ДРЖАВНА
РЕВИЗОРСКА
ИНСТИТУЦИЈА

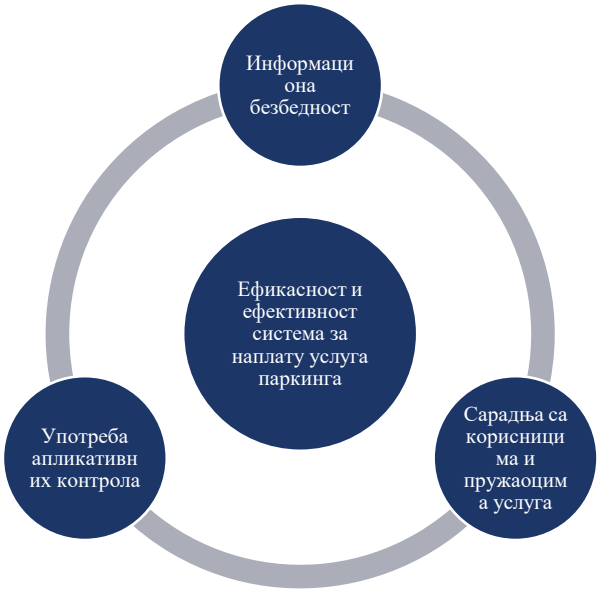
ИЗВЕШТАЈ
О РЕВИЗИЈИ СВРСИСХОДНОСТИ ПОСЛОВАЊА

Информациони системи за наплату услуга паркинга

Број: 400-1058/2024-07/59
Београд, 23. април 2025. године

Информациони системи за наплату паркинга у Србији показују значајан напредак у Београду и Новом Саду, али Чачак, Краљево и Крушевац морају унапредити безбедност података, контролу приступа и континуитет пружања услуга како би системи постали потпуно поуздани и транспарентни.

Информациони системи за услуге паркирања треба да обезбеде контролу наплате и коришћења паркинг места, ефикасно управљање паркинг простором и информисање грађана у реалном времену. Међутим, утврђени су недостаци у приступу базама података, континуитету пословања и механизмима за контролу наплате и управљања.



Слика 1. Тема ревизије

Мере информационе безбедности у јавним комуналним предузећима обезбеђују различит ниво поузданости информационих система, са значајним напретком у Новом Саду и Београду, док Чачак, Краљево и Крушевац остају са озбиљним недостацима који угрожавају сигурност и континуитет пословања.

Сарадња са корисницима система у Београду и Новом Саду значајно је унапређена, али остаје простор за додатни напредак кроз успостављање криптовања и потпуну примену процедура за архивирање, миграцију и уништавање података код Новог Сада.

Механизам сарадње са пружаоцима услуга у Чачку, Краљеву и Крушевцу није у потпуности испунио неопходне циљеве, укључујући и поузданост података, због недостатка процедура за сарадњу, надзор и планирање континуитета пословања у случају раскида сарадње, што указује на потребу за системским унапређењем и јачањем контролних механизама.

Апликативне контроле обезбеђују основну контролу наплате и пружених услуга, док је у Београду и Новом Саду постигнут напредак, али у Чачку, Краљеву и Крушевцу недостају механизми за потпуну транспарентност и ефикасност.

Препоруке

Након спроведене ревизије, Државна ревизорска институција је субјектима ревизије, дала препоруке:

- да развију и примене свеобухватне планове континуитета пословања који укључују поступке за ванредне околности и раскид сарадње са пружаоцима услуга.
- да унапреде механизме заштите података који обухватају криптовање осетљивих информација, контролу приступа и примену стандарда за информациону безбедност.
- да обезбеде функционалност апликативних контрола за праћење наплате, управљање корисничким налозима и евиденцију активности ради побољшања транспарентности и поузданости података.
- да унапреде доступност информација о паркинг зонама и слободним местима интеграцијом са мобилним апликацијама и отвореним платформама.
- да успоставе јасне процедуре и уговорне обавезе за надзор и сарадњу са пружаоцима услуга, укључујући дефинисање одговорности за заштиту података и континуитет пословања.

Садржај

Скраћенице и термини

Табела број 1: Коришћене скраћенице у извештају

Пун назив	Скраћеница
Информационе технологије	ИТ
Информациони систем	ИС
Информационо-комуникациони систем	ИКТ систем
Јавно комунално предузеће за јавне гараже и паркиралишта „Паркинг сервис“, Београд	ЈКП „Паркинг сервис“, Београд
Јавно комунално предузеће „Паркинг сервис“, Нови Сад	ЈКП „Паркинг сервис“, Нови Сад
Јавно комунално предузеће „Паркинг сервис“, Чачак	ЈКП „Паркинг сервис“, Чачак
Јавно комунално предузеће „Чистоћа“, Краљево	ЈКП „Чистоћа“, Краљево
Јавно предузеће „Пословни центар“, Крушевац	ЈП „Пословни центар“, Крушевац
Јединица локалне самоуправе	ЈЛС
Општа регулатива о заштити података о личности (General Data Protection Regulation)	GDPR
Државна ревизорска институција	Институција

I Резиме извештаја

1. Резиме откривених несврсисходности и препорука

Државна ревизорска институција је спровела ревизију сврсисходности пословања „Информациони системи за наплату услуга паркинга“.

Информациони системи у локалним самоуправама који се односе на јавну услугу паркинга треба да имају основне функције: контролу наплате карата (сатне, дневне, месечне, трафик и посебне) и информације о доступности паркинга како би се плаћање вршило у складу са квалитетом и квантитетом пружених услуга.

Циљ ревизије је да се оцени ефективност и ефикасност информационог система у јавним предузећима за контролу и наплату услуга паркирања који се односе на услуге паркинга, односно да се испита у којој мери су примењене мере испуниле неопходне циљеве када је у питању управљање системима, поузданост информационих система и управљање подацима корисника – грађана, као и да се испита у којој мери систем омогућава ефикасност контроле наплате и плаћања услуга паркинга. Поузданост електронских података и информационих система подразумева интегритет, тачност, конзистентност и очување података, безбедност информационог система и континуитет пословања, имајући у виду сврху за коју се ти подаци и системи користе.

Након спроведене ревизије утврдили смо:

Информациони системи за наплату паркинга у Републици Србији показују значајан напредак у Београду и Новом Саду, али Чачак, Краљево и Крушевац морају унапредити безбедност података, контролу приступа и континуитет пружања услуга како би системи постали потпуно поуздани и транспарентни.

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

1. Мере информационе безбедности у јавним комуналним предузећима обезбеђују различит ниво поузданости информационих система, са значајним напретком у Новом Саду и Београду, док Чачак, Краљево и Крушевац остају са озбиљним недостацима који угрожавају сигурност и континуитет пословања.
   - Законом о информационој безбедности и Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја прописано је да сваки оператор ИКТ система мора успоставити процедуре за управљање безбедносним инцидентима. Ове процедуре треба да обухвате дефинисање одговорних лица, план поступања у случају инцидената, евиденцију активности, извештавање и размену информација о безбедносним слабостима, претњама и инцидентима. Анализа је показала да само ЈКП „Паркинг сервис“, Београд, и ЈКП „Паркинг сервис“, Нови Сад, имају успостављене процедуре за управљање безбедносним инцидентима. Ове процедуре су усклађене са важећим прописима и укључују дефинисане механизме за идентификацију, анализу, реаговање и праћење инцидената. Насупрот томе, ЈКП „Паркинг сервис“, Чачак, ЈКП „Чистоћа“, Краљево, и ЈП „Пословни центар“, Крушевац, немају утврђене формалне процедуре за управљање инцидентима, нити су дефинисани механизми за њихову евиденцију и извештавање. Недовољно улагање у развој процедура, недостатак кадрова са потребним компетенцијама и недовољна свест о

значају формализованих процедура за управљање инцидентима довели су до овог стања. Такође, у појединим предузећима није постојао систематски приступ развоју мера заштите у складу са регулаторним оквиром. Недостатак формалних процедура за управљање безбедносним инцидентима значајно смањује могућност правовременог реаговања на претње, што може довести до нарушавања континуитета пословања, губитка података, компромитације система и повећања ризика од поновљених инцидената. Ово стање представља слабост у безбедносном оквиру предузећа која се одражава и на квалитет пружених услуга.

- Законом о информационој безбедности и Уредбом о ближем уређењу мера заштите ИКТ система од посебног значаја прописано је да оператори ИКТ система морају обезбедити контролу приступа, ограничење и надзор администраторских овлашћења, чување и редовно преиспитивање логова, као и успостављање механизама за контролу и надзор над услугама које пружају трећа лица. Уговори са пружаоцима услуга треба да садрже клаузуле којима се обезбеђује ниво безбедности података у складу са прописаним мерама. У ЈКП „Паркинг сервис“, Београд, и ЈКП „Паркинг сервис“, Нови Сад, успостављени су детаљни акти и процедуре који регулишу доделу и укидање приступа, контролу администраторских налога, евидентирање активности, као и редовну ревизију корисничких налога. У Чачку, Краљеву и Крушевцу утврђени су значајни недостаци: не постоје формализоване процедуре за деактивацију налога, лог фајлови се не чувају или нису доступни предузећу, а администраторске овлашћења имају и лица којима по опису посла не припадају. Поред тога, уговори са пружаоцима услуга не садрже одредбе о надзору над њиховим активностима, нити је обезбеђен увид у рад администратора код трећих лица. Недовољан развој интерних процедура, недостатак стручних капацитета за контролу и надзор, као и изостанак свеобухватног уговарања безбедносних обавеза са пружаоцима услуга доприносе неадекватном управљању приступима и активностима у ИКТ системима. Овакво стање доводи до повећаног ризика од неовлашћеног приступа и компромитације података, онемогућава утврђивање одговорности у случају инцидената и угрожава сигурност, интегритет и континуитет рада информационих система.
- Законом о информационој безбедности и Уредбом о ближем уређењу мера заштите ИКТ система од посебног значаја прописано је да оператори ИКТ система морају да успоставе мере заштите које обезбеђују континуитет обављања послова у ванредним околностима, као и мере заштите од губитка података. Ове мере подразумевају доношење формализованих планова континуитета пословања и плана опоравка од катастрофе (DRP), као и процедуре за израду, проверу и безбедно чување резервних копија података. ЈКП „Паркинг сервис“, Нови Сад је једино предузеће које је успоставило три формализована плана континуитета за различите критичне сценарије, уз дефинисане одговорности и редовно тестирање применљивости. Поред тога, систем израде резервних копија у овом предузећу је уређен, са копијама које се чувају и на удаљеним локацијама, у складу са безбедносним политикама. У Београду је поступак за израду планова формално дефинисан и обухвата више ризичних сценарија, али појединачни планови за те ситуације нису развијени. Резервне копије се

редовно праве и чувају, укључујући и ван примарне локације, уз полугодишњу проверу исправности. Са друге стране, у Чачку, Краљеву и Крушевцу нису донети формални планови континуитета, нити су утврђене интерне процедуре за поступање у случају ванредних околности. У овим предузећима ослањање на пружаоце услуга није праћено уговорним клаузулама које би осигурале усклађеност са прописаним стандардима. Када је реч о резервним копијама, у Чачку и Краљеву нема доказа о постојању интерне политике израде и тестирања копија, а подаци се чувају искључиво код пружаоца услуга. У Крушевцу су резервне копије предвиђене актом, али се не чувају ван основне локације, чиме се смањује њихова ефективност у кризним ситуацијама. Недовољна уређеност система за континуитет пословања и управљање резервним копијама произилази из непотпуне примене прописаних мера, недостатка стручних капацитета и неадекватне процене ризика. Ово доводи до повећаног ризика од губитка података, продуженог прекида рада и немогућности наставка пружања услуга грађанима у случају већих хаварија или сајбер инцидената, што може имати озбиљне последице по функционисање предузећа и поузданост њихових ИКТ система.

- Законом о информационој безбедности и Уредбом о ближем уређењу мера заштите ИКТ система прописано је да оператори ИКТ система морају успоставити механизме за управљање ИТ ризицима. Ови механизми треба да обухвате идентификацију, процену, третман и мониторинг ризика, како би се осигурала сигурност, интегритет и доступност информационих система. ЈКП „Паркинг сервис“, Нови Сад, већ је имало успостављен систем за управљање ризицима, који укључује Стратегију управљања ризицима и регистар ризика. Током ревизије, предузеће је ревидирало и ажурирало своје класификације ризика, чиме је побољшана процена утицаја и дефинисани додатни механизми за смањење ризика. ЈКП „Паркинг сервис“, Београд, је у току ревизије допунило свој Правилник о систематизацији послова и унапредило процедуре управљања ризицима, чиме је омогућило бољу интеграцију процене ризика у редовне пословне активности. Насупрот томе, у ЈКП „Паркинг сервис“, Чачак, ЈКП „Чистоћа“, Краљево, и ЈП „Пословни центар“, Крушевац, механизми управљања ризицима нису успостављени. У овим предузећима није формализована одговорност запослених за управљање ИТ ризицима, нити су дефинисане процедуре за идентификацију и процену ризика. Ова предузећа нису показала значајан напредак у овој области током ревизије. Недостатак довољних улагања, ограничени кадровски капацитети и свест о значају управљања ризицима представљају главне узроке оваквог стања. Последице ових недостатака укључују повећан ризик од безбедносних инцидената, губитка података и нарушавања континуитета пословања. Предузећа која нису успоставила механизме за управљање ризицима остају подложна негативним последицама које могу значајно утицати на њихову ефикасност и поузданост.

2. Сарадња са корисницима система у Београду и Новом Саду значајно је унапређена, али остаје простор за додатни напредак кроз успостављање криптовања и потпуну примену процедура за архивирање, миграцију и уништавање података код Новог Сада.

- ЈКП „Паркинг сервис“, Београд и ЈКП „Паркинг сервис“, Нови Сад су правилницима, процедурама и физичком заштитом обезбедили безбедност података корисницима система.
- Законом о заштити података о личности и Уредбом о ближем уређењу мера заштите ИКТ система од посебног значаја, пружаоци ИТ услуга морају успоставити свеобухватне механизме за заштиту података корисника. Ови механизми треба да укључују јасно дефинисане улоге руковаоца, обрађивача и подобрађивача података, као и мере за контролу приступа, надзор активности и осигурање поверљивости и интегритета података. ЈКП „Паркинг сервис“, Београд, је успоставило систематску заштиту података кроз Правилник о заштити података о личности и друге интерне акте, чиме је обезбеђена контрола приступа, евиденција активности и сарадња са подобрађивачем. Подаци корисника су заштићени кроз процедуре које укључују изјаве о поверљивости и процену ризика, уз јасну поделу улога између руковаоца, обрађивача и подобрађивача. У Новом Саду, у току ревизије су донете нове процедуре и уговори који прецизно дефинишу права и обавезе свих страна у обради података. Такође, предузете су мере за уклањање приступа осетљивим подацима и планирана је имплементација криптовања података, што је значајно унапредило ниво заштите. Иницијални недостаци у систематизацији и процедурама били су резултат недостатка свести о значају управљања подацима, као и недовољног техничког капацитета. Током ревизије, ова питања су делимично решена увођењем нових мера и процедура. Систематским унапређењем заштите података корисника, ризик од компромитације је значајно смањен. Ово је омогућило већу поузданост система, бољу сарадњу са корисницима и усклађеност са законским и стандардним захтевима за информациону безбедност. Ипак, неопходно је наставити са редовним надзором и ажурирањем процедура како би се обезбедио континуитет у високом нивоу заштите.
- Законом о заштити података о личности и релевантним стандардима, као што су ISO/IEC 27001 и ISO/IEC 27018, прописано је да пружаоци услуга морају успоставити механизме за сигурно управљање подацима након раскида уговора. Ове мере укључују архивирање, сигурно уништавање и омогућавање повраћаја података клијентима, уз строго дефинисане процедуре и контроле. Анализом је утврђено да ЈКП „Паркинг сервис“, Београд, иницијално није имало успостављене процедуре за сигурно управљање подацима након раскида уговора. Услед ревизије, предузеће је усвојило процедуру „Предаја и брисање података са сервера услед престанка уговорних обавеза“ (ПС.П64), која обезбеђује извоз података, пренос криптографских кључева и трајно брисање података уз примену сертификованих метода. Овај процес је усклађен са стандардима и документован како би се обезбедила транспарентност и сигурност. У ЈКП „Паркинг сервис“, Нови Сад, иницијално су недостајале формализоване процедуре за уништавање и повраћај података. Током ревизије, предузеће је закључило нове уговоре са прецизно дефинисаним правима и обавезама, укључујући обавезу преноса података у електронском формату, трајно брисање података на захтев корисника и коришћење апликације „SWAT“ у периоду од три месеца након истека уговора. Такође, уведена је процедура надзора над процесом брисања, која укључује извештавање и

документовање свих активности. Недостатак иницијалних мера у оба предузећа проистицао је из недовољне техничке уређености и свести о значају ових активности. Током ревизије, ова питања су успешно решена увођењем процедура и технолошких решења. Резултат ових мера је значајно унапређење сигурности управљања подацима након раскида уговора. Ова унапређења су смањила ризик од компромитације података, обезбедила усклађеност са прописима и повећала поверење корисника у системе који се користе за наплату услуга паркинга.

3. Механизам сарадње са пружаоцима услуга у Чачку, Краљеву и Крушевцу није у потпуности испунио неопходне циљеве, укључујући и поузданост података, због недостатка процедура за сарадњу, надзор и планирање континуитета пословања у случају раскида сарадње, што указује на потребу за системским унапређењем и јачањем контролних механизама.
   - У складу са Законом о информационој безбедности и најбољим праксама, сва предузећа која су корисници услуга морају успоставити процедуре за сарадњу са пружаоцима услуга и надзор над извршењем уговорних обавеза. Ове процедуре треба да обезбеде контролу приступа, праћење активности и спровођење мера које осигуравају сигурност и поузданост информационих система. ЈКП „Паркинг сервис“, Чачак, ЈКП „Чистоћа“, Краљево, и ЈП „Пословни центар“, Крушевац, нису успоставили адекватне процедуре за сарадњу и надзор над активностима пружалаца услуга. У Чачку је одговорност за надзор дефинисана Актом о безбедности ИКТ система, али недостају документи који потврђују редовно праћење активности. У Краљеву и Крушевцу, иако су надзорне функције дефинисане интерним актима, процедуре нису формализоване, нити постоји евиденција о спровођењу надзора. Главни узроци оваквог стања су недовољна свест о значају надзора, недостатак техничких капацитета и формализованих процедура, као и ограничени кадровски ресурси. Недостатак адекватних процедура за сарадњу и надзор значајно умањује способност ових предузећа да обезбеде сигурност и поузданост својих информационих система. Ово повећава ризик од компромитације података, непридржавања уговорних обавеза и потенцијалних прекида у континуитету пословања.
   - У складу са Законом о заштити података о личности и Законом о информационој безбедности, предузећа која користе услуге спољних пружалаца дужна су да успоставе механизме за контролу заштите података. Ове мере укључују дефинисање одговорности пружалаца услуга, ограничење приступа осетљивим подацима, као и увођење процедура за праћење активности и осигурање усаглашености са законским прописима. Анализа стања у ЈКП „Паркинг сервис“, Чачак, ЈКП „Чистоћа“, Краљево, и ЈП „Пословни центар“, Крушевац, показала је да ове организације нису успоставиле адекватне контроле заштите података. У Чачку, пружалац услуга има приступ базама података са осетљивим информацијама, али уговори не прецизирају мере заштите, нити је обезбеђен надзор над обрадом података. У Краљеву и Крушевцу слично, недостају механизми који би осигурали да се подаци користе искључиво у предвиђене сврхе. Крушевцу такође недостаје сагласност корисника пре обраде података, што представља ризик за угрожавање поверљивости и права грађана. Главни узроци оваквог стања су недовољна техничка и кадровска опремљеност, као и недостатак свести о значају примене стандарда и процедура у области

заштите података. Поред тога, уговори са пружаоцима услуга не садрже прецизне одредбе о управљању подацима. Овакви недостаци повећавају ризик од неовлашћене обраде и злоупотребе података, чиме се угрожавају права корисника и сигурност информационих система. Неопходно је да предузећа успоставе јасне механизме заштите података кроз уговорне обавезе и примену процедура које гарантују усаглашеност са прописима и минимизирање ризика од компромитације података.

- Уредбом о ближем уређењу мера заштите ИКТ система од посебног значаја, прописано је да оператор ИКТ система треба да предвиди мере којима се обезбеђује обављање послова у ванредним околностима, укључујући процедуре за опоравак система и континуитет рада у случају прекида сарадње са пружаоцем услуга. Ове мере подразумевају јасно дефинисане планове, одговорности и механизме заштите података, укључујући миграцију података и одржавање доступности критичних функционалности система. План континуитета пословања треба да обухвати и сценарије у којима више не постоји сарадња са досадашњим пружаоцем услуга, што је нарочито важно за системе који се ослањају на екстерну инфраструктуру. У ЈКП „Чистоћа“, Краљево, и ЈП „Пословни центар“, Крушевац, нису успостављени планови континуитета пословања у случају раскида сарадње са пружаоцима услуга, нити су уговорима предвиђене активности које би обезбедиле наставак функционисања кључних компоненти система. У случају прекида уговора, било би онемогућено праћење расположивости паркинг места, продаја карата и контрола услуга, што би негативно утицало на кориснике и приходе. Такође, уговори не садрже одредбе о миграцији података, што повећава ризик од њихове недоступности или губитка. У ЈКП „Паркинг сервис“, Чачак, уговором са пружаоцем услуга предвиђен је наставак функционисања одређених функционалности и у случају раскида сарадње, али предузеће није успоставило интерне планове нити дефинисало обавезе у погледу миграције података, што представља потенцијалну слабост. У недостатку формализованих интерних планова и уговорне заштите у случају прекида сарадње, ова предузећа се ослањају искључиво на текуће уговоре без предвиђања алтернативних решења и механизама опоравка. Недостају прецизне процедуре које би дефинисале шта се дешава након прекида сарадње, ко обезбеђује техничку инфраструктуру, где се чувају подаци и како се успоставља нови начин рада у периоду до успостављања новог система. Одсуство ових механизама смањује отпорност система на ванредне околности и повећава зависност од једног пружаоца услуга. Овакво стање значајно повећава ризик од оперативних прекида, губитка података и умањења квалитета услуге за крајње кориснике. Уколико не постоје јасно дефинисани уговорни и интерни механизми за превазилажење прекида сарадње, предузећа су изложена ризику да неће бити у могућности да одмах наставе пружање услуга, што може довести до финансијских губитака, оштећења репутације и смањења поузданости система.

4. Апликативне контроле обезбеђују основну контролу наплате и пружених услуга, док је у Београду и Новом Саду постигнут напредак, али у Чачку, Краљеву и Крушевцу недостају механизми за потпуну транспарентност и ефикасност.

- Законом о информационој безбедности и Уредбом о ближем уређењу мера заштите ИКТ система од посебног значаја прописано је да оператор ИКТ система мора успоставити механизме за управљање приступом, деактивацију корисничких налога и контролу над активностима унутар апликација. Ови механизми треба да обезбеде да само овлашћена лица имају приступ осетљивим подацима и да се све активности евидентирају, без угрожавања интегритета података. У ЈКП „Паркинг сервис“, Београд, и ЈКП „Паркинг сервис“, Нови Сад, иницијално су постојали пропусти у апликативним контролама, као што је неконтролисано преименовање налога и приступ осетљивим подацима од стране неовлашћених запослених. Током ревизије су ови пропусти отклоњени кроз увођење механизама за ограничење приступа, евидентирање активности и спречавање измена налога без одобрења. Насупрот томе, у Чачку, Краљеву и Крушевцу апликативне контроле нису адекватно развијене. У Чачку уопште не постоје процедуре за управљање налозима; у Краљеву, иако постоје интерни акти, они нису примењени у пракси; у Крушевцу је целокупна контрола препуштена пружаоцу услуга, без интерног надзора. У Чачку запослени имају неограничен приступ базама података, а механизам деактивације налога није успостављен, што оставља простор за злоупотребу. У Краљеву деактивација није аутоматизована, а уговори са пружаоцем услуга не предвиђају мере за заштиту података у складу са безбедносним стандардима. У Крушевцу не постоји увид у поступке које пружалац примењује, па није могуће ни утврдити да ли се уопште примењују механизми контроле приступа и деактивације налога. У свим овим случајевима постоји ризик од компромитације података и губитка интегритета система. Недостатак контроле приступа, непостојање механизама за деактивацију налога и могућност неконтролисаног приступа осетљивим подацима представљају озбиљне слабости које могу довести до неовлашћене обраде података, губитка историје активности, правне одговорности и нарушавања поверења грађана. Унапређење апликативних контрола и увођење формализованих процедура је неопходно ради обезбеђења поузданости информационог система и заштите личних података корисника.
- Апликативни софтвер за продају карата у свих пет предузећа обезбеђује функционалност и поуздано праћење продаје.
- Законом о заштити података о личности и релевантним стандардима, као што су ISO/IEC 27001 и ISO/IEC 27018, прописано је да пружаоци услуга морају успоставити механизме за сигурно управљање подацима након раскида уговора. Ове мере укључују архивирање, сигурно уништавање и омогућавање повраћаја података клијентима, уз строго дефинисане процедуре и контроле. Анализом је утврђено да ЈКП „Паркинг сервис“, Београд, иницијално није имало успостављене процедуре за сигурно управљање подацима након раскида уговора. Услед ревизије, предузеће је усвојило процедуру „Предаја и брисање података са сервера услед престанка уговорних обавеза“ (ПС.П64), која обезбеђује извоз података, пренос криптографских кључева и трајно брисање података уз примену сертификованих метода. Овај процес је усклађен са стандардима и документован како би се обезбедила транспарентност и сигурност. У ЈКП „Паркинг сервис“, Нови Сад, иницијално су недостајале формализоване

процедуре за уништавање и повраћај података. Током ревизије, предузеће је закључило нове уговоре са прецизно дефинисаним правима и обавезама, укључујући обавезу преноса података у електронском формату, трајно брисање података на захтев корисника и коришћење апликације „SWAT“ у периоду од три месеца након истека уговора. Такође, уведена је процедура надзора над процесом брисања, која укључује извештавање и документовање свих активности. Недостатак иницијалних мера у оба предузећа проистицао је из недовољне техничке уређености и свести о значају ових активности. Током ревизије, ова питања су успешно решена увођењем процедура и технолошких решења. Резултат ових мера је значајно унапређење сигурности управљања подацима након раскида уговора. Ова унапређења су смањила ризик од компромитације података, обезбедила усклађеност са прописима и повећала поверење корисника у системе који се користе за наплату услуга паркинга.

