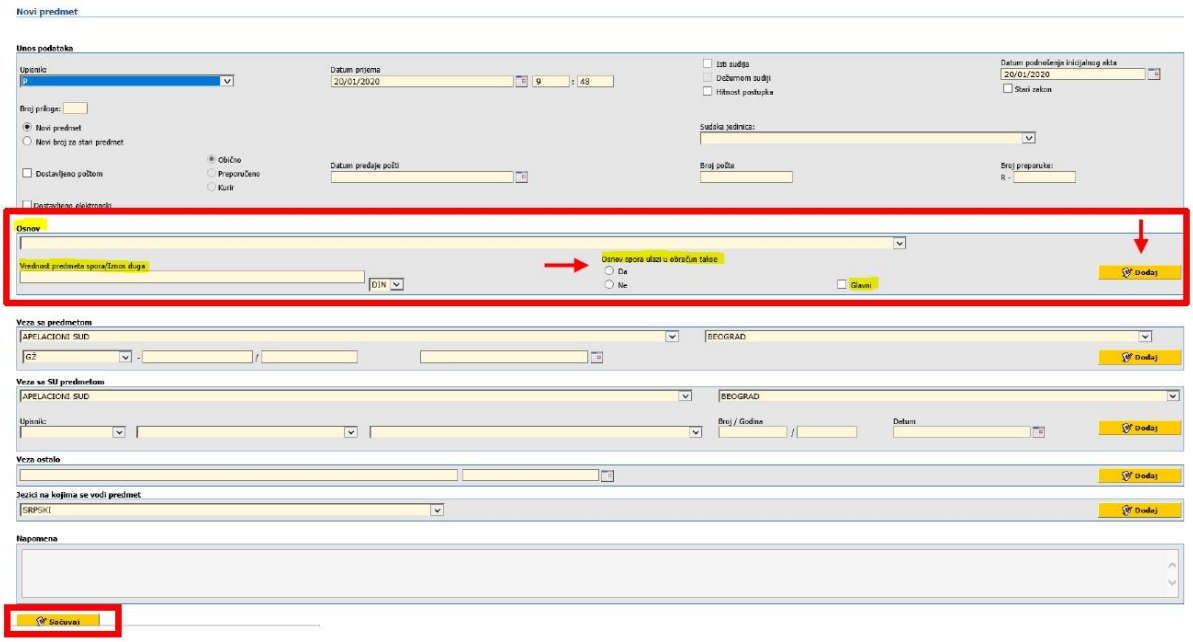
Судови опште надлежности	
Апелационих судова	4
Виших судова	25
Основних судова	66

Судови посебне надлежности			
Управни суд	1	**Прекршајних суд**	44
Седиште Управног суда у Београду	1	Одељења Прекршајног суда	3
Одељења Управног суда	3	**Привредни Апелациони суд**	1
Прекршајни Апелациони суд	1	**Привредних судова**	16
Седиште Апелационог суда у Београду	1	Подручја Виших судова	25

Илустрација 1. *Број судова у Републици Србији*

2. Информациони системи АВП, САПС, СИПРЕС и ПИС

АВП (Аутоматско Вођење Предмета). Сви основни и виши судови, осим Вишег суда у Сремској Митровици, са припадајућим судским јединица, користе децентрализован систем за управљање судским предметима, популарни назван АВП (аутоматско вођење предмета). Настао још давне 2006. године, АВП је информациони систем за управљање предметима на бази Adobe ColdFusion технологије. Ова врста архитектуре је данас застарела, а систем не представља document management system, јер не поседује ни један од елемената за ову технологију. Карактеристике у погледу могућности за међусобно повезивање АВП су на ниском нивоу и прецизност прикупљених података није задовољавајућа. Сви привредни судови користе АВП од 2008. године. Овај систем испуњава већину функционалности које су потребне привредним судовима, но иста врста проблема се јавља у погледу технологије и архитектуре самог решења. Извршава се на серверима који се налазе у судовима, за разлику од преостала три система.



Илустрација 2. *Изглед једне од функционалности система АВП*

САПС (Стандардизована апликација правосуђа Србије). САПС представља напор Министарства правде, да у сарадњи и кроз донације Европске Делегације у Србији, направи централни систем за управљање садржајем (енг. case management system), кроз унификацију свих процеса, чиме би се олакшало прикупљање прецизних информација о ефикасности у раду, како за судове, тако и за појединачне судије и пружи приступ јавних информације које се односе на судске поступке и статистику. САПС тренутно је у употреби у: Врховном касационом суду и Управном суду у Београду, свим Апелационим судовима (Београд, Ниш, Нови Сад и Крагујевац) и Вишем суду у Сремској Митровици. САПС је информациони систем која се води и којом се управља централизовано, за све типове судова и осмишљен је као модуларан софтвер, који је преузео све функционалности постојећег АВП система, али су додате и оне функције које нису биле имплементиране у АВП систему. Основу чини платформа за управљање садржајем (енг. Enterprise Content Management) да би пружио потпуну подршку процесу дигитализације докумената и послова који се обављају преко папирне документације у оквиру судова.

СИПРЕС. Прекршајни судови су тренутно у последњој фази имплементације информационог система на Windows технологији. Пројекат је започет средином 2012, са циљем да се аутоматизују ове врсте судова, односно да свих 45 прекршајних судова има аутоматизовани, централни информациони систем. Пројекат је финансиран од стране УСАИД-а кроз јединствену реформу прекршајних судова.

ПИС. Преко правосудног информационог система сви судови, јавна тужилаштва, јавни бележници и јавни извршитељи могу електронским путем проверити податке из Централног регистра обавезног социјалног осигурања (подаци о обавезном социјалном осигурању које послодавац плаћа за одређени временски период); Прекршајне евиденције (осуђујуће пресуде); Управе за извршење кривичних санкција (да ли особа

издржава казну у затвору); Министарства унутрашњих послова (подаци о пребивалишту и историји боравка, казнена евиденција); Матичне књиге (подаци из матичних књига рођених, умрлих, венчаних); Агенција за привредне субјекте (подаци о физичким и правним лицима која су повезана са компанијама и историја њихових функција); Републичка геодетски завод (подаци о томе да ли неко поседује некретнину на територији РС и коју); Судови опште надлежности (Регистар лица лишених родитељског права, Регистар лица учесника у поступку); Фонд пензијског и инвалидског осигурања (Подаци о исплаћеним пензијама, накнадама за помоћ и негу и накнадама за физичко оштећење); Регистар трансакција некретнинама који садрже податке о нотарским записима и солемнизацији уговора о промету некретнина, податке о јавним бележницима који су спровели поступак, податке о судовима који врше проверу уписа у Регистар; Народна банка Србије (Јединствени регистар рачуна правних лица и предузетника и Регистар извршних дужника) и Пореска управа.

IV Закључци

У овом поглављу износимо закључке до којих смо дошли спроводећи ревизију сврсисходности на тему „Информациони системи у правосуђу“, код субјекта ревизије:
1. Министарство правде, Београд

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: Ефективно управљање информационим системима у правосуђу није у потпуности успостављено због недостатка финансијских средстава у буџету Министарства правде за финансирање информационих система (дакле не мисли се само на годишње одржавање софтвера, потребно је финансирати и обнављање опреме, других компоненти, набавку нових верзија софтвера, антивирусних пакета, обуку ИТ кадра итд.), зато што организација ИТ није успостављена тако да су усвојена правила и процедуре у области ИТ и да је организациона структура таква да може да одговори захтевима који обухватају сложеност послова, континуитет пословања и контролу, и што није омогућено равноправно коришћење папирних и електронских докумената.

Циљ увођења информационих система у правосуђе, као и у друге области, свакако јесте повећање ефикасности у раду. Приликом израде софтверских решења, примарно је постизање пословних циљева који се односе на послове којима се баве Министарство правде, судови, тужилаштва итд. У случају информационих система у области правосуђа који су предмет ове ревизије, управљање се обавља на два нивоа: на нивоу Министарства правде и на нивоу судова. Када су у питању функционалности софтвера, то је дефинисано техничким захтевима приликом набавке софтвера, или приликом набавке услуге одржавања софтвера, и то је било у ингеренцији Министарства правде. Међутим, када су у питању сви остали циљеви, као што је то администрирање, одржавање хардвера, мреже, помоћ корисницима итд., они су на неки начин подељени између Министарства правде, судова и пружалаца услуга. На крају, развој е-управе, е-услуга и е-правосуђа поставио је и нове циљеве када су у питању информациони системи, нарочито у јавном сектору, па тако и у области правосуђа, као што је могућност коришћења електронске комуникације и електронских докумената између грађана и судова.

Развој ИТ система у правосуђу, као уосталом и у другим областима у јавном сектору је сложен процес, који захтева:

- анализу постојећег стања, проблема, предлога и нових законских прописа (по речима одговорних у Министарству правде, последња анализа хардверских ресурса у судовима обављена је 2017. године. Подаци се прикупљају и преко активног директоријума);

- планирање (овде треба истаћи да је усвојена Стратегија развоја ИКТ система у правосуђу 2022–2027. године, а да се у претходном периоду развој ослањао на Смернице развоја ИКТ система у сектору правосуђа од 2016. године), које у сваком тренутку треба да буде базирано на тренутном стању информационих система, евидентираним проблемима, кадровским ресурсима и расположивом знању, и новим функционалним захтевима;
- финансијска средства;
- успостављање система интерних контрола која обухватају и одговарајућу (интерну) правну регулативу, али и одговарајућу кадровску и организациону структуру;
- евидентирање и имплементацију нових функционалности, било из разлога ефикасности система, било да је то нова законска обавеза.

У току успостављања и коришћења информационих система евидентирани су проблеми у вези са управљањем ИТ система у правосуђу.

Буџетска (финансијска) ограничења, с обзиром на стални и брзи развој ИТ технологија, јесу (као и у другим областима у јавном сектору) узрок проблема када је у питању опремљеност судова, а што се огледа у великом броју застарелих рачунара и оперативних система и у непостојању адекватне антивирусне заштите. Како је показала анализа података које су у току ревизије доставили судови, застарело и небезбедно је 60% рачунара. Како се наводи у Стратегији развоја ИКТ система у правосуђу 2022–2027. просечна старост рачунара је десет година. Поред могућих кварова, ризик је утолико већи имајући у виду чињеницу да су рачунари повезани на глобалну интернет мрежу, па су изложени и могућим хакерским (вирусним) нападима.

Такође, показало се да се организациона структура разликује од суда до суда, да постоје случајеви где нема ниједног запосленог на ИТ пословима, али и бројни случајеви где те послове обавља само један запослени. У таквим случајевима не можемо говорити о адекватном ИТ управљању из више разлога: не постоји подела одговорности, контрола послова, пренос знања, континуитет пословања итд.

На основу прикупљених података, може се закључити да не постоје усвојена правила и процедуре које се односе на ИТ послове. То последично значи да не постоји са једне стране могућност контроле тих послова (јер нису ни прописани), а са друге стране не постоји ни могућност преноса знања на ново запослене у случају замене. На основу наведеног, ризик по адекватан, потребан континуитет пословања постоји.

Новоуспостављени портал ПИС – Правосудно-информациони систем, успостављен је са циљем ефикаснијег рада правосудних органа, како у смислу уштеде у времену, тако и у смислу финансијске уштеде. Успостављањем Правосудног информационог система електронским путем су повезане базе података државних и правосудних органа, чиме је замењена дотадашња размена података на папиру. По подацима Министарства правде, од почетка коришћења је процењена уштеда више од 7 милијарди динара. Међутим, није у потпуности успостављена електронска комуникација између грађана и судова, тачније, није омогућен равноправан третман папирних и електронских докумената, а чиме би се постигли позитивни ефекти како у смислу финансијских уштеда, тако и у смислу квалитетније услуге коју би грађани добили (правовремена достава позива, олакшана размена докумената итд.).

Имајући у виду све уочене несврсисходности и ризике у овој ревизији, између осталог, наш циљ је био да у оквиру првог ревизијског питања утврдимо у којој мери су успостављени системи управљања информационим системима у правосуђу омогућили испуњење пословних и других циљева када ја у питању област правосуђа.

Како бисмо одговорили на ово питање, разматрали смо да ли је обезбеђено стабилно финансирање набавке, одржавања и развоја информационих система, да ли су усвојена и да ли се примењују правила и процедуре у вези са управљањем ИТ пословима, као и да ли је и на који начин омогућен равноправан третман папирних и електронских докумената.

Наш закључак заснивамо на следећим налазима:

Налаз 1.1: Није обезбеђено стабилно финансирање информационих система у правосуђу

Није обезбеђено стабилно финансирање информационих система у правосуђу због недостатка финансијских средстава, што за последицу има застареле рачунаре и застареле, самим тим и небезбедне оперативне системе, и недовољан број запослених на ИТ пословима. Законом о уређењу судова прописано је да су између осталог послови правосудне управе које врши министарство надлежно за правосуђе: уређење и развој правосудног информационог система. Број запослених на ИТ пословима у суду одређује председник суда актом о унутрашњем уређењу и систематизацији радних места у суду, у складу са кадровским планом.

У овој ревизији циљ је, између осталог, био да се, поред података о финансирању информационих система, анализира и организациони део који се односи на ИТ послове у вези са овим системом, у Министарству правде и у судовима, као и спроведене обуке запослених који раде на тим пословима.

Стратегија развоја ИКТ у правосуђу за период 2022–2027. и Акциони план за реализацију су усвојени од стране Секторског Савета за информационо-комуникационе технологије фебруара 2022. године. Исти савет је пре Стратегије усвојио и Смернице за ИКТ, у априлу 2016. године. Секторски савет подноси Министарству правде, Врховном касационом суду и Републичком јавном тужилаштву, Високом савету судства и Државном већу тужилаштва иницијативе, предлоге, мишљења и анализе које се односе на информационо-комуникационе технологије (у даљем тексту: ИКТ) у оквиру сектора правосуђа Републике Србије. Основан је Одлуком о оснивању Секторског савета за информационо-комуникационе технологије, Министра правде, председника Врховног касационог суда и Републичког јавног тужиоца („Службени гласник РС“, број 33 од 1. априла 2016).

Акционим планом за спровођење преговарачког поглавља 23 предвиђена је активност која се односила на успостављање платформе за размену података у електронском облику. Поједини државни органи су своје базе припремили у електронском облику и изложили за размену како не би одговарали на масовне писане дописе (2017. године ЦРОСО и НБС) и у том смислу је тренд преласка на електронску размену указао на неопходност примене овог средства и начина за размену. Правосудна платформа за размену података заснована је на Enterprise Service Bus (ЕСБ) који је вендорско решење компаније Мајкрософт (Microsoft BizTalk Server), док

се остали ИКТ системи правосуђа наслањају на ову платформу путем веб сервиса размењујући оптимизоване и стандардизоване податке. Правосудни информациони систем – портал (ПИС)– намењен је за приступ корисника сету података за који су посебно овлашћени користећи наведени ЕСБ односно Правосудну платформу за размену података.

