ДРЖАВНА РЕВИЗОРСКА ИНСТИТУЦИЈА

РЕЗИМЕ ИЗВЕШТАЈА О РЕВИЗИЈИ СВРСИСХОДНОСТИ ПОСЛОВАЊА

„Информациони системи у правосуђу”

6. фебруар 2023. године

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.

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.

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.

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.

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.

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.

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.

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.

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

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); 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; приликом будућег развоја и одржавања информационих система омогући равноправно коришћење папирне и електронске документације; 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; 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; 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; 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; 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; успостави управљање ИТ ризицима, што подразумева евидентирање, анализу, класификацију ИТ ризика и дефинисање стратегије за смањивање/отклањање ризика; 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; 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; 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;