Након спроведене ревизије „Информациони системи за наплату услуга паркинга“, Државна ревизорска институција даје субјектима ревизије следеће препоруке:

ЈКП „Паркинг сервис“, Београд:

1) да развије и имплементира планове континуитета за све критичне сценарије прекида ИТ функција како би се осигурао несметан опоравак у ванредним ситуацијама (Налаз 1.3) – Приоритет 2[1].

ЈКП „Паркинг сервис“, Нови Сад:

1) да спроведе криптовање осетљивих података корисника система и осигура да управљање криптографским кључевима буде у надлежности руковаоца података, уз редовну проверу сигурности овог процеса (Налаз 2.2) – Приоритет 2[2];
2) да усвоји правилник и процедуре које ће регулисати архивирање, уништавање и миграцију података у случају раскида сарадње са корисницима услуга, укључујући извоз података и пренос криптографских кључева (Налаз 2.3) – Приоритет 2;
3) да омогући коришћење отворених података и даљи развој мобилне апликације, како би побољшао доступност информација о паркинг местима и унапредио услуге за грађане (Налаз 4.3) – Приоритет 3[3].

ЈКП „Паркинг сервис“, Чачак:

1) да ажурира Акт о безбедности информационо-комуникационог система како би укључио све специфичности које се односе на информациони систем за наплату паркинг услуга, укључујући јасно дефинисане одредбе о поверавању послова и односу са пружаоцима услуга (Налаз 1.1) – Приоритет 1;
2) да усвоји и имплементира процедуре које детаљно уређују послове из области информационе безбедности, укључујући превенцију и реаговање на безбедносне инциденте, вођење евиденције о предузетим активностима, као и

[1] Приоритет 2 – Несврсисходности које је могуће отклонити у року до једне године.
[2] Приоритет 2 – Несврсисходности које је могуће отклонити у року до једне године.
[3] Приоритет 3 – Несврсисходности које је могуће отклонити у року до три године.

обавезу извештавања и размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама (Налаз 1.1) – Приоритет 2;

3) да јасно дефинише одговорна лица задужена за све аспекте информационе безбедности, укључујући превенцију и реаговање на безбедносне инциденте, како би се обезбедила јасна подела дужности и одговорности и омогућио ефикасан надзор над свим аспектима информационе безбедности (Налаз 1.1) – Приоритет 1;
4) да успостави и имплементира процедуру чувања и контроле активности корисника и администратора кроз лог фајлове, како би се осигурало праћење и надзор над свим активностима на ИКТ систему (Налаз 1.2) – Приоритет 2;
5) да осигура да се у пракси води евиденција и контрола приватних уређаја који приступају ИКТ систему, како би се смањио ризик од неовлашћеног приступа и обезбедила безбедност система (Налаз 1.2) – Приоритет 1;
6) да ажурира Акт о безбедности информационо-комуникационог система како би укључио одредбе о изнајмљивању сервера и администрирању система од стране пружаоца услуга, са јасно дефинисаним мерама заштите и контроле приступа, у складу са важећим прописима и стандардима (Налаз 1.2) – Приоритет 1;
7) да развије и усвоји план континуитета пословања у ванредним околностима, који ће обезбедити континуитет пословања и неометано функционисање система у складу са уговорним обавезама према пружаоцу услуга (Налаз 1.3) – Приоритет 2;
8) да успостави процес управљања ИТ ризицима, укључујући дефинисање послова и одговорности у овој области у Правилнику о систематизацији радних места (Налаз 1.4) – Приоритет 1;
9) да усвоји и имплементира процедуре које ће уредити сарадњу са пружаоцима услуга, укључујући јасно дефинисане одговорности за контролу приступа подацима и надзор над извршењем уговорних обавеза (Налаз 3.1) – Приоритет 2;
10) да документује све активности везане за надзор над пружаоцима услуга, укључујући праћење приступа подацима и извршење уговорних обавеза, како би се обезбедила адекватна заштита података и поузданост система (Налаз 3.1) – Приоритет 2;
11) да успостави механизам за контролу усаглашености пружаоца услуга са условима за заштиту података, укључујући редовне провере и документацију свих активности везаних за безбедност података (Налаз 3.2) – Приоритет 1;
12) да ревидира уговор са пружаоцем услуга како би укључио одредбе о заштити и обради података у складу са Законом о заштити података о личности, са јасно дефинисаним одговорностима и обавезама обе стране (Налаз 3.2) – Приоритет 2;
13) да успостави јасне процедуре за управљање корисничким налозима, укључујући процедуре за деактивацију корисничких налога приликом престанка радног односа или промене радног места (Налаз 4.1) – Приоритет 2;
14) да обезбеди механизме за спречавање трајног брисања налога без угрожавања интегритета података, као и да омогући праћење активности корисника како би се осигурао потпуни траг активности у систему (Налаз 4.1) – Приоритет 2;

15) да спроведе редовну проверу и ажурирање корисничких налога како би се осигурало да приступ систему имају само овлашћена лица (Налаз 4.1) – Приоритет 1;
16) да омогући коришћење отворених података и развој мобилне апликације како би се грађанима омогућио лакши приступ информацијама о паркинг услугама (Налаз 4.3) – Приоритет 3.

ЈКП „Чистоћа“, Краљево:

1) да ажурира Акт о безбедности информационо-комуникационог система како би био усклађен са специфичностима система за наплату паркинг услуга, укључујући тачну дефиницију на који се информациони систем који део акта односи (Налаз 1.1) – Приоритет 1;
2) да усвоји и имплементира процедуре које на детаљан начин уређују послове из области информационе безбедности, укључујући процедуре за праћење активности, ревизију и надзор у оквиру управљања информационом безбедношћу (Налаз 1.1) – Приоритет 2;
3) да јасно дефинише одговорна лица задужена за све аспекте информационе безбедности, укључујући превенцију, реаговање и извештавање о безбедносним инцидентима, како би се осигурала јасна подела дужности и одговорности и обезбедила ефикасна контрола (Налаз 1.1) – Приоритет 1;
4) да успостави процедуре за деактивацију корисничких налога у случају промене радног места или престанка радног ангажовања запослених, како би се смањио ризик од неовлашћеног приступа ИКТ систему (Налаз 1.2) – Приоритет 2;
5) да успостави процедуре за чување и контролу активности корисника и администратора кроз чување лог фајлова, што би омогућило ефикаснији надзор над коришћењем система и спречавање потенцијалних злоупотреба (Налаз 1.2) – Приоритет 2;
6) да успостави систем евиденције и контроле приступа приватних уређаја који се користе за приступ ИКТ систему, уз обезбеђење адекватних мера заштите података (Налаз 1.2) – Приоритет 2;
7) да у Акт о безбедности ИКТ система укључи одредбе које регулишу изнајмљивање сервера и администрирање од стране пружаоца услуга, како би се осигурао адекватан надзор над тим процесима (Налаз 1.2) – Приоритет 1;
8) да успостави план континуитета пословања у ванредним околностима, који ће обезбедити неометано функционисање система за наплату и контролу паркирања у складу са уговорним обавезама и захтевима информационе безбедности (Налаз 1.3) – Приоритет 2;
9) да успостави процес управљања ИТ ризицима, укључујући дефинисање послова и одговорности у овој области у Правилнику о систематизацији радних места (Налаз 1.4) – Приоритет 1;
10) да усвоји и имплементира процедуре које ће уредити сарадњу са пружаоцима услуга (Налаз 3.1) – Приоритет 2;
11) да документује све активности везане за надзор над пружаоцима услуга, укључујући праћење приступа подацима и извршење уговорних обавеза (Налаз 3.1) – (Приоритет 1;

12) да ревидира уговор са пружаоцем услуга како би укључио одредбе о заштити и обради података у складу са Законом о заштити података о личности, са јасно дефинисаним одговорностима и обавезама обе стране (Налаз 3.2) – Приоритет 2;
13) да у Правилнику о систематизацији радних места дефинише лице задужено за сарадњу са пружаоцима услуга, са јасно одређеним одговорностима у погледу заштите података (Налаз 3.2) – Приоритет 1;
14) да успостави механизам за праћење и контролу приступа поверљивим подацима од стране пружаоца услуга и да ограничи приступ само на неопходне податке (Налаз 3.2) – Приоритет 2;
15) да успостави план континуитета пословања у случају раскида сарадње са пружаоцем услуга, како би се осигурало непрекинуто функционисање система за контролу и наплату паркинга (Налаз 3.3) – Приоритет 2;
16) да ревидира уговоре са пружаоцем услуга како би укључили одредбе о активностима и обавезама пружаоца услуга у случају раскида сарадње, као и миграцију података, са циљем обезбеђивања континуитета пословања и несметаног наставка коришћења података у новом систему (Налаз 3.3) – Приоритет 2;
17) да успостави механизам за деактивацију корисничких налога који ће омогућити задржавање свих података које је корисник унео у систем (Налаз 4.1) – Приоритет 1;
18) да омогући праћење активности сваког корисника, како би се задржао траг уноса и одговорности запослених, чак и након престанка њиховог радног ангажовања (Налаз 4.1) – Приоритет 1;
19) да се модул „Мапа“ прилагоди и учини доступним за јавност како би грађани могли да се информишу о тренутној доступности паркинг места у реалном времену (Налаз 4.3) – Приоритет 1;
20) да омогући приступ отвореним подацима о паркинг услугама, како би грађани и правна лица могли лакше да користе и развијају апликације за боље информисање о доступности паркинг места и другим услугама (Налаз 4.3) – Приоритет 3.

ЈП „Пословни центар“, Крушевац:

1) да ажурира Акт о безбедности информационо-комуникационог система од посебног значаја, тако да у потпуности обухвати специфичности свих коришћених информационих система, укључујући и систем за контролу и наплату паркирања (Налаз 1.1) – Приоритет 1;
2) да успостави и формализује процедуре за управљање безбедносним инцидентима, које ће обухватити превенцију, реаговање, евиденцију и извештавање о безбедносним инцидентима у складу са Актом о безбедности (Налаз 1.1) – Приоритет 2;
3) да усклади описе послова и радних задатака запослених који су одговорни за ИТ безбедност са одредбама Акта о безбедности, како би се обезбедило да сви релевантни аспекти безбедности и управљања инцидентима буду адекватно покривени (Налаз 1.1) – Приоритет 1;
4) да ограничи администраторска права само на лица која су непосредно одговорна за администрацију ИКТ система, уз јасно дефинисане надлежности

и одговорности, и да осигура да лица пружаоца услуга немају администраторска овлашћења без претходног знања и сагласности одговорних лица у предузећу (Налаз 1.2) – Приоритет 2;

5) да ажурира Акт о безбедности тако да јасно дефинише методе физичко-техничке заштите просторија у којима се налазе средства и документи ИКТ система, како би се смањио ризик од неовлашћеног приступа (Налаз 1.2) – Приоритет 1;
6) да уведе механизам за редовно праћење и ревизију права приступа ИКТ систему, уз обезбеђење чувања и надзора лог фајлова активности корисника унутар предузећа, како би се осигурао интегритет и безбедност система (Налаз 1.2) – Приоритет 1;
7) да успостави и усвоји план континуитета пословања и план опоравка активности у случају хаварије (Disaster Recovery Plan - DRP) који ће обезбедити континуитет пословања и брз опоравак у случају ванредних околности, као и да се осигура примена ових планова у пракси (Налаз 1.3) – Приоритет 2;
8) да обезбеди да резервне копије података буду смештене у безбедан простор за одлагање ван објекта, у складу са прописаним мерама заштите, како би се минимизирао ризик од губитка података у случају инцидента (Налаз 1.3) – Приоритет 1;
9) да успостави и имплементира процес управљања ИТ ризицима који ће укључити идентификацију, процену, праћење и управљање ИТ ризицима, како би се осигурало благовремено реаговање и смањење потенцијалних финансијских и нефинансијских губитака у случају нежељеног догађаја (Налаз 1.4) – Приоритет 2;
10) да усвоји и имплементира процедуре које ће уредити сарадњу са пружаоцима услуга софтвера за наплату и контролу паркирања, укључујући јасно дефинисане споразуме који обезбеђују адекватан ниво заштите информација и средстава, у складу са прописима и техничким стандардима (Налаз 3.1) – Приоритет 2;
11) да успостави процедуре за надзор над пружаоцима услуга, укључујући праћење реализације пружања услуга и испуњење услова информационе безбедности, као и да документује све активности везане за овај надзор (Налаз 3.1) – Приоритет 2;
12) да ажурира Правилник о унутрашњој организацији и систематизацији послова како би укључио послове Администратора ИТ система, са јасно дефинисаним одговорностима везаним за надзор над пружаоцима услуга (Налаз 3.1) – Приоритет 1;
13) да успостави механизам за надзор и контролу заштите података који обрађује пружалац услуга, као и да дефинише уговорне одредбе о обради и заштити података у складу са Законом о заштити података о личности (Налаз 3.2) – Приоритет 2;
14) да одреди лице одговорно за сарадњу и контролу пружалаца услуга у погледу заштите података и безбедности система (Налаз 3.2) – Приоритет 1;
15) да обезбеди адекватну контролу приступа поверљивим подацима, ограничавајући приступ корисницима пружаоца услуга само на податке који су неопходни за извршење уговора (Налаз 3.2) – Приоритет 2;

16) да успостави механизам за брисање или шифровање података по истеку њихове употребе, како би се обезбедила заштита осетљивих података (Налаз 3.2) – Приоритет 1;
17) да развије и усвоји план континуитета пословања који ће обезбедити неометано функционисање система у случају раскида сарадње са пружаоцем услуга, укључујући мере за брзо и ефикасно решавање потенцијалних прекида у услузи (Налаз 3.3) – Приоритет 2;
18) да ревидира уговоре са пружаоцем услуга како би укључили одредбе о активностима и обавезама пружаоца услуга у случају раскида сарадње, са циљем обезбеђивања континуитета пословања (Налаз 3.3) – Приоритет 2;
19) да успостави јасне процедуре и упутства за управљање пословним процесима РЈ Паркинг сервиса, а који се односе на коришћење апликације за наплату и апликације за доступност паркинг места, како би се обезбедила ефикасност и стандардизација у коришћењу ових система (Налаз 4.1) – Приоритет 2;
20) да омогући коришћење отворених података и информисање грађана путем стандардних мобилних апликација, како би побољшао доступност информација о паркинг местима и унапредио услуге за грађане (Налаз 4.3) – Приоритет 3.

2. Мере предузете у поступку ревизије

У току ревизије јавних комуналних предузећа за контролу и наплату паркинг услуга, спроведене су значајне активности и унапређења у домену информационих система, управљања подацима и заштите личних података корисника. Предузећа су предузела различите мере како би унапредила своје пословне процесе, осигурала усклађеност са важећим прописима и стандардима и побољшала квалитет услуга које пружају. Ове активности укључују доношење нових процедура, ажурирање постојећих правилника, као и имплементацију техничких мера за унапређење безбедности и транспарентности у управљању информационим системима.

ЈКП „Паркинг сервис“, Београд је предузео следеће мере:

1) У току поступка ревизије, дана 28. октобра 2024. године в.д. директора ЈКП „Паркинг сервис“, Београд донео је Одлуку о измени и допуни Правилника о унутрашњој организацији и систематизацији послова ЈКП „Паркинг сервис“, Београд. Овом Одлуком је измењен члан 3 Правилника о систематизацији у којем се наводи да је руководилац Службе за информационе технологије одговоран за успостављање, одржавање и примену мера које се односе на процену ризика по безбедност информација из домена Службе, док су извршни руководилац службе, координатор за послове унапређења информационог система, шеф одељења за информатику, шеф контролно оперативног центра и главни организатор информационог система дужни да спроводе мере које се односе на процену ризика по безбедност информација из домена Службе.
2) Надзорни одбор ЈКП „Паркинг сервис“, Београд је дана 21. новембра 2024. године усвојио нови Правилник о безбедности ИКТ система, са циљем да у потпуности обухвати специфичности свих коришћених информационих подсистема, укључујући и систем за контролу и наплату паркирања. Ове измене произашле су из потребе за унапређењем мера безбедности и припреме за ресертификацију стандарда ISO/IEC 27001:2013.

Нови Правилник укључује прецизирање надлежности, процедуре за управљање ризицима и детаљан Регистар ИКТ подсистема (Прилог 1). Такође, ажуриран је Регистар апликативних подсистема (Прилог 2), који обухвата критичне апликације попут система за препознавање регистарских таблица (SCANCAR) и система за електронско архивирање докумената. Додатно, Правилником су уведени стандарди за класификацију и заштиту података у складу са нивоом њихове критичности, чиме се унапређује безбедност ИКТ ресурса и управљање инцидентима.

Овим изменама осигурана је потпуна усклађеност са захтевима стандарда и смањени су ризици од неовлашћеног приступа и поремећаја у раду критичних система. Приложена документација пружа транспарентан увид у спроведене мере и утврђује основе за даље побољшање безбедносне инфраструктуре предузећа.

3) Директор ЈКП „Паркинг сервис“, Београд је дана 14. новембра 2024. године одобрио нову процедуру „Предаја и брисање података са сервера услед престанка уговорних обавеза“ (ПС.П64). Ова процедура има за циљ да обезбеди адекватну заштиту података корисника у случају раскида или истека сарадње са ЈКП „Паркинг сервис“, Београд, у складу са стандардима ISO/IEC 27001 и ISO/IEC 27018, као и релевантним прописима, укључујући Закон о заштити података о личности.

   У оквиру процедуре дефинисан је поступак предаје података, који укључује извоз података, пренос криптографских кључева и пружање техничке подршке у прелазном периоду ради осигурања континуитета пословања корисника. Предаја се врши у договореном формату и уз примену одговарајућих техничких и организационих мера, попут шифровања и верификације интегритета података. За сваки поступак предаје података издаје се налог који детаљно описује тип података, начин преноса и рокове за извршење.

   Након предаје, ЈКП „Паркинг сервис“, Београд је обавезан да трајно обрише све копије података корисника, осим ако законом није другачије прописано. Брисање се спроводи коришћењем сертификованих метода за трајно уклањање података, као што су алгоритми shred или wipe. По завршетку, обрађивач доставља писани доказ о уништењу података, који укључује датум, примењене методе и потврду о уништењу.

   Руковалац података задржава право на проверу спровођења процедуре, укључујући увид у релевантну документацију и, по потреби, техничке провере. Уговором је прецизирана одговорност ЈКП „Паркинг сервис“, Београд за евентуалне пропусте или насталу штету, како би се обезбедила пуна заштита права корисника и усклађеност са правним и стандардним захтевима.

4) Корисници услуга ЈКП „Паркинг сервис“, Београд су, на иницијативу овог предузећа, а засновано на процедури „Предаја и брисање података са сервера услед престанка уговорних обавеза“, коју је ЈКП „Паркинг сервис“, Београд донео 14. новембра 2024. године, донели одлуке о успостављању процедура за примопредају података прикупљених током реализације уговора за набавку система за контролу и наплату паркирања путем мобилног видео надзора. Ове процедуре су постале саставни део уговора које су корисници услуга, попут ЈКП „Паркинг сервис“ Ниш и ЈКП „Златибор“ Чајетина, закључили са ЈКП „Паркинг сервис“, Београд.

Процедуре су детаљно дефинисале кораке за примопредају података, укључујући идентификацију и опис података, верификацију њихове исправности и избор методе за пренос (попут заштићеног електронског трансфера или шифрованих уређаја). Такође, предвиђено је креирање листе података који се бришу након завршетка уговора, укључујући базе података, логове, конфигурације и сигурносне копије. Налози за предају и брисање података постали су обавезан део поступка, чиме се обезбеђује транспарентност и сигурност у руковању подацима.

5) ЈКП „Паркинг сервис“, Београд је у информационом систему укинуо право приступа личним подацима корисницима који за то немају потребу при обављању радних обавеза. Осим тога на нивоу целе апликације онемогућено је експортовање података из табела у XLSX без осетљивих података.
6) У информационом систему за наплату и контролу паркирања укинута је могућност измене корисничког имена. Сада је при измени података username „бледо“ и само приказано без могућности за измену.

ЈКП „Паркинг сервис“, Нови Сад је предузео следеће мере:

1) Директор ЈКП „Паркинг сервис“, Нови Сад је дана 1. октобра 2024. године донео Одлуку о измени и допуни Правилника о безбедности информационо-комуникационог система Јавног комуналног предузећа „Паркинг сервис“, Нови Сад број 2024-0-1164/1, којом је предвиђено у члану 35 да Администратор ИКТ система од посебног значаја врши проверу ИКТ система предузећа. Проверу спроводи кроз три основна корака: прво, утврђује се усклађеност Правилника о безбедности ИКТ система са прописаним условима и мерама заштите, овлашћењима и процедурама; друго, проверава се примена тих мера у оперативном раду кроз интервјуе, симулације и преглед документације; и треће, врши се техничка провера безбедносних слабости у ИКТ систему кроз анализу конфигурација, техничких података и тестирање познатих слабости. На овај начин, радне дужности Администратора ИКТ система од посебног значаја усклађене су у Правилнику о безбедности ИКТ система са радним дужностима дефинисаним за ово радно место у Правилнику о систематизацији.
2) Директор ЈКП „Паркинг сервис“, Нови Сад је дана 14. новембра 2024. године донео измене и допуне Правилника о безбедности ИКТ система, са циљем да унапреди безбедност и функционалност информационих система, укључујући и систем за контролу и наплату паркирања. Ове измене су резултирале прецизним дефинисањем одговорности, процедура и мера заштите, како би се осигурали интегритет, поверљивост и доступност података. СМС систем за наплату паркирања је додатно регулисан кроз детаљне процедуре које обухватају праћење, надзор и измене сервера, мониторинг СМС центара и подршку корисницима. Уведене су и мере за прављење резервних копија података и одржавање ВПН веза, чиме је обезбеђена стабилност и безбедност система. ФРИП књиговодствени софтвер је организован на начин који омогућава да корисници имају приступ искључиво оним модулима који су неопходни за њихове радне задатке. На овај начин су ограничене потенцијалне злоупотребе и унапређена је контрола приступа. Апликација SWAT, која се користи за анализу и праћење активности, добила је додатне безбедносне мере.

Приступ овој апликацији сада захтева инсталацију безбедносног сертификата и коришћење јединствених корисничких налога са строго дефинисаним правима приступа, што знатно повећава ниво заштите. Додатно, уређене су процедуре за размену података са државним органима и трећим лицима. Уговорима су дефинисане обавезе у вези са заштитом података о личности и поверљивости, као и услови под којима се врши размена података, у складу са Законом о заштити података о личности.

3) ЈКП „Паркинг сервис“, Нови Сад је донело процедуру о обради података (Уговор о обради података) као и процедуру о поверљивости података (Уговор о поверљивости) у којој је дефинисало да су при потписивању уговора стране сагласне.

   У Уговору о обради података ЈКП „Паркинг сервис“, Нови Сад је обрађивач и детаљно су дефинисана права и обавезе руковаоца и обрађивача у вези са обрадом личних података коју врши обрађивач у име руковаоца, у циљу заштите права лица на која се подаци односе. Такође у уговору су дефинисана права и подобрађивача као и да обрађивач може да ангажује подобрађивача само уз писмену сагласност руковаоца. Пренос података о личности може се вршити у државе потписнице Конвенције о заштити лица у односу на аутоматску обраду личних података Савета Европе - бр.108 . односно у државе за које је Влада Републике Србије утврдила да обезбеђују примерени ниво заштите.

   У процедури о поверљивости података дефинисане су врсте поверљивих података као и њихов приступ и мере заштите.

4) ЈКП „Паркинг сервис“, Нови Сад је закључио уговоре о вршењу услуге одржавања и подршке систему наплате и контроле паркирања са два јавно комунална предузећа на територији Републике Србије, којима су укључене одредбе о преносу података у електронској форми, као и о брисању података који се обрађују у току трајања уговора. Посебним чланом уговора дефинисано је да ће ЈКП „Паркинг сервис“, Нови Сад обезбедити јавним комуналним предузећима пренос података у електронској форми (у CSV формату) након истека пословне сарадње. Такође наводи се да ће ЈКП „Паркинг сервис“, Нови Сад обезбедити коришћење апликације „SWAT“ у периоду до три месеца након истека или раскида уговора о пословној сарадњи. На крају, наводи се да ће ЈКП „Паркинг сервис“, Нови Сад на захтев корисника услуга омогућити брисање свих података који су обрађивани током трајања уговора, у складу са Законом о заштити података о личности.

5) ЈКП „Паркинг сервис“, Нови Сад уклонио је приступ прегледа осетљивих података својих корисника, а исте податке ће у наредном периоду криптовати и кључеве крипције ће доставити руковаоцима података.

6) ЈКП „Паркинг сервис“, Нови Сад је у FRIP систему укинуо право приступа личним подацима корисницима који за то немају потребу при обављању радних обавеза. Такође, остављени су само неопходни модули за одговарајућа права корисника нпр. Благајник не може да види личне податке грађана, а такође и нема приступ матичној евиденцији јер му то није у опису посла укинуте су и опције које се више не користе као што су „благајна листица“ и „инкасант промет“. Осим тога на нивоу целе

апликације FRIP онемогућено је експортовање података из табела у CSV, XLSX и друге формате.

7) ЈКП „Паркинг сервис“, Нови Сад је у SWAT софтверу за наплату и контролу паркирања укинуо могућност измене корисничког имена. Сада је при измени података username „бледо“ и само приказано без могућности за измену, а такође не могу да се виде лични подаци грађана.

ЈКП „Паркинг сервис“, Чачак је омогућио функционалност модула „Мапа“ за праћење доступности паркинг места у реалном времену.

Радна јединица Паркинг сервис ЈКП „Чистоћа“, Краљево је почела да на захтевима за издавање месечних повлашћених и неповлашћених карата обавештава своје клијенте да се лични подаци користе само у сврху за које су и тражени, а да се у друге сврхе не могу користити.