Акциони планом за Поглавље 23 – Правосуђе и основна права је Влада Републике Србије усвојила 27.априла 2016. године. Након четири године спровођења, донета је одлука о његовој ревизији и усвојена у јулу 2020. године. У делу који се односи на информационе системе у правосуђу, у њему је наведено да се улажу напори како би се што пре завршио рад на увођењу модерног ефикасног система за судове опште надлежности. Циљ је да тај софтвер омогући управљање предметима које покрива цео ток и циклус предмета, од подношења иницијалног акта до коначне одлуке и архивирања. Визија тог модерног е-система подразумева централизоване системе управљања предметима праћеним одговарајућом хардверском инфраструктуром и јасним законским оквиром. Наведено је такође да се обука корисника и обезбеђивање опреме реализују као континуиране активности. Истакнуто је да су добити од увођења Правосудног информационог система – ПИС, а које се огледају у већем степену ефикасности пре свега због убрзања судског процеса (процена која је изнешена је да се поступак скраћује за 3–6 месеци) и финансијским уштедама.[12]

Смерницама развоја ИКТ система у сектору правосуђа, донетим у априлу 2016. године, предвиђено је да ће Одсек за ИКТ користити све донаторске организације за велике инвестиционе пројекте који су већи од националног буџета Сектора правосуђа, док ће национални буџет бити коришћен за унапређење мреже и основне софтверске инфраструктуре, замену радних станица широм целог Сектора, одржавање антивирусног софтвера, обуку ИКТ особља и нека мања оперативна унапређења, односно мање развојне пројекте које су у надлежности Сектора правосуђа.[13]

Финансирање једног информационог система, у најширем смислу, обухвата набавку и одржавање хардвера (рачунара, сервера, штампача, мрежне опреме и других уређаја), набавку и развој софтвера (набавку оперативних система, апликативног софтвера – често набавку одржавања софтвера, када су у питању специфични послови), одржавање софтвера, људске ресурсе и обуке, и у неким случајевима израду одговарајућих правних аката којима се рад тог система уређује.

Законом о уређењу судова, у члану 70. прописано је да су, између осталог, послови правосудне управе које врши министарство надлежно за правосуђе: уређење и развој правосудног информационог система. Истим законом, у члану 57. прописано је да судско особље чине судијски помоћници, судијски приправници и државни службеници и намештеници запослени на административним, техничким, рачуноводственим, информационим и осталим пратећим пословима значајним за судску власт. Број судског особља одређује председник суда актом о унутрашњем уређењу и систематизацији радних места у суду, у складу са кадровским планом.

[12] Акциони план sa поглавље 23, јул 2020. година
[13] Смернице развоја ИКТ система у сектору правосуђа, април 2016. година

Мерила за одређивање броја судског особља утврђује министар надлежан за послове правосуђа.

У члану 1. истог закона прописано је да су судови самостални и независни државни органи. Чланом 51. прописано је Судску управу чине послови који служе вршењу судске власти, између осталог и финансијско и материјално пословање суда. Судска управа детаљније се уређује Судским пословником.

Чланом 52. прописано је да Председник суда руководи судском управом и одговоран је за правилан и благовремен рад суда.

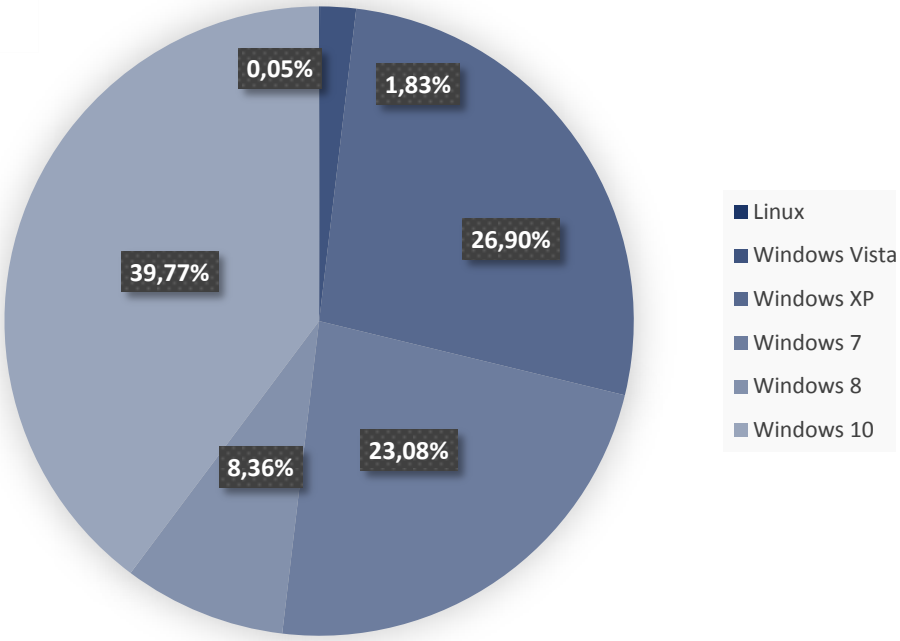
Чланом 55а. прописано је да суд републичког ранга, апелациони суд и суд са 30 и више судија има управитеља суда. Председник суда поверава управитељу суда обављање материјално-финансијских и организационо-техничких послова. Послови управитеља суда се детаљније уређују Судским пословником.

Како би се на што бољи начин стекла слика о стању хардверских и софтверских ресурса у судовима, на адресе свих судова (укупно 159) послат је упитник. Одговоре су упутила 94 суда, а од тог броја, комплетне одговоре је доставило њих 53.

Планирање, када су у питању информациони системи у правосуђу обухвата планирање на републичком нивоу и планирање на нивоу сваког суда. Према речима одговорних лица у Министарству правде, они врше набавку рачунара, судови немају обезбеђена средства у буџету за ту намену. 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. С обзиром на то да се рачунари користе тако да су повезани у глобалну мрежу, њихова „рањивост“ у безбедносном смислу директно зависи од „рањивости“ оперативног система и антивирусног софтвера, између осталог.

Оперативни систем	Број рачунара	Процентуално учешће
Linux	2	0,05%
Windows Vista	74	1,83%
Windows XP	1085	26,90%
Windows 7	931	23,08%
Windows 8	337	8,36%
Windows 10	1604	39,77%

Илустрација 3. *Број рачунара и оперативних система*



Илустрација 4. *Који оперативни систем се користе у информационим системима у правосуђу?*

Укупно, на бази података прикупљених за 4033 рачунара, анализа је показала да преко 60% рачунара користи застареле оперативне системе, тачније системе за које више не постоји ажурирање и инсталација безбедносних закрпа. Око 40% рачунара користи оперативни систем Windows 10.

Подршка за оперативни систем Windows XP је укинута 2014. године. Анализом прикупљених података од судова, установљено је да 26,9% рачунара користи овај оперативни систем. Подршка за оперативни систем Windows 7 је укинута почетком 2020. године. У анализи коју смо спровели, од укупног броја рачунара 23,08% рачунара има овај оперативни систем. Око 8,36% рачунара користи оперативни систем Windows 8, за који не постоји подршка од 2016. године. Такође, подршка је укинута и за Windows Vista, још од априла 2017. године, а 1,83% рачунара користи тај оперативни систем. Најављени датум укидања подршке од стране Microsoft-а за оперативни систем Windows 10 је октобар 2025. године. Од 4033 рачунара за које су прикупљени подаци, два рачунара користе оперативни систем Linux. Како то показују прикупљени подаци, када је у питању антивирусни софтвер постоје случајеви где су одговорна лица навела да антивирусни софтвер уопште не постоји. Треба имати у виду и да је и поред постојања антивирусног софтвера, у случају застарелог оперативног система немогуће обезбедити одговарајући ниво заштите због безбедносних слабости самог оперативног система.

Правилником о номенклатури нематеријалних улагања и основних средстава са стопама амортизације, прописано је да је годишња стопа амортизације за ставку „Електронски рачунари и остала опрема за обраду података“ износи 20%. То практично значи да је књиговодствена вредност рачунара после пет година коришћења нула динара. Другачије речено, сматра се да су рачунари након пет година 100% амортизовани.

У Смерницама развоја ИКТ система у сектору правосуђа се наводи да су Министарству правде потребна додатна средства из донација јер се националним буџетом предвиђа улагање само у ИКТ инфраструктуру до оптималног нивоа док све остала улагања у ИКТ систем мора бити део правилно пројектованих донаторских средстава.

Стратегија развоја ИКТ у правосуђу 2022–2027. године у делу „Посебан циљ 3: Успостављање ИКТ инфраструктуре која омогућава несметано функционисање софтверских решења е-правосуђа и рад корисника“, као показатеље резултата набраја број нових персоналних рачунара и пратеће рачунарске опреме у правосудним органима стандардизоване конфигурације, као и просечну старост рачунара у правосуђу, што је такође и предвиђена мера 3.3 „Обнављање персоналних рачунара и пратеће рачунарске опреме у правосудним органима и стандардизација његове конфигурације“.

Како су навела одговорна лица из Министарства правде кроз активни директоријум (око 15000 корисника) прати се број али и стање радних станица (оперативни систем указује на старост рачунара). У оквиру стратегије постоје циљ и активност који се односе на просечну старост рачунара. Кроз донацију ЕУ, уговорена је испорука 5700 рачунара у наредне две године, а прошле године је прибављено око 600 рачунара. У овом случају, постоји ризик од тога да се не реализују донације ЕУ, што значи да би број застарелих рачунара (па самим тим и небезбедних) био процентуално још већи.

Мера 3.3: Обнављање персоналних рачунара и пратеће рачунарске опреме у правосудним органима и стандардизација њихове конфигурације							
Институција одговорна за праћење и контролу реализације: Министарство правде							
Тип мере: Обезбеђење добара и пружање услуга							
Период спровођења: 2022 – 2025. година							
Показатељ(и) резултата на нивоу мере	Јединица мере	Извор провере	Почетна вредност	Базна година	Циљана вредност у 2023. години	Циљана вредност у 2024. години	Циљана вредност у 2025. години
Број нових персоналних рачунара стандардизоване конфигурације са пратећом рачунарском опремом у правосудним органима	Број нових рачунара	Извештаји са примопредаја	0	2022.	500	6000	6500
Просечна старост рачунара у правосуђу	Просечна старост	Извештај анализе старости	10	2022.	7 година	5 година	4 године

Илустрација 5. *План Министарства правде – обнављање персоналних рачунара и опрене*

Када је у питању начин на који се планирају средства за набавку система и касније годишње одржавање, Министарство је навело да планом јавних набавки опредељује средства за набавку услуге одржавања и развоја информационих система које одржава и развија.

Како је приказано у табели која следи, а према подацима које је доставило Министарство правде, трошкови одржавања информационих система АВП, САПС, СИПРЕС и ПИС у приказаном периоду износили су преко 195 милиона динара.

Ако се посматрају трошкови набавке и одржавања наведених система, као и улагања у хардвер, према достављеним подацима Министарства правде, они су износили нешто више од 777.468.000,00 динара. Са друге стране, уштеде остварене након увођења Правосудно информационог система су скоро десет пута веће. Другим речима, уштеде остварене дигитализацијом неких послова омогућавају не само обнављање хардвера у наредном периоду, већ и модернизацију постојећих система.

Р.Бр.	Назив Јавне набавке	Датум закључења уговора	Уговорена вредност без ПДВ-а	Уговор додељен
АВП (Аутоматско вођење предмета). Апликацију користе основни и виши судови, осим вишег суда у Сремској Митровици, са припадајућим судским јединицама користе децентрализован систем за управљање судским предметима, популарно назван АВП (Аутоматско вођење предмета).				
1	Имплементација и одржавање АВП софтвера у новооснованим судовима и одржавање АВП софтвера у постојећим судовима	16. јул 2014.	16.930.000,00	Mega computer engineering д. о. о., Мис Ирбијеве 48г., Београд
2	Одржавање АВП пословног софтвера	29. септембар 2015.	33.510.000,00	Mega computer engineering д. о. о., Мис Ирбијеве 48г., Београд
3	Одржавање АВП пословног софтвера	13. октобар 2016.	9.804.000,00	E-Smart Systems д. о. о., Кнеза Вишеслава 70а, Београд.
4	Одржавање АВП пословног софтвера	11. октобар 2017.	9.848.000,00	E-Smart Systems д. о. о., Кнеза Вишеслава 70а, Београд.
5	Одржавање и унапређење апликације АВП	30. новембар 2018.	21.999.996,00	E-Smart Systems д. о. о., Кнеза Вишеслава 70а, Београд.
6	Одржавање и унапређење апликације АВП уз припреме за увођење јединствене апликације судова опште надлежности	29. новембар 2019.	29.910.157,20	Информатика а. д. Београд, Јеврејска 32, Београд
7	Одржавање АВП, одржавање и унапређење апликације СИПРЕС, одржавање и унапређење ЦССТ	15. јануар 2021.	59.850.000,00	C&T Serbia д.о.о. Београд И Атос ИТ Солутионс анд сервицес д. о. о. Београд
САПС (стандардизована апликација правосуђа Србије), имплементиран од маја 2012. године. Тренутно је у употреби у: Врховном касационом суду и Управном суду у Београду, свим Апелационим судовима (Београд, Ниш, Нови Сад и Крагујевац) и Вишем суду у Сремској Митровици. САПС је информациони систем која се води и којом се управља централизовано, за све типове судова и осмишљен је као модуларан софтвер, који је преузео све функционалности постојећег АВП система, али су додате и оне функције које нису биле имплементиране у АВП систему.				
1	Одрживи развој са услугама одржавања пословног софтвера за управљање предметима и садржајима у судовима (САПС)	16. септембар 2013.	9.971.124,00	Atos IT solutions and services д. о. о. Париске комуне 22, Београд.
2	Одржавање софтвера САПС	17. децембар 2014.	2.994.000,00	Atos IT solutions and services д. о. о. Париске комуне 22, Београд.