Радна јединица Паркинг сервис ЈП „Пословни центра“, Крушевац је почела уз захтеве и рачуне за издавање месечних повлашћених и неповлашћених карата и за резервисана места да својим клијентима издаје Сагласност за обраду података о личности. Овом сагласношћу се клијенти информишу и прихватају да ће њихови лични подаци бити коришћени у складу са Законом о заштити података о личности.

В. Ф. Генералног државног ревизора

Марија Обреновић
Државна ревизорска институција
Макензијева 41
11000 Београд, Србија
23. април 2025. године

II Увод

Државна ревизорска институција спровела је ревизију сврсисходности на тему „Информациони системи за наплату услуга паркинга“. Ревизија је спроведена у складу са Законом о Државној ревизорској институцији[4], Пословником Државне ревизорске институције[5] и Програмом ревизије Државне ревизорске институције за 2024. годину.

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

Ревизија информационог система за наплату услуга паркинга подразумева преглед и анализу постојећег система ради идентификације недостатака и предлога за побољшања. Ревизија се обично врши како би се осигурала ефикасност и поузданост система, као и како би се идентификовале могућности за унапређење.

У конкретним случајевима, ревизија обухвата ревизијске поступке над оба подсистема: контролу наплате паркирања и контролу доступних паркинг места како би се плаћање вршило у складу са квалитетом и квантитетом пружених услуга (monitoring).

Информациони системи за наплату услуга паркинга користе се за побољшање ефикасности, као и за пружање информација грађанима.

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. Институција 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.

Базе података у овим системима садрже осетљиве личне податке (за месечне карте које се издају за паркинг место прикупљају се подаци из личне карте и саобраћајних дозвола) и изискују примену одређених мера заштите. Закон о заштити података о личности и Закон о информационој безбедности, својим уредбама уређују обавезне мере заштите, које даље, треба примењивати са циљем очувања интегритета, поверљивости и расположивости података.

2. Циљ ревизије

Циљ ревизије је био да се оцени ефективност и ефикасност информационог система у ЈКП „Паркинг сервис“, Београд који се односи на јавни паркинг, односно у којој мери су примењене мере испуниле неопходне циљеве када је у питању управљање системима, поузданост информационих система и управљање подацима корисника –

[4] „Службени гласник РС“, бр. 101/05, 54/07, 36/10 и 44/18-др.закон
[5] „Службени гласник РС“, број 9/2009

грађана, и у којој мери систем омогућава ефикасност контроле наплате и плаћања услуга паркинга. Поузданост електронских података и информационих система подразумева интегритет, комплетност, тачност, конзистентност и очување података, безбедност информационог система и континуитет пословања, имајући у виду сврху за коју се ти подаци и системи користе.

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

3. Ревизорска питања

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

1. У којој мери успостављене мере информационе безбедности обезбеђују поузданост информационих система који се користе за наплату услуга паркинга?

- Да ли постоје имплементирана правила и процедуре за информациону безбедност?
- Да ли је и на који начин успостављена организација ИТ безбедности и на који начин су успостављене мере физичке заштите и контроле логичког приступа системима?
- На који начин се управља континуитетом пословања у ванредним околностима?
- На који начин се спроводи управљање ИТ ризицима и како се управља инцидентима?

2. У којој мери је успостављен механизам сарадње са корисницима система како би се испунили сви неопходни циљеви, укључујући и поузданост података?

- На који начин су обезбедили безбедност података када су упитању корисници система?
- Да ли је субјект ревизије успоставио механизам којим је дефинисао услове за заштиту и безбедност података корисника, а и код себе и да ли их спроводи?
- На који начин је обезбеђено архивирање података или уништавање у случају да корисник система промени пружаоца услуга?
- Да ли је сарадња успостављена у складу са Законом о заштити података о личности?

3. У којој мери је успостављен механизам сарадње са пружаоцима услуга испунио све неопходне циљеве, укључујући и поузданост података?

- Да ли постоје правила и процедуре које се односе на безбедност података када су у питању уговори са пружаоцима услуга?
- Да ли постоји механизам којим се осигурава да је пружалац услуге усвојио услове за заштиту и безбедност података и да ли их спроводи и на који начин се прати реализација извршења уговора?
- Да ли је успостављен план континуитета пословања у случају раскида уговора са пружаоцем услуга?
- Да ли је сарадња успостављена у складу са Законом о заштити података о личности?

4. У којој мери успостављене апликативне контроле обезбеђују контролу наплате карата пружених услуга?

- Да ли постоје правила и процедуре које се односе на употребу апликације за наплату и апликације за доступност паркинг места?
- Да ли постоји механизам којим се осигурава валидација улазних података, детекција и корекција грешака и на који начин се прати тачност података који се односе на наплату услуга паркирања?
- Да ли информациони систем генерише све потребне извештаје - када је у питању временски интервал и свеобухватност?

Како је циљ ревизије да се оцени ефективност и ефикасност информационих система 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.

Прво 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. С обзиром да је реч о осетљивим подацима које третира Закон о заштити података о личности и други закони, безбедност података је важно питање ове ревизије, због чега се анализирају и 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 такође и законска обавеза. И као последње питање у овој области, што је исто законска обавеза, јесте управљање и пријављивање ИТ инцидената.

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

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 Закона о заштити података о личности.

Четврто питање се односи на успостављање ефективних апликативних контрола. Апликативне контроле обухватају унос података (настанак и унос података); обраду трансакције; излазне податке (дистрибуција резултата) и безбедност (евидентирање, комуникација, чување).

4. Обим и ограничења ревизије

Ревизијом смо обухватили јавна предузећа за пружање услуга паркирања на територији пет градова: Београда, Новог Сада, Крушевца, Краљева и Чачка. На територији ових градова налази се 38,04% од укупног броја регистрованих возила у Републици Србији, међутим 50,40% од укупног броја регистрованих возила у предузећима која користе информациони систем за наплату услуга паркирања. Такође, на територији наведених градова се налази 49,36% укупног броја паркинг места под контролом предузећа која користе информациони систем за наплату услуга паркирања у Републици Србији.

Детаљније испитивање смо извршили код субјеката ревизије који су приказани на следећој слици:

Слика 2. Преглед субјеката ревизије

Поступке ревизије: прикупљање доказа, доношење налаза и закључака, писање извештаја, спровели смо од априла до новембра 2024. године.

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

Ограничење ове ревизије је био ризик да одговори које су јавна комунална предузећа доставила на Упитник о стању ИТ не одражавају стварно стање у јавним комуналним предузећима за пружање паркинг услуга, јер тачност одговора нисмо могли да потврдимо код свих предузећа непосредним увидом у документацију, податке и систем.

5. Методологија у поступку рада

Да бисмо одговорили на ревизорска питања, анализирали смо законску и подзаконску регулативу, користили стручну литературу (WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions[6]), као и све податке добијене од субјеката. Анализирали смо податке и информације за период од 2021. до 2023. године.

[6] https://idi.no/work-streams/relevant-sais/lota/wgita-idi-handbook-on-it-audit

У вези са информационим системима јавних предузећа за контролу и наплату услуга паркинга, анализиране су области информациона безбедност, успостављање ефективног механизма сарадње са пружаоцима услуга и корисницима услуга и апликативне контроле.

У циљу потврђивања информација из документације и прикупљања података који нису доступни у документима, обавили смо интервјуе и послали анкете и упитнике корисницима информационог система у јавним предузећима које пружају услуге паркинга.

Током поступка ревизије спроведена је ревизија код пет субјеката, а извештаји су објављени на сајту Државне ревизорске институције.

Детаљнији опис коришћене методологије дат је у Прилогу 1.

III Опис предмета ревизије

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 и аутентичност тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица[7].

Успостављање ефективног механизма сарадње са корисницима услуга софтвера је од кључне важности за осигурање да се услуге пружају у складу са очекивањима корисника. Потребно је имати успостављене процесе за периодично праћење статуса пројеката, квалитета услуга, као и тестирање софтверских производа пре њиховог увођења у оперативно окружење корисника. Поред тога, као део процеса надзора над извршењем обавеза према корисницима, могу се спроводити и ревизије интерних процеса осигурања квалитета, како би се обезбедило да се рад корисника прати и усклађује са уговореним политикама и плановима за све релевантне послове.

Апликативне контроле обухватају унос података (настанак и унос података); обраду трансакције; излазне податке (дистрибуција резултата) и безбедност (евидентирање, комуникација, чување). Циљ контроле улазних података је да се осигура да је извор података валидан, тачан и потпун и да ће апликација одбацити неважеће податке. Циљ мера контрола обраде је да се осигура интегритет података, њихова ваљаност и поузданост и да се сачувају од погрешних обрада кроз циклус обраде трансакција – од времена пријема података, па уноса у систем до времена када се податак шаље у базу података, даљу комуникацију или подсистеме за излазне податке. Оне такође осигуравају да се ваљани унети подаци обрађују само једном и да детекција погрешних трансакција не ремети обраду ваљаних трансакција. Циљеви контроле излазних података представљају мере уграђене у апликацију како би се осигурало да су излазни подаци трансакције комплетни, тачни и тачно дистрибуирани. Такође контроле настоје да се подаци који су обрађени у апликацији заштите од недозвољених модификација или дистрибуције.

1. Законодавни и институционални оквир

Законодавни оквир

Управљање јавним паркиралиштима, регулисано је у више закона и у наставку дајемо преглед најважнијих одредби према надлежностима.

Закон о локалној самоуправи

Законом је експлицитно дата општини надлежност[8] да, преко својих органа, у складу са Уставом и законом, уређује и обезбеђује обављање комуналних делатности. У том циљу, у складу са законом, јединица локалне самоуправе за остваривање својих права и дужности и за задовољавање потреба локалног становништва може основати предузећа, установе и друге организације које врше јавну службу, али и уговором, у складу са начелима конкуренције и јавности, поверити правном или физичком лицу обављање својих послова.

[7] Члан 7 став 3 Закона о информационој безбедности.
[8] „Службени гласник РС“, бр. 129/07, 83/14 – др. закон, 101/16 – др. закон и 47/18, члан 20 став 1 тачка 2

Закон о комуналним делатностима

Комуналним делатностима, сматрају се делатности пружања комуналних услуга од значаја за остварење животних потреба физичких и правних лица код којих је јединица локалне самоуправе дужна да створи услове за обезбеђење одговарајућег квалитета, обима, доступности и континуитета, као и надзор над њиховим вршењем[9].

Управљање јавним паркиралиштима, је законом дефинисано као комунална делатност од општег интереса. Према члану 3 став 1 тачка 7 Закона о комуналним делатностима управљање јавним паркиралиштима је услуга одржавања јавних паркиралишта и простора за паркирање на обележеним местима (затворени и отворени простори), организација и вршење контроле и наплате паркирања, услуга уклањања непрописно паркираних, одбачених или остављених возила, премештање паркираних возила под условима прописаним овим и другим посебним законом, постављање уређаја којима се по налогу надлежног органа спречава одвожење возила, као и уклањање, премештање возила и постављање уређаја којима се спречава одвожење возила у случајевима предвиђеним посебном одлуком скупштине јединице локалне самоуправе којом се уређује начин обављања комуналне делатности управљања јавним паркиралиштима, као и вршење наплате ових услуга.

Одлуке о јавним паркиралиштима

Управљање јавним паркиралиштима у Републици Србији уређено је одлукама локалних самоуправа које дефинишу услове, начин обављања и организацију ове делатности. Ове одлуке имају за циљ да обезбеде ефикасно и уредно коришћење јавних простора за паркирање, уз уважавање потреба грађана и специфичности локалних заједница. Уобичајене активности које обухватају управљање јавним паркиралиштима укључују одржавање паркинг простора, организацију и контролу паркирања, наплату услуга, као и уклањање и премештање непрописно паркираних возила. Одлуке такође предвиђају постављање уређаја који спречавају одвожење возила, као и зонирање паркинг простора са различитим условима и тарифама.

Иако се основне функције управљања јавним паркиралиштима могу идентификовати у свим локалним самоуправама, постоје специфичности у приступу. У Београду, на пример, ЈКП „Паркинг сервис“ управља јавним гаражама и паркиралиштима уз примену напредних електронских система за контролу и надзор. У Новом Саду, поред управљања постојећим капацитетима, значајна пажња посвећена је изградњи нових паркинг гаража. У Чачку, управљање јавним паркиралиштима оријентисано је на задовољење потреба корисника кроз висок квалитет услуга. У Краљеву, ЈКП „Чистоћа“ овај сегмент делатности интегрише у шири оквир комуналних услуга, док се у Крушевцу ЈП „Пословни центар“ бави управљањем паркинг просторима као делом својих активности, укључујући одржавање саобраћајне сигнализације.

Ове одлуке омогућавају да се управљање јавним паркиралиштима прилагоди локалним потребама, урбанистичким плановима и специфичностима саобраћаја, чиме се доприноси уређењу урбаног простора, унапређењу саобраћајне културе и побољшању квалитета живота грађана. Савремена технолошка решења, као што су електронска наплата и апликације за информисање о доступности паркинг места, све више се интегришу у системе управљања, пружајући грађанима брже, транспарентније и квалитетније услуге.

[9] „Службени гласник РС“, бр. 88/11, 104/16 и 95/18, члан 2 став 1

Одлуке о усклађивању оснивачких аката јавних комуналних предузећа са Законом о јавним предузећима

Одлуке о усклађивању оснивачких аката јавних комуналних предузећа са Законом о јавним предузећима представљају правни оквир који дефинише делатност, надлежности и организацију ових предузећа. У складу са овим одлукама, сва јавна комунална предузећа на територији Републике Србије прилагођавају своје пословање законским прописима како би се обезбедила транспарентност, ефикасност и уредно задовољење потреба грађана за услугама од јавног интереса. Усклађивање аката је такође значајно за дефинисање одговорности у управљању, као и за интеграцију савремених стандарда пословања.

ЈКП „Паркинг сервис“ у Београду свој оснивачки акт прилагодио је тако да обухвати не само делатност управљања јавним гаражама и паркиралиштима већ и коришћење електронских система за контролу паркинг простора и уређаје за спречавање одвожења возила. У Новом Саду, оснивачки акт предузећа укључује широк спектар активности од изградње инфраструктуре до рачунарског програмирања, са нагласком на унапређење капацитета за паркирање. У Чачку, усклађивање акта обезбедило је јасно дефинисање делатности и стандарда који се односе на квалитет услуга и задовољење потреба корисника. ЈКП „Чистоћа“ у Краљеву обухватило је у оквиру свог акта и пратеће активности попут одржавања јавних паркиралишта, док је у Крушевцу ЈП „Пословни центар“ свој оснивачки акт прилагодило тако да укључи специфичне делатности попут одржавања саобраћајне сигнализације и регулисања саобраћаја.

Ове одлуке су одраз настојања да се јавна комунална предузећа учине савременим, ефикасним и прилагођеним потребама грађана и захтевима локалних заједница. Усклађивање са Законом о јавним предузећима такође доприноси унапређењу управљања и стварању предуслова за бољу интеграцију технолошких иновација у њихов рад.

Закон о информационој безбедности[10]

У складу са Законом о информационој безбедности 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.

[10] „Службени гласник РС“, бр. 6/16, 94/17 и 77/19

Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја[11]

Уредба уређује мере заштите информационо-комуникационих система од посебног значаја. 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.

Уредба 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[12]

Уредба уређује ближи садржај акта о безбедности информационо-комуникационих система од посебног значаја, начин провере информационо-комуникационих система од посебног значаја и садржај извештаја о провери информационо-комуникационог система од посебног значаја.

Закон о заштити података о личности[13]

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.

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

[11] „Службени гласник РС“, број 94/16
[12] „Службени гласник РС“, број 94/16
[13] „Службени гласник РС“, број 87/18

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 ставова 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.

Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању[14]

Чланом 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 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[15]

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.

[14] „Службени гласник РС“, број 94/17 и 52/21
[15] „Службени гласник РС“, број 27/2018

Институционални оквир

ЈКП „Паркинг сервис“, Београд основано је 1971. године са циљем управљања јавним паркиралиштима, укључујући организовање, одржавање и наплату услуга паркинга. Предузеће послује у оквиру Града Београда и управља великим бројем паркинг зона које су организоване према временским ограничењима и ценовним категоријама. Напредни системи као што су „Око соколово“ омогућавају аутоматизовани надзор и контролу паркирања. Поред класичних метода наплате, уведене су и савремене опције као што су СМС поруке и мобилна апликација, чиме је побољшана доступност услуга. Предузеће такође пружа услуге уклањања непрописно паркираних возила, чиме доприноси уређености градског саобраћаја.

ЈКП „Паркинг сервис“, Нови Сад основано је 2004. године као градско јавно комунално предузеће са задатком да унапреди организацију стационарног саобраћаја. Управљање паркиралиштима организовано је у четири паркинг зоне, а систем наплате укључује СМС поруке, електронске карте и претплатне карте. Информациони систем уведен је 2005. године, обезбеђујући електронску евиденцију корисника и наплату услуга. Предузеће улаже у модернизацију услуга, укључујући имплементацију софтвера који омогућава праћење доступности паркинг места.

ЈКП „Паркинг сервис“, Чачак основано је 2008. године за потребе организовања и регулисања стационарног саобраћаја у граду. Увођење софтвера „Synapse tech“ 2015. године омогућило је електронско плаћање путем СМС порука, као и продају електронских карата. Предузеће управља паркинг просторима у више зона и обезбеђује основну евиденцију коришћења услуга. Иако су основе управљања успостављене, постоји потреба за додатним унапређењима у области апликативних контрола и безбедности података.

ЈКП „Чистоћа“, Краљево од 2018. године управља услугама паркирања, укључујући организацију паркинг зона, продају папирних карата и наплату путем СМС порука. Коришћењем софтвера „Ђоковић Софтвер“, предузеће обезбеђује евиденцију наплате и управљање паркинг местима. Иако су основе система постављене, недостаје интеграција са савременим платформама и могућност праћења доступности паркинг места у реалном времену.

ЈП „Пословни центар“, Крушевац управља паркинг просторима од 2002. године, а од 2007. године користи софтвер „EPSEE MS“ за евиденцију и наплату услуга паркинга. Наплата се врши путем СМС порука и продаје карата, док инфо-табле и камере у гаражама омогућавају праћење расположивости паркинг места. Иако је систем функционалан, недостају напредни механизми за интеграцију са мобилним апликацијама и платформама за праћење у реалном времену.

Ова предузећа представљају различите моделе управљања информационим системима за паркирање, са значајним варијацијама у нивоу модернизације и интеграције, што указује на потребу за унапређењем у мање развијеним срединама ради постизања униформности и ефикасности.

2. Информациони системи у јавним комуналним предузећима

Информациони системи који се користе за управљање паркинг просторима и наплату услуга паркирања играју кључну улогу у обезбеђивању ефикасног управљања ресурсима, контроле наплате и транспарентности. Ови системи обухватају различите софтверске модуле и подсистеме који се користе у јавним комуналним предузећима широм Србије за аутоматизацију процеса и подршку корисницима.

Детаљан опис информационих система по предузећима дат је у прилозима извештаја:

- Прилог 2 описује систем који користи ЈКП „Паркинг сервис“, Београд, укључујући напредне апликације и систем Scan Car за мобилни надзор;
- Прилог 3 наводи подсистеме у ЈКП „Паркинг сервис“, Нови Сад, као што су СМС систем за наплату и књиговодствени софтвер;
- Прилог 4 обрађује софтвер „Synapse tech“ који користи ЈКП „Паркинг сервис“, Чачак;
- Прилог 5 садржи детаље о систему „Ђоковић Софтвер“ који примењује ЈКП „Чистоћа“, Краљево;
- Прилог 6 представља софтвер „EPSEE MS“ који користи ЈП „Пословни центар“, Крушевац, за наплату и управљање паркинг местима.

Ови прилози пружају дубљи увид у структуру, функционалности и начине коришћења система у сваком од предузећа, указујући на њихове специфичности, као и на могућности за унапређење.

IV Закључци

На основу анализе података и документације достављене од стране јавних предузећа за контролу и наплату паркинг услуга, као и обављених интервјуа и прегледа коришћеног система за наплату паркинга, дошли смо до следећих закључака који се односе на управљање информационим системима, безбедност података и ефикасност коришћења апликација за наплату паркинг услуга:

1. Мере информационе безбедности у јавним комуналним предузећима обезбеђују различит ниво поузданости информационих система, са значајним напретком у Новом Саду и Београду, док Чачак, Краљево и Крушевац остају са озбиљним недостатцима који угрожавају сигурност и континуитет пословања.
2. Сарадња са корисницима система у Београду и Новом Саду значајно је унапређена, али остаје простор за додатни напредак кроз успостављање криптовања и потпуну примену процедура за архивирање, миграцију и уништавање података код Новог Сада.
3. Механизам сарадње са пружаоцима услуга у Чачку, Краљеву и Крушевцу није у потпуности испунио неопходне циљеве, укључујући и поузданост података, због недостатка процедура за сарадњу, надзор и планирање континуитета пословања у случају раскида сарадње, што указује на потребу за системским унапређењем и јачањем контролних механизама.
4. Апликативне контроле обезбеђују основну контролу наплате и пружених услуга, док је у Београду и Новом Саду постигнут напредак, али у Чачку, Краљеву и Крушевцу недостају механизми за потпуну транспарентност и ефикасност.

У наставку извештаја наводимо закључке са одговарајућим налазима.

ЗАКЉУЧАК 1: Мере информационе безбедности у јавним комуналним предузећима обезбеђују различит ниво поузданости информационих система, са значајним напретком у Новом Саду и Београду, док Чачак, Краљево и Крушевац остају са озбиљним недостацима који угрожавају сигурност и континуитет пословања

Циљ овог дела извештаја је да утврди у којој мери су успостављене мере информационе безбедности у информационим системима за наплату услуга паркинга и да ли оне обезбеђују поузданост и сигурност података у складу са законским обавезама оператера ИКТ система од посебног значаја. Ова анализа обухвата процену усвајања и примене релевантних планова и процедура за ИТ безбедност, организационе структуре, мера физичке заштите, контроле логичког приступа и управљања резервним копијама. Посебна пажња посвећена је утврђивању да ли је обезбеђен континуитет пословања у ванредним околностима, укључујући и постојање плана за опоравак од катастрофе.

С обзиром на осетљивост података који подлежу Закону о заштити података о личности, истражени су механизми заштите и управљања ИТ ризицима, што подразумева идентификацију, процену и стратегије за ублажавање или отклањање тих ризика. Овај део извештаја обухвата и анализу управљања ИТ инцидентима, у складу са законским захтевима, чиме се осигурава интегритет, доступност и поверљивост података, као и континуитет у раду система.

Слика 3. Графички приказ информационе безбедности

На основу анализе законских и подзаконских аката, документације субјекта ревизије и одржаних интервјуа, донели смо закључак који темељимо на следећим налазима:

Налаз 1.1: Управљање безбедносним инцидентима у јавним комуналним предузећима није уједначено, са формализованим процедурама у Београду и Новом Саду, док остала предузећа немају успостављене формалне процедуре

Законом о информационој безбедности и Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја прописано је да сваки оператор ИКТ система мора успоставити процедуре за управљање безбедносним инцидентима. Ове процедуре треба да обухвате дефинисање одговорних лица, план поступања у случају инцидената, евиденцију активности, извештавање и размену информација о безбедносним слабостима, претњама и инцидентима.

Анализа је показала да само ЈКП „Паркинг сервис“, Београд, и ЈКП „Паркинг сервис“, Нови Сад, имају успостављене процедуре за управљање безбедносним инцидентима. Ове процедуре су усклађене са важећим прописима и укључују дефинисане механизме за идентификацију, анализу, реаговање и праћење инцидената. Насупрот томе, ЈКП „Паркинг сервис“, Чачак, ЈКП „Чистоћа“, Краљево, и ЈП „Пословни центар“, Крушевац, немају утврђене формалне процедуре за управљање инцидентима, нити су дефинисани механизми за њихову евиденцију и извештавање.

Недовољно улагање у развој процедура, недостатак кадрова са потребним компетенцијама и недовољна свест о значају формализованих процедура за управљање инцидентима довели су до овог стања. Такође, у појединим предузећима није постојао систематски приступ развоју мера заштите у складу са регулаторним оквиром.

Недостатак формалних процедура за управљање безбедносним инцидентима значајно смањује могућност правовременог реаговања на претње, што може довести до нарушавања континуитета пословања, губитка података, компромитације система и повећања ризика од поновљених инцидената. Ово стање представља слабост у безбедносном оквиру предузећа која се одражава и на квалитет пружених услуга.

Стратешки документ за ИТ капацитете	
Визија: План употребе и развоја ИТ капацитета.	Компонента: Стратешки планови интегрисани у пословне циљеве.

Ниједно од предузећа, субјеката ревизије, нема усвојен стратешки документ којим се планира употреба и развој ИТ капацитета.

Ажуриран Акт о безбедности ИКТ система	
Визија: Документ прилагођен тренутном стању и различитим системима у употреби.	Компонента: Дефинисане одредбе о физичкој сигурности информатичких ресурса.

Акт о безбедности информационо-комуникационог система (ИКТ) представља кључни документ за регулисање употребе и заштите ИКТ ресурса у јавним комуналним предузећима. Утврђено је да ниједно од предузећа, субјеката ревизије, нема у потпуности ажуриран документ који би обухватио специфичности система за контролу и наплату паркирања.

У ЈКП „Паркинг сервис“, Београд, постоји Правилник о безбедности ИКТ система који је више пута ажуриран, укључујући најновију измену ради ресертификације стандарда ISO/IEC 27001:2013. Ипак, овај документ се односи на све системе у предузећу и не садржи прецизне одредбе у вези са системом за наплату паркирања. Поред тога, организационе промене које су настале након измена у систематизацији нису у потпуности интегрисане у овај документ.

У ЈКП „Паркинг сервис“, Нови Сад, Правилник о безбедности ИКТ система, донет 2019. године, није ажуриран у складу са актуелним технолошким променама и системима у употреби. Одређене одредбе у документу нису усклађене са другим интерним актима, што доводи до потенцијалних нејасноћа у погледу одговорности и надлежности запослених у области информационе безбедности.

ЈКП „Паркинг сервис“, Чачак је 2024. године донело документ који регулише безбедност ИКТ система. Овај документ не укључује одредбе о специфичностима система за наплату паркирања нити дефинише односе са пружаоцима услуга, што ограничава његову примену у овој области.