Р.Бр.	Назив Јавне набавке	Датум закључења уговора	Уговорена вредност без ПДВ-а	Уговор додељен
3	Одржавање САПС пословног софтвера	19. новембар 2015.	15.984.000,00	Atos IT solutions and services д. о. о. Париске комуне 22, Београд.
4	Одржавање САПС пословног софтвера	14. октобар 2016.	11.988.000,00	Atos IT solutions and services д. о. о.Париске комуне 22, Београд.
5	Одржавање САПС пословног софтвера	25. децембар 2017.	20.975.024,00	Atos IT solutions and services д. о. о. Данила Лекића Шпанца 31, Београд.
6	Одржавање и унапређење апликације САПС	15. јануар 2019.	15.995.100,00	Atos IT solutions and services д. о. о. Данила Лекића Шпанца 31, Београд.
7	Одржавање и унапређење апликације САПС	23. јануар 2020.	55.987.500,00	Atos IT solutions and services д. о. о. Данила Лекића Шпанца 31, Београд.
8	Одржавање и унапређење апликације САПС	30. март 2022.	7.945.000,00	Atos IT solutions and services д. о. о. Данила Лекића Шпанца 31, Београд.
Апликација СИПРЕС (Систем прекршајних судова), почео са радом од 2016. године и користи се у раду у прекршајним судовима, одељењима прекршајних судова, Прекршајном апелационом суду, одељењима Прекршајног апелационог суда и у делу Врховног касационог суда. Пројекат је започет средином 2012. године, са циљем да се аутоматизују ове врсте судова, односно да свих 45 прекршајних судова има аутоматизовани централни информациони систем. У Министарству правде примењен је регистар санкција и регистар неплаћених новчаних казни, као део целине коју чини и обједињује СИПРЕС. СИПРЕС први систем у српском правосуђу који је повезан са осталим органима у оквиру мреже правосудних органа и мреже Управе за заједничке послове републичких органа (УЗ ЗПРО) и то су за сада Управа за трезор, Управа саобраћајне полиције МУП Србије и Централни регистар обавезног социјалног осигурања. "Повезивањем са МУП Србије омогућена је електронска достава десетина хиљада прекршајних налога судовима.				
1	Одржавање СИПРЕС система	1. април 2016.	13.500.000,00	E-Smart Systems д. о. о., Кнеза Вишеслава 70а, Београд.
2	Одржавање СИПРЕС система	12. мај 2017.	19.800.000,00	E-Smart Systems д. о. о., Кнеза Вишеслава 70а, Београд.
3	Одржавање и унапређење апликације СИПРЕС	11. јул 2018.	21.999.996,00	E-Smart Systems д. о. о., Кнеза Вишеслава 70а, Београд.
4	Одржавање и унапређење апликације СИПРЕС	15. новембар 2019.	24.882.000,00	Информатика а. д. Београд, Јеврејска 32, Београд

Р.Бр.	Назив Јавне набавке	Датум закључења уговора	Уговорена вредност без ПДВ-а	Уговор додељен
Предмет јавне набавке су услуге одржавања и одрживог развоја пословног софтвера за аутоматизовано вођење предмета (АВП) у основним, вишим и привредним судовима у Републици Србији, потом услуге одржавања и унапређења апликације СИПРЕС која се користи у раду у прекршајним судовима, одељењима прекршајних судова, Прекршајном апелационом суду, одељењима Прекршајног апелационог суда и у делу Врховног касационог суда, као и услуге одржавања и унапређења Централног система за судске таксе – ЦССТ за период од 12 месеци.				
1	Одржавање и унапређење апликација за вођење предмета у основним и прекршајним судовима	21 јануар 2021.	59.850.000,00	Atos IT solutions and services д. о. о., Данила Лекића Шпанца 31, Београд
1	Одржавање серверске опреме у судовима и јавним тужилаштвима	6. јун 2017.	34.982.888,00	Atos IT solutions and services д. о. о., Данила Лекића Шпанца 31, Београд
2	Одржавање серверске опреме у судовима и јавним тужилаштвима	24. јул 2018.	34.987.165,00	Atos IT solutions and services д. о. о., Данила Лекића Шпанца 31, Београд
3	Одржавање серверске опреме у судовима и јавним тужилаштвима	11. септембар 2019.	34.992.000,00	Atos IT solutions and services д. о. о., Данила Лекића Шпанца 31, Београд
4	Одржавање серверске опреме у судовима и јавним тужилаштвима	4. јануар 2021.	54.989.998,04	Atos IT solutions and services д. о. о., Данила Лекића Шпанца 31, Београд

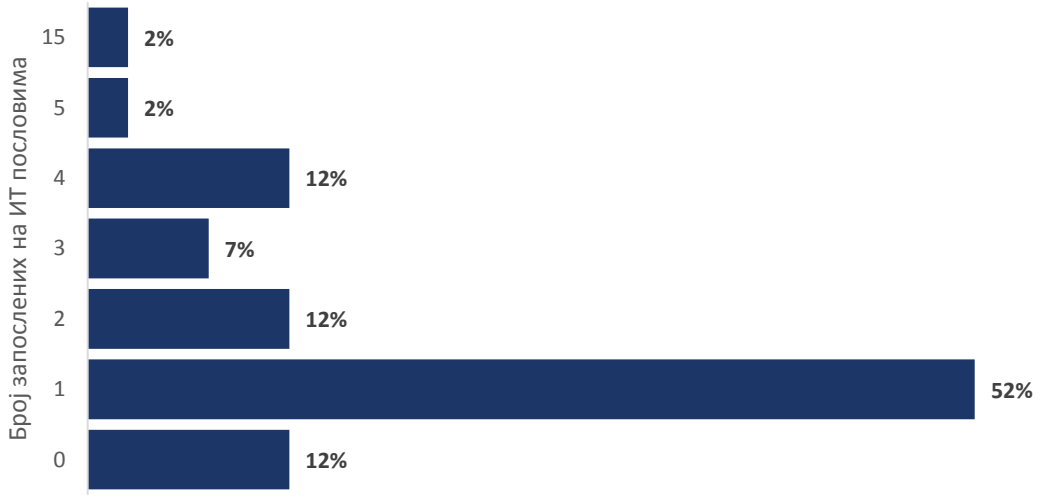
Илустрација 6. *Финансирање информационих система у правосуђу*

Судским пословником су прописани послови управитеља суда и у члану 14в је наведено да, између осталог, управитељ обавља послове у вези са организовањем и координирањем рада суда у материјално-финансијским пословима и организационо-техничким пословима суда и да припрема предлог плана развоја информационог система суда. Такође, чланом 39. предвиђено је да се за послове који се односе на успостављање и одржавање информационо-комуникационих технологија (у даљем тексту: ИКТ) и електронску обраду података, складиштење и пренос информација у суду, може образовати служба за информатику и аналитику. У циљу решавања питања у судовима о начину примене пословног софтвера за управљање предметима у поступку прикупљања и обраде података и сачињавања извештаја, министар може образовати посебну комисију за стандардизацију начина прикупљања и обраде података. Састав комисије из става 2. овог члана, одређује министар. Коришћење информационо-комуникационих технологија (ИКТ) у раду суда је прописано чланом 139, где је дефинисано да се у судовима се, по правилу, у раду користи ИКТ за обраду текста, вођење свих врста евиденција (уписници, помоћне књиге и сл.), обраду и прикупљање статистичких података, електронску размену података, штампање (омоти списа, доставнице и сл.), рачуноводствене послове, праћење прописа и судске праксе, као и у судској управи и писарници. У раду са ИКТ, сходно се примењују посебни прописи и одредбе овог пословника.

Број запослених на ИТ пословима	Број судова
0	5
1	22
2	5
3	3
4	5
5	1
15	1

Илустрација 7. *Број запослених на ИТ пословима у судовима*

Када су у питању судови, на основу прикупљених података и њихове анализе, може се дати оцена да је организациона ИТ структура неадекватна а број запослених који раде на ИТ пословима недовољан. Као што је већ наведено, на упитник достављен на 159 мејл адреса судова у Србији, одговоре смо добили од њих 53. Од тог броја, у 22 суда на ИТ пословима ради само по један запослени, у пет судова на ИТ пословима постоје по два запослена, у само три суда раде по три ИТ стручњака, у пет судова тај број је четири, док у једном случају има пет запослених на ИТ пословима. Када су у питању судови који имају запослене на ИТ пословима, у једном суду ради 15 ИТ стручњака. Мада, треба истаћи и да се ради о највећем суду у Републици Србији. У пет судова нема запослених који обављају ИТ послове.



Илустрација 8. *Однос броја судова према броју запослених на ИТ пословима*

Имајући у виду сложеност ИТ послова у судовима, потребу успостављања интерних контрола, континуитета пословања у случају одсуства итд. може се закључити да на нивоу судова постоји ризик од тога да у краћем или дужем временском периоду буде отежано обављање послова који зависе од ИТ технологија,

нарочито у случајевима када нема запослених који раде на ИТ пословима (што је случај и код судова који имају само по једног ИТ стручњака).

Како су навели у Министарству правде, четири године уназад обуке се врше сваке године и то за ИСО 21500 због управљања пројектима развоја, ИСО 20000 због успостављања сервисима, ИСО27000 и 27701 и слично. Планирају се кроз јавне набавке и ангажују се сертификовани предавачи. Што се тиче самог ПИС-а, у смислу портала за размену података одржаване су презентације на нивоу Апелационих судова и већих виших и основних и обуке за правосудне професије и дистрибуирана су упутства у видео формату за регистрацију. Тај систем је најједноставнији за коришћење. Када се ради о другим системима, по правилу увек су организоване обуке за кориснике и дистрибуирана су упутства са контактима за подршку. Нека видео упутства су доступна и на страници Министарства правде. Представници Министарства правде су навели да лица за ИТ у судовима пролазе обуке за информациону безбедност и заштиту приватности података. Постоји посебна процедура добијања овлашћења да се приступи ПИС-у (писано овлашћење председника суда за приступ појединим скуповима података) и слично. Међутим, анализа података добијених од судова показала је да су у 32 од 53 суда запослени који раде на ИТ пословима похађали једну или више обука које се односе на ИТ технологије.

На основу свега наведеног, може се закључити да због неадекватног планирања средстава, непостојања анализа, недовољно средстава, ослањања на донације, и чињенице да број запослених у суду одређује суд а не Министарство правде, што се односи и на запослене на ИТ пословима, финансирање информационих система у правосуђу не обезбеђује њихов одрживи развој.

Препоручујемо Министарству правде да приликом припреме финансијских планова осигура стабилно финансирање циљева који обухватају одрживи развој, набавку и одржавање свих компоненти информационих система (хардвер, софтвер, људске ресурсе, стручну обуку).

Налаз 1.2: Непостојање ИТ процедура и одговарајуће ИТ организационе структуре онемогућава контролу обављања послова, пренос знања на новозапослене и континуитет пословања у случају замене запослених

Због тога што сваки суд посебно уређује ИТ послове, на нивоу целокупног система правосуђа није успостављено управљање тако да су прописане процедуре које уређују ову област и није успостављена адекватна ИТ организациона структура, што за последицу има отежану или онемогућену контролу обављања ових послова, континуитет пословања и/или пренос знања у случају раскида радног односа са запосленим који обавља те послове, или замену запосленог. Потребно је обезбедити одговарајући ниво образовања и способности лицима који управљају и користе систем, неопходно је успоставити праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу, тачније, потребно је процедурама уредити ове и друге послове како је прописано Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја.

ИТ послове је неопходно детаљно уредити одговарајућим процедурама зато што се на тај начин 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. Како би биле функционалне, неопходно је да процедуре буду довољно детаљне и свеобухватне, да поред описа свих процеса садрже и податке о томе ко ради на којој активности (навођење одређеног радног места, а не именовање запосленог), као и податке о изменама итд.

Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја прописано је да оператор ИКТ система од посебног значаја, у овом случају МП, између осталог, успоставља организациону структуру, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система од посебног значаја, 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; идентификовање информационих добара и одређивање одговорности за њихову заштиту итд.

Информационим системима у Министарству правде се управља тако што је у оквиру унутрашње јединице Сектора за правосуђе образовано Одељење за ИКТ у оквиру ког постоје две групе, Група за ИКТ у грађанској и управној материји и Група за ИКТ у кривичној и прекршајној материји.

Група за ИКТ системе у грађанско-правној и управној материји обавља послове који се односе на: развој ИКТ у системима правосудних професија, судова опште надлежности за грађанско-правну материју, привредних судова, система Управног суда, регистара у правосуђу, правосудне мреже, система за размену података, система за централно извештавање о раду судова и смештајних капацитета и рада дата центра и серверске опреме у правосуђу; учешће у припреми закона, других прописа, стандарда и мера у области примене ИКТ у правосудним професијама, привредним судовима, Управном суду и у судовима опште надлежности у грађанско-правној материји; учествовање у остваривању функције праћења, усмеравања и координације активности на развоју електронског система правосудних професија, судова опште надлежности у грађанско-правној материји, привредних судова и Управног суда; примену ИКТ у циљу унапређења организације, развоја и начина рада у правосудним професијама, судовима опште надлежности у грађанско-правној материји, привредним судовима и Управном суду; администрирање порталом електронске продаје покретних и непокретних ствари путем јавног надметања у извршном поступку; развој електронске платформе за успостављање портала за е-аукцију; давање налога за унапређење портала за е-аукцију, одобравање захтева за учешће у електронској продаји покретних и непокретних ствари путем јавног надметања корисницима портала; учествовање у подизању квалитета података о странкама у поступку и организација која омогућава ефикасну електронску размену између правосудних органа у држави као и успостављање основа за електронску размену са другим регионалним и ЕУ правосудним системима и регистрима; учествовање у реализацији ИТ програма и пројеката ЕУ и других организација за потребе правосуђа као и одржавање и

унапређење ових система након имплементације и друге послове који се односе на ИКТ у правосудним оранима, обавља и друге послове из делокруга Групе.

Послови у Групи (тренутно броји 1+3), према Правилнику, обављају се у оквиру шест радних места, и то:

- радног места руководилац Групе, разврстаног у звање самостални саветник (1);
- радног места за припрему, планирање и управљање ИТ пројектима и заштиту података, разврстаног у звање самостални саветник, на коме је систематизован један извршилац;
- радног места за информатичку подршку у системима правосудних професија, у звању млађи саветник, на коме су систематизована два извршиоца (1);
- радног места за пројектовање, израду, имплементацију и одржавање пословних система у звању саветник, на коме је систематизован један извршилац;
- радног места за е-аукцију, у звању саветник, на коме су систематизован један извршилац;
- радног места за пројектанта информационих система у правосуђу у звању самостални саветник, на коме су систематизована два извршиоца (2).

Активности на којима раде запослени у групи:

1. Пружање подршке правосудним органима у поступку спровођења прописа од утицаја на развој електронског правосуђа у циљу унапређења квалитета и ефикасности рада правосудних органа.

2. Сазивање и руковођење седницама Комисије за стандардизацију начина прикупљања и обраде података у примени пословног софтвера за управљање предметима у поступку прикупљања, обраде података, као и сачињавања извештаја у судовима Републике Србије.

3. Давање мишљења и одговора на питања странака, у вези са пословима из делокруга Сектора.

4. Учествовање у реализацији ИТ програма и пројеката ЕУ и других организација за потребе правосуђа.

5. Предузимање адекватних мера ради тога да се постојеће ИКТ инфраструктуре и услуге редовно одржавају и унапређују, путем закључења уговора са добављачима кроз поступке јавних набавки.

6. Надзор над исправношћу информација на Порталу судова Србије (www.portal.sud.rs), као и ажурирање у случају промена релевантних података, као што су основне информације о правосудним органима, о њиховој месној надлежности, о поштанским бројевима релевантним за међународну правну помоћ и друго, изузев сервиса који се односи на ток предмета.

7. Вршење процене о потребама појединачних правосудних органа те, у случају позитивне одлуке, давање сагласности за набавку опреме из области информационо-комуникационих технологија.

8. Администрирање платформи е-Аукција и администрација корисничким налозима за целокупне ИКТ системе правосуђа.

Група за ИКТ системе у кривично-правној материји, прекршајној материји, унутрашњим јединицама Министарства и органима управе у саставу Министарства обавља послове који се односе на: развој ИКТ у јавним тужилаштвима, судовима опште надлежности у кривично-правној материји, прекршајним судовима и унутрашњим јединицама и органима управе у саставу Министарства (Управа и заводи за извршење кривичних санкција и Дирекција за управљање одузетом имовином) и то: учешће у припреми закона, других прописа и стандарда и мера у области примене ИКТ у јавним тужилаштвима, судовима опште надлежности у кривично-правној материји, прекршајним судовима и органима управе у саставу Министарства; учествовање у остваривању функције праћења, усмеравања и координације активности на развоју ИКТ система у наведеним органима; послове међународне сарадње у примени ИКТ у наведеним органима; примену ИКТ с циљем унапређења организације, развоја и начина рада у наведеним органима из делокруга Групе; сарадњу са надлежним органима у поступку припреме, израде и спровођења стратегије, прописа, стандарда, планова, програма, пројеката и хардверско-софтверских решења од утицаја на развој ИКТ у наведеним органима; учествовање у подизању квалитета података о странкама у поступку и организација која омогућава ефикасну електронску размену између правосудних органа у држави као и успостављање основа за електронску размену са другим регионалним и ЕУ правосудним системима и регистрима и друге послове који се односе на ИКТ у органима из делокруга Групе.

Послови у Групи, према Правилнику, обављају се у оквиру пет радних места, и то:

- радног места руководилац Групе, разврстаног у звање самостални саветник;
- радног места за информатичко-аналитичке послове у звању млађи саветник, на коме је систематизован један извршилац (1);
- радног места за подршку развоја информационог система, у звању млађег саветника, на коме су систематизован један извршилац (2);
- радног места за подршку дигитализацији у прекршајним судовима, у звању млађи саветник, на коме је систематизован један извршилац.

Нису прописане процедуре које се односе на наведене послове, мада се како су навели у Министарству правде, неке налазе у фази нацрта.

Локалне процедуре у вези са ИКТ заснивају се на пословним политикама које се не креирају у потпуности, нити се контролишу централизовано, већ се израђују локално. Локално системско и апликативно окружење у правосудним органима је хетерогено, па је и размена докумената понекад отежана због различитих формата докумената (нпр. MS Word 2003, 2007, Open Office, итд.). Иако за неке активности постоје унификовани софтвери које сви правосудни органи једнако користе (као нпр. за рачуноводство или за Управу за трезор), поједине апликације се и даље праве

локално, за исте или врло сличне намене (као што су судска пракса, архива, база судских вештака, преводилаца и тумача, јавних бележника и јавних извршитеља, књига поште итд.).[14]

Када је у питању организациона структура, од 53, у 32 суда не постоји посебна организациона јединица која обавља ИТ послове. Када су у питању називи посебних јединица- одељења-служби у 53 суда постоји осам различитих назива, а разликују се и називи радних места која се односе на ИТ послове.

Може се закључити да у систему не постоје усвојене и имплементиране процедуре које уређују ИТ послове који су у вези са информационим системима у правосуђу, као и да организациона структура у судовима, у целини гледано, није адекватно успостављена, тачније, није могуће успоставити одговарајући систем контроле или „преношења знања“, што је неопходно у случајевима кадровских замена на овим пословима.

Министарству правде препоручујемо да изради и судовима упути одговарајућа упутства у циљу успостављања организационе ИТ структуре и процедура које ће дефинисати послове који се односе на ИТ и обезбедити континуитет обављања послова у случају замене запослених на ИТ пословима.

Налаз 1.3: Није омогућено равноправно коришћење папирних и електронских докумената.

Због функционалних недостатака у садашњим софтверским решењима и потребе измене одговарајућих закона, није омогућено равноправно коришћење папирних и електронских докумената, у складу са Законом о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању, што за последицу има смањену ефикасност система и то како када су у питању финансијска средства која се троше због папирне доставе, тако и када је у питању време потребно за штампу, паковање, слање и доставу.

Стратегија развоја правосуђа за период 2020–2025. године као посебан циљ 5 дефинише развој е-правосуђа. У њој се наводи да примена алата и механизама е-правосуђа превазилази његову улогу у унапређењу ефикасности и представља хоризонтални механизам који се прожима кроз свих пет кључних принципа организације и реформе правосуђа тако што између осталог доприноси ефикаснијем раду правосуђа кроз аутоматизацију управљања предметима, могућност подношења електронских поднесака, размену података међу правосудним органима, снимање суђења и електронске доставе странкама.

[14] Стратегија развоја ИКТ у правосуђу 2022–2027

У Акционом плану за Поглавље 23, наведено је и да је успостављен систем е-фајлинга као средство које служи грађанима и професионалцима као средство за електронско достављање докумената у и из предмета и вршења увида у судске предмете. Грађани још увек немају могућност да документа достављају у електронској форми, нити да врше увид у судске предмете.

Закон о електронском документу и електронској идентификацији, у члану 7. прописано је да се електронском документу не може оспорити пуноважност, доказна снага, као ни писана форма само зато што је у електронском облику. Такође, у истом закону, у члану 15. прописано је да се електронско општење и електронско достављање између органа јавне власти и странака врше у складу са законом којим се уређује општи управни поступак, законом којим се уређује електронска управа и другим прописима, као и путем услуге квалификоване електронске доставе.

Закон о електронској управи као једно од начела управо наводи ефикасност управљања опремом, где прописује да је орган дужан да ефикасно управља опремом којом располаже тако да омогући њено правилно и економично коришћење.

Увођење Правосудно-информационог система и велике уштеде које су већ остварене у протеклом периоду (процена Министарства правде да се ради о износу већем од 7 милијарди динара) прави је пример и доказ да се исти послови могу обављати на много ефикаснији начин коришћењем ИТ технологија, односно у конкретном случају разменом докумената у електронском, уместо у папирном формату.

Путем ПИС-а правосудним органима омогућен је тренутни увид у податке, што за судске поступке значи да се и на рочиштима могу проверити подаци из званичних регистара који су од значаја за конкретан предмет и које странке или адвокати оспоре или истакну, а што повећава правну сигурност и убрзава решавање самих поступака.

Од почетка примене система остварено је преко 20.057.727 електронских упита, чиме је замењено преко 40.155.454 дописа (један за упит и један за одговор), што је довело до уштеде више од 7.8 милијарди дин. уштеде у државном буџету (број упита * 2 * 45 дин. за поштарину + број упита * 20 минута уштеде у раду запосленог рачунајући по бруто просечној плати).

Број упита: 20.057.727

Број дописа који је тиме замењен: 40.155.454
(два, један ка органу, други од органа ка суду)

Критеријум за обрачун:
А. Број електронских упита: 20.057.727

Б. Поштарина, по упиту: 90 дин. (Цена једне пошиљке 45 дин. х 2 због слања у оба смера) уштеда износи на овом делу процеса износи:

90 дин. х 40.155.454 = 3.610.390.860 дин.

В. Рад

- **Електронски упит** је еквивалент начину рада традиционално, папирним дописима: 20 минута, и то 10 минута за израду и обраду једног дописа x 2 због слања у оба смера
- **Вредност рада**: Просечна бруто месечна зарада: 100.937 дин. за 8-часовно радно време, 20 радних дана у месецу Извор: РЗС (https://www.stat.gov.rs/sr-latn/vesti/statisticalrelease/?p=8842&a=24&s=2403?s=2403)

160 радних сати (8 часова x 20 дана) месечно x 60 минута је 9600 минута, а та количина рада одговара изради 960 дописа чему је еквивалент 480 електронских упита односно новчани еквивалент од 100.937 дин. Један упит је 210 дин. уштеде у смислу плаћеног рада.

210 дин. x 20.057.727 = 4.212.122.670 дин.

Уштеда на овом делу процеса износи: 4.212.122.670 дин.
Новчана вредност уштеде износи: 7.822.513.530 дин.

Забрана дискриминације је прописана чланом 7, где се наводи да свако има права да користи услугу електронске управе у складу са овим законом.

Закон је у члану 15. прописао да физичка и правна лица могу да користе услуге електронске управе, ако се за то региструју. Надлежни орган отвара налог кориснику електронске управе и дужан је да кориснику обезбеди Јединствени електронски сандучић.

У члану 16, прописано је да је орган дужан да изради софтверско решење које омогућава коришћење услуга електронске управе, у складу са прописима којима се уређује електронски документ, електронска идентификација и заштита података о личности.

Члан 23. прописује да корисник услуга електронске управе преко Портала еУправа може, између осталог, да подноси електронске поднеске и комуницира са органом, прима обавештења о предузетим радњама и донетим актима надлежних органа и прати статус свог предмета и прима акте надлежних органа у Јединствени електронски сандучић.

Чланом 38. прописано је да је орган дужан да припреми електронске обрасце за подношење електронских поднесака. Уколико је прописана обавезност потписивања, електронски поднесак се потписује регистрованом шемом електронске идентификације високог нивоа поузданости. Даље, у члану 39. је прописано да је орган дужан да омогући пријем електронског поднеска преко Портала еУправа, другог електронског јединственог управног места или другим путем достављања између органа и корисника, у складу са законом којим се уређује електронски документ и услуге од поверења у електронском пословању. Пријем електронског поднеска евидентира се у електронској писарници.

Важно је напоменути да је чланом 40. прописано да се на захтев корисника достављање уверења, одлука, решења, закључака и других докумената у поступку

врши се и у папирном облику. Електронско достављање електронског документа врши се у Јединствени електронски сандучић корисника услуга електронске управе или другим електронским путем у складу са законом којим се уређује електронски документ и услуге од поверења у електронском пословању.

Како је прописано чланом 41, електронски документ сматра се лично преузетим када корисник органу потврди пријем отварањем електронске повратнице која се аутоматски израђује након пријема документа у Јединствени електронски сандучић.

Имајући у виду позитивна искуства у смислу ефикасности система након увођења Правосудног информационог система (ПИС), како у смислу финансијске уштеде тако и у смислу скраћеног времена потребног за размену докумената и имајући у виду општу интенцију дигитализације која подразумева већу ефикасност и употребу е-услуга, а у складу са могућностима које пружају закони који се односе на ова питања – пре свега закон о електронском документу и закон о електронској управи, може се закључити да је потребно/неопходно омогућити равноправно коришћење папирних и електронских докумената у информационим системима у правосуђу.

Препоручујемо Министарству правде да приликом будућег развоја и одржавања информационих система омогући равноправно коришћење папирне и електронске документације.

ЗАКЉУЧАК 2: Министарство правде и судови нису успоставили управљање информационом безбедношћу информационих система у правосуђу на свеобухватан начин јер нису усвојене и примењене мере заштите које обухватају управљање ИТ ризицима, организациону ИТ структуру и усвајање и примену одговарајућих правила и процедура у области информационе безбедности и управљање процесом континуитета пословања, што је неопходно како би била осигурана поузданост система.

У области правосуђа у Републици Србији, 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 Министарству правде, за управљање информационом безбедношћу у информационим системима који су обухваћени овом ревизијом, одговорна су и лица која управљају судовима, запослени који раде на ИТ пословима и у крајњој инстанци сви корисници ових система.

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.

Поред основног акта о безбедности информационог система, 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.

Даље, потребна је одговарајућа организациона ИТ структура, зато што је спровођење мера 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.

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. Оператери ИКТ система од посебног значаја су обавезни 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.

Ризик у области управљања континуитета пословања се може посматрати из два угла: у случају ванредних околности, и у случају раскида сарадње са пружаоцима услуга. У случају ванредних околности, потребно је да постоји план који ће пре свега обухватати активности и опрему потребну за поновно и што брже успостављање пословања. У случају раскида сарадње са пружаоцима услуга, највећи ризик може бити то што неће бити могућ даљи развој софтвера, у складу са потребама или законским изменама, али и отежано или онемогућено отклањање пре свега софтверских проблема уколико до њих дође, са једне стране, али и са друге стране отежана миграција података у случају преласка на ново софтверско решење.

Управљање ИТ ризицима представља једно од начела Закона о информационој безбедности. Сва питања разматрана у овој ревизији у основи имају процену одређених ризика (организација ИТ безбедности, приступ систему, континуитет пословања, итд.).

Циљ у оквиру другог ревизијског питања је анализа система у области информационе безбедности која треба да да оцену примењених мера заштите, да ли је у информационим системима у правосуђу успостављен ефективан оквир за континуитет пословања у случају ванредних околности и раскида уговора са пружаоцима услуга и да ли је Министарство правде успоставило свеобухватно управљање ИТ ризицима.

Наш закључак заснивамо на следећим налазима:

Налаз 2.1: Није у потпуности успостављена организација ИТ безбедности у правосуђу

Организација ИТ безбедности у правосуђу, због недостатка довољно стручног знања и недостатка кадровских капацитета, није успостављена тако да обухвата примену адекватних докумената која уређују ову област – акт о информационој безбедности, управљање инцидентима, приступ систему и примену других мера заштите ИКТ система, и адекватну организациону структуру ИТ безбедности, што за последицу има већи степен рањивости информационог система.

У овом делу циљ је био да се изврши анализа којом се утврђује да ли су усвојена и примењена одговарајућа документа која се односе на информациону безбедност – акт о безбедности информационог система и одговарајуће процедуре, да ли је успостављено управљање инцидентима и примена других мера заштите ИКТ система, што је и законска обавеза свих оператора ИКТ система од посебног значаја, да ли је успостављена организациона ИТ структура са утврђеним пословима и одговорностима запослених за управљање информационом безбедношћу и да ли су запослени оспособљени за посао који раде и разумеју своју одговорност.

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

Као што је раније наведено, Законом о уређењу судова је прописано да су између осталог послови правосудне управе које врши министарство надлежно за правосуђе: уређење и развој правосудног информационог система.

Законом о информационој безбедности, у члану 7. тачка 1. прописано је да се мере заштите ИКТ система односе на успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система.

Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, у члану 2. прописано је: оператор ИКТ система од посебног значаја (у даљем тексту: оператор ИКТ система) дужан је 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.