ЈКП „Чистоћа“, Краљево, донело је свој Акт о безбедности ИКТ система почетком 2024. године. Овај документ се односи на све системе у предузећу, али не садржи детаљне мере заштите које су специфичне за системе за контролу и наплату паркирања. Такође, није укључена физичка заштита информатичких ресурса ни мере које регулишу приступ подацима доступним пружаоцима услуга.

ЈП „Пословни центар“, Крушевац, има Акт о безбедности ИКТ система који је донет 2017. године, али он није ажуриран у складу са развојем нових информационих система у предузећу. Недостатак ажурирања доводи у питање примену мера заштите у складу са савременим технолошким захтевима и стварним стањем система.

Описано стање указује на уочене разлике у приступу и нивоу развијености докумената за безбедност ИКТ система међу субјектима ревизије. Сви документи се односе на свеобухватне системе, без специфичних одредби за подсистеме за контролу и наплату паркирања, што утиче на њихову применљивост и ефикасност.

Адекватне процедуре за праћење и надзор	
Визија: Јасно дефинисани послови, одговорности, и контролни механизми.	Компонента: Детаљне процедуре за управљање ИТ инцидентима и активностима.

Процедуре за праћење, ревизију и надзор у области информационе безбедности међу субјектима ревизије показују значајне разлике у степену развијености и примени. Ове процедуре представљају основ за ефикасно управљање информационим системима, али њихова примена није уједначена у свих пет предузећа.

У ЈКП „Паркинг сервис“, Београд, развијен је свеобухватан оквир процедура у складу са стандардима ISO/IEC 27001 и ISO 9001:2015. Ове процедуре укључују управљање ризицима, реаговање на инциденте, израду плана пословног континуитета и надзор над радом софтверских решења. Праћење усклађености и примена прописаних мера безбедности спроводи се кроз редовне интерне ревизије које организује Служба за

информационе технологије. Сваки запослени који користи ИКТ ресурсе упознат је са својим обавезама кроз потписивање изјава, чиме се осигурава транспарентност и уредно праћење примене процедура.

У ЈКП „Паркинг сервис“, Нови Сад, усвојен је низ процедура и упутстава којима се уређују кључни аспекти информационе безбедности и управљања ИТ системима. Оне обухватају управљање ИТ ресурсима, реаговање на инциденте, континуитет безбедности информација, идентификацију ризика и прилика, као и поступање са уређајима за контролу наплате паркинга. Посебна пажња посвећена је праћењу и надзору над радом софтверских решења, који се спроводи кроз поступке дефинисане у оквиру Процедуре рада Службе за информационе технологије. Надзор укључује иницијативе руководилаца служби, евидентиране путем електронске комуникације, тимске договоре за мање активности и формалне састанке са подизвођачима за сложеније задатке, уз пратећу документацију и извештаје. Сва документација се чува у електронској или писаној форми, а подносиоци захтева добијају повратну информацију по окончању поступка.

У ЈКП „Паркинг сервис“, Чачак, процедуре за праћење и надзор нису формално успостављене. Недостатак дефинисаних правила и процедура ограничава могућност ефикасног надзора и управљања информационим системима, укључујући системе за наплату паркинга. Запослени који се баве овим областима углавном раде по интерним договорима, што ствара ризик од недоследне примене мера безбедности.

ЈКП „Чистоћа“, Краљево, такође нема формално усвојене процедуре које би регулисале праћење и надзор над информационим системима. Овај недостатак може утицати на ефикасност у примени мера безбедности, посебно када је реч о управљању подсистемима за наплату паркинга и контроли приступа подацима.

У ЈП „Пословни центар“, Крушевац, основне процедуре су делимично дефинисане кроз интерне акте, али недостаје свеобухватан оквир за праћење и надзор информационих система. Постојеће активности у овом домену углавном се ослањају на индивидуални приступ запослених, без јасно дефинисаних правила и процедура, што може утицати на укупну сигурност система.

Разлике у развијености и примени процедура за праћење и надзор у области информационе безбедности утичу на укупну ефикасност управљања информационим системима и њихову безбедност. ЈКП „Паркинг сервис“, Београд, и ЈКП „Паркинг сервис“, Нови Сад, показују виши степен формализације, са процедурама које су усклађене са међународним стандардима и укључују редовне ревизије, управљање ризицима и надзор над софтверским решењима. Насупрот томе, ЈКП „Паркинг сервис“, Чачак, ЈКП „Чистоћа“, Краљево, и ЈП „Пословни центар“, Крушевац, углавном немају формално успостављене или свеобухватне процедуре, што оставља простор за недоследности у примени мера безбедности и смањује могућности за унапређење система. Ове разлике указују на потребу за уједначеним приступом у дефинисању и примени процедура, како би се осигурала ефикасност и сигурност у раду свих предузећа.

Организација и систематизација радних места у области информационих технологија и безбедности знатно се разликују међу субјектима ревизије, што утиче на ефикасност и капацитете у управљању информационим системима. Анализа стања указује на разноврсне приступе и изазове са којима се предузећа суочавају.

У ЈКП „Паркинг сервис“, Београд, систематизоване су две службе које се баве аспектима информационих технологија: Служба за информационе технологије и Служба за заједничке послове, са Одељењем за развој паркирања и управљање аутоматским паркинг системима. Укупно је систематизовано 27 радних места са 38

предвиђених извршилаца, од којих је тренутно попуњено 70%. Кључну улогу у одржавању система имају Систем администратори и Администратори база података, који се баве контролом приступа ресурсима, ажурирањем софтвера и управљањем сигурносним мерама. Поред тога, у служби су предвиђена радна места за специјализоване улоге, као што су Инжењери развоја и Администратори аутоматских система, који су задужени за специфичне технолошке аспекте система за наплату паркинга.

У ЈКП „Паркинг сервис“, Нови Сад, организација укључује 12 систематизованих радних места, од којих је 8 тренутно попуњено. Поред Службе за информационе технологије, која обухвата већину ИТ активности, предвиђена су и два радна места ван службе, али њихове одговорности нису прецизно дефинисане. Посебну улогу имају Администратори ИКТ система, који управљају критичним подсистемима, укључујући системе за наплату паркинга. Ипак, недостатак јасно дефинисаних процедура у актима може довести до преклапања надлежности или пропуста у примени мера безбедности.

У ЈКП „Паркинг сервис“, Чачак, постоје две позиције које се односе на ИТ послове: Помоћник директора и Координатор послова. Тренутно је попуњена само позиција Координатора послова, која укључује активности као што су сарадња са техничком службом, рад на видео надзору и управљање уређајима за СМС наплату паркинга. Ограничавајући фактор је недовољно систематизованих позиција и недостатак особља, што утиче на капацитет за ефикасно управљање информационим системима.

У ЈКП „Чистоћа“, Краљево, предузеће има систематизована радна места која укључују активности у области информационих технологија, али постоји изразит недостатак попуњености позиција. Радна места везана за информациону безбедност и управљање информационим системима нису довољно дефинисана, што ограничава могућности предузећа да одговори на потребе савременог пословања.

У ЈП „Пословни центар“, Крушевац, систематизација обухвата два кључна радна места: Координатора послова информационог система и технологија и Референта комерцијале и пројектанта информационих система. Док Координатор обухвата широк спектар активности као што су управљање мрежом и анализа ризика, Референт комбиновано ради на развоју информационих система и другим административним пословима. Овај хибридни приступ доводи до нејасноћа у расподели времена и одговорности, што ограничава капацитет предузећа за фокусирање на информационе системе.

Разлике у систематизацији и организацији међу субјектима ревизије утичу на ниво ефикасности и капацитет предузећа да управљају својим информационим системима. Док поједина предузећа, као што су ЈКП „Паркинг сервис“, Београд, и ЈКП „Паркинг сервис“, Нови Сад, показују висок степен формализације и поделе одговорности, друга, попут ЈКП „Паркинг сервис“, Чачак, ЈКП „Чистоћа“, Краљево, и ЈП „Пословни центар“, Крушевац, сусрећу се са изазовима у погледу попуњености радних места и јасноће улога. Ова разноликост у организацији и систематизацији представља основ за даље разматрање могућности унапређења у циљу јачања капацитета за управљање информационим системима и њихову безбедност.

Процедуре за управљање безбедносним инцидентима представљају кључни део система заштите информационо-комуникационих технологија, али се међу субјектима ревизије уочавају значајне разлике у њиховој развијености и примени. Ове процедуре одређују мере превенције, реаговања и управљања ризицима насталим услед инцидената који могу угрозити сигурност система.

ЈКП „Паркинг сервис“, Београд, има утврђену процедуру управљања инцидентима нарушавања безбедности информација, која је последњи пут ажурирана у септембру 2023. године. Ова процедура обухвата дефинисање врста инцидената, формирање тима за реаговање, прикупљање доказа и евиденцију инцидената. Централизован систем за управљање инцидентима омогућава брзо и ефикасно решавање инцидената уз праћење примене мера заштите, чиме се смањују ризици и одржава континуитет пословања.

У ЈКП „Паркинг сервис“, Нови Сад, утврђена је процедура за управљање инцидентима информационе безбедности, која обухвата идентификацију, анализу и класификацију инцидената, као и примену корективних мера. Ова процедура посебно наглашава превентивне активности и континуирано унапређење мера заштите, укључујући мере специфичне за системе наплате паркирања. Додатно, ажурирани Правилник о безбедности ИКТ система прецизно дефинише улоге и одговорности запослених у случају безбедносних претњи.

ЈКП „Паркинг сервис“, Чачак, није утврдило формалне процедуре за управљање безбедносним инцидентима нити дефинисало одговорна лица задужена за превенцију и реаговање. Овај недостатак може утицати на спремност предузећа да се адекватно суочи са безбедносним претњама и смањи ризике по информационе системе.

ЈКП „Чистоћа“, Краљево, такође нема утврђене процедуре за управљање инцидентима, нити су дефинисани механизми за евиденцију и извештавање о безбедносним слабостима и претњама. Ово стање указује на потребу за унапређењем постојећег система безбедности.

ЈП „Пословни центар“, Крушевац, у свом акту о безбедности предвиђа одређене активности у вези са инцидентима, али нема утврђене процедуре које би обезбедиле ефикасно реаговање и праћење безбедносних претњи. Радно место Координатора послова информационог система и технологија обухвата низ активности, али нема изричиту обавезу праћења и извештавања о инцидентима, што ограничава могућности за побољшање система.

Док су ЈКП „Паркинг сервис“, Београд, и ЈКП „Паркинг сервис“, Нови Сад, успоставили формализоване процедуре за управљање безбедносним инцидентима, остали субјекти ревизије – ЈКП „Паркинг сервис“, Чачак, ЈКП „Чистоћа“, Краљево, и ЈП „Пословни центар“, Крушевац – немају развијене или применљиве процедуре у овој области. Ова разлика у приступу може значајно утицати на њихову способност да одговоре на безбедносне претње и обезбеде стабилност својих информационих система.

ИТ стратегија представља међусобно усклађивање између ИТ технологије и пословних стратешких циљева. Стратешки циљеви ИТ треба да размотре тренутне и будуће потребе пословања, тренутни ИТ капацитет за пружање услуга и захтеве за ресурсима. Стратегија треба да размотри постојећу ИТ инфраструктуру и архитектуру, инвестиције, модел испоруке, ресурсе, укључујући кадар, и постави стратегију која их интегрише у заједнички приступ за подршку пословним циљевима[16].

ИТ стратегија обично обухвата планирање, имплементацију, одржавање и управљање ИТ системима. ИТ стратегија обично садржи анализу тренутног стања (процена тренутних ИТ ресурса, инфраструктуре, процеса и капацитета), дефинисање визије у погледу примене ИТ технологија, идентификовање потреба организације и утврђивање како ИТ може најбоље подржати те потребе, одређивање кључних пројеката

[16] IT Audit Handbook

како би се остварили циљеви ИТ стратегије, затим планирање потребних финансијских, људских и техничких ресурса за спровођење стратегије, примену заштитиних мера у циљу заштите информационих система и праћење напретка у остваривању циљева ИТ стратегије те редовно извештавање о резултатима.

ИТ стратегија треба да буде усвојена јер помаже у усклађивању ИТ технолошких решења са пословним циљевима. ИТ послове из области информационе безбедности је неопходно детаљно уредити одговарајућим процедурама у смислу праћења активности, ревизије и надзора у оквиру управљања информационом безбедношћу, 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 ко ради на којој активности (не у смислу имена него у смислу одређеног радног места), као и податке о изменама итд. У оквиру организационе структуре утврђују се послови и одговорности запослених за заштиту информационих добара, односно средстава и имовине за надзор над пословним процесима од значаја за информациону безбедност, за управљање инцидентима у области информационе безбедности, као и за послове предвиђене процедурама у области информационе безбедности.

Законом о информационој безбедности, у складу са чланом 6а тачка 3 и тачка 4, прописано је да је обавеза оператора ИКТ система од посебног значаја да донесе акт о безбедности ИКТ система, и да врши проверу усклађености примењених мера заштите ИКТ система са актом о безбедности ИКТ система и то најмање једном годишње.

Законом о информационој безбедности, члан 8, дефинисано је да Акт из става 1 овог члана мора да буде усклађен с променама у окружењу и у самом ИКТ систему.

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 ко ради на којој активности (не у смислу имена него у смислу одређеног радног места), 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, 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.

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) је дужан да, у оквиру организационе структуре, у складу са природом, обимом и сложеношћу пословања утврди послове и одговорности запослених, у циљу управљања информационом безбедношћу.

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

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

Раздвајање одговорности (енг. separation of duties, SoD) је кључни концепт у информационим технологијама и управљању сигурношћу који има за циљ спречавање злоупотреба и минимизирање ризика унутар организације. Овај концепт подразумева да се одређене функције и одговорности раздвајају између различитих особа или улога како би се осигурало да ниједан појединац или ентитет нема превише контроле над критичним процесима или ресурсима. Раздвајање одговорности помаже у спречавању ситуација у којима би појединац могао да злоупотреби своје овлашћење или да направи грешку која би могла проузроковати озбиљне проблеме. Кључни принципи раздвајања одговорности у ИТ систему између осталих обухватају принцип двоструког одобрења (енг. dual authorization) - за критичне трансакције или промене, захтева се одобрење од две различите особе, затим принцип најмањих привилегија (енг. principle of least privilege) - особе или системи добијају само оне привилегије и овлашћења који су им потребни да обављају свој посао и ништа више, затим веома важан принцип раздвајања администратора и ИТ ревизора или особе која врши надзор - особе које су одговорне за администрацију система и ресурса не би требале бити исте особе које врше ревизију и надзор над тим истим системима. Чест је случај и неусклађености са принципом раздвајања између развоја и имплементације – наиме особе или тимови који развијају софтвер или апликације не би требали имати директну контролу над њиховим имплементирањем у продукцијском окружењу. Раздвајање одговорности захтева пажљиво планирање и правилну организацију, али може значајно допринети јачању сигурности и смањењу ризика у ИТ системима.

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.

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 ИКТ системима 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 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.).

Налаз 1.2: Контрола приступа, евидентирање активности и надзор над администраторским овлашћењима нису у пуној мери обезбеђени у Чачку, Краљеву и Крушевцу, док су у Београду и Новом Саду успостављене усклађене и функционалне мере

Законом о информационој безбедности и Уредбом о ближем уређењу мера заштите ИКТ система од посебног значаја прописано је да оператори ИКТ система морају обезбедити контролу приступа, ограничење и надзор администраторских овлашћења, чување и редовно преиспитивање логова, као и успостављање механизама за контролу и надзор над услугама које пружају трећа лица. Уговори са пружаоцима услуга треба да садрже клаузуле којима се обезбеђује ниво безбедности података у складу са прописаним мерама.

У ЈКП „Паркинг сервис“, Београд, и ЈКП „Паркинг сервис“, Нови Сад, успостављени су детаљни акти и процедуре који регулишу доделу и укидање приступа, контролу администраторских налога, евидентирање активности, као и редовну ревизију корисничких налога. У Чачку, Краљеву и Крушевцу утврђени су значајни недостаци: не постоје формализоване процедуре за деактивацију налога, лог фајлови се не чувају или нису доступни предузећу, а администраторске овлашћења имају и лица којима по опису посла не припадају. Поред тога, уговори са пружаоцима услуга не садрже одредбе о надзору над њиховим активностима, нити је обезбеђен увид у рад администратора код трећих лица.

Недовољан развој интерних процедура, недостатак стручних капацитета за контролу и надзор, као и изостанак свеобухватног уговарања безбедносних обавеза са пружаоцима услуга доприносе неадекватном управљању приступима и активностима у ИКТ системима.

Овакво стање доводи до повећаног ризика од неовлашћеног приступа и компромитације података, онемогућава утврђивање одговорности у случају инцидената и угрожава сигурност, интегритет и континуитет рада информационих система.

Контрола приступа и логовање активности	
Визија: Систем за праћење и контролу приступа ИКТ ресурсима.	Компонента: Евидентирање активности корисника и администратора.

Контрола приступа информационим системима представља основни елемент управљања безбедношћу ИКТ система у јавним комуналним предузећима. Утврђено је да постоје значајне разлике у степену уређености ове области међу субјектима ревизије.

ЈКП „Паркинг сервис“, Београд, има детаљно разрађене акта и процедуре који регулишу приступ ресурсима ИКТ система. Чланови 13 и 14 Правилника о безбедности ИКТ система дефинишу ограничења приступа, доделу права корисницима, контролу над администраторским и корисничким налозима, као и евиденцију коришћења ресурса. Процедура Безбедносне политике за администраторе ИТ система додатно уређује процес доделе, промене и укидања права приступа, уз редовну ревизију корисничких налога.

Слично томе, ЈКП „Паркинг сервис“, Нови Сад, има формализовану политику приступа која укључује дефинисање права приступа на основу пословних потреба. Кориснички налози су јасно евидентирани, а њихова ревизија спроводи се редовно како би се осигурало усклађивање са актуелним радним задацима. Правилник о безбедности ИКТ система и процедура управљања ИТ ресурсима омогућавају свеобухватну контролу приступа и надзор над коришћењем ресурса.

У ЈКП „Паркинг сервис“, Чачак, и ЈКП „Чистоћа“, Краљево, додела корисничких налога и надзор над активностима корисника дефинисани су Актом о безбедности ИКТ система. У Чачку је за ове послове задужен Координатор ИКТ послова, док је у Краљеву надлежност поверена руководиоцу сектора или запосленом кога он овласти. Иако је формално утврђена одговорност за контролу приступа, у оба предузећа није предвиђена деактивација налога у случају промене радног места или престанка радног ангажовања, што представља безбедносни ризик. Недостају и поступци који би обезбедили систематичну ревизију активних налога и праћење активности корисника, што указује на потребу за додатним унапређењем процедура у области контроле приступа.

У ЈП „Пословни центар“, Крушевац, управљање приступом мрежним ресурсима и апликативном подршком дефинисано је Актом о безбедности ИКТ система од посебног значаја. Права приступа одобравају се и укидају по налогу руководилаца организационих јединица, а захтеви се достављају администраторима путем електронске поште или у писаној форми. Надлежност за мрежне ресурсе припада Администратору ИТ система, док је надлежност за апликативни софтвер поверена Администратору апликативног софтвера. Ипак, није јасно дефинисано да ли ова два административна посла обављају различита или иста лица, јер они нису наведени у Правилнику о унутрашњој организацији и систематизацији. Контрола приступа

подразумева разликовање овлашћеног и неовлашћеног приступа, праћење локације приступа и нивоа додељених права, али из документације се не види јединствена процедура којом се осигурава доследна примена ових критеријума у пракси.

Разлике у уређености ове области указују на потребу за уједначавањем приступа кроз јасно дефинисане актове и процедуре, које би обезбедиле ефикасну контролу приступа и повећале сигурност информационих система. Док Београд и Нови Сад показују висок ниво уређености, остала предузећа се суочавају са изазовима који угрожавају сигурност и интегритет њихових система.

Бележење активности корисника и администраторских операција представља важан елемент система безбедности ИКТ система у јавним комуналним предузећима. Анализа стања показује значајне разлике у степену развијености ове области међу субјектима ревизије.

У ЈКП „Паркинг сервис“, Београд, чување података о догађајима који могу бити од значаја за безбедност ИКТ система регулисано је Правилником о безбедности ИКТ система. Активности администратора и корисника прате се кроз више врста дневника активности (activitylog, history, securitylog, transactionlog), који се архивирају сваког последњег радног дана у недељи у складу са процедуром за израду резервних копија. Систем администратор и администратор база података дужни су да најмање једном месечно, или чешће ако је потребно, анализирају садржај ових логова ради уочавања потенцијалних слабости ИКТ система.

У ЈКП „Паркинг сервис“, Нови Сад, постоји успостављена пракса евидентирања и архивирања лог фајлова, која је регулисана чланом 22 Правилника о безбедности ИКТ система. Логови активности (activitylog, history, securitylog, transactionlog) чувају се у складу са процедурама за израду резервних копија сваког последњег радног дана у недељи. Додатно, систем за контролу и дојаву о грешкама подешен је тако да у реалном времену обавештава администратора и Руководиоца Службе за ИТ о свим нерегуларним активностима и покушајима неовлашћеног приступа систему.

У ЈКП „Паркинг сервис“, Чачак, иако је дефинисана улога Координатора ИКТ послова у погледу контроле приступа и праћења евентуалних приступа са непознатих уређаја, није успостављена формализована процедура за евидентирање и чување лог фајлова. Логови активности корисника и администратора се не чувају, чиме је умањена могућност праћења и анализе безбедносних догађаја у ИКТ систему.

У ЈКП „Чистоћа“, Краљево, унутрашњим актима је предвиђено да надлежни руководиоци сектора врше свакодневну контролу приступа ИКТ ресурсима и идентификују евентуалне приступе са непознатих уређаја. Ипак, у предузећу није успостављена процедура за евидентирање и чување лог фајлова, те не постоји трајна евиденција о активностима корисника и администратора у ИКТ систему.

У ЈП „Пословни центар“, Крушевац, Актом о безбедности ИКТ система од посебног значаја прописано је формирање и чување логова који бележе активности корисника, грешке и безбедносне догађаје. За проверу логова задужен је администратор ИТ система. Ипак, лог фајлови се физички чувају код пружаоца услуга, а не у самом предузећу, при чему ЈП „Пословни центар“ не добија копију базе података, што умањује његову способност да самостално управља и анализира безбедносне догађаје.

Разлике у пракси бележења и чувања података о активностима у оквиру ИКТ система указују на потребу за стандардизацијом и унапређењем ове области. Док су у појединим предузећима, попут Београда и Новог Сада, успостављени системи за евиденцију, архивирање и анализу лог фајлова, у осталим ревидираним предузећима

недостају формализоване процедуре и техничка решења за систематско праћење активности. Овакви пропусти могу довести до смањене способности откривања и реаговања на инциденте, чиме се угрожавају сигурност и интегритет информационих система. Централизовано бележење активности и њихова редовна анализа представљају кључне кораке ка унапређењу нивоа информационе безбедности.

Физичко-техничка безбедност представља кључни аспект заштите информационих система, који подразумева обезбеђење просторија, опреме и мрежне инфраструктуре од неовлашћеног приступа и физичког оштећења. Анализа стања показала је да се ниво физичко-техничке заштите значајно разликује међу субјектима ревизије.

У ЈКП „Паркинг сервис“, Београд, физичко-техничка заштита ИКТ система је детаљно регулисана Правилником о безбедности ИКТ система. Просторије у којима се налазе сервери, мрежна и комуникациона опрема организоване су као административна зона са контролисаним приступом, механичком и електронском заштитом, уз видљиво означавање. Простор је заштићен од електромагнетног зрачења, пожара и елементарних непогода, климатизован је ради одржавања стабилне температуре, а обезбеђен је УПС уређајима и агрегатима за континуирано напајање. Евиденција улаза у зону води се унутар надлежних организационих јединица.

У ЈКП „Паркинг сервис“, Нови Сад, просторија у којој се налази серверска и мрежна опрема уређена је као административна зона са механичком бравом и видео надзором. Приступ је контролисан и надгледан од стране Руководиоца службе за ИТ или овлашћеног лица. Простор је технички заштићен од електромагнетног зрачења, пожара и других непогода, уз регулисану температуру. Улаз трећих лица дозвољен је искључиво уз претходно одобрење и у пратњи овлашћеног особља.

У ЈКП „Паркинг сервис“, Чачак, унутрашњим актом је одређено да је Координатор ИКТ послова надлежан за контролу приступа ИКТ ресурсима и идентификацију евентуалних неовлашћених приступа. Међутим, у доступној документацији нису описане конкретне мере физичко-техничке заштите просторија у којима се налази ИКТ опрема.

У ЈКП „Чистоћа“, Краљево, актом је дефинисано да надлежни руководиоци сектора врше свакодневну контролу приступа ИКТ ресурсима и откривају евентуалне приступе са непознатих уређаја. Ипак, није детаљно описано које се конкретне мере физичко-техничке заштите примењују у просторијама у којима се налази критична ИКТ опрема.

У ЈП „Пословни центар“, Крушевац, Актом о безбедности ИКТ система прописане су мере физичке заштите, укључујући забрану неовлашћеног приступа безбедносним зонама и условљавање уласка у просторије присуством овлашћеног лица. Иако је наведена потреба за применом физичко-техничке заштите, конкретне методе које би биле примењене нису јасно дефинисане у акту, што може довести до неуједначене примене мера у пракси.

Разлике у нивоу физичко-техничке заштите указују на недостатак уједначеног приступа међу ревидираним предузећима. Док су у Београду, а делимично и у Новом Саду, успостављени системи који укључују електронску контролу приступа, видео надзор и заштиту од елементарних непогода, остала предузећа се у већој мери ослањају на основне мере или немају довољно развијене процедуре. Недостатак јасно дефинисаних и примењених метода физичко-техничке заштите повећава ризик од неовлашћеног физичког приступа и могућих оштећења опреме, чиме се доводи у питање безбедност и континуитет рада информационих система.

Удаљени приступ информационим системима омогућава запосленима и администраторима да обављају своје послове са удаљених локација, али истовремено представља један од најкритичнијих аспеката безбедности који захтева строгу контролу и јасно дефинисане мере заштите. Анализа је показала различите нивое регулисања и примене удаљеног приступа међу субјектима ревизије.