Информационим системима у Министарству правде се управља тако што је у оквиру унутрашње јединице Сектора за правосуђе образовано Одељење за ИКТ у оквиру ког постоје две групе, Група за ИКТ у грађанској и управној материји и Група за ИКТ у кривичној и прекршајној материји.

Група за ИКТ системе у грађанско – правној и управној материји обавља послове који се односе на: развој ИКТ у системима правосудних професија, судова опште надлежности за грађанско-правну материју, привредних судова, систему Управног суда, регистара у правосуђу, правосудне мреже, система за размену података, система за централно извештавање о раду судова и смештајних капацитета и рада дата центра и серверске опреме у правосуђу; учешће у припреми закона, других прописа, стандарда и мера у области примене ИКТ у правосудним професијама, привредним судовима, Управном суду и у судовима опште надлежности у грађанско-правној материји; учествовање у остваривању функције праћења, усмеравања и координације активности на развоју електронског система правосудних професија, судова опште надлежности у грађанско-правној материји, привредних судова и Управног суда; примену ИКТ у циљу унапређења организације, развоја и начина рада у правосудним професијама, судовима опште надлежности у грађанско-правној материји, привредним судовима и Управном суду; администрирање порталом електронске продаје покретних и непокретних ствари путем јавног надметања у извршном поступку; развој електронске платформе за успостављање портала за е-аукцију; давање налога за унапређење портала за е-аукцију, одобравање захтева за учешће у електронској продаји покретних и непокретних ствари путем јавног надметања корисницима портала; учествовање у подизању квалитета података о странкама у поступку и организација која омогућава ефикасну електронску размену између правосудних органа у држави као и успостављање основа за електронску размену са другим регионалним и ЕУ правосудним системима и регистрима; учествовање у реализацији ИТ програма и пројеката ЕУ и других организација за потребе правосуђа као и одржавање и унапређење ових система након имплементације и друге послове који се односе на ИКТ у правосудним оранима, обавља и друге послове из делокруга Групе.

Послови у Групи (тренутно броји 1+3), према Правилнику, обављају се у оквиру шест радних места, и то:

- радног места руководилац Групе, разврстаног у звање самостални саветник (1);

- радног место за припрему, планирање и управљање ИТ пројектима и заштиту података, разврстаног у звање самостални саветник, на коме је систематизован један извршилац;

- радног места за информатичку подршку у системима правосудних професија, у звању млађи саветник, на коме су систематизована два извршиоца (1);

- радног места за пројектовање, израду, имплементацију и одржавање пословних система у звању саветник, на коме је систематизован један извршилац;

- радног места за е-аукцију, у звању саветник, на коме су систематизован један извршилац;

- радног места за пројектанта информационих система у правосуђу у звању самостални саветник, на коме су систематизована два извршиоца (2).

Од шест радних места систематизованих Правилником о унутрашњем уређењу и систематизацији радних места, у Сектору за правосуђе, у Групи за ИКТ системе у грађанско – правној и управној материји у опису послова не постоје описи који се односе на информациону безбедност.

Група за ИКТ системе у кривично-правној материји, прекршајној материји, унутрашњим јединицама Министарства и органима управе у саставу Министарства обавља послове који се односе на: развој ИКТ у јавним тужилаштвима, судовима опште надлежности у кривично-правној материји, прекршајним судовима и унутрашњим јединицама и органима управе у саставу Министарства (Управа и заводи за извршење кривичних санкција и Дирекција за управљање одузетом имовином) и то: учешће у припреми закона, других прописа и стандарда и мера у области примене ИКТ у јавним тужилаштвима, судовима опште надлежности у кривично-правној материји, прекршајним судовима и органима управе у саставу Министарства; учествовање у остваривању функције праћења, усмеравања и координације активности на развоју ИКТ система у наведеним органима; послове међународне сарадње у примени ИКТ у наведеним органима; примену ИКТ с циљем унапређења организације, развоја и начина рада у наведеним органима из делокруга Групе; сарадњу са надлежним органима у поступку припреме, израде и спровођења стратегије, прописа, стандарда, планова, програма, пројеката и хардверско-софтверских решења од утицаја на развој ИКТ у наведеним органима; учествовање у подизању квалитета података о странкама у поступку и организација која омогућава ефикасну електронску размену између правосудних органа у држави као и успостављање основа за електронску размену са другим регионалним и ЕУ правосудним системима и регистрима и друге послове који се односе на ИКТ у органима из делокруга Групе.“

Послови у Групи, према Правилнику, обављају се у оквиру пет радних места, и то:

- радног места руководилац Групе, разврстаног у звање самостални саветник;

- радног места за информатичко-аналитичке послове у звању млађи саветник, на коме је систематизован један извршилац (1);

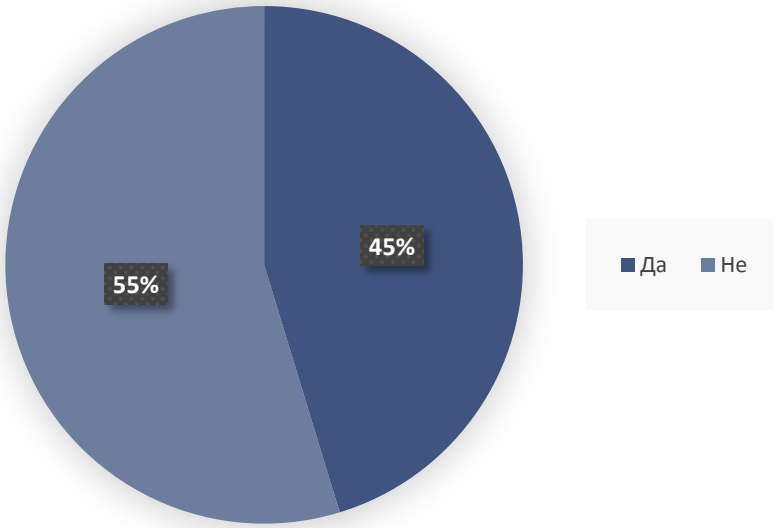
- радног места за подршку развоја информационог система, у звању млађег саветника, на коме су систематизован један извршилац (2);

- радног места за подршку дигитализацији у прекршајним судовим, у звању млађи саветник, на коме је систематизован један извршилац.

Од пет радних места систематизованих Правилником о унутрашњем уређењу и систематизацији радних места, у Сектору за правосуђе, у Групи за ИКТ системе у кривично-правној материји у опису послова не постоје описи који се односе на информациону безбедност.

Министарство правде није документовало да је другим актима послове информационе безбедности уредило на начин дефинисан наведеном уредбом и на начин који омогућава јасну поделу дужности и одговорности, али и контролу свих тих послова.

Када су судови у питању, 24 од 53 суда одговорило је да у суду постоји запослени који је одговоран за информациону безбедност.



Илустрација 9. *Да ли суд има одговорно лице за информациону безбедност?*

Како прописује Закон о информационој безбедности, 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.

Оператор ИКТ система утврђује процедуре комуникације са другим институцијама у случају инцидента у циљу благовремене пријаве, односно решавања насталог безбедносног инцидента.

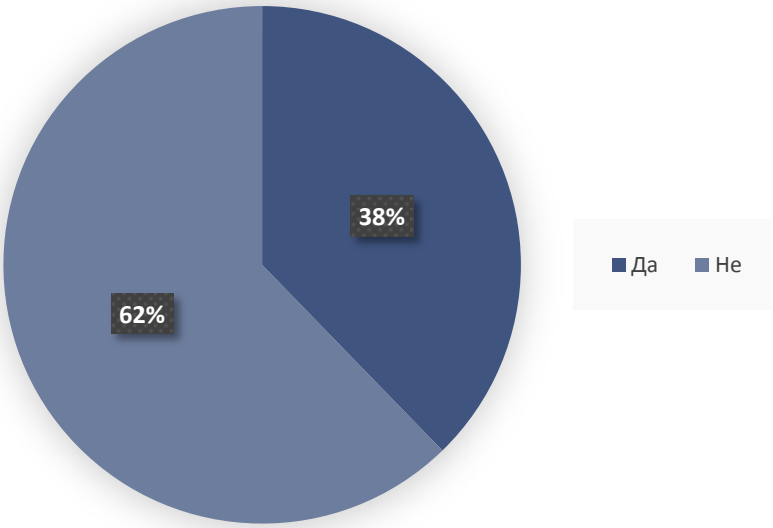
Акционим планом за поглавље 23 (јул 2020) дефинисано је да се активности на успостављању нормативног оквира и предузимање других мера ради унапређења ИКТ безбедности реализује до краја 2021. године, а као показатељи резултата наведени су:

- Успостављен одговарајући антивирус програм и редовно ажурирање кроз периодичне обуке за систем администраторе у судовима
- Израђен Закон о безбедности информација за највеће судове
- Планиране и спроведене обуке о информационој безбедности према ISO стандардима за судско ИТ особље
- Прописани поступци управљања ризиком
- Оптимизирани поступци контроле и сигурности у размени података

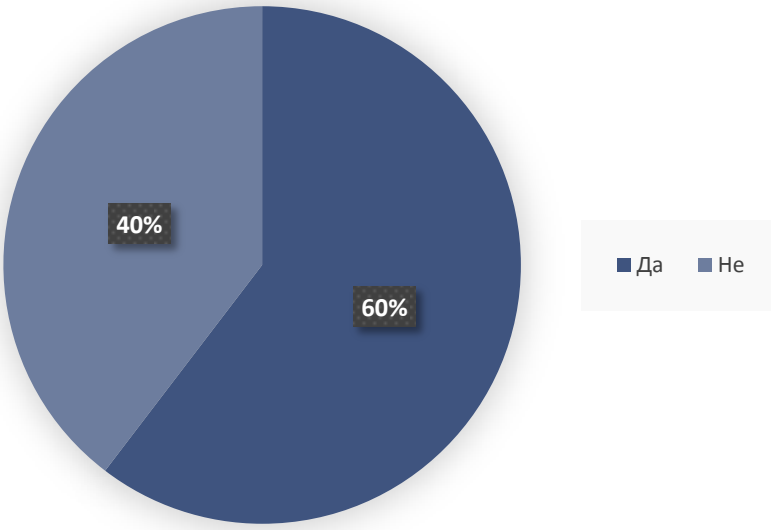
Министарство правде није усвојило акт о безбедности информационог система, већ је тај акт како су навели у министарству у фази нацрта.

Такође, Министарство правде није усвојило све неопходне процедуре које се односе на информациону безбедност, и навело је да су неке од њих у фази нацрта.

Када су у питању судови, 20 од 53 њих има усвојен акт о информационој безбедности.



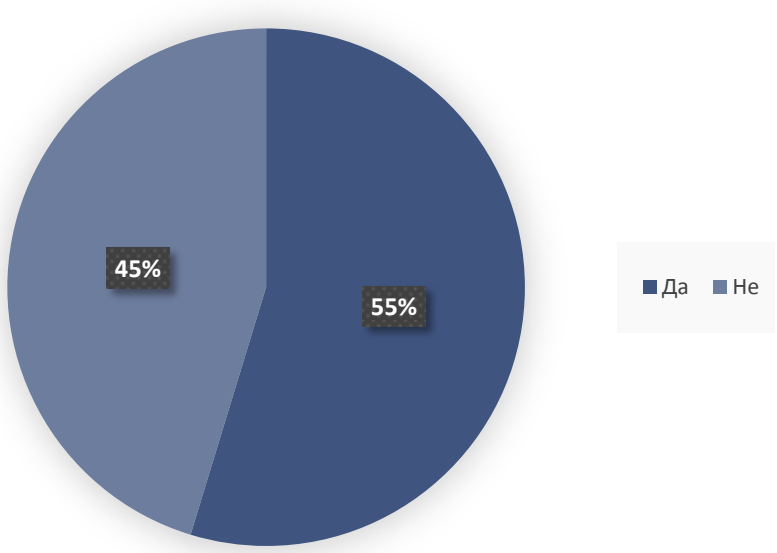
Илустрација 10. *Да ли је суд донео акт о информационој безбедности?*



Илустрација 11. *Да ли је суд организовао обуке запослених о ИТ темама?*

Од 53, у 32 суда су организоване обуке за запослене који користе информационе системе. Сталне обуке на ИТ теме, нарочито када се односе на безбедносна питања, умањују ризик да запослени нису у довољној мери информисани о могућим безбедносним претњама, нити довољно обучени да на њих одговоре правовременим предузимањем мера (вируси, фишинг итд.).

Један број судова (29 од 53) упознао је запослене са политиком информационе безбедности у суду, што се такође може подвести као један од видова обуке на ту тему.



Илустрација 12. *Да ли су запослени у суду упознати са политиком информационе безбедности?*

Чланом 11. Закона о информационој безбедности, прописана је обавеза оператора ИКТ система да обавештавају Надлежни орган о инцидентима који могу имати значајан утицај на нарушавање информационе безбедности.

Поступак достављања података о инцидентима у информационо-комуникационим системима од посебног значаја (у даљем тексту: ИКТ системи од посебног значаја) који могу да имају значајан утицај на нарушавање информационе безбедности, листа, врсте и значај инцидената и поступак обавештавања о инцидентима у ИКТ системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности прописан је Уредбом о поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја.

Чланом 28. Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, прописано је да је оператор ИКТ система у обавези да утврди процедуре којима се дефинишу одговорна лица задужена за превенцију и реаговање, план поступања у случају опасности од настанка безбедносних инцидената или настанка безбедносних инцидената, обавезу вођења евиденције о предузетим активностима, обавезу извештавања и размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама.

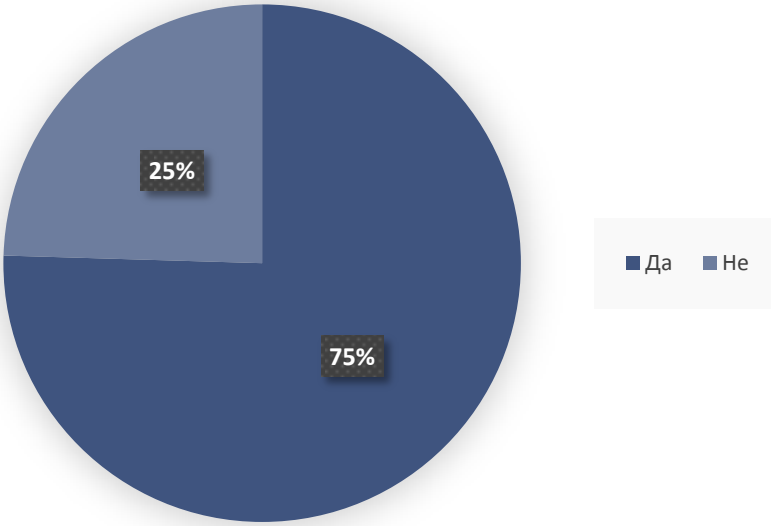
Циљ управљања инцидентима је успостављање механизама који доводи до тога да се најпре инциденти евидентирају, а затим и да се правовремено реагује. Како се инцидент може десити било где у систему, запослени који уочи настали проблем треба обавестити надлежно лице, које ће предузети даље кораке или дати 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, 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.).