У ЈКП „Паркинг сервис“, Београд, удаљени приступ је детаљно уређен интерним актима и процедурама. Приступ службеној мрежи са нерегистрованих уређаја је забрањен, а рад на даљину је дозвољен искључиво уз писмено одобрење и под строго дефинисаним техничким условима. Мобилни уређаји морају бити конфигурисани са VPN приступом и заштитним софтвером, уз забрану самосталне инсталације и уступања трећим лицима. Приступ са приватних уређаја је изузетно ограничен и захтева додатне мере контроле. Све активности се евидентирају, а надзор се спроводи свакодневно.

У ЈКП „Паркинг сервис“, Нови Сад, удаљени приступ је омогућен искључиво преко службених мобилних уређаја који су конфигурисани од стране Службе за ИТ и заштићени путем VPN-а, антивирусног софтвера и дефинисаних MAC адреса. Забрањена је самостална инсталација софтвера и коришћење уређаја од стране неовлашћених лица. Администратори и овлашћени запослени имају могућност удаљеног приступа ради хитних интервенција, уз претходну сагласност и попуњавање формализованог захтева. Приступ са приватних уређаја није дозвољен.

У ЈКП „Паркинг сервис“, Чачак, и ЈКП „Чистоћа“, Краљево, предвиђена је могућност удаљеног приступа путем приватних уређаја, али само у случајевима када службени уређај није доступан и уз претходно подешавање од стране надлежних лица. Међутим, у пракси се не води евиденција нити врши контрола над уређајима са којих се остварује приступ ИКТ систему, што представља озбиљан недостатак у систему безбедности и може довести до неовлашћеног приступа и компромитовања података.

У ЈП „Пословни центар“, Крушевац, Актом о безбедности ИКТ система прописане су детаљне мере заштите у случају удаљеног приступа, укључујући примену VPN технологије, сертификата, статичких ИП адреса, специјализоване опреме и вишеструких механизама аутентификације. Такође су дефинисани услови за безбедно коришћење мобилних уређаја и поступци пријаве неправилности. Ипак, у пракси се удаљени приступ не користи, што у потпуности елиминише ризике који могу настати услед рада са даљине.

Разлике у примени и контроли удаљеног приступа указују на неуједначене праксе међу ревидираним предузећима. Док су у Београду и Новом Саду успостављене процедуре које омогућавају безбедан приступ путем службених уређаја, уз примену VPN технологије, антивирусне заштите и ограничених права, у Чачку и Краљеву се у пракси не врши адекватна евиденција и контрола удаљених приступа, што повећава ризик од неовлашћеног коришћења ИКТ ресурса. У Крушевцу је удаљени приступ формално предвиђен, али се у пракси не користи, чиме се ризици везани за овај вид приступа елиминишу.

Заштита података и уговори са пружаоцима услуга	
Визија: Обезбеђење да пружаоци услуга примењују прописане мере заштите.	Компонента: Уговори који дефинишу приступ, заштиту и обраду података.

Заштита података и управљање односима са пружаоцима услуга у ЈКП „Паркинг сервис“, Чачак, ЈКП „Чистоћа“, Краљево, и ЈП „Пословни центар“, Крушевац показују значајне слабости у организацији и примени безбедносних мера.

У ЈКП „Паркинг сервис“, Чачак, сервери су смештени код пружаоца услуга „Synapse tech“ д.о.о., Београд, на основу уговора о јавној набавци. Администраторски приступ систему има и пружалац услуга, иако Актом о информационој безбедности није предвиђено нити регулисано измештање сервера нити обављање администраторских функција од стране спољног лица. Оваква организација није у складу са интерним актима и представља ризик за заштиту података и контролу активности у систему.

У ЈКП „Чистоћа“, Краљево, сервери се такође налазе код пружаоца услуга – предузећа „Ђоковић Софтвер“ д.о.о. из Чачка. Администраторски приступ имају и запослени тог пружаоца услуга, што није усклађено са Актом о информационој безбедности предузећа, у коме такође није регулисан овакав модел сарадње. Одговорна лица у предузећу нису навела да имају увид у активности корисника са администраторским правима, нити су уговори са пружаоцима услуга допуњени клаузулама које би прецизније дефинисале обавезе у погледу заштите података и администрирања.

У ЈП „Пословни центар“, Крушевац, администраторски приступ систему имају и запослени пружаоца услуга, као и интерни корисници са статусом „менаџмент“ и „пословођа“, иако по опису посла не би требало да поседују та овлашћења. У администраторском модулу идентификовано је 13 активних администраторских налога, од којих за неке одговорна лица нису била упозната. Ово указује на непотпуну контролу над правима приступа и повећава ризик од неовлашћених измена у систему. Уговори са пружаоцима услуга такође не садрже прецизне одредбе које би регулисале начин администрирања и надзора над активностима трећих лица.

Недостаци у интерним актима, неуједначено управљање приступима и недовољно дефинисане уговорне обавезе са пружаоцима услуга у овим предузећима представљају значајан ризик по интегритет, поверљивост и доступност информација.

Мере заштите ИКТ система се између осталог односе на одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа, такође и на безбедан приступ када је у питању рад на даљину.

Чланом 10 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја, прописано је 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).

Чланом 18 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја прописано је чување података о догађајима који могу бити од значаја за безбедност ИКТ система тако да оператор ИКТ система треба да обезбеди да се у ИКТ систему формирају записи о догађајима (логови) у вези активности корисника, грешкама и догађајима у вези са информационом безбедношћу, а који се морају чувати и редовно проверавати. Средства за записивање и записи треба да буду заштићени од неовлашћеног приступа и промене. У оквиру ИКТ система записују се активности администратора и корисника и редовно преиспитују у циљу заштите. У циљу обезбеђивања поузданости записа, времена у свим подсистемима ИКТ система морају бити синхронизована међусобно, као и са референтним тачним временом.

Чланом 3 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја, прописано је постизање безбедности рада на даљину и употребе мобилних уређаја.

Оператор ИКТ система који у свом систему дозвољава рад на даљину и употребу мобилних уређаја дужан је да успостави и одржава безбедност рада на даљину и употребе мобилних уређаја, узимајући у обзир ризике који могу постојати услед неадекватног коришћења мобилних уређаја (став 1).

Оператор ИКТ система је дужан да дефинише услове и ограничења за рад на даљину тако да се не угрози безбедност ИКТ система, при чему оператор ИКТ система узима у обзир физичку безбедност места и окружења са кога се обавља рад на даљину, услове за безбедност комуникације између ИКТ система оператора и места са којег се ради на даљину, превенцију или свођење на неопходни минимум обраде и чувања информација на личном уређају лица које ради на даљину, превенцију од неовлашћеног приступа, услове за коришћење локалне мреже и бежичних мрежних сервиса, захтеве за заштиту од злонамерних софтвера и друге мере које су потребне за безбедност рада на даљину (став 2).

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

1) евиденцију мобилних уређаја;
2) мере физичке заштите мобилних уређаја (од уништења, оштећења, губитка или неовлашћеног приступа уређајима и подацима од интереса за оператора ИКТ система);
3) ограничења за инсталацију и ажурирање софтвера;
4) инсталацију адекватних софтвера за мобилне уређаје и њихово редовно ажурирање;

5) ограничење коришћења услуга информационог друштва које би угрозиле информациону безбедност ИКТ система;
6) контроле приступа мобилном уређају и подацима на њему;
7) криптографске технике;
8) заштиту од вируса и других злонамерних софтвера;
9) даљинско управљање мобилним уређајем у случају инцидента, од стране овлашћеног лица оператора ИКТ система, путем којег је могуће да се изврши неповратно брисање података и онемогућавање даљег коришћења уређаја;
10) успостављање и одржавање резервне копије (backup) података;
11) омогућавање безбедног коришћења интернет сервиса и апликација (став 3).

Ако оператор ИКТ система дозвољава у свом систему коришћење приватних мобилних уређаја дужан је да обезбеди услове из става 3 овог члана и предузме мере ради раздавајања приватног од пословног коришћења ових уређаја (став 4).

Чланом 27 Уредбе прописано је 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.

Налаз 1.3: Мере за континуитет пословања и управљање резервним копијама података у потпуности су успостављене само у Новом Саду, делимично у Београду, док остала предузећа нису развила планове континуитета нити адекватно управљају резервним копијама података

Законом о информационој безбедности и Уредбом о ближем уређењу мера заштите ИКТ система од посебног значаја прописано је да оператори ИКТ система морају да успоставе мере заштите које обезбеђују континуитет обављања послова у ванредним околностима, као и мере заштите од губитка података. Ове мере подразумевају доношење формализованих планова континуитета пословања и плана опоравка од катастрофе (DRP), као и процедуре за израду, проверу и безбедно чување резервних копија података.

ЈКП „Паркинг сервис“, Нови Сад је једино предузеће које је успоставило три формализована плана континуитета за различите критичне сценарије, уз дефинисане одговорности и редовно тестирање применљивости. Поред тога, систем израде резервних копија у овом предузећу је уређен, са копијама које се чувају и на удаљеним локацијама, у складу са безбедносним политикама. У Београду је поступак за израду планова формално дефинисан и обухвата више ризичних сценарија, али појединачни планови за те ситуације нису развијени. Резервне копије се редовно праве и чувају, укључујући и ван примарне локације, уз полугодишњу проверу исправности.

Са друге стране, у Чачку, Краљеву и Крушевцу нису донети формални планови континуитета, нити су утврђене интерне процедуре за поступање у случају ванредних околности. У овим предузећима ослањање на пружаоце услуга није праћено уговорним клаузулама које би осигурале усклађеност са прописаним стандардима. Када је реч о резервним копијама, у Чачку и Краљеву нема доказа о постојању интерне политике израде и тестирања

копија, а подаци се чувају искључиво код пружаоца услуга. У Крушевцу су резервне копије предвиђене актом, али се не чувају ван основне локације, чиме се смањује њихова ефективност у кризним ситуацијама.

Недовољна уређеност система за континуитет пословања и управљање резервним копијама произилази из непотпуне примене прописаних мера, недостатка стручних капацитета и неадекватне процене ризика. Ово доводи до повећаног ризика од губитка података, продуженог прекида рада и немогућности наставка пружања услуга грађанима у случају већих хаварија или сајбер инцидената, што може имати озбиљне последице по функционисање предузећа и поузданост њихових ИКТ система.

План континуитета пословања	
Визија: Обезбеђење континуитета пословања у ванредним околностима.	Компонента: План опоравка од катастрофе и управљање резервним копијама.

Планови континуитета пословања нису уједначено развијени међу субјектима ревизије, што указује на потребу за доследнијом применом прописаних мера.

У ЈКП „Паркинг сервис“, Београд, постоји процедура за израду плана континуитета пословања, која је ажурирана у септембру 2023. године и предвиђа развој планова за више сценарија прекида ИТ функција. Међутим, иако је поступак формално прописан, појединачни планови за предвиђене сценарије до сада нису развијени. Унутрашњи акти дефинишу обавезу измештања и активирања критичних ресурса у случају ванредних околности, али формализовани планови у складу са процедуром нису достављени на увид.

Супротно томе, у ЈКП „Паркинг сервис“, Нови Сад, развијена су три конкретна плана континуитета (за случај прекида снабдевања електричном енергијом, пожара и отказа критичног ИКТ ресурса). Планови су усклађени са интерном процедуром и подлежу редовном тестирању кроз вежбе и симулације, што указује на унапређени ниво припремљености и организационе зрелости у овој области.

У ЈКП „Паркинг сервис“, Чачак, као и у ЈКП „Чистоћа“, Краљево, и ЈП „Пословни центар“, Крушевац, нису донети формални планови континуитета. Иако се у уговорима са пружаоцима услуга налазе одредбе о неометаном функционисању система и подршци у случају прекида, интерне процедуре које би дефинисале улоге, активности и одговорности у ванредним околностима нису развијене. У Крушевцу је Актом о безбедности ИКТ система предвиђена израда оваквих планова, али активности на њиховој реализацији до сада нису спроведене, нити је успостављен план за опоравак након хаварије.

Указано стање одражава значајне разлике у примени прописа и процедура у области континуитета пословања. Док је Нови Сад успоставио функционалан систем планирања, код осталих предузећа идентификован је изостанак формализованих планова и активности, што може утицати на способност предузећа да брзо реагују и обезбеде наставак пословања у случају прекида.

Стање у области израде и чувања резервних копија показује значајне разлике међу субјектима ревизије. У ЈКП „Паркинг сервис“, Београд, резервне копије података се израђују у складу са интерним процедурама и чланом 21 Правилника о безбедности

ИКТ система. Архивирање се спроводи на дневном, недељном, месечном и годишњем нивоу, при чему се годишње копије чувају у два примерка, од којих је један на дислоцираној локацији. Исправност копија проверава се на сваких шест месеци, а поступак је формализован кроз безбедоносне политике и упутства службе за ИТ.

У ЈКП „Паркинг сервис“, Нови Сад, успостављене су формализоване процедуре израде резервних копија које обухватају недељно и годишње архивирање база података, као и месечно и годишње архивирање осталих докумената. Годишње копије се чувају у два примерка, од којих је један на другој локацији у оквиру архиве предузећа. Исправност архива се формално проверава сваких пет година, уз примену безбедносне политике и надзор од стране администратора и руководиоца службе. Архивирање се врши у складу са планом континуитета безбедности информација, и не ремети редовно функционисање система.

У ЈКП „Паркинг сервис“, Чачак, не постоји унутрашња процедура за израду и чување резервних копија, нити су исте успостављене у оквиру интерних аката. Уговор са пружаоцем услуга „Synapse tech“ предвиђа функционалност система, али не дефинише процедуре прављења и тестирања резервних копија нити њихово складиштење ван примарне инфраструктуре. То указује на ослањање на екстерне ресурсе без јасно дефинисаних механизама заштите података од губитка.

Слично томе, у ЈКП „Чистоћа“, Краљево, уговори са пружаоцем услуга „Ђоковић Софтвер“ предвиђају израду резервних копија, али предузеће нема успостављене интерне процедуре које би уредиле начин прављења, тестирања и чувања тих копија. Нема доказа да се копије чувају на независним, безбедним локацијама, што повећава ризик у случају техничких проблема.

У ЈП „Пословни центар“, Крушевац, Актом о безбедности ИКТ система предвиђена је редовна израда резервних копија и заштита од губитка података, али у пракси није успостављен систем за складиштење ван примарне локације. Резервне копије се чувају искључиво у оквиру објеката предузећа, без примене физичке и логичке изолованости од продукционог система, што смањује њихову ефикасност у случају озбиљних инцидената.

Описано стање указује на потребу за стандардизацијом поступака израде и чувања резервних копија, као и унапређењем постојећих процедура у предузећима која се ослањају на екстерне пружаоце услуга. Док Београд и Нови Сад показују висок ниво уређености у овој области, у осталим предузећима недостају или нису адекватно примењени механизми који би обезбедили поуздану заштиту података и континуитет пословања у случају прекида.

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

Влада Републике Србије је обавезе оператора ИКТ система детаљније уредила Уредбом о ближем уређењу мера заштите информационо-комуникационих система од

посебног значаја. Члан 29 наведене Уредбе уређује мере које обезбеђују континуитет обављања посла у ванредним околностима и то:

- Оператор ИКТ система треба да предвиди мере којима се обезбеђује обављање послова у ванредним околностима, а које подразумевају одржавање информационе безбедности на задовољавајућем нивоу, дефинисање одговорности, планова, поступака у случају ванредних догађаја и процедура за опоравак ИКТ система, у оквиру редовних процедура за одржавање информационе безбедности или доношењем посебних процедура.
- Оператор ИКТ система треба да успостави, документује, имплементира и одржава процесе, процедуре и контроле да би осигурао захтевани ниво континуитета пословања током ванредне ситуације.
- Оператор ИКТ система треба да верификује успостављене и имплементиране контроле континуитета пословања у редовним условима рада, како би оне биле важеће и ефективне током ванредне ситуације.
- Оператор ИКТ система треба да идентификује захтеве за доступност ИКТ система. Редундантне компоненте треба размотрити онда када се доступност не може гарантовати коришћењем постојећих архитектура система.

Напретком ИТ, ниво знања у тој области расте код све већег броја грађана, па и оних недобронамерних (хакери), повећава се ризик и могућност да поред проблема изазваних кваровима, или незнањем, информациони системи постану и предмет хакерских, сајбер напада.

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

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

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

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

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

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

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

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

Нестанак електричне енергије, нарочито у дужем периоду, поплава, земљотрес, пожар, па чак и крађа или намерно оштећење опреме су догађаји које се не могу предвидети, а који могу систем или део система оштетити у толиком проценту да је

онемогућено његово функционисање. Ово се чак може односити и на саму зграду у којој се систем налази.

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

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

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

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

Такође, за успостављање континуитета пословања неопходно је успоставити и управљање резервним копијама података. Уредбом је прописан заштита од губитка података, која се постиже редовном израдом резервних копија података, софтвера и система путем одговарајућих средстава за израду резервних копија. Оператор ИКТ система дефинише време чувања и заштите резервних копија, обим и учесталост резервних копија, безбедно место чувања резервних копија, обезбеђује физичку заштиту резервних копија и заштиту од спољашњих утицаја, проверава носаче података како би се осигурало њихово исправно функционисање и поузданост у складу са планом израде резервних копија. Оператор ИКТ система врши израду резервних копија које треба да обухвате све системске информације, апликације и податке који су неопходни за опоравак целокупног система у случају наступања последица изазваних ванредним околностима (члан 17).

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

Налаз 1.4: Систем управљања ИТ ризицима успостављен је и унапређен у Београду и Новом Саду, док Чачак, Краљево и Крушевац нису развили овај механизам

Законом о информационој безбедности и Уредбом о ближем уређењу мера заштите ИКТ система прописано је да оператори ИКТ система морају успоставити механизме за управљање ИТ ризицима. Ови механизми треба да обухвате идентификацију, процену, третман и мониторинг ризика, како би се осигурала сигурност, интегритет и доступност информационих система.

ЈКП „Паркинг сервис“, Нови Сад, већ је имало успостављен систем за управљање ризицима, који укључује Стратегију управљања ризицима и

регистар ризика. Током ревизије, предузеће је ревидирало и ажурирало своје класификације ризика, чиме је побољшана процена утицаја и дефинисани додатни механизми за смањење ризика. ЈКП „Паркинг сервис“, Београд, је у току ревизије допунило свој Правилник о систематизацији послова и унапредило процедуре управљања ризицима, чиме је омогућило бољу интеграцију процене ризика у редовне пословне активности.

Насупрот томе, у ЈКП „Паркинг сервис“, Чачак, ЈКП „Чистоћа“, Краљево, и ЈП „Пословни центар“, Крушевац, механизми управљања ризицима нису успостављени. У овим предузећима није формализована одговорност запослених за управљање ИТ ризицима, нити су дефинисане процедуре за идентификацију и процену ризика. Ова предузећа нису показала значајан напредак у овој области током ревизије.

Недостатак довољних улагања, ограничени кадровски капацитети и свест о значају управљања ризицима представљају главне узроке оваквог стања.

Последице ових недостатака укључују повећан ризик од безбедносних инцидената, губитка података и нарушавања континуитета пословања. Предузећа која нису успоставила механизме за управљање ризицима остају подложна негативним последицама које могу значајно утицати на њихову ефикасност и поузданост.

Механизам управљања ИТ ризицима	
Визија: Процес идентификације, процене и управљања ИТ ризицима.	Компонента: Интеграција управљања ризицима у свакодневне пословне процесе.

Механизам управљања ИТ ризицима у јавним комуналним предузећима показује значајне разлике у примени и развијености, али су уочени и позитивни помаци у току ревизије код појединих субјеката.

У ЈКП „Паркинг сервис“, Београд, иницијално је утврђено да механизам управљања ризицима није у потпуности интегрисан у систематизацију послова. Процедура за идентификацију, процену и третман ризика је постојала, али је њена примена била ограничена. Током ревизије, предузеће је ажурирало своје интерне акте и унапредило праксе, укључујући укључивање процене ризика у редовне активности Службе за информационе технологије. Ове мере допринеле су већој ефикасности и отпорности система.

ЈКП „Паркинг сервис“, Нови Сад, је у старту имало успостављен механизам за управљање ризицима који укључује Стратегију управљања ризицима и регистар са четири идентификована ризика. У току ревизије, предузеће је спровело додатну процену ризика, чиме су ревидиране класификације и предложене мере за смањење идентификованих ризика, посебно код подсистема за наплату паркирања. Овај приступ показао је висок степен свести о значају систематског управљања ризицима.

Насупрот томе, ЈКП „Паркинг сервис“, Чачак, ЈКП „Чистоћа“, Краљево, и ЈП „Пословни центар“, Крушевац, нису предузели значајне мере у овој области. У овим предузећима механизми за управљање ИТ ризицима нису успостављени, а послови који се односе на процену и управљање ризицима нису формализовани у Правилницима о систематизацији. Запослени нису обучени за примену мера процене и третмана ризика,

нити постоје интерни акти који би регулисали ову област. Током ревизије, ова предузећа нису показала значајан напредак у овој области.

Док су Београд и Нови Сад током ревизије предузели мере за унапређење својих механизама за управљање ИТ ризицима, остала предузећа се суочавају са озбиљним ограничењима која угрожавају сигурност њихових информационих система и континуитет пословања. Ова разлика у приступу указује на потребу за стандардизацијом и широм применом добрих пракси у овој области.

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

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

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

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.

ЗАКЉУЧАК 2: Сарадња са корисницима система у Београду и Новом Саду значајно је унапређена, али остаје простор за додатни напредак кроз успостављање криптовања и потпуну примену процедура за архивирање, миграцију и уништавање података код Новог Сада

Циљ овог дела извештаја био је да оцени степен до којег су ЈКП „Паркинг сервис“, Београд и ЈКП „Паркинг сервис“, Нови Сад успоставили ефикасан механизам сарадње са корисницима система, с акцентом на поузданост и заштиту података у складу са Законом о заштити података о личности. Испитивање је обухватило анализу постојећих правила и процедура које су регулисале безбедност података корисника и начин на који су дефинисани услови за њихову заштиту у уговорима и интерним актима. Такође, циљ је био да се утврди да ли је субјект ревизије обезбедио адекватне механизме за архивирање и уништавање података у случајевима прекида сарадње, као и да се испита да ли су предузете мере за контролу и надзор над спровођењем уговорних обавеза, нарочито у погледу поверљивости и поузданости података.

На основу анализе законских и подзаконских аката, документације субјекта ревизије и одржаних интервјуа, донели смо закључак који темељимо на следећим налазима:

Налаз 2.1: ЈКП „Паркинг сервис“, Београд и ЈКП „Паркинг сервис“, Нови Сад су правилницима, процедурама и физичком заштитом обезбедили безбедност података корисницима система

Свеобухватна безбедност ИКТ система		
Успостављање докумената и ажурирање процедура.	Физичка и логичка заштита инфраструктуре.	Континуитет пословања и прављење резервних копија.

ЈКП „Паркинг сервис“, Београд, и ЈКП „Паркинг сервис“, Нови Сад, успоставили су мере за свеобухватну безбедност ИКТ система, укључујући усвајање правилника, процедура и упутстава, физичко обезбеђење просторија и системско чување резервних копија. Ове мере имају за циљ заштиту података корисника и сигурност система који се користе за наплату услуга паркинга.

ЈКП „Паркинг сервис“, Београд, је уредио безбедност података кроз више докумената, као што су Правилник о безбедности ИКТ система и Безбедносне политике и поступци за кориснике и администраторе ИТ система. Простор у којем се налази критична инфраструктура организован је као административна зона са контролисаним приступом, електронском контролом, заштитом од електромагнетног зрачења, пожара и климатизацијом. Резервне копије података се креирају на дневном, недељном, месечном и годишњем нивоу и чувају на две локације, уз редовну проверу исправности сваких шест месеци.

ЈКП „Паркинг сервис“, Нови Сад, је успоставио сличне мере, укључујући Правилник о безбедности ИКТ система, процедуре за управљање ИТ ресурсима и континуитет безбедности информација. Сервер собе су обезбеђене механичком бравом и видео надзором, уз контролу приступа и евиденцију улазака. Током ревизије је започета поставка секундарног сервера на другој локацији, што додатно осигурава

континуитет рада. Резервне копије података се свакодневно праве и чувају у посебној просторији, у складу са интерним актом.

Ови механизми осигуравају висок ниво безбедности ИКТ система код оба пружаоца услуга, уз континуирано унапређење мера за заштиту података и стабилност система.

Организација која пружа услуге другим корисницима треба да успостави и примењује свеобухватан скуп докумената који регулише безбедност ИКТ система, укључујући правилнике, процедуре и упутства. Ови документи треба да обухватају начин евидентирања, заштите и коришћења електронских докумената, управљање ИТ ресурсима, континуитет безбедности информација и одржавање ИКТ опреме. Такође, потребно је да се ови документи редовно ажурирају у складу са најбољим праксама и стандардима, попут ISO/IEC 27001:2022 – Системи за управљање безбедношћу информација и ISO 22301:2019 – Системи за управљање континуитетом пословања.

Просторије у којима се налази критична ИКТ инфраструктура морају бити одговарајуће означене и физички заштићене. Ова заштита укључује механичке браве, видео надзор и заштиту од електромагнетног зрачења, пожара и других ризика. Такође, неопходно је одржавати стабилну температуру у просторијама како би се спречило оштећење опреме. Приступ просторијама мора бити строго контролисан, а сваки улазак документован и надзиран од стране овлашћених лица.

Организација треба да обезбеди континуитет пословања кроз инсталацију система резервног напајања, попут УПС уређаја, како би систем наставио да функционише и у случају нестанка електричне енергије. Постављање секундарног сервера на другој локацији додатно повећава отпорност система и обезбеђује несметан рад у случају непредвиђених ситуација.

Редовно прављење резервних копија података, како корисничких тако и интерних, кључно је за заштиту података. Ове резервне копије треба чувати у посебно обезбеђеној просторији која је физички и логички заштићена. Процес прављења и чувања резервних копија мора бити дефинисан интерним актима организације, а његово спровођење редовно праћено и документовано.

Налаз 2.2: ЈКП „Паркинг сервис“, Београд је успоставио систем заштите података који обезбеђује сигурност података корисника услуга, док је ЈКП „Паркинг сервис“, Нови Сад предузео значајне мере за заштиту података, уз потребу за увођењем криптовања података

Законом о заштити података о личности и Уредбом о ближем уређењу мера заштите ИКТ система од посебног значаја, пружаоци ИТ услуга морају успоставити свеобухватне механизме за заштиту података корисника. Ови механизми треба да укључују јасно дефинисане улоге руковаоца, обрађивача и подобрађивача података, као и мере за контролу приступа, надзор активности и осигурање поверљивости и интегритета података.

ЈКП „Паркинг сервис“, Београд, је успоставило систематску заштиту података кроз Правилник о заштити података о личности и друге интерне акте, чиме је обезбеђена контрола приступа, евиденција активности и сарадња са подобрађивачем. Подаци корисника су заштићени кроз процедуре које укључују изјаве о поверљивости и процену ризика, уз јасну поделу улога између руковаоца, обрађивача и подобрађивача. У Новом Саду, у току ревизије

су донете нове процедуре и уговори који прецизно дефинишу права и обавезе свих страна у обради података. Такође, предузете су мере за уклањање приступа осетљивим подацима и планирана је имплементација криптовања података, што је значајно унапредило ниво заштите.

Иницијални недостаци у систематизацији и процедурама били су резултат недостатка свести о значају управљања подацима, као и недовољног техничког капацитета. Током ревизије, ова питања су делимично решена увођењем нових мера и процедура.

Систематским унапређењем заштите података корисника, ризик од компромитације је значајно смањен. Ово је омогућило већу поузданост система, бољу сарадњу са корисницима и усклађеност са законским и стандардним захтевима за информациону безбедност. Ипак, неопходно је наставити са редовним надзором и ажурирањем процедура како би се обезбедио континуитет у високом нивоу заштите.

Систематска заштита података корисника		
Дефинисање процедура за заштиту података.	Контрола приступа и транспарентност.	Уговори са јасно дефинисаним правима и обавезама.

Систематска заштита података корисника представља критичан елемент безбедности у ИКТ системима који се користе за наплату услуга паркинга. Анализа је показала различите нивое уређености ове области у ЈКП „Паркинг сервис“, Београд и ЈКП „Паркинг сервис“, Нови Сад, као и значајан напредак током ревизије.

У ЈКП „Паркинг сервис“, Београд, заштита података је регулисана кроз Правилник о безбедности информационо-комуникационог система и Правилник о заштити података о личности, који су усклађени са Законом о заштити података о личности. Улоге руковаоца, обрађивача и подобрађивача података јасно су дефинисане, што омогућава прецизну контролу над обрадом података. Предузеће је постављено као обрађивач података, док су корисници услуга руковаоци, а ангажована је компанија „Prokomsoft“ д.о.о. као подобрађивач за специфичне аспекте обраде. Обезбеђена је контрола приступа и поверљивост података кроз стандардне уговорне клаузуле и додатне мере као што су изјаве о поверљивости и процена ризика.

У ЈКП „Паркинг сервис“, Нови Сад, иницијално су постојали недостаци у погледу процедура за сарадњу са корисницима услуга и приступа осетљивим подацима од стране подобрађивача. Подаци у базама нису били криптовани, што је представљало ризик за њихову поверљивост и интегритет. Током ревизије, предузеће је донело нове процедуре, укључујући Уговор о обради података и Уговор о поверљивости, којима су прецизно дефинисана права и обавезе руковаоца, обрађивача и подобрађивача. Предузете су мере за уклањање приступа осетљивим подацима и планирана је имплементација криптовања података, при чему ће кључеви бити поверени руковаоцима података.

Оба предузећа су у значајној мери унапредила систематску заштиту података корисника, чиме је смањен ризик од компромитације и осигурана већа поузданост информационих система који се користе за наплату услуга паркинга.

Организације које пружају ИТ услуге корисницима треба да детаљно уреде правила и процедуре које се односе на заштиту података корисника, праћење активности и ревизију у контексту управљања информационом безбедношћу. Такође треба да успоставе свеобухватан механизам за управљање пружањем услуга који укључује политике, процедуре и активности усмерене на испуњење циљева корисника. Овај механизам треба да покрива идентификацију специфичних захтева корисника у погледу хардверских, софтверских и људских ресурса, примену одговарајућих стандарда информационе безбедности, као и начин на који се формализује и прати сарадња са корисницима.

Процедуре морају омогућити транспарентан и безбедан приступ корисничким подацима, као и контролу квалитета пружених услуга. Ове процедуре треба да буду структурисане тако да обезбеде континуитет у случају кадровских промена, омогућавајући новим запосленима да брзо наставе са обављањем задатака без поремећаја у сервисима за кориснике.

Процедуре морају бити довољно детаљне и укључивати опис свих процеса који се односе на кориснике услуга, као и податке о томе које радне позиције су одговорне за одређене активности. Поред тога, морају бити доступне информације о свим изменама у процедурама како би се осигурала њихова актуелност и примењивост.

У складу са Уредбом о ближем уређењу мера заштите ИКТ система од посебног значаја, организације морају осигурати да су подаци и ресурси корисника заштићени од неовлашћеног приступа. Ово подразумева успостављање јасних процедура за ниво приступа информацијама корисника, начине приступа и надзор над приступом. Корисници морају бити информисани о томе како се њихови подаци користе и осигурати да су заштићени у складу са стандардима информационе безбедности, као што су ISO/IEC 27001:2022 и други релевантни стандарди.

Уговори или споразуми са корисницима услуга треба да јасно дефинишу права и обавезе обе стране у погледу приступа и заштите информација. Организација је одговорна да обезбеди да сви корисници имају једнак ниво заштите података, у складу са актом о безбедности ИКТ система и другим релевантним прописима.

Пружање услуга мора обухватити ефикасну заштиту података корисника, надзор над приступом информацијама и ресурсима, као и евидентирање свих активности у вези са пружањем услуга. Ово укључује редовно праћење перформанси услуга, прилагођавање новим захтевима корисника и континуирано побољшање услуга на основу добијених повратних информација.

Налаз 2.3: ЈКП „Паркинг сервис“, Београд у ревидираном периоду није успоставио механизам за архивирање, уништавање или повраћај података у случају промене пружаоца услуга, док ЈКП „Паркинг сервис“, Нови Сад није успоставило процедуре за архивирање, уништавање и миграцију података у случају раскида сарадње са корисницима

Законом о заштити података о личности и релевантним стандардима, као што су ISO/IEC 27001 и ISO/IEC 27018, прописано је да пружаоци услуга морају успоставити механизме за сигурно управљање подацима након раскида уговора. Ове мере укључују архивирање, сигурно уништавање и омогућавање повраћаја података клијентима, уз строго дефинисане процедуре и контроле.

Анализом је утврђено да ЈКП „Паркинг сервис“, Београд, иницијално није имало успостављене процедуре за сигурно управљање подацима након раскида уговора. Услед ревизије, предузеће је усвојило процедуру „Предаја и брисање података са сервера услед престанка уговорних обавеза“ (ПС.П64), која обезбеђује извоз података, пренос криптографских кључева и трајно брисање података уз примену сертификованих метода. Овај процес је усклађен са стандардима и документован како би се обезбедила транспарентност и сигурност.

У ЈКП „Паркинг сервис“, Нови Сад, иницијално су недостајале формализоване процедуре за уништавање и повраћај података. Током ревизије, предузеће је закључило нове уговоре са прецизно дефинисаним правима и обавезама, укључујући обавезу преноса података у електронском формату, трајно брисање података на захтев корисника и коришћење апликације „SWAT“ у периоду од три месеца након истека уговора. Такође, уведена је процедура надзора над процесом брисања, која укључује извештавање и документовање свих активности.

Недостатак иницијалних мера у оба предузећа проистицао је из недовољне техничке уређености и свести о значају ових активности. Током ревизије, ова питања су успешно решена увођењем процедура и технолошких решења.

Резултат ових мера је значајно унапређење сигурности управљања подацима након раскида уговора. Ова унапређења су смањила ризик од компромитације података, обезбедила усклађеност са прописима и повећала поверење корисника у системе који се користе за наплату услуга паркинга.

Сигурно управљање подацима при раскиду уговора		
Архивирање и контролисано чување података.	Уништавање података у складу са стандардима.	Повраћај података клијенту и документација процеса.

Сигурно управљање подацима у случају раскида уговора представља један од кључних аспеката заштите корисничких података и очувања интегритета система за наплату услуга паркинга. Анализа стања у ЈКП „Паркинг сервис“, Београд, и ЈКП „Паркинг сервис“, Нови Сад, показала је иницијалне недостатке у овој области, али и значајне унапређења током ревизије.

У ЈКП „Паркинг сервис“, Београд, у почетку нису постојале формализоване процедуре за управљање подацима након раскида уговора са корисницима или добављачима услуга. Ово је укључивало недостатак дефинисаних активности за извоз података, пренос криптографских кључева и брисање података са сервера. Као резултат ревизије, донета је процедура „Предаја и брисање података са сервера услед престанка уговорних обавеза“ (ПС.П64). Ова процедура садржи детаљне кораке који укључују

идентификацију података за извоз, употребу сертификованих метода за трајно брисање података и документовање целог процеса. Поред тога, предузеће је увело и обавезу издавања потврде корисницима о успешно завршеном процесу брисања, чиме је обезбеђена усклађеност са стандардима ISO/IEC 27001 и ISO/IEC 27018. Ове мере значајно су побољшале сигурност и усклађеност са законским захтевима.

ЈКП „Паркинг сервис“, Нови Сад, такође је започео ревизију са недостатком формализованих процедура за управљање подацима при раскиду уговора. Подаци корисника су били у опасности од неадекватног брисања или губитка у недостатку одговарајућих мера. Током ревизије, предузеће је унапредило своје праксе кроз закључивање нових уговора који предвиђају пренос података у електронском формату, попут CSV фајлова, трајно брисање података на захтев корисника и омогућавање коришћења апликације „SWAT“ у ограниченом периоду након истека уговора. Поред тога, дефинисана је процедура за надзор над процесом брисања података, укључујући извештавање о активностима и документовање коришћених метода.

У оба предузећа су успостављене контроле које осигуравају да се подаци корисника ефикасно и сигурно управљају након раскида уговора. Док је Београд имплементирао јасне процедуре које обухватају цео процес, Нови Сад је усвојио напредна технолошка решења за пренос и брисање података, чиме је осигурана поузданост и усклађеност са важећим прописима. Ова унапређења значајно су смањила ризик од губитка или злоупотребе података, повећавајући сигурност и поверење у системе који се користе за наплату услуга паркинга.

Приликом раскида уговора са пружаоцима ИТ услуга, механизам управљања подацима мора бити пажљиво осмишљен како би осигурао да се подаци корисника адекватно архивирају, безбедно уништавају или врате клијенту у складу са највишим стандардима информационе безбедности и заштите података, као што су ISO/IEC 27001, ISO/IEC 27018, ISO/IEC 20000, и GDPR. Пружаоци услуга морају следити јасне и прописане политике и процедуре како би се заштитили поверљивост, интегритет и доступност података након завршетка сарадње.

Прво и основно, архивирање података мора бити усклађено са захтевима стандарда ISO/IEC 27001 и ISO/IEC 20000, који постављају основе за безбедно чување података у договореном периоду. Пружаоци услуга су обавезни да дефинишу рокове за чување података, у складу са правним и регулаторним оквиром, а подаци морају бити чувани на сигуран начин, уз примену мера као што је криптографска заштита. Приступ архивираним подацима мора бити строго контролисан и ограничен само на овлашћена лица, што спречава могућност неовлашћеног приступа.

Када је реч о уништавању података, пружаоци услуга морају обезбедити да се оно обавља у складу са захтевима ISO/IEC 27001 и ISO/IEC 27018 стандарда. Уништавање мора бити извршено на начин који осигурава неповратност података, што подразумева примену сигурних метода као што су вишефазно преписивање података или физичко уништавање медија. Циљ је да се осигура да никакви остаци података не могу бити искоришћени након завршетка процеса уништавања.

Препорука је да клијенту буде омогућен повратак података пре него што дође до њиховог уништења. У складу са регулативама GDPR и стандардом ISO/IEC 27018, клијент има право да добије своје податке у договореном формату пре њиховог уклањања. Пружаоци услуга морају осигурати да се процес повраћаја података одвија безбедно, у оквиру договореног временског оквира, и потврдити да након повраћаја не постоје резервне копије које нису предвиђене уговором.

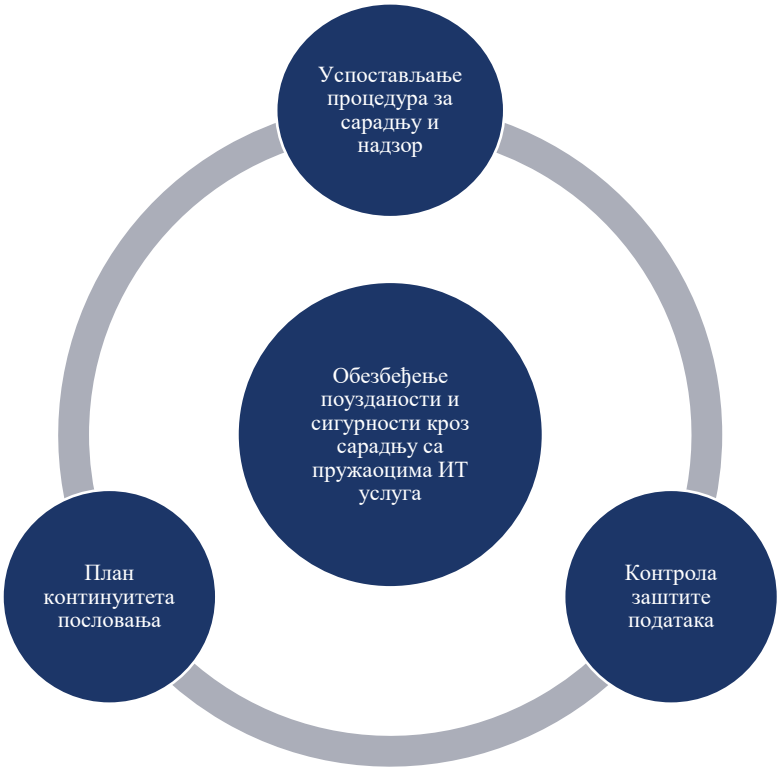
Важан аспект овог процеса је и документовање свих активности у вези са уништавањем података. Према захтевима ISO/IEC 27001 и ISO/IEC 27018, потребно је водити евиденцију о врсти и количини уништених података, примењеним методама уништавања и потврдама да су сви подаци неповратно уништени. Ова евиденција служи као доказ да је процес уништавања обављен у складу са законским и уговорним обавезама.

Поред тога, неопходно је успоставити механизме надзора и ревизије поступака архивирања и уништавања података, у складу са ISO/IEC 20000 стандардом. Оператори ИКТ система треба да именују одговорна лица која ће надгледати ове активности и осигурати да се сви аспекти архивирања и уништавања обављају у складу са уговореним условима и стандардима информационе безбедности. Редовне ревизије су кључне за обезбеђивање усклађености процеса са прописаним процедурама.

На крају, сви ови аспекти морају бити усклађени са законским и уговорним обавезама које регулишу чување и уништавање података. Уговори са пружаоцима услуга треба да садрже одредбе које обезбеђују да се подаци уништавају у складу са захтевима GDPR, али и националним законима о заштити података. Оператори ИКТ система су дужни да осигурају да је процес уништавања података транспарентан, документован и у потпуности у складу са важећим прописима.

ЗАКЉУЧАК 3: Механизам сарадње са пружаоцима услуга у Чачку, Краљеву и Крушевцу није у потпуности испунио неопходне циљеве, укључујући и поузданост података, због недостатка процедура за сарадњу, надзор и планирање континуитета пословања у случају раскида сарадње, што указује на потребу за системским унапређењем и јачањем контролних механизама

Циљ овог дела извештаја био је да утврди у којој мери је механизам сарадње са пружаоцима услуга био ефикасан у обезбеђивању заштите и поузданости података у ЈКП „Паркинг сервис“, Чачак, ЈКП „Чистоћа“, Краљево и ЈП „Пословни центар“, Крушевац. Испитивање је обухватило анализу постојећих правила и процедура за безбедност података у оквиру уговора са пружаоцима услуга, као и механизме којима су пружаоци услуга осигурали усвајање и спровођење неопходних услова за заштиту података. Додатно, анализиран је процес праћења реализације уговора, укључујући и примену плана континуитета пословања у случају раскида уговора, као и усклађеност сарадње са Законом о заштити података о личности.



Слика 4. Графички приказ обезбеђења поузданости и сигурности кроз сарадњу са пружаоцима ИТ услуга

На основу анализе законских и подзаконских аката, документације субјекта ревизије и одржаних интервјуа, донели смо закључак који темељимо на следећим налазима:

Налаз 3.1: ЈКП „Паркинг сервис“, Чачак, ЈКП „Чистоћа“, Краљево и ЈП „Пословни центар“, Крушевац нису успоставили процедуре за сарадњу и надзор над пружаоцима услуга

У складу са Законом о информационој безбедности и најбољим праксама, сва предузећа која су корисници услуга морају успоставити процедуре за сарадњу са пружаоцима услуга и надзор над извршењем уговорних обавеза. Ове процедуре треба да обезбеде контролу приступа, праћење активности и спровођење мера које осигуравају сигурност и поузданост информационих система.

ЈКП „Паркинг сервис“, Чачак, ЈКП „Чистоћа“, Краљево, и ЈП „Пословни центар“, Крушевац, нису успоставили адекватне процедуре за сарадњу и надзор над активностима пружалаца услуга. У Чачку је одговорност за надзор дефинисана Актом о безбедности ИКТ система, али недостају документи који потврђују редовно праћење активности. У Краљеву и Крушевцу, иако су надзорне функције дефинисане интерним актима, процедуре нису формализоване, нити постоји евиденција о спровођењу надзора.

Главни узроци оваквог стања су недовољна свест о значају надзора, недостатак техничких капацитета и формализованих процедура, као и ограничени кадровски ресурси.

Недостатак адекватних процедура за сарадњу и надзор значајно умањује способност ових предузећа да обезбеде сигурност и поузданост својих информационих система. Ово повећава ризик од компромитације података, непридржавања уговорних обавеза и потенцијалних прекида у континуитету пословања.

Успостављање процедура за сарадњу и надзор		
Јасно дефинисане процедуре за сарадњу са пружаоцима услуга.	Дефинисање одговорности и задатака у оквиру сарадње.	Континуиран надзор над пружаоцима услуга.

Анализа стања у ЈКП „Паркинг сервис“, Чачак, ЈКП „Чистоћа“, Краљево, и ЈП „Пословни центар“, Крушевац, показала је да ова предузећа нису успоставила адекватне процедуре за сарадњу са пружаоцима услуга и надзор над извршењем уговорних обавеза, што представља значајан ризик за сигурност и поузданост информационих система.

У ЈКП „Паркинг сервис“, Чачак, Актом о безбедности ИКТ система дефинисано је да пружаоци услуга могу приступити само подацима који су део софтвера који су они израдили или за које је уговором дефинисан приступ. Одговорност за надзор и контролу приступа додељена је Координатору ИКТ послова. Ипак, није документовало на који начин се овај надзор спроводи, нити постоје докази о редовном праћењу активности пружаоца услуга.

Слична ситуација је утврђена у ЈКП „Чистоћа“, Краљево, где је чланом 34 Акта о безбедности ИКТ система дефинисано да су надлежни субјекти одговорни за контролу приступа и надзор над извршењем уговорних обавеза. Међутим, као и у Чачку, недостају

процедуре које би уредиле сарадњу и надзор, као и документација која потврђује да се овај надзор обавља.

У ЈП „Пословни центар“, Крушевац, чланови 26 и 27 Акта о безбедности ИКТ система од посебног значаја предвиђају да се информације и средства доступна пружаоцима услуга регулишу уговором, док је Администратор ИТ система задужен за праћење пружања услуга и испуњење услова информационе безбедности. Ипак, ове процедуре нису успостављене, а радно место Администратор ИТ система није наведено у Правилнику о унутрашњој организацији и систематизацији послова. Поред тога, недостају докази о спровођењу надзора над активностима пружаоца услуга.

Овај недостатак процедура и недовољно спровођење надзора значајно умањује способност ових предузећа да обезбеде сигурност и поузданост својих информационих система, повећавајући ризик од угрожавања података и континуитета пословања.

ИТ послове из области информационе безбедности када је у питању сарадња са пружаоцима услуга је неопходно детаљно уредити у смислу примене правила и процедуре које се односе на безбедност података, праћења активности, ревизије и надзора у оквиру управљања информационом безбедношћу. На тај начин се 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 ко ради на којој активности (не у смислу имена него у смислу одређеног радног места), као и податке о изменама итд.

Уредбом о ближем уређењу мера заштите ИКТ система од посебног значаја предвиђена је заштита средстава оператора ИКТ система која су доступна пружаоцима услуга тако 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 (члан 26).

Налаз 3.2: ЈКП „Паркинг сервис“, Чачак, ЈКП „Чистоћа“, Краљево и ЈП „Пословни центар“, Крушевац нису успоставили механизам за контролу заштите података од стране пружалаца услуга

У складу са Законом о заштити података о личности и Законом о информационој безбедности, предузећа која користе услуге спољних пружалаца дужна су да успоставе механизме за контролу заштите података. Ове мере укључују дефинисање одговорности пружалаца услуга, ограничење

приступа осетљивим подацима, као и увођење процедура за праћење активности и осигурање усаглашености са законским прописима.

Анализа стања у ЈКП „Паркинг сервис“, Чачак, ЈКП „Чистоћа“, Краљево, и ЈП „Пословни центар“, Крушевац, показала је да ове организације нису успоставиле адекватне контроле заштите података. У Чачку, пружалац услуга има приступ базама података са осетљивим информацијама, али уговори не прецизирају мере заштите, нити је обезбеђен надзор над обрадом података. У Краљеву и Крушевцу слично, недостају механизми који би осигурали да се подаци користе искључиво у предвиђене сврхе. Крушевцу такође недостаје сагласност корисника пре обраде података, што представља ризик за угрожавање поверљивости и права грађана.

Главни узроци оваквог стања су недовољна техничка и кадровска опремљеност, као и недостатак свести о значају примене стандарда и процедура у области заштите података. Поред тога, уговори са пружаоцима услуга не садрже прецизне одредбе о управљању подацима.

Овакви недостаци повећавају ризик од неовлашћене обраде и злоупотребе података, чиме се угрожавају права корисника и сигурност информационих система. Неопходно је да предузећа успоставе јасне механизме заштите података кроз уговорне обавезе и примену процедура које гарантују усаглашеност са прописима и минимизирање ризика од компромитације података.

Контрола заштите података		
Усаглашеност са Законом о заштити података о личности.	Механизам за праћење и контролу приступа личним подацима.	Обезбеђивање да пружаоци услуга имају само неопходан приступ подацима и да су подаци адекватно заштићени.

Утврђено је да ЈКП „Паркинг сервис“, Чачак, ЈКП „Чистоћа“, Краљево, и ЈП „Пословни центар“, Крушевац, нису успоставили адекватне механизме за контролу заштите података који би обезбедили усклађеност са Законом о заштити података о личности и спречили неовлашћену обраду података од стране пружалаца услуга.

У Чачку, пружалац услуга „Synapse tech“ има приступ базама података које садрже личне податке грађана, укључујући име, презиме, адресу и контакт телефон. Међутим, уговором није прецизно дефинисано управљање и заштита тих података. Одредбе Закона нису у потпуности примењене, а недостаје контрола која би ограничила пружаоца у погледу обраде података изван договореног оквира.

У Краљеву, пружалац услуга „Ђоковић Софтвер“ такође има приступ подацима који су осетљиви и укључују информације о грађанима који добијају дневне или месечне карте. Међутим, није успостављен механизам надзора који би осигурао да се ови подаци користе искључиво у предвиђене сврхе. Поред тога, нема процедура за криптовање или брисање података након истека рока за њихову обраду.

У Крушевцу, пружалац услуга „EPSEE MS“ има широк приступ подацима о грађанима, али није обезбеђена сагласност корисника за обраду њихових личних података пре њиховог уноса у систем. Иако су током ревизије предузети кораци за

увођење сагласности и информисање клијената, приступ поверљивим подацима остаје недовољно контролисан.

Недостаци у контролама у сва три предузећа указују на критичну потребу за унапређењем механизама заштите података кроз прецизно дефинисање обавеза пружалаца услуга, увођење процедура за ограничење приступа подацима и примену мера као што су криптовање и редовно брисање података. Ови кораци би значајно смањили ризик од компромитације података и осигурали поштовање права грађана.

Механизам сарадње са пружаоцима ИТ услуга може да обухвати скуп политика, процедура, упутстава, докумената, али и активности које су усмерене на идентификацију циљева и послова за чије остварење, тј. обављање се користе информациони системи, израду специфичних захтева у смислу потреба за хардверским, софтверским и људским ресурсима, али и примене стандарда, начине на које се ангажују пружаоци услуга, стандардизацију уговора који се потписују са пружаоцима услуга, а који подразумевају и делове који се односе на информациону безбедност, начин на који се прате пружене услуге, осигурава законитост у раду, обезбеђује континуирана сарадња и комуникација, евидентирање будућих потреба, припрему и имплементацију нових захтева, одређивање лица која су задужена за сарадњу са пружаоцима услуга итд. ИТ послове из области информационе безбедности када је у питању сарадња са пружаоцима услуга је неопходно детаљно уредити у смислу примене правила и процедура које се односе на безбедност података, праћења активности, ревизије и надзора у оквиру управљања информационом безбедношћу. Када су у питању информациони системи у јавним предузећима за наплату услуга паркинга, предузећа су руковаоци подацима, док су у случају ангажовања пружаоца услуга, они обрађивачи. Законом о заштити података о личности, прописане су обавезе и однос руковаоца и обрађивача, нарочито када су у питању безбедносне мере. 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 мера заштите, може се закључити да ли су све неопходне мере прописане и примењене. Законом о информационој безбедности уређују се мере заштите ИКТ система од посебног значаја.

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.