Нису усвојене и успостављене процедуре које се односе на управљање инцидентима ни када је у питању Министарство правде, ни када су у питању судови.

Процедура која уређује питање пријављивања проблема је дефинисана у уговорима о пружању услуга одржавања и унапређења система, тачније у техничким спецификацијама које су саставни део уговора које Министарство правде потписује са пружаоцима услуга. У ту сврху, Добављач се обавезује да пружи подршку кориснику у суду путем on-line система за пријављивање грешака и захтева (у наставку: тикетинг система) који је корисницима у суду доступан 24 часа, 7 дана у недељи. Одговорни представници свих корисника у суду морају имати активан налог на тикетинг систему. Сви захтеви морају бити поднети преко тикетинг система на Интернет сајту који добављач постави за ову намену.

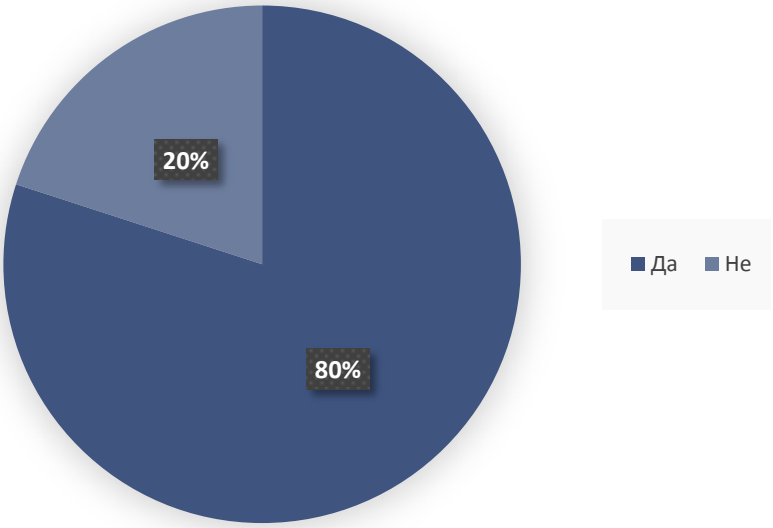
Члан 10. Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја прописује одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа и то:

- 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).



Илустрација 13. *Да ли је ради контроле приступа информационом систему успостављен систем управљања корисничким правима приступа?*

Када је у питању управљање корисничким налозима, у 40 судова је успостављен систем управљања корисничким налозима.



Илустрација 14. *Да ли се примењује физичко-техничка заштита ресурса ИС (непрекидно напајање електричном енергијом, климатизација…)?*

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.

Од 45, 36 судова је навело у одговору да примењују физичко-техничка заштиту ресурса ИС (непрекидно напајање електричном енергијом, климатизација…), док је девет судова одговорило да немају успостављену свеобухватну заштиту.

На основу свега наведеног, може се закључити да организација ИТ безбедности није успостављена тако да обухвата питања усвајања и примене адекватних докумената (процедуре, директиве итд.) која уређују ову област, а односи се на организациону

структуру ИТ безбедности, управљање инцидентима, приступ систему и примену других мера заштите ИКТ система, што за последицу има већи степен рањивости информационог система.

Како је већ наведено раније, судови сами уређују организациону структуру када су у питању ИТ послови, па самим тим и послове који се односе на информациону безбедност. Са друге стране, судови нису у овој ревизији субјекти ревизије, већ само Министарство правде. Због тога су препоруке које се односе на ова питања дате Министарству правде ради предузимања одређених мера у самом министарству и ради израде одговарајућих упутстава која би била упућена судовима ради предузимања мера у области информационе безбедности у сваком суду понаособ.

Препоручујемо Министарству правде да успостави мере информационе безбедности које обухватају усвајање и имплементацију аката која уређују ову област – акт о информационој безбедности, управљање инцидентима, приступ систему , и адекватну организациону структуру ИТ безбедности, како би биле примењене све неопходне мере безбедности и заштите података у информационим системима у правосуђу.

Препоручујемо Министарству правде да изради и судовима упути одговарајућа упутства у циљу успостављања мера информационе безбедности које обухватају усвајање и имплементацију аката која уређују ову област – акт о информационој безбедности, управљање инцидентима, приступ систему , и адекватну организациону структуру ИТ безбедности, како би биле примењене све неопходне мере безбедности и заштите података у информационим системима у правосуђу.

Налаз 2.2: Нису усвојени и имплантирани планови континуитета пословања у ванредним ситуацијама и у случају раскида уговора са пружаоцем услуга

Министарство правде и судови у Србији, због тога што не располажу потребним ресурсима, нису у потпуности успоставили мере које обезбеђују континуитет пословања у ванредним околностима и у случају прекида сарадње са пружаоцем услуга, што за последицу може имати нефункционисање информационог система у дужем временском периоду.

Један од циљева ревизије био је – анализа процеса континуитета пословања у ванредним околностима и у случају прекида сарадње са пружаоцима услуга. План континуитета пословања треба да обухвати: донета правила и процедуре које уређују континуитет пословања, успостављање плана опоравка од катастрофе, управљање резервним копијама и тестирање ових планова и резервних копија.

Законом о информационој безбедности, у члану 7. који прецизира мере заштите ИКТ система од посебног значаја, прописано је, између осталог, 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.

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.

Када су у питању посматрани системи у овој ревизији, три система су инсталирана и раде на серверима који су у Министарству правде (СИПРЕС, САПС И ПИС), док је АВП систем инсталиран на серверима који се налазе у судовима.

У сва четири случаја, тј. у сва четири система, потребно је обезбедити планове континуитета пословања у случају прекида сарадње са пружаоцем услуга који у овом случају не обухвата и план опоравка од катастрофе, али је ради будућег развоја и коришћења система неопходно да обухвати миграцију података.

Када су у питању планови континуитета пословања у ванредним околностима, њих је неопходно успоставити и у Министарству правде, али и у судовима, с обзиром на то да се у судовима налазе сервери на којима се извршава АВП систем.

Министарство правде нема усвојен јединствени план континуитета пословања. Уговором са пружаоцем услуга за појединачне информационе системе предвиђено је да се обезбеде планови континуитета. За процедуре које се односе на континуитет пословања и опоравак од катастрофе постоје нацрти.

Такође, не постоји тим за континуитет пословања и опоравак од катастрофе као такав, нити посебно дефинисана радна места у чијим описима послова су наведене активности у вези са наведеним плановима.

Током ванредног стања 2020. године, одређени су приоритети за обуке за коришћење ресурса за случај да лица која су обучена на појединачним системима буду онеспособљена услед епидемије. Том приликом су одређени и приоритети међу системима за случај да се ограниче буџети за одржавање.

Када је у питању управљање резервним копијама, постоји посебна резервна локација у Нишу, али није документовано са којим функционалностима, нити како се управља резервним копијама.

Није вршено тестирање плана континуитета пословања (резервних копија итд.).

Посебан циљ 4 Стратегије развоја ИКТ-а у правосуђу 2022–2027. године се управо односи на успостављање оквира за стандаризовање система управљања информационом безбедношћу, заштитом података о личности и континуитетом пословања е-правосуђа.

Уговорима о пружању услуга одржавања и унапређења (развоја) које Министарство правде потписује сваке године са пружаоцима услуга, прописана је обавеза пружаоца да обезбеди континуитет пословања за ИКТ системе.

Део техничке спецификације, који је саставни део уговора, а који се односи на основни ниво одржавања и подршке, дефинише да се под подршком рада подразумева корисничка подршка за несметани рад софтвера 24/7. Због тога је неопходно обезбедити услуге одржавања, као и подршку рада у периоду од 365 дана од дана потписивања Уговора.

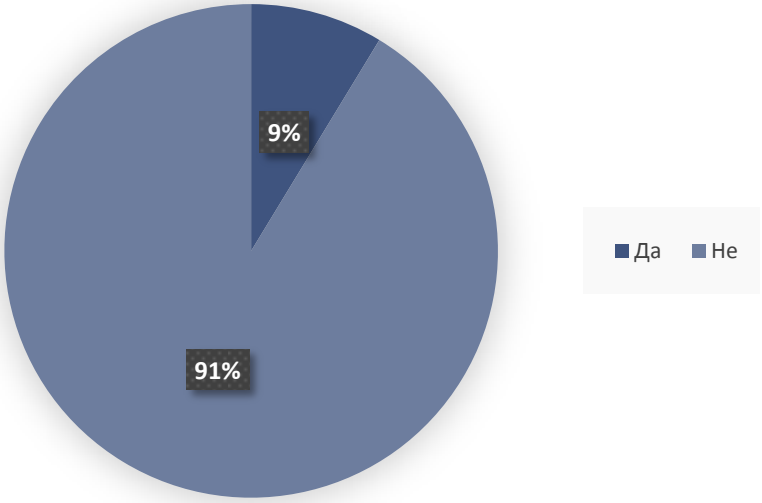
Услуге основног нивоа одржавања морају да обухвате: праћење рада постојећих система предвиђених одржавањем, превентивне и/или корективне мере које су у вези са идентификовањем грешака, превазилажење и отклањање грешака и сигурносних пропуста на постојећим системима предвиђених одржавањем, надоградњом платформе и системског софтвера и пружањем услуге консултација у вези са могућностима за унапређење, оптимизовање, усклађивање и конфигурисање већ постојећих апликативних решења, као и измене имплементираних решења услед законских промена.

Међутим, одговорност добављача, између осталог, не обухвата: измене у процесима имплементираног решења и грешке које су изазване проблемима у раду оперативних система, хардверу или рачунарско-комуникационој мрежи и измене у процесима имплементираног решења и грешке који су изазвани погрешним коришћењем система од стране корисника у суду.

Када је у питању континуитет пословања, у случају нежељених догађаја, пружаоци услуга немају одговорност и обавезу да успоставе опоравак од катастрофе, па и континуитет пословања. А са друге стране, Министарство правде нема капацитета да обави те послове (у конкретном случају, МПНТР није обезбедило континуитет јер поред софтверског решења треба обезбедити и одговарајуће техничке услове – хардвер, инфраструктуру итд., али и потребно стручно знање за инсталацију софтвера, базе података, техничку и стручну подршку корисницима итд.), тако да постоји висок ризик од тога да би у случају хаварије (нежељеног догађаја) дошло до прекида у раду система у дужем временском периоду. Уговором је предвиђено да Министарство

правде као власник кода добија сва потребна права да организује наставак одржавања на други начин.

Када су судови у питању, већ је речено: у сва четири система, потребно је обезбедити планове континуитета пословања у случају прекида сарадње са пружаоцем услуга који у овом случају не обухвата и план опоравка од катастрофе, али је ради будућег развоја и коришћења система неопходно да обухвати миграцију података.



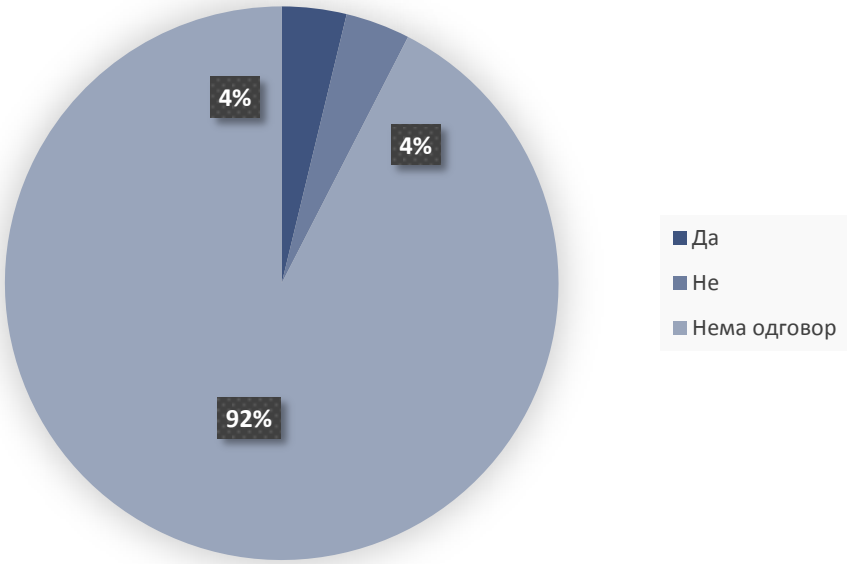
Илустрација 15. *Да ли постоји План континуитета пословања (BCP) у судовима?*

Када су у питању планови континуитета пословања у ванредним околностима, њих је неопходно успоставити и у судовима, с обзиром на то да се у судовима налазе сервери на којима се извршава АВП систем.

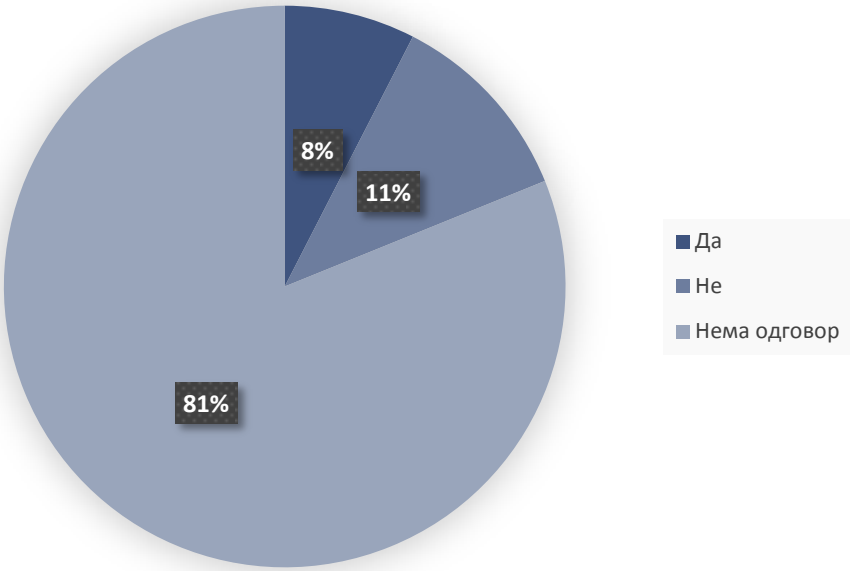
Велика већина судова који су доставили одговоре на питање да ли имају план континуитета пословања одговорила је да такав план нема (42 од 46).

На питање – да ли је, у склопу управљања континуитетом пословања, усвојен план опоравка активности у случају хаварије (DRP), већина судова није уопште одговорила, док су два суда навела да такав план имају.

На питање – да ли се спроводи тестирање планова континуитета, само четири суда је навело да врши тестирање, шест судова је навело да не тестира планове (мада су они већ навели да те планове и немају), док остали судови нису одговорили.

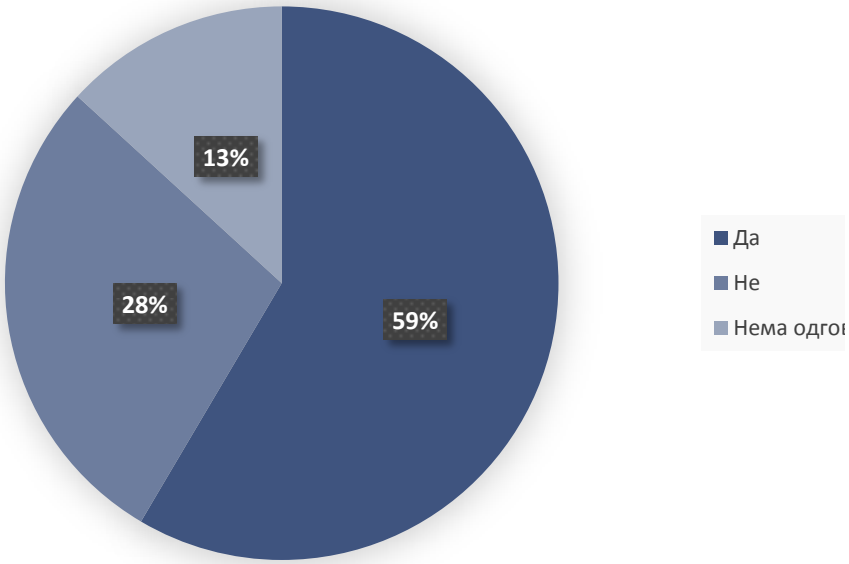


Илустрација 16. *Да ли је, у склопу управљања континуитетом пословања, у судовима усвојен план опоравка активности у случају хаварије (DRP)?*



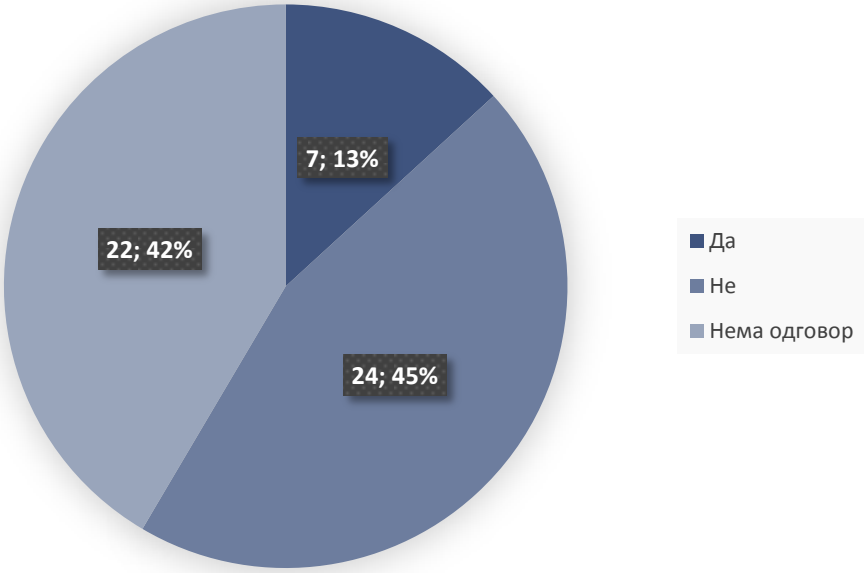
Илустрација 17. *Да ли се спроводи тестирање планова?*

Када је у питању управљање резервним копијама, што је обично активност у склопу планова континуитета пословања, 31 суд је навео да има усвојене процедуре и дефинисане одговорности у вези са креирањем резервних копија података.



Илустрација 18. *Да ли суд има усвојене процедуре и дефинисане одговорности у вези са креирањем резервних копија података?*

Седам судова је навело да се резервне копије складиште у безбедном простору (ван главног објекта), код 24 суда то није случај, док остали судови нису дали одговор на то питање.



Илустрација 19. *Да ли су резервне копије смештене у безбедан простор за одлагање ван објекта?*

Подаци који постоје у информационим системима судова постоје и у традиционалном папирном облику и они су приоритет што се тиче заштите, тако се поступа и на основу прописа о чувању судских предмета. Дакле, када су судови у питању, то један од начина да се обезбеди континуитет пословања, али у том случају не може се говорити о континуитету ИТ пословања.

На основу прикупљених података и обављене анализе, може се закључити да континуитет пословања није на адекватан начин успостављен ни у Министарству

правде ни у судовима. Поред тога што је то законска обавеза, план континуитета пословања пружа значајан одговор на ризике који постоје у вези са губитком података и треба да буде успостављен, и периодично тестиран. Ризик је већи када је у питању раскид сарадње са пружаоцима услуга јер у том случају недостаје неопходно знање потребно за наставак одржавања и развоја, а нарочито у случају преласка на нови систем и неопходну миграцију података. Када је у питању опоравак од нежељених догађаја (опоравак од катастрофе ДРП), такође не постоје одговарајући ни хардверски, а ни стручни ресурси, али како се још увек подаци налазе у папирном облику, не би дошло до губитка података, већ до значајног успоравања свих процеса. Из тих разлога дате су препоруке које следе.

Министарству правде препоручујемо да изради и судовима упути одговарајућа упутства у циљу успостављања континуитета пословања у ванредним околностима тако да обезбеде функционисање система у ванредним ситуацијама и у случају прекида сарадње са пружаоцима услуга, а што подразумева неопходан хардвер, апликативни софтвер, изворни код, стручно знање, базе података, управљање резервним копијама података и процес тестирања планова континуитета пословања.

Министарству правде препоручујемо да успостави континуитет пословања у ванредним околностима тако да обезбеди функционисање система у ванредним ситуацијама и у случају прекида сарадње са пружаоцима услуга, а што подразумева неопходан хардвер, апликативни софтвер, изворни код, стручно знање, базе података, управљање резервним копијама података и процес тестирања планова континуитета пословања.

Налаз 2.3: Управљање ИТ ризицима у правосуђу није успостављено

Министарство правде и судови у Србији, због непознавања ове проблематике, недовољно искуства и обученог ИТ кадра, нису успоставили управљање ИТ ризицима, 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, нарочито када се документација налази у електронском облику.

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

Разлози због којих је то тако јесу 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.

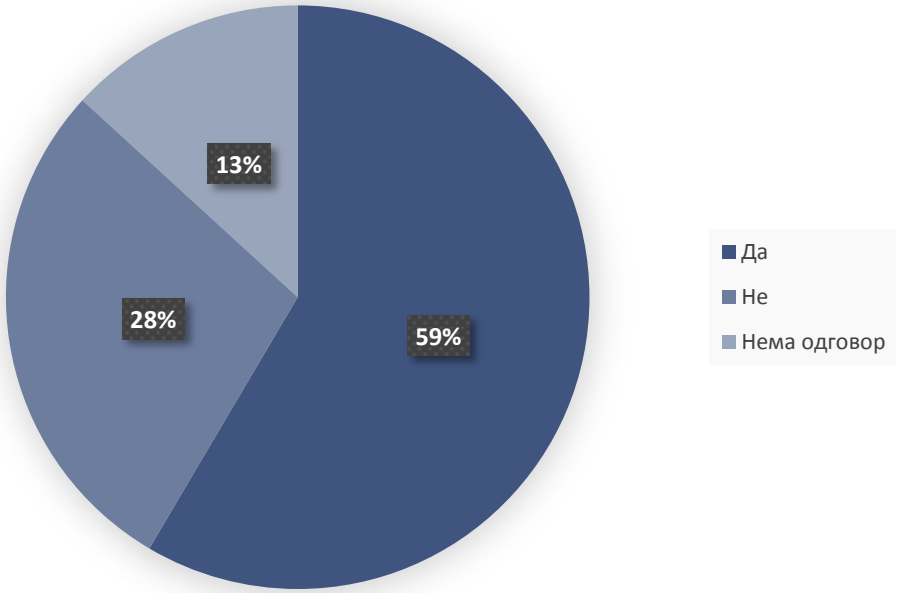
Другим речима, уколико се жели поуздан, али истовремено и ефикасан систем, без процене ризика то се не може постићи. На пример, могуће је све елементе система дуплирати и тако постићи скоро 100% поуздан систем. Али због цене дуплирања, такав систем се не може сматрати ефикасним јер се можда исти циљ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

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.

Министарство није успоставило управљање ИТ ризицима. Како је навело Министарство, израђени су нацрти аката за управљање ИТ ризицима, али нису усвојени. Процена ризика на нивоу система је рађена у оквиру ФУК-а, урађени су и нацрти аката за поступање. Није рађена анализа утицаја и нова процена ризика.



Илустрација 20. *Да ли су у систему управљања ризицима обухваћени и ИТ ризици?*

Министарство није успоставило управљање ИТ ризицима. Како је навело Министарство, израђени су нацрти аката за управљање ИТ ризицима, али нису усвојени. Процена ризика на нивоу система је рађена у оквиру ФУК-а, урађени су и нацрти аката за поступање. Није рађена анализа утицаја и нова процена ризика.

Када су у питању судови, на питање – да ли су у систему управљања ризицима обухваћени и ИТ ризици, у 31 суду су навели да јесу, 15 судова није успоставило управљање ИТ ризицима, док седам судова није доставило одговор.

Дакле, може се закључити да Министарство правде и судови нису успоставили управљање ризицима, што подразумева евидентирање, класификацију, анализу ИТ

ризика и дефинисање стратегије за смањивање/отклањање ризика. Из тог разлога, Министарству су дате одговарајуће препоруке.

Министарству правде препоручујемо да изради и судовима упути одговарајућа упутства у циљу успостављања управљања ИТ ризицима, што подразумева евидентирање, класификацију, анализу ИТ ризика и дефинисање стратегије за смањивање/отклањање ризика.

Министарству правде препоручујемо да успостави управљање ИТ ризицима, што подразумева евидентирање, анализу, класификацију ИТ ризика и дефинисање стратегије за смањивање/отклањање ризика.

ЗАКЉУЧАК 3: Није успостављен ефективан механизам сарадње Министарства правде и судова са пружаоцима услуге, зато што нису усвојена и имплементирана правила и процедуре када је у питању ова област, пружаоци услуга имају приступ продукционим базама и процес обраде података о личности није уређен на начин прописан законом

У случајевима када неке послове обавља пружалац услуге, уговором је потребно дефинисати све обавезе пружаоца услуга када је у питању информациона безбедност. Поред тога, послове који се односе на пружаоце услуга потребно је уредити и одговарајућим процедурама зато што акт о безбедности као општи акт обично не садржи детаљне инструкције како се неки процес спроводи и ко је за то одговоран. Усвајање и имплементација акта о информационој безбедности и одговарајућих процедура су и законска обавеза, при чему се посебна пажња треба посветити питањима приступа систему: физичком и логичком приступу, али и успостављању континуитета пословања, нарочито у случају када је то уговором дефинисана обавеза пружаоца услуга, зато што у случају раскида уговора постоји ризик од тога да систем неће моћи да функционише у дужем временском периоду.

Министарство правде није донело акт о информационој безбедности и процедуре (исто то није урадио и један број судова обухваћених упитником), које уређују сарадњу са пружаоцима услуга, посебно када је у питању информациона безбедност. То је онемогућило свеобухватан механизам контроле извршења обавеза које у том смислу законски има и Министарство и пружалац услуге. Треба додати: када су у питању системи обухваћени овом ревизијом, судови нису уговарали услуге пружалаца услуга, самим тим нису ни имали могућност да утичу на садржаје уговора, па и када је у питању информациона безбедност. То их, међутим, не ослобађа законских обавеза.

Слична ситуација је и када је у питању обрада података о личности. Због сложеног система у којем су судови руковаоци подацима, а информационе системе у којима се обрађују подаци набавља Министарство правде, које је обраду поверило другим обрађивачима – пружаоцима услуга, без посебног или општег овлашћења како то прописује Закон о заштити података о личности. У закону о уређењу судова чланом 70. прописано је, између осталог, да су послови правосудне управе које врши министарство надлежно за правосуђе – уређење и развој правосудног информационог система. Остали информациони системи нису поменути, нити је назначено да ли се

појам „правосудни информациони системи“ односи и на друге информационе системе или само на правосудни информациони систем. Такође, Законом о заштити података о личности, прописан је однос руковаоца и обрађивача, нарочито када су у питању безбедносне мере, поверавање обраде другом обрађивачу итд.

Наш закључак заснивамо на следећим налазима:

Налаз 3.1: Сарадња са пружаоцем услуга није уређена процедурама

Због недовољно стручног кадра и знања, Министарство правде и судови у Србији није усвојили и имлементирали правила и процедуре које се односе на безбедност података када је у питању сарадња са пружаоцима услуга тако да и поред тога што у уговорима са пружаоцима услуга постоји део који се односи на поверљивост података, није успостављен механизам за контролу којом се утврђује да ли пружалац услуга поштује обавезе у вези са поверљивошћу података па је самим тим и нижи степен поузданости система. Пружаоци услуга имају приступ продукционим базама. Законом о информационој безбедности и Уредбом о ближем уређењу мера заштите информационо-комуникационих система прописана је обавеза обезбеђивања механизма који одржава уговорени ниво

Када су у питању пружаоци услуга, 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).

Уредбом о ближем уређењу мера заштите ИКТ система од посебног значаја прописано је у члану 26. да оператор ИКТ система у својим процедурама предвиђа ниво доступности и врсту информација и средства којима могу да приступе пружаоци услуга, начине приступа информацијама и средствима и надзор над приступом. Оператор ИКТ система треба да идентификује и успостави процедуре безбедности информација које се конкретно баве приступом информацијама пружаоца услуга унутар организације. Обавезе пружаоца услуга у вези са информацијама и средствима која су доступна пружаоцима услуга оператора ИКТ система регулишу се споразумом између оператора ИКТ система и пружаоца услуга, чијим одредбама се обезбеђује адекватан ниво заштите информација и средстава, у складу са прописима и техничким стандардима. Оператор ИКТ система дужан је да обезбеди да пружалац услуга обавља поверене активности у складу са актом о безбедности ИКТ система, односно другим актима којима се уређује безбедност његовог информационог система. У члану 27. је

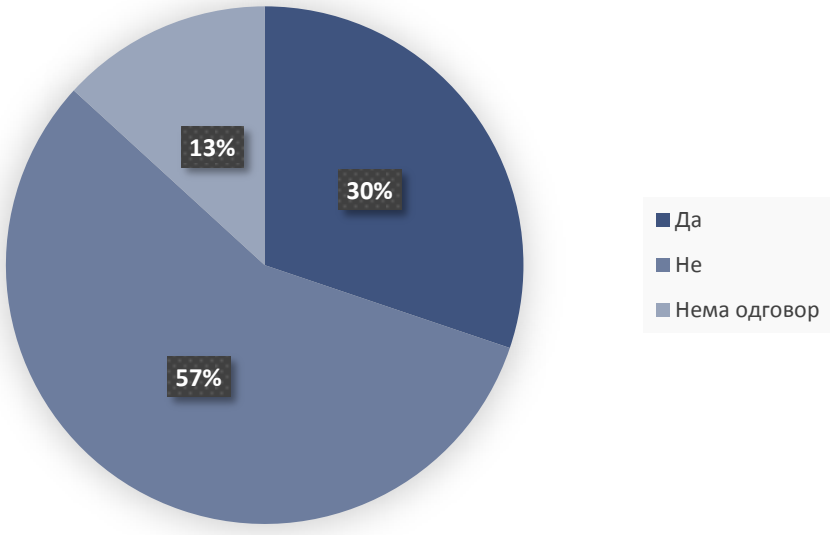
прописано да у циљу одржавања уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга, оператор ИКТ система успоставља механизме надзора над пружањем услуга, именује лице које је задужено за праћење реализације пружања услуга и контролу испуњености нивоа информационе безбедности, применом одговарајућих процедура и успоставом надзора.