Налаз 3.3: ЈКП „Чистоћа“, Краљево, и ЈП „Пословни центар“, Крушевац, немају успостављен план континуитета пословања у случају раскида сарадње са пружаоцем услуга, док је у ЈКП „Паркинг сервис“, Чачак, ова област делимично уређена, али без интерних процедура и мера за миграцију података

Уредбом о ближем уређењу мера заштите ИКТ система од посебног значаја, прописано је да оператор ИКТ система треба да предвиди мере којима се обезбеђује обављање послова у ванредним околностима, укључујући процедуре за опоравак система и континуитет рада у случају прекида сарадње са пружаоцем услуга. Ове мере подразумевају јасно дефинисане планове, одговорности и механизме заштите података, укључујући миграцију података и одржавање доступности критичних функционалности система. План континуитета пословања треба да обухвати и сценарије у којима више не постоји сарадња са досадашњим пружаоцем услуга, што је нарочито важно за системе који се ослањају на екстерну инфраструктуру.

У ЈКП „Чистоћа“, Краљево, и ЈП „Пословни центар“, Крушевац, нису успостављени планови континуитета пословања у случају раскида сарадње са пружаоцима услуга, нити су уговорима предвиђене активности које би обезбедиле наставак функционисања кључних компоненти система. У случају прекида уговора, било би онемогућено праћење расположивости паркинг места, продаја карата и контрола услуга, што би негативно утицало на кориснике и приходе. Такође, уговори не садрже одредбе о миграцији података, што повећава ризик од њихове недоступности или губитка. У ЈКП „Паркинг сервис“, Чачак, уговором са пружаоцем услуга предвиђен је наставак функционисања одређених функционалности и у случају раскида сарадње, али предузеће није успоставило интерне планове нити дефинисало обавезе у погледу миграције података, што представља потенцијалну слабост.

У недостатку формализованих интерних планова и уговорне заштите у случају прекида сарадње, ова предузећа се ослањају искључиво на текуће уговоре без предвиђања алтернативних решења и механизама опоравка. Недостају прецизне процедуре које би дефинисале шта се дешава након прекида сарадње, ко обезбеђује техничку инфраструктуру, где се чувају подаци и како се

успоставља нови начин рада у периоду до успостављања новог система. Одсуство ових механизама смањује отпорност система на ванредне околности и повећава зависност од једног пружаоца услуга.

Овакво стање значајно повећава ризик од оперативних прекида, губитка података и умањења квалитета услуге за крајње кориснике. Уколико не постоје јасно дефинисани уговорни и интерни механизми за превазилажење прекида сарадње, предузећа су изложена ризику да неће бити у могућности да одмах наставе пружање услуга, што може довести до финансијских губитака, оштећења репутације и смањења поузданости система.

План континуитета пословања		
Развој плана континуитета пословања у случају раскида сарадње са пружаоцем услуга.	Обавезе пружаоца услуга у случају раскида сарадње.	Миграција података и осигурање континуитета услуга.

ЈКП „Чистоћа“, Краљево и ЈП „Пословни центар“, Крушевац нису успоставили план континуитета пословања у случају раскида сарадње са пружаоцем услуга. Уговори са пружаоцима услуга не садрже одредбе које би обезбедиле несметано функционисање кључних функционалности у случају прекида сарадње. Уколико би дошло до раскида или непродужења уговора, ометено би било праћење расположивости паркинг места, продаја паркинг карата и контрола коришћења услуга, што би имало директан утицај на грађане и приходе предузећа. Уговори такође не предвиђају миграцију података, што повећава ризик од губитка или недоступности података у новим системима.

У ЈКП „Паркинг сервис“, Чачак, иако формални план континуитета пословања није успостављен, уговор са пружаоцем услуга садржи одредбе које омогућавају наставак функционисања кључних компоненти система у случају раскида сарадње. Предвиђено је да би и у том случају било могуће пратити расположивост паркинг места, обављати продају карата и вршити контролу коришћења паркинг услуга. Ипак, одсуство интерног плана и механизама за миграцију података остаје као потенцијални ризик.

Недостатак формалних планова и недовољна уговорна заштита у два од три предузећа, као и делимично ослањање на пружаоца услуга у Чачку, указују на потребу за јасно дефинисаним процедурама и обавезама у случају прекида сарадње. Успостављање планова континуитета и предвиђање миграције података кључни су за очување стабилности система и заштиту интереса крајњих корисника.

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.

Међутим, план континуитета пословања се може посматрати као „дводелни“ план – план континуитета пословања у случају ванредних околности у периоду када

постоји сарадња са пружаоцем услуга, где је чест случај да се мере и активности дефинишу уговорима и/или техничким спецификацијама и да их у тим ситуацијама спроводи пружалац услуге, и као план континуитета пословања у случају раскида сарадње са пружаоцима услуга, дакле када више нема сарадње са пружаоцем услуга.

Раскид сарадње може наступити у периоду трајања уговора, или може наступити услед непродужавања уговора. У том случају, план континуитета пословања обухвата мере које треба предвидети у уговорима (као што је то на пример миграција података, власништво над кодом итд), и мере које се предузимају након раскида (хардвер, софтвер, просторије, интернет, итд), или успостављање другачијег начина рада, на пример прелазак на продају наплатних карата, другачији начин евидентирања/мерења кретања возила.

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.

Напретком ИТ, нивоа знања у тој области расте код све већег броја грађана, па и оних недобронамерних (хакери), повећава се ризик и могућност да поред проблема изазваних кваровима, или незнањем, информациони системи постану и предмет хакерских, сајбер напада.

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

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

ЗАКЉУЧАК 4: Апликативне контроле обезбеђују основну контролу наплате и пружених услуга, док је у Београду и Новом Саду постигнут напредак, али у Чачку, Краљеву и Крушевцу недостају механизми за потпуну транспарентност и ефикасност

Циљ овог дела извештаја био је да оцени у којој мери успостављене апликативне контроле обезбеђују ефикасну контролу наплате и тачност пружених услуга у предузећима за контролу и наплату услуга паркирања. Испитивање је обухватило проверу постојања и примене правила и процедура за управљање апликацијама које се користе за наплату и контролу услуга, као и механизме који обезбеђују валидацију улазних података и откривање грешака. Посебан акценат био је на праћењу тачности података у систему, укључујући и процену могућности система за генерисање извештаја који су свеобухватни и редовни. Анализа је обухватила процесе уноса, обраде и дистрибуције резултата, као и мере за евидентирање, комуникацију и чување података.

На основу тестирања које смо спровели у самом софтверу, донели смо закључак који темељимо на следећим налазима:

Налаз 4.1: ЈКП „Паркинг сервис“, Београд и Нови Сад су унапредили апликативне контроле и ограничили приступ осетљивим подацима, док Чачак, Краљево и Крушевац нису успоставили адекватне процедуре и механизме за управљање корисничким налозима и пословним процесима у апликацијама за наплату и контролу паркинга

Законом о информационој безбедности и Уредбом о ближем уређењу мера заштите ИКТ система од посебног значаја прописано је да оператор ИКТ система мора успоставити механизме за управљање приступом, деактивацију корисничких налога и контролу над активностима унутар апликација. Ови механизми треба да обезбеде да само овлашћена лица имају приступ осетљивим подацима и да се све активности евидентирају, без угрожавања интегритета података.

У ЈКП „Паркинг сервис“, Београд, и ЈКП „Паркинг сервис“, Нови Сад, иницијално су постојали пропусти у апликативним контролама, као што је неконтролисано преименовање налога и приступ осетљивим подацима од стране неовлашћених запослених. Током ревизије су ови пропусти отклоњени кроз увођење механизама за ограничење приступа, евидентирање активности и спречавање измена налога без одобрења. Насупрот томе, у Чачку, Краљеву и Крушевцу апликативне контроле нису адекватно развијене. У Чачку уопште не постоје процедуре за управљање налозима; у Краљеву, иако постоје интерни акти, они нису примењени у пракси; у Крушевцу је целокупна контрола препуштена пружаоцу услуга, без интерног надзора.

У Чачку запослени имају неограничен приступ базама података, а механизам деактивације налога није успостављен, што оставља простор за злоупотребу. У Краљеву деактивација није аутоматизована, а уговори са пружаоцем услуга не предвиђају мере за заштиту података у складу са безбедносним стандардима. У Крушевцу не постоји увид у поступке које пружалац примењује, па није могуће ни утврдити да ли се уопште примењују механизми

контроле приступа и деактивације налога. У свим овим случајевима постоји ризик од компромитације података и губитка интегритета система.

Недостатак контроле приступа, непостојање механизама за деактивацију налога и могућност неконтролисаног приступа осетљивим подацима представљају озбиљне слабости које могу довести до неовлашћене обраде података, губитка историје активности, правне одговорности и нарушавања поверења грађана. Унапређење апликативних контрола и увођење формализованих процедура је неопходно ради обезбеђења поузданости информационог система и заштите личних података корисника.

Апликативне контроле и приступ осетљивим подацима у јавним комуналним предузећима за наплату паркинга показују значајне разлике у развијености и примени. Утврђено је да, иако су предузете мере за унапређење у Београду и Новом Саду, постоје изазови који угрожавају интегритет података и поузданост информационих система.

Информациони систем Scan Car у Београду користи се за контролу и наплату паркирања, али иницијално није успостављен комплетан механизам апликативне контроле. Током ревизије је утврђено да недостају контроле приликом преименовања корисничких налога, што је доводило до губитка историје уноса података. Запослени на позицијама Благајника и Call Centar имали су приступ личним подацима корисника система, укључујући име, адресу и контакт телефон, што није било неопходно за њихове радне обавезе. Као резултат ревизије, предузеће је предузело следеће мере: онемогућен је приступ осетљивим подацима запосленима који за то нису овлашћени, уведена је контрола приступа која спречава извоз података из система, спречена је измена корисничких налога без одговарајућег праћења и успостављен је механизам деактивације налога који евидентира историју уноса.

Нови Сад користи два софтвера, FRIP и SWAT, за наплату и контролу паркирања. Утврђено је да су запослени на позицијама Благајника и Call Centar имали приступ осетљивим подацима грађана, укључујући регистарске бројеве возила и историју плаћања, што није било у складу са њиховим радним задацима. Поред тога, недостатак контроле приликом преименовања корисничких налога представљао је ризик за интегритет података. У току ревизије, предузете су следеће мере: укинут је приступ осетљивим подацима за запослене којима то није неопходно, ограничене су функције извоза података како би се спречила њихова неовлашћена обрада, уведен је механизам који спречава измену корисничких налога без одговарајућег одобрења и започет је развој додатних безбедносних функција за бољу контролу приступа и праћење активности корисника.

У Чачку, механизми апликативне контроле уопште нису успостављени. Уговор са пружаоцем услуга предвиђа коришћење софтвера „Synapse“, али предузеће није успоставило процедуре за управљање корисничким налозима или праћење активности. Непостојање механизма за деактивацију налога омогућава потенцијалну злоупотребу приступа од стране бивших корисника система. Такође, запослени који обављају административне послове имају неограничен приступ базама података, што представља озбиљан ризик за заштиту осетљивих података.

У Краљеву, апликативне контроле су делимично уређене интерним актима, али механизми за праћење и ограничење приступа нису применљиви у пракси. Деактивација корисничких налога није аутоматизована, што омогућава неовлашћени приступ подацима након престанка коришћења система. Такође, уговор са пружаоцем услуга

„Ђоковић Софтвер“ не предвиђа експлицитне обавезе за заштиту података у складу са стандардима информационе безбедности.

У Крушевцу, управљање апликативним контролама је у потпуности препуштено пружаоцу услуга „EPSEE MS“. Предузеће нема увиде у процедуре које пружалац примењује, нити су кориснички налози подложни интерном надзору. Одсуство механизама контроле омогућава потенцијалну компромитацију података и губитак интегритета система.

Унапређење апликативних контрола у Београду и Новом Саду, као и развој одговарајућих механизама у осталим предузећима, неопходно је за обезбеђивање интегритета података, сигурности система и поверења корисника у услуге наплате паркинга.

Управљање корисничким налозима у апликацији за наплату и контролу паркинг места требало би да обухвати успостављање јасних и дефинисаних процедура које регулишу сваки аспект управљања корисничким правима, приступом и деактивацијом налога. Процедуре би требало да укључе механизме за безбедно деактивирање корисничких налога у случају престанка радног односа или промене у улогама запослених, без угрожавања интегритета података или континуитета пословања.

Свака корисничка улога у систему би требало да буде прецизно дефинисана, укључујући јасне границе приступа одређеним деловима апликације. Поред тога, механизам деактивације корисника требало би да обезбеди да кориснички налози буду онемогућени чим корисник више не буде имао потребу за приступом, без ризика од даљег приступа или губитка података.

Корисничке активности треба да буду евидентиране у сваком тренутку, што значи да би се уместо трајног брисања или преименовања налога, кориснички налози требали бити архивирани и означени као деактивирани. На тај начин би се сачувала историја активности корисника, а систем би задржао интегритет података и омогућио праћење уноса и измена у апликацији.

Налаз 4.2: Апликативни софтвер за продају карата у свих пет предузећа обезбеђује функционалност и поуздано праћење продаје

У свих пет предузећа субјеката ревизије, апликативни софтвер за продају карата је функционалан и подржава различите методе наплате, укључујући месечне карте, сатне карте путем СМС порука и греб карте. Системи обезбеђују евиденцију пазара, преглед броја продатих карата и извештавање о продаји по врстама карата.

Иако постоје одређене разлике у примени, сва предузећа користе софтвер који омогућава поуздано праћење продаје и управљање подацима. У Краљеву се истиче додатна пракса усклађивања података са мобилним операторима, чиме се додатно осигурава тачност извештаја.

Сви субјекти ревизије успешно примењују системе за продају карата, што указује на њихову стабилност и усклађеност са очекиваним функционалностима.

Апликативне контроле које се користе за продају карата у паркинг сервисима треба да омогуће прецизну и ажурну евиденцију свих трансакција у вези са продајом паркинг карата. Ове контроле морају бити дизајниране тако да обухвате све врсте карата – месечне, сатне и греб картице – како би се осигурало да се сви подаци о продаји тачно бележе и буду доступни за извештавање. Систем мора омогућити праћење броја

продатих карата и дневних пазара у реалном времену, чиме се обезбеђује транспарентност и тачност у управљању финансијским подацима.

Апликативни софтвер треба да буде интегрисан са свим продајним каналима, било да се ради о продаји карата у објектима предузећа, путем СМС порука или кроз друге методе, као што су трафике или греб карте. Софтвер би требао бити дизајниран тако да омогућава свеобухватну анализу и преглед по врстама карата, чиме се обезбеђује ефикасно управљање и контрола продајних активности.

Поред тога, неопходно је редовно усклађивање података између система за евиденцију продаје карата и података добијених од мобилних оператера или других пружалаца услуга који учествују у процесу продаје. Ово усклађивање је кључно за осигурање да сви подаци буду тачни и да нема разлике између извештаја мобилних оператера и унутрашњих података предузећа.

Ефикасне апликативне контроле такође треба да омогуће генерисање извештаја који се користе за надзор над радом запослених, као и за финансијско извештавање, чиме се осигурава потпуна контрола над продајом и усклађеност са прописаним стандардима и интерним процедурама.

Налаз 4.3: ЈКП „Паркинг сервис“, Београд и Нови Сад редовно ажурирају податке о паркинг зонама и користе мобилне апликације за информисање корисника, док остала предузећа ажурирају податке, али нису омогућила коришћење отворених података и интеграцију са мобилним апликацијама

У складу са Законом о информационој безбедности и најбољим праксама у управљању отвореним подацима, предузећа која пружају услуге наплате паркинга треба да осигурају редовно ажурирање и доступност података о расположивим паркинг местима, паркинг зонама и ценама у реалном времену, као и интеграцију са отвореним платформама ради побољшања приступачности информација.

ЈКП „Паркинг сервис“, Београд, обезбеђује ажуриране информације о паркинг местима и зонама путем мобилне апликације и инфо-табли, омогућавајући корисницима приступ подацима у реалном времену. Међутим, интеграција са отвореним платформама, попут Google Maps, још увек није у потпуности реализована.

ЈКП „Паркинг сервис“, Нови Сад, такође пружа податке о паркинг зонама и ценама преко сајта и апликације, али приступ информацијама о доступним местима је ограничен на инфо-табле у јавним гаражама. Развој функционалности за праћење у реалном времену је у току, што показује напредак у унапређењу овог аспекта.

ЈКП „Паркинг сервис“, Чачак, користи софтвер са модулом „Мапа“ за праћење доступности места, али он није био функционалан у време ревизије. Ово ограничава могућност корисника да добију ажуриране информације, што негативно утиче на транспарентност и корисничко искуство.

ЈКП „Чистоћа“, Краљево, користи софтвер „Ђоковић Софтвер“ за праћење расположивости паркинг места, али приступ тим подацима је ограничен на запослене. Подаци нису доступни у реалном времену, а недостаје интеграција

са платформама трећих страна, што сужава видљивост и доступност информација.

ЈП „Пословни центар“, Крушевац, користи инфо-табле и камере за праћење слободних места, али подаци нису интегрисани са мобилним апликацијама или отвореним платформама. Ово значајно ограничава приступачност података широј јавности.

Недостатак униформности у ажурирању и доступности података, као и ограничена интеграција са отвореним платформама, указују на потребу за даљим унапређењем апликативних контрола. Ове мере су неопходне како би се осигурала транспарентност, ефикасност управљања паркинг ресурсима и побољшало корисничко искуство.

Анализа апликативних контрола за податке о доступним паркинг местима и коришћење отворених података у пет предузећа субјеката ревизије показала је различит ниво развоја и примене, са значајним просторима за унапређење, посебно у области транспарентности и доступности података корисницима.

ЈКП „Паркинг сервис“, Београд, представља пример добро развијеног система за управљање паркинг ресурсима. Информације о паркинг зонама, ценама и могућностима плаћања редовно се ажурирају и доступне су на званичном сајту и мобилној апликацији. Корисници могу у реалном времену приступити информацијама о доступним местима, укључујући и плаћање путем QR кода. Инфо-табле су постављене на улазима у гараже и пружају ажуриране информације о броју слободних места. Додатно, систем је интегрисан са функцијама обавештавања путем мобилне апликације, што значајно побољшава корисничко искуство.

ЈКП „Паркинг сервис“, Нови Сад, такође има функционалан систем за управљање паркинг просторима, али са одређеним ограничењима. Сајт и мобилна апликација омогућавају преглед информација о паркинг зонама и ценама, али подаци о доступности места су тренутно доступни само путем инфо-табли у јавним гаражама. Функционалност праћења доступних места у реалном времену је у развоју. Поред тога, постоји ограничена интеграција са стандардним платформама за навигацију, што умањује видљивост података широј публици.

ЈКП „Паркинг сервис“, Чачак, користи софтвер који укључује модул „Мапа“ за праћење доступности места, али овај модул није био оперативан у време ревизије. Сајт пружа основне информације о зонама, ценама и плаћању, али недостају функције које би омогућиле праћење у реалном времену или интеграцију са мобилним апликацијама. Овај недостатак ограничава ефикасност управљања паркинг ресурсима и приступачност информација корисницима.

ЈКП „Чистоћа“, Краљево, користи софтвер „Ђоковић Софтвер“ који укључује функцију праћења доступности паркинг места кроз модул „Мапа“. Међутим, ове информације су ограничене само на запослене, а јавности није омогућен приступ подацима у реалном времену. Сајт редовно ажурира информације о зонама и ценама, али је приступ отвореним подацима ограничен, што умањује транспарентност и корисничко искуство.

ЈП „Пословни центар“, Крушевац, користи инфо-табле и камере за праћење слободних места у гаражама. Основне информације о зонама и ценама доступне су на сајту, али недостаје интеграција са мобилним апликацијама или стандардним платформама као што је Google Maps. Овај недостатак значајно сужава доступност

података корисницима, посебно туристима и онима који се ослањају на дигиталне платформе за планирање.

Иако сва предузећа показују основни ниво функционалности у управљању подацима о доступним местима, недостаци у приступу подацима у реалном времену, ограничена интеграција са отвореним платформама и недостатак унифицираних пракси представљају значајне области за унапређење. Боља интеграција са мобилним апликацијама, редовно ажурирање података и ширење приступа отвореним подацима допринели би већој транспарентности, ефикаснијем управљању паркинг просторима и бољем корисничком искуству.

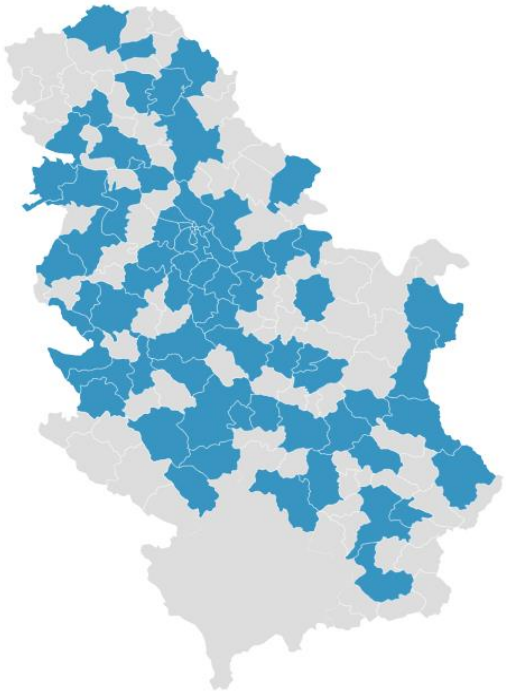
Јавна комунална предузећа треба да настоје да редовно ажурирају податке о паркинг зонама, ценама, доступности паркинг места и могућностима плаћања у реалном времену. Пожељно је да ти подаци буду доступни не само путем званичних веб сајтова, већ и у формату отворених података који омогућавају лакшу интеграцију у мобилне апликације трећих страна. Такав приступ би омогућио корисницима бржи и ефикаснији приступ релевантним информацијама, што би олакшало планирање коришћења паркинг услуга и побољшало укупно искуство корисника.

Пожељно је да подаци буду у машински читљивом формату, што би омогућило њихову лакшу употребу од стране физичких и правних лица, без додатних трошкова. Уз примену отворених података, предузећа би могла значајно побољшати транспарентност и приступачност својих услуга, омогућавајући корисницима да информације добијају преко мобилних апликација и других дигиталних платформи, што би унапредило квалитет услуга и комуникацију са грађанима.

V Прилози

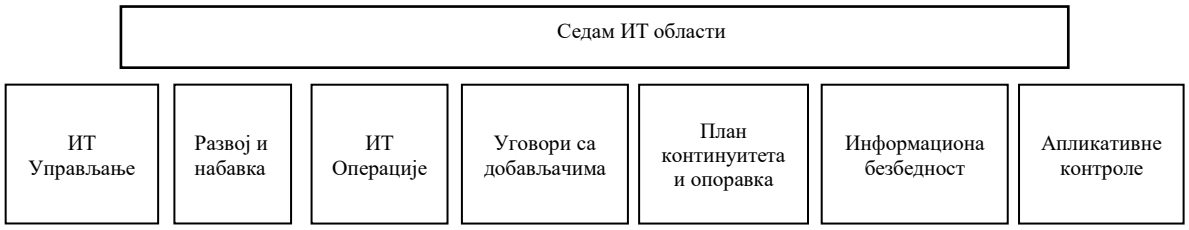
Прилог 1. Методологија у поступку рада

У току предстудије послали смо упитник[17] свим јединицама локалне самоуправе које на својој територији имају јавно предузеће које се бави наплатом услуга паркирања.



Слика 5. 61 ЈЛС које имају информациони систем преког које врше паркинг сервис услуге

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



Слика 6. ИТ области

На основу прикупљених података ревизорски тим је одрадио процену ризика. Одабране су следеће три области: Информациона безбедност, Успостављање ефективног механизма сарадње са пружаоцима услуга и Апликативна контрола. Не постоји идеално решење, али је циљ ове ревизије да се дође до бољег решења у овој области него што је то сада.

[17] 24-039-0075 упитник

У циљу одговора на ревизорска питања, а имајући у виду законодавни и институционални оквир у периоду 2021 – 2023. године, за субјекте ревизије изабрани су[18]:

- ЈКП „Паркинг сервис“, Београд,
- ЈКП „Паркинг сервис“, Нови Сад,
- ЈКП „Паркинг сервис“, Чачак,
- ЈКП „Чистоћа“, Краљево и
- ЈП „Пословни центар“, Крушевац.

Да бисмо одговорили на ревизорска питања, анализирали смо законодавни и институционални оквир, и спровели следећа испитивања:

За прво ревизијско питање:

- 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 информационо-комуникационих система од посебног значаја;
- Анализа Правилника о унутрашњем уређењу и систематизацији радних места, посебно 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;
- Анализа шта су примарне контроле физичке безбедности организације субјекта ревизије. Провера да ли одговарају најновијој анализи ризика ако постоји;
- 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 мапирања 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;

[18] 24-039-0016 Избор субјеката на основу бодовања

- 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 ради оцене ажурности;
- Провера процедуралних мера које је предузеће предузело да би се ускладила са захтевима поверљивости;
- Провера да ли уговорни услови и обавезе дефинишу безбедносна ограничења и обавезе које контролишу како ће извођачи користити имовину организације и приступати информационим системима и услугама;
- Провера да ли су извођачи извршили повреде безбедности информација. Провера активности руководства у погледу таквих кршења;
- 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 да је доступна права верзија резервне копије;
- Преглед докумената да би се проценила адекватност локације резервне копије и начина транспорта датотека, итд., резервне копије на локацију резервне копије;
- Провера да је безбедност, како логична тако и физичка, адекватна за локацију резервне копије;
- Провера да се резервне копије датотека могу користити за опоравак;
- Преглед докумената да би се проценило да су израђене детаље процедуре за опоравак и да садрже параметре за поновно постављање система, инсталационе закрпе, успостављајући поставку конфигурације, доступност системске документације и оперативних процедура, реинсталацију апликативних и системских софтвера, доступност најновијих резервних копија, тестирање система;
- Преглед докумената да би се проценило да је ИТ кадар обучен на пољу процедура за прављење резервних копија и опоравак;

- Преглед докумената да би се проценило да ли су све релевантне ставке обухваћене тестирањем;
- Преглед докумената да би се проценило да ли се реализују тестирања у одређеним временским интервалима, и благовремено;
- Преглед докумената да би се проценило да су препоруке након тестирања адекватно праћене и да су план за континуитет пословања и план за опоравак након катастрофе адекватно ажурирани;
- Провера да ли организација контролише да ли су подаци, апликативни софтвер и хардвер били подвргнути променама током поступка прављења резервне копије или током опоравка након катастрофе;
- Провера да ли се организација постарала да је континуитет пословања садржан у споразуму о пружању услуге;
- Анализа стратегије за управљање ризицима.