Министарство правде није усвојило процедуре које се односе на одржавање уговореног нивоа информационе безбедности и пружених услуга, у складу са условима који су уговорени са пружаоцем услуга.

Између осталог, у складу са обавезама из Уговора о пружању услуга одржавања, дефинисано је чување пословне тајне у члану 14, где се наводи да се Пружалац услуга обавезује да чува као пословну тајну сваки документ, информацију, податак или друге чињенице које су у вези са Наручиоцем и његовим пословањем, а који му буду доступни током реализације Уговора, како за време трајања Уговора, тако и по истеку истог, сходно члану 4. Закона о заштити пословне тајне („Службени гласник РС“, бр. 72/11). Уколико пословна тајна која садржи податак од интереса за Републику Србију, а који се сматра тајним податком и штити се по одредбама закона којим се уређује тајност података, Пружалац услуга је дужан да исту чува као тајни податак у складу са одредбама закона којим се уређује тајност података. Изјава о чувању поверљивих података Наручиоца је саставни део Уговора (Прилог 4).

Не постоје друге одредбе нити механизми који су у функцији заштите података. Пружаоци услуга имају приступ продукционим базама увек, без обавезе да приступ најаве или да траже дозволу за приступ.

Када су у питању судови, 16 судова је навело да има усвојене процедуре којима се уређује питања информационе безбедности, заштите пословних или личних података којима имају приступ добављачи услуга. тридесет судова је навело да такву врсту процедуре нема, док седам судова није одговорило на то питање.



Илустрација 21. *Да ли постоји процедура/акт којим се уређује питања информационе безбедности, заштите пословних или личних података којима имају приступ добављачи услуга?*

На основу наведеног, може се закључити да ови послови ни у Министарству правде ни у судовима нису уређени процедурама и другим актима, самим тим нису успостављени/уређени ни сви неопходни механизми контроле када је у питању сарадња са пружаоцима услуга. Зато су Министарству правде упућене одговарајуће препоруке.

Министарству правде препоручујемо да изради и судовима упути одговарајућа упутства у циљу усвајања и имплементирања правила и процедура за безбедност података када је у питању сарадња са пружаоцима услуга, што подразумева обавезну примену мера заштите података, и успостављање механизма за праћење примене тих мера.

Препоручујемо Министарству правде да усвоји и имплементира правила и процедуре за безбедност података када је у питању сарадња са пружаоцима услуга, што подразумева обавезну примену мера заштите података, и успостављање механизма за праћење примене тих мера.

Налаз 3.2: Министарство правде није успоставило сарадњу са пружаоцима услуга на начин који јасно разграничава улоге Министарства, судова и пружалаца услуга када је у питању обрада података о личности

Због сложеног система у којем су судови руковаоци подацима, а информационе системе у којима се обрађују подаци набавља Министарство правде, није успостављена обрада података о личности на начин који је законом прописан јер је обрађивач – Министарство правде, обраду поверило другим обрађивачима – пружаоцима услуга, без посебног или општег овлашћења како то прописује Закон о заштити података о личности. Последица је смањени степен поузданости система.

Чланом 4. Закона о заштити података о личности, прописано је да поједини изрази у овом закону имају следеће значење:

1) „податак о личности“ је сваки податак који се односи на физичко лице чији је идентитет одређен или одредив, непосредно или посредно, посебно на основу ознаке идентитета, као што име и идентификациони број, података о локацији, идентификатора у електронским комуникационим мрежама или једног, односно више обележја његовог физичког, физиолошког, генетског, менталног, економског, културног и друштвеног идентитета;
2) „лице на које се подаци односе“ је физичко лице чији се подаци о личности обрађују;
3) „обрада података о личности“ је свака радња или скуп радњи које се врше аутоматизовано или неаутоматизовано са подацима о личности или њиховим скуповима, као што су прикупљање, бележење, разврставање, груписање, односно структурисање, похрањивање, уподобљавање или мењање, откривање, увид, употреба, откривање преносом, односно достављањем, умножавање, ширење или на други начин чињење доступним, упоређивање, ограничавање, брисање или уништавање (у даљем тексту: обрада).

Чланом 42. Закона о заштити података о личности, прописано је да се мере заштите уређују 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, истим чланом прописано је 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).

Члан 45. овог закона прописује да, 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 о 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 тако да 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).

Руковалац и обрађивач дужни су да предузму мере у циљу обезбеђивања система по којем 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).

Када је правосуђе у Србији у питању, као и конкретни системи обухваћени ревизијом, руковаоци су судови. Министарство правде је, ако се узме у обзир дефиниција обраде података – обрађивач („обрада података о личности“ је свака радња или скуп радњи које се врше аутоматизовано или неаутоматизовано са подацима о личности или њиховим скуповима, као што су прикупљање, бележење, разврставање, груписање, односно структурисање, похрањивање, уподобљавање или мењање, откривање, увид, употреба, откривање преносом, односно достављањем, умножавање, ширење или на други начин чињење доступним, упоређивање, ограничавање, брисање или уништавање, у даљем тексту: обрада). Пошто је Министарство правде набавило све посматране информационе системе, оно је практично обраду података поверило другом обрађивачу, без посебног или општег овлашћења. У закону о уређењу судова, чланом 70. прописано је, између осталог, да су послови правосудне управе које врши министарство надлежно за правосуђе – уређење и развој правосудног информационог система. Остали информациони системи нису поменути, нити је назначено да ли се појам „правосудни информациони системи“ односи и на друге информационе системе или само на правосудни информациони систем.

Такође, Законом о заштити података о личности, прописане су обавезе и однос руковаоца и обрађивача, нарочито када су у питању безбедносне мере. Једина мера коју може суд да примени када је у питању заштита од неовлашћеног приступа јесте (поред контроле физичког приступа сервер салама) неодавање података за приступ које користе запослени у суду. То међутим није довољна мера, имајући у виду раније наведену чињеницу да пружаоци услуга имају приступ продукционим базама, али и резервним копијама података. 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). Анализом претходно описаних постојећих и недостајућих мера заштите може се закључити да све неопходне мере нису прописане.

Министарству је на основу свега наведеног дата препорука.

Министарству правде препоручујемо да уреди процес обраде података када је у питању сарадња са пружаоцима услуга на начин који јасно разграничава улоге Министарства, судова и пружалаца услуга када је у питању обрада података о личности.

V Захтев за доставу одазивног извештаја

Субјект ревизије је, 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.

Субјект ревизије је обавезни да у одазивном извештају искаже 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 субјект ревизије је у обавези да достави 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 субјект ревизије је у обавези да достави 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 субјект ревизије је у обавези да достави 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

Ревизија је спроведена у складу са Методолошким правилима и смерницама за ревизију сврсисходности пословања.

Да бисмо одговорили на ревизијска питања, анализирали смо законску и подзаконску регулативу, користили стручну литературу (WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions[15]), као и све податке добијене од субјекта ревизије и извора информација – судова. Анализирали смо податке и информације за период од 2019. до 2021. године.

На основу прикупљених података у току предстудије и у складу са Приручником за спровођење ревизије, одабране су три ИТ области у оквиру којих су обављени поступци ревизије: ИТ управљање, Информациона безбедност и Сарадња са пружаоцем услуга.

Илустрација 22. *ИТ области*

У циљу одговора на ревизијска питања, а имајући у виду законодавни и институционални оквир у периоду 2019–2021. године, за субјект ревизије изабрано је Министарство правде.

У циљу прикупљања података послали смо упитнике корисницима информационих система обухваћених ревизијом.

У току спровођења ревизије судовима је послат упитник, у коме су тражени следећи подаци:

[15] INTOSAI Радна група за ИТ ревизију

- Назив суда и адреса,
- Број запослених на ИТ пословима,
- Број рачунара,
- Да ли суд има ИТ стратешки план,
    - Да ли суд има орган/радну групу или еквивалентно тело у чијој је надлежности ИТ?
    - Да ли су правилником о унутрашњој организацији и систематизацији радних места обухваћени послови у вези ИТ?
- Број рачунара и оперативни систем који се користи,
    - Да ли суд има лице које је одговорно за функционисање и безбедност ИС/ИТ?
    - Да ли суд врши обуку запослених у вези са ИТ темама?
    - Да ли су у систему управљања ризицима обухваћени и ИТ ризици?
    - Да ли постоји процедура/акт којим се уређује питања информационе безбедности, заштите пословних или личних података којима имају приступ добављачи услуга?
    - Да ли су усвојене процедуре и дефинисане одговорности у вези са креирањем резервних копија података?
    - Да ли постоји План континуитета пословања (BCP)?
    - Да ли је, у склопу управљања континуитетом пословања, усвојен план опоравка активности у случају хаварије (DRP)?
    - Да ли се спроводи тестирање планова?
    - Да ли сте усвојили Акт о информационој безбедности?
    - Да ли је ради контроле приступа информационом систему успостављен систем управљања корисничким правима приступа?
    - Да ли се примењује физичко-техничка заштита ресурса ИС (непрекидно напајање електричном енергијом, климатизација…)?
    - Да ли се примењује енкрипција осетљивих/личних података?

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

Ревизијско питање 1:

- Преглед ИТ стратегије или интервјуисање руководства да би се утврдило на који начин су утврђени и одобрени циљеви;
- 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;
- Анализа документације;
- Увид у евиденцију о рачунарској опреми у судовима и тужилаштвима, и поређење са њиховим евиденцијама;
- Преглед одобрених или одбијених захтева за изменом система;
- Преглед документације у вези са пријавом и решавањем проблема корисника;
- Периодичан преглед белешки са састанка руководства да би се осигурало да су стратешке ИТ одлуке донете на највишем 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 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 у информационим системима;

Ревизијско питање 2:

- Анализа Акта о безбедности ИКТ система;
- Преглед докумената за процену да су правила и процедуре у складу са Законом о информационој безбедности и Уредбом о ближем уређењу мера заштите;
- Анализа Правилника о унутрашњем уређењу и систематизацији радних места, у делу који се односи на информациону безбедност;
- Утврђивање – да ли је одговорност за ИТ безбедност формално и јасно наведена;
- Преглед извештаја о спроведеним обукама који се односе на информациону безбедност;
- Утврђивање – да ли су и у којој мери примењене препоруке из Извештаја повереника;
- Анализа којом се утврђује 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;
- Анализа извештаја о инцидентима ради процене шта је предузето;
- 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;
- 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 којом се утврђује да ли су квалитативни захтеви за лозинке дефинисани и примењени у складу са правилима и процедурама и/или најбољом праксом;
- Провера којом се утврђује 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;
- Анализа 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;
- Анализа спискова корисника у судовима и у МП ради оцене ажурности;
- Провера процедуралних мера које је установа предузела да би се ускладила са захтевима поверљивости;
- Провера којом се утврђује 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 којом се утврђује да ли су извођачи извршили повреде безбедности информација. Провера активности руководства у погледу таквих кршења;
- Прегледање матрица улога за утврђивање одговорности за администрирање конфигурације и опсега контроле конфигурације у операцијама;
- 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 прављење резервних копија почело у утврђеним временским оквирима и да су резервне копије задржане за назначен временски период;
- Провера којом се утврђује 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 којом се утврђује да је безбедност, како логична тако и физичка, адекватна за локацију резервне копије;
- Провера којом се утврђује 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 којом се утврђује да ли МП контролише да ли су сачувани број и статус датотека, апликативног софтвера и хардвера током прављења резервних копија и поступка опоравка података;
- Провера којом се утврђује 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;
- Провера којом се утврђује да ли се организација постарала да је континуитет пословања садржан у споразуму о пружању услуге;
- Анализа стратегије за управљање ризицима;

Ревизијско питање 3:

- Анализирати како је уређен приступ пружаоца услуге информационим системима и серверима, као и другим потребним ресурсима и да ли се то евидентира и где;
- Проверити да ли се прати извршење обавеза пружаоца услуге када су у питању нивои услуга дефинисани уговором;
- Провера извештаја о безбедносним инцидентима и докумената за праћење како би се утврдило које активности МП предузима када пружаоц услуге крши безбедносна правила и процедуре;
- Провера процедура које је МП предузело, а које се односе на питања поверљивости;
- Провера којом се утврђује да ли уговорни услови и обавезе дефинишу безбедносна ограничења и обавезе које контролишу како ће пружалац услуге користити имовину организације и приступати информационим системима и услугама;

- Провера којом се утврђује да ли су пружаоци услуга извршили повреде безбедности информација. Провера активности руководства у погледу таквих кршења;
- Анализа којом се утврђује шта су примарне контроле физичке безбедности система. Провера којом се утврђује да ли одговарају најновијој анализи ризика;
- Прегледање локацијских и физичких мера предострожности у смислу кључних елемената ИТ инфраструктуре. Провера којом се утврђује какве су контроле за заштиту животне средине успостављене (апарат за гашење пожара, аларм, системи за напајање, итд.);
- Провера процедура у циљу утврђивања учесталости прегледања различитих приступа и привилегија које запослени код пружаоца услуга имају;
- Провера којом се утврђује 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;
- Провера којом се утврђује да ли је, уз нулте или минималне трошкове, могуће из постојећег система добити додатне услуге, превасходно у области услуга ка грађанима;
- Утврђивање – да ли постоје капацитети да се услуге које сада обезбеђује пружаоц услуга реализују унутар МП?

Да ли је однос између МП, правосудних органа и пружаоца услуга у складу са Законом о заштити података о личности?

Обавили смо интервјуе са одговорним лицима Министарства правде.

Такође, у циљу прикупљања доказа и одговора на ревизијска питања, послат је велики број захтева за доставу одговора судовима, да би се одвојено посматрало како је успостављен систем код субјекта ревизије, а како код судова.