За друго ревизијско питање:

- Анализирали смо како је пружалац услуга уредио приступ корисницима информационим системима и серверима, као и другим потребним ресурсима, те да ли се ови приступи евидентирају на одговарајући начин;
- Проверавали смо да ли пружалац услуга прати извршење обавеза корисника услуга у складу са нивоима услуга дефинисаним уговором;
- Прегледали смо извештаје о безбедносним инцидентима и пратили документацију како бисмо утврдили које активности пружалац услуга предузима када корисници крше безбедносна правила и процедуре;
- Проверавали смо процедуре пружаоца услуга које се односе на питања поверљивости података;
- Испитивали смо уговорне услове и обавезе којима пружалац услуга регулише безбедносна ограничења и контролу приступа информационом систему и ресурсима које користе корисници услуга;
- Проверавали смо да ли је дошло до безбедносних инцидената са стране корисника, као и како је руководство пружаоца услуга поступало у тим случајевима;
- Анализирали смо мере физичке заштите система које је пружалац услуга успоставио и проверили да ли одговарају најновијим анализама ризика;
- Прегледали смо локацијске и физичке мере предострожности за кључне елементе ИТ инфраструктуре, као што су системи за напајање, аларми и системи заштите од пожара;
- Испитивали смо учесталост прегледа приступа и привилегија које запослени код корисника услуга имају у вези са системом;
- Проверавали смо да ли постоје документоване процедуре за обележавање осетљивих података у оквиру апликација и контролу њиховог слања;
- Добијена је документација и процењен је приступ пружаоца услуга у имплементацији система и пружању услуга;

- Испитивали смо да ли постоје могућности за добијање додатних услуга из постојећег система са минималним трошковима, пре свега у вези са услугама према грађанима;
- Анализирали смо да ли постоје капацитети унутар пружаоца услуга да обезбеде континуитет пружања услуга у случају прекида сарадње са корисницима;
- Проверавали смо да ли је однос између пружаоца услуга и корисника усклађен са Законом о заштити података о личности.

За треће ревизијско питање:

- Анализа Матрице приступа са улогама и привилегијама како би се утврдило да ли су корисници добили улоге и права у складу са пословима и одговорностима које имају;
- Анализа Log фајлова како би се утврдило да ли су само овлашћена лица приступала систему, и у које сврхе, као и у ком временском тренутку;
- Да ли се систему приступало у „необично“ време, ко је и зашто приступао;
- Анализа Извештаја о тестирању апликација: када се тестирала апликација, како, итд.
- Тестирање евидентирања уплате у реалном времену;
- Документација која се односи на ИТ правила и процедуре, које се односе на употребу апликације, процес развоја, техничким захтевима приликом набавке итд;
- Организациона ИТ структура и опис послова;
- Извештаји о спроведеним обукама - да ли су обављене обуке, када, шта су обухватиле итд.;
- Обављање интервјуа са одговорним лицима и једним бројем корисника система како би се проверило да ли су упознати са свим доступним функционалностима, да ли су имали предлоге за измене и допуне програма итд;
- Документација субјекта ревизије - анализа шта садржи и у ком обиму, колико је детаљна;
- Уговори са пружаоцима услуга и техничка спецификација;
- Извештаји са продајних места - структура извештаја, динамика достављања, провера тачности и свеобухватности;
- Извештаји који садрже финансијске податке везане за финансирање - провера тачности, свеобухватности.

Прилог 2. Информациони систем ЈКП „Паркинг сервис“, Београд

ЈКП „Паркинг сервис“, Београд је само развило софтвер који омогућава ефикасно управљање процесима паркирања и контроле, пружајући подршку за све кључне активности у систему наплате и надзора паркинг места. Овај софтвер омогућава:

- обраду информација из делокруга рада контроле паркирања;
- обраду трансакција по плаћеним картама за паркирање по започињаном сату;
- преглед претплатних карата;
- администрацију система;
- ГИС подлогу – укључивање и искључивање сваког паркинг места из система наплате и контроле паркирања на целом зонском подручју града Београда;
- пријем и обраду дојава са возила Scan Car за издавање дневних карата и проверу плаћања паркирања.

У апликацији је омогућено праћење помоћу возила Scan Car са специјалном надоградњом, која су активна и снимају улице у реалном времену.

Систем за администрацију пословних процеса контроле паркирања омогућава обраду информација насталих плаћањем услуга паркирања, слање и обраду дојава са возила Scan Car, слање и обраду дојава од стране контролора паркинга, администрацију пословних процеса, администрацију ГИС подлоге и праћење кретања возила Scan Car и контролора у реалном времену.

Опажање паркираних возила и њихових регистарских таблица на јавним паркиралиштима врши се путем мобилног видео надзора који се састоји од рачунара са камерама постављеним на возило Scan Car. Камере континуирано скенирају и препознају регистарске таблице паркираних, заустављених или напуштених возила, анализирају њихов садржај и одређују регистарску ознаку, зону услуге, ГПС локацију и време опажања. Прикупљени подаци се аутоматски шаљу СМС центру на проверу преко 4Г мобилне мреже.

Возило са специјалном надоградњом, у које је уграђен наменски софтвер и хардвер, односно, систем за аутоматско препознавање регистарских таблица путем мобилног видео надзора у зонском делу града Београда, врши снимање возила и регистарских таблица на јавним паркиралиштима користећи систем Scan Car. Притом се прикупљају и бележе подаци о возилима.

За потребе рада система Scan Car израђена је геодетска подлога, којом је успостављена просторна основа за приказ мреже улица, паркинг места, знакова и других елемената. Геодетска подлога је израђена у Државном координатном систему, у складу са Правилником Републичког геодетског завода.

Систем Scan Car, у зависности од своје позиције у односу на електронску подлогу уцртаних паркинг места и других елемената, аутоматски разврстава и одваја прикупљене податке о регистарским таблицама возила са фотографијама у две категорије:

- Фотографије непрописно паркираних возила са одговарајућим подацима ради утврђивања прекршаја или повреде комуналног реда;
- Фотографије возила са одговарајућим подацима у сврху помоћи ЈКП „Паркинг сервис“ у контроли и наплати комуналних услуга.

Сви подаци у Scan Car возилима, софтверске компоненте, фотографије и резултати обраде фотографија су физички криптовани.

У случају Система за аутоматско препознавање регистарских таблица путем мобилног видео надзора, идентификовани су следећи програмски и хардверски подсистеми:

Програмски подсистеми:

- PS GIS, Просторна база података Београда која је од интереса за рад ЈКП „Паркинг сервис“;
- PS LPR, Програмски подсистем за аутоматско препознавање регистарских таблица паркираних возила на основу слика високе резолуције;
- PS GPS, Програмски систем за одређивање географских координата возила са видео камерама;
- PS COMM, Програмски систем заштићене размене података између рачунара у возилу и сервера у просторијама ЈКП „Паркинг сервис“ коришћењем сервиса за пренос података мобилног оператера;
- PS ADMIN, Програмски систем за ауторизацију корисника и заштиту података;
- PS SCANCAR, Главни програм рачунара у возилу који управља радом Scan Car система и интегрише све програмске подсистеме у функционалну целину. Радни предмети су фотографије и поруке које шаље СМС центру, слично као што то раде ПДА уређаји контролора.

Пословни процес у поступку контроле и наплате паркирања

Овај процес обухвата снимање ситуације на терену путем мобилног видео надзора на возилима кроз систем ScanCar, креирање дојава и њихово слање ка диспечерском центру контроле паркирања.

Нормалан ток – Возило има валидну електронску паркинг карту

1. Камере на специјалном возилу са надоградњом очитавају регистарске ознаке возила на терену и кроз систем ScanCar генеришу фотографију.
2. На основу обраде података у систему ScanCar, врши се аутоматско разврставање и раздвајање података о уоченим возилима, које укључује најмање две фотографије, регистарски број возила, време очитавања, назив улице, кућни број и графички приказ возила на дигиталној мапи паркинг места.
3. Ови подаци се шаљу у Back Office апликацију у улогу СМС центра.
4. Back Office апликација проверава да ли за паркирано возило постоји евиденција о плаћеном паркингу.
5. Ако возило има валидну електронску паркинг карту, процес се завршава.

Нормалан ток – Возило нема валидну електронску паркинг карту

1. Ако возило нема плаћен паркинг према евиденцији у СМС центру и Back Office апликацији, апликација бележи податке о регистарским ознакама, времену очитавања и геолокацији возила са фотографијом регистарских ознака.
2. За возила која немају плаћен паркинг, Back Office апликација шаље предлог контролору за израду електронске дневне паркинг карте (еДПК). Контролори паркирања проверавају тачност података и ако су валидни, наставља се процес.

3. У случају погрешно очитаних регистарских ознака, контролор може извршити измену и поново проверити постојање плаћеног паркинга. Ако плаћање није извршено, процес се наставља.
4. Контролор након прегледа података верификује предлог за израду еДПК.
5. Back Office апликација генерише електронски налог за плаћање еДПК са свим релевантним подацима о возилу, времену паркирања и цени карте.
6. Ови подаци се шаљу на сајт предузећа и у финансијски информациони систем (ФИС), а корисницима се по потреби шаљу и СМС поруке или нотификације путем мобилне апликације.

Систем за контролу и наплату паркирања омогућава аутоматизовану обраду података о паркирању возила, уз помоћ мобилног видео надзора и интегрисаних апликативних решења. Комбинацијом геолокационих података, аутоматског препознавања регистарских ознака и комуникације са сервером, систем обезбеђује прецизно праћење и управљање паркинг просторима у реалном времену. Овим поступком се врши контролисање и наплата паркирања на јавним паркинг местима, а корисницима се пружа могућност правовременог плаћања и корекције информација.

Прилог 3. Информациони систем ЈКП „Паркинг сервис“, Нови Сад

Јавно комунално предузеће „Паркинг сервис“ Нови Сад користи више информационих подсистема за управљање контролом и наплатом паркирања. Поред основне делатности одржавања и наплате паркирања, предузеће се бави имплементацијом и одржавањем СМС система наплате у више од 30 градова у Србији. Ови подсистеми обухватају различите сегменте пословања, од наплате и књиговодства до праћења активности и анализа, и интегришу се у све аспекте управљања паркирањем и пружања услуга корисницима.

Подсистеми у оквиру система за контролу и наплату паркирања:

1) СМС систем за наплату паркирања;
2) Књиговодствени софтвер FRIP (финансијско рачуноводствени информациони систем);
3) Апликација SWAT за анализу и праћење активности.

1) СМС систем за наплату паркирања.

СМС систем за наплату паркирања представља један од кључних информационих подсистема који ЈКП „Паркинг сервис“ Нови Сад користи за омогућавање плаћања паркирања путем мобилних телефона. Овај подсистем корисницима омогућава да једноставним слањем СМС поруке изврше уплату за коришћење паркинг места. Након извршене уплате, корисници добијају електронску потврду са бројем трансакције, као и СМС подсетник пре истека плаћеног времена за паркирање.

Подсистем такође подржава контролу паркирања од стране овлашћених лица. Контролори користе уређаје који им омогућавају да провере уплату, а уређајем могу и да направе фотографије и пренесу податке у финансијско-рачуноводствени систем ФРИП и апликацију SWAT. Ови подаци се затим користе за даље праћење и анализу активности у систему наплате паркирања.

СМС систем обухвата неколико важних активности које осигуравају његово несметано функционисање. То укључује праћење и надзор сервера, као и база података, мониторинг СМС центара према оператерима мобилне телефоније, праћење и евиденцију статистичких извештаја, као и прављење резервних копија података. Поред тога, систем је организован по Open Source концепту, са ВПН везама ка свим провајдерима мобилне телефоније ради сталног праћења и обезбеђивања континуитета услуге.

Овај подсистем је посебно важан због свог обухвата – не само да се користи у Новом Саду, већ је имплементиран и у другим градовима широм Србије, чинећи га важним делом пословних процеса ЈКП „Паркинг сервис“. Он обезбеђује подршку корисницима градова кроз пријем и обраду жалби и рекламација, чиме је осигурано да корисници добијају правовремене информације и решавање проблема.

2) Књиговодствени софтвер FRIP.

Књиговодствени софтвер ФРИП (финансијско-рачуноводствени информациони систем) је други кључни подсистем који ЈКП „Паркинг сервис“ Нови Сад користи за управљање финансијама и књиговодственим активностима. Овај софтвер је интегрисан у више различитих аспеката

пословања, укључујући матичне евиденције о лицима, финансијску оперативу, управљање возилима, као и издавање паркинг карата и фактура.

ФРИП је модуларно организован, са различитим модулима који омогућавају евиденцију активности попут уклањања возила („паук“), обраду налога за уклањање или покушај уклањања возила, као и фактурисање и набавку. Додатни модули укључују евиденцију претплатних и посебних паркинг карата, тужби, складишног и материјалног пословања, зарада запослених и благајне. Систем такође подржава електронску писарницу и управљање кадровским евиденцијама.

ФРИП омогућава корисницима приступ различитим модулима у зависности од радног места и овлашћења, при чему се права приступа додељују у складу са специфичним захтевима сваког корисника. Овај систем игра важну улогу у интеграцији финансијских и оперативних активности у оквиру предузећа, чиме се обезбеђује ефикасно вођење пословних процеса и одржавање прецизних финансијских података.

3) Апликација SWAT за анализу и праћење активности.

Апликација SWAT је трећи значајан информациони подсистем који ЈКП „Паркинг сервис“ Нови Сад користи за анализу и праћење различитих активности повезаних са СМС системом и пословањем паркинг сервиса. SWAT омогућава детаљну контролу уплата за паркирање путем СМС-а, преглед издатих налога за паркирање, као и различите врсте статистичких података о пословању.

Апликација укључује модули за управљање претплатницима, тужбама, киоск картама, распоређивање контролора на терен, као и модуле за статистику и праћење СМС уплата. Поред тога, обезбеђена је и ГПС подршка за праћење позиција контролора при провери паркирања, што додатно побољшава транспарентност и ефикасност у контроли рада.

За приступ апликацији неопходан је сигурносни сертификат, а корисници се пријављују са јединственим налогом и лозинком. Систем је организован на основу доделе права, што омогућава да корисници имају приступ само оним функцијама које су неопходне за њихов посао, чиме се осигурава безбедност података и ефикасно управљање различитим аспектима паркирања и контроле.

Прилог 4. Информациони систем „Synapse tech“ doo из Београда

ЈКП „Паркинг сервис“, Чачак користи информациони систем за наплату паркирања „Synapse tech“ doo из Београда. Систем је развијен како би пружио свеобухватну подршку у процесима наплате паркирања, управљања паркинг местима, као и комуникацији са мобилним операторима. Софтвер обухвата неколико подсистема, који заједно омогућавају функционисање услуге паркирања у Чачку. Систем нуди висок степен аутоматизације процеса, од наплате путем СМС порука до евиденције података о уплатама и контроле паркинг места.. У наставку су наведени подсистеми који се користе у овом систему:

1. **Подсистем за наплату и обраду СМС порука –** омогућава корисницима да плаћају паркинг путем СМС порука, при чему је процес плаћања потпуно аутоматизован. Корисник шаље СМС поруку са регистрацијом возила и бројем паркинг зоне на одређени број мобилног оператера. Након тога, систем прима поруку, обрађује податке о возилу и проверава зону паркирања. Аутоматски шаље повратну поруку кориснику, потврђујући успешно активирање паркинга или указујући на грешку у уносу података. Систем је повезан са базом података која садржи информације о ценама, доступним зонама и важећим правилима за паркирање. Обрађене поруке се чувају у бази података ради даље евиденције и извештавања. Овај подсистем је такође интегрисан са контролорским уређајима који омогућавају брзу проверу плаћених услуга паркинга, осигуравајући да се корисници правилно тарифирају у складу са зонама у којима паркирају своја возила.
2. **Подсистем за наплату путем мобилне апликације** – омогућава корисницима да путем својих мобилних уређаја лако и брзо изврше плаћање паркинг услуга. Овај подсистем је интегрисан са централним системом за наплату паркинга и омогућава евиденцију свих уплата извршених преко мобилне апликације у реалном времену. Он прикупља и обрађује податке као што су регистарска ознака возила, време почетка паркирања и локација, а затим прослеђује те податке у централну базу. Поред обраде уплата, подсистем омогућава и аутоматско ажурирање стања паркинг места, што помаже у праћењу доступности унутар паркинг зона.
3. **Подсистем за наплату паркинга трећим лицима** – омогућава наплату паркинг услуга преко пословних партнера као што су трафике, киосци и други дистрибутери паркинг карата. Овај подсистем је дизајниран да интегрише плаћања која се врше преко ових спољних извора са централним системом наплате. Систем омогућава дистрибутерима да издају паркинг карте, а све трансакције се аутоматски евидентирају у бази података. Подсистем обрађује информације о времену, локацији и трајању паркирања, омогућавајући тачно праћење уплата и продаје паркинг карата од стране трећих лица.
4. **Подсистеми за комуникацију са мобилним операторима** – укључује три засебна подсистема за сваког од мобилних оператера: Телеком Србија, A1 и Yettel. Ови подсистеми омогућавају размену података између система ЈКП „Паркинг сервис“, Чачак и оператера, где корисници путем СМС порука врше плаћање паркинга. Сваки од подсистема обрађује и шаље информације у реалном времену, а примљене поруке се одмах ажурирају у централној бази података. Комуникација са операторима је сигурна и стабилна, чиме се омогућава поуздана и ефикасна наплата паркинг услуга.

5. **Подсистем за теренску и backoffice апликацију** – омогућава интегрисано управљање и надзор над паркинг услугама. Теренска апликација служи контролорима на терену за проверу и контролу паркираних возила, издавање казни и праћење статуса уплата путем мобилних уређаја. Ова апликација омогућава тренутно ажурирање података у систему, чиме се обезбеђује тачност информација у реалном времену. Backoffice апликација је административни алат који се користи у канцеларијама за управљање базом података, обраду података о наплати и контролу теренских активности. Омогућава приступ свим подацима у систему и подржава креирање извештаја, анализа и праћење свих аспеката паркинг система.
6. **Подсистем за обраду података захтева за сторнирање посебних дневних карата** – омогућава обраду захтева за сторнирање Посебних дневних карата (ПДК). Он аутоматизује процес провере и обраде захтева за сторнирање, укључујући проверу унетих података, валидност разлога за сторнирање и одобрење или одбијање захтева на основу дефинисаних правила и процедура. Циљ овог подсистема је да поједностави и убрза процес решавања захтева, смањи административно оптерећење и омогући бољу контролу над обрадом и евиденцијом оваквих захтева.

Прилог 5. Информациони систем „Ђоковић Софтвер“ доо из Чачка

ЈКП „Чистоћа“, Краљево користи информациони систем за наплату паркирања „Ђоковић Софтвер“ доо из Чачка. Систем за наплату и контролу паркирања, састоји се од неколико софтверских модула који су кључни за управљање јавним паркинг местима и наплату услуга. Овај софтвер омогућава електронску наплату путем мобилних телефона, контролу паркинг простора уз коришћење преносивих уређаја и администрацију читавог система кроз backoffice модул. У наставку су наведени модули који се користе у овом систему:

1. **СМС центар за плаћање паркирања путем мобилних телефона.** Овај модул представља један од основних механизама за наплату услуга паркирања у ЈКП „Чистоћа“, Краљево, и омогућава корисницима да плате паркинг брзо и једноставно путем СМС порука. Корисник шаље СМС са регистарским бројем свог возила на одговарајући кратки број који одговара зони паркирања у којој се налази. Систем аутоматски препознаје зону на основу броја и омогућава паркирање у одређеном временском периоду, у зависности од зоне. Плаћено време може се продужавати слањем нове СМС поруке, чиме се корисницима обезбеђује флексибилност у плаћању. Систем истовремено шаље кориснику потврду о успешној трансакцији у виду повратне СМС поруке, која служи као доказ плаћања. Овај модул је такође повезан са контролним системом, омогућавајући контролорима да у реалном времену проверавају да ли је возило регистровано за паркинг у одговарајућој зони, што значајно побољшава ефикасност контроле. Модул подржава различите паркинг зоне и временска ограничења, прилагођавајући се специфичним захтевима корисника и зона.
2. **Модул за контролу паркирања коришћењем преносивих ПДА уређаја.** Овај модул омогућава ефикасно управљање и праћење продаје физичких паркинг карата, које се могу купити на одређеним продајним местима у граду. Паркинг карте обухватају дневне, месечне и посебне врсте карата, укључујући карте за инвалиде или резидентне карте. Систем је дизајниран тако да региструје сваки трансфер карата – од пријема у систем до продаје корисницима. Продаја карата се евидентира у реалном времену, чиме се обезбеђује ажурност и прецизност у евидентирању промета и извршених трансакција.

   Контролори паркирања могу приступити овом модулу и проверити статус плаћања карата у случају потребе за провером, чиме се осигурава да возила која користе физичке паркинг карте буду подједнако подложна контроли као и она која плаћају путем дигиталних система. Овај модул је директно повезан са финансијским системом, што омогућава детаљно извештавање о броју продатих карата, укључујући расподелу по типовима карата и продајним локацијама.

   Такође, модул укључује функцију за управљање залихама карата, што омогућава праћење доступности карата на сваком продајном месту.
3. **Backoffice модул за наплату и контролу (Административни модул).** Backoffice модул за наплату и контролу представља централни административни систем који омогућава свеобухватно управљање апликацијом за наплату паркирања. Овај модул је кључан за администрирање и контролу процеса у реалном времену, укључујући креирање корисничких налога, праћење трансакција, као и подешавање система у складу са

променама у зонирању паркинга и ценовним политикама. Модул омогућава брзу реакцију на оперативне изазове, као и аналитичку обраду података који се користе за побољшање услуга паркирања.

Главне функционалности Backoffice модула укључују:

1) **Контрола података о паркинг налозима** – Управљање свим паркинг налозима и евидентирање трансакција у систему. Ова функција укључује и праћење уплата по корисницима, чиме се омогућава прецизна контрола над финансијским токовима услуга паркирања.
2) **Евиденција зона и ценовне политике** – Администраторски модул омогућава ажурирање паркинг зона и одређивање цена паркинг карата на основу зоне. Ово је кључно за одржавање ажурних информација у систему и обезбеђивање да цене одговарају важећој регулативи.
3) **Креирање корисничких налога и управљање приступом** – Ова функционалност омогућава креирање налога за контролоре на терену и управљање њиховим правима приступа. Уграђена безбедносна подешавања штите систем од неовлашћеног приступа подацима.
4) **Параметризација система** – Систем омогућава флексибилну параметризацију, односно прилагођавање поставки и правила, чиме се осигурава да систем функционише у складу са захтевима ЈКП "Чистоћа", Краљево.
5) **Контрола неактивности** – Уграђена временска контрола неактивности осигурава да се, у случају неактивности корисника у одређеном временском периоду, корисник мора поново пријавити, чиме се обезбеђује додатна безбедност података.
6) **Евиденција уплата** – Систем води детаљну евиденцију свих уплата које се односе на паркинг услуге, укључујући и аналитичке картице власника возила и месечне претплате.
7) **Штампање опомена пред тужбу** – Ова функција омогућава припрему и штампање опомена за кориснике који нису извршили уплату за паркинг у предвиђеном року.

Back Office модул за наплату и контролу игра кључну улогу у одржавању ефикасности и контроле система за наплату паркирања, омогућавајући истовремено и стратешко управљање подацима, финансијама и корисницима.

Прилог 6. Информациони систем „EPSEE MS“ DOO из Београда

ЈП „Пословни центар“, Крушевац користи информациони систем за наплату паркирања „EPSEE MS“ DOO из Београда. Софтвер за контролу и наплату паркирања, који субјекат ревизије користи, састоји се од неколико модула који су интегрисани у један систем. Сваки од ових модула има специфичну функцију која доприноси ефикасности и безбедности система за наплату паркирања, као и бољој услузи корисницима. Систем је осмишљен тако да омогућава интеграцију постојећих система и функција као што су паркомати и мобилне апликације, уз обезбеђивање високе доступности, скалабилности и сигурности података. У наставку су представљени модули који чине овај софтверски систем:

1. **Модул за плаћање паркирања путем мобилног телефона (СМС центар)**

Овај модул омогућава корисницима да на брз и једноставан начин плате паркирање путем СМС поруке. Корисник уноси регистарски број свог возила и шаље га на одређени кратки број који је повезан са одређеном паркинг зоном. Систем аутоматски препознаје паркинг зону на основу броја и омогућава наплату у реалном времену. Након успешне трансакције, корисник добија потврду о уплати путем повратне СМС поруке, као и информације о истеку времена паркирања. Модул је дизајниран тако да буде поуздан и да обрађује велики број СМС порука у кратком временском периоду, а такође пружа и могућност продужења времена паркирања са исте СМС линије.

2. **Модул за контролу паркирања путем преносивих рачунара (Pocket PC)**

Овај модул омогућава контролорима да користе преносиве уређаје (PDA) за проверу статуса плаћања паркирања у реалном времену. Контролори уносе регистарски број возила у апликацију на свом уређају, која је повезана са системом за наплату путем GPRS технологије. Уређај брзо враћа податке о томе да ли је возило платило паркирање или не, што омогућава контролорима да ефикасно раде на терену. Модул је осмишљен тако да минимизира време потребно за добијање података, што повећава ефикасност контроле и смањује могућност грешака.

3. **Backoffice модул за праћење и управљање процесима наплате и контроле паркирања**

Овај модул представља централни систем за управљање свим процесима наплате и контроле паркирања. Он омогућава праћење свих трансакција везаних за наплату паркирања, било да су плаћене путем СМС-а, мобилних апликација или паркомата. Модул такође омогућава администрацију претплатничких карата, надзор над корисничким налозима, генерисање извештаја и обраду плаћања. Backoffice модул пружа операторима централизован поглед на све активности у систему, што омогућава бољу контролу, планирање и управљање ресурсима у реалном времену.

4. **Модул за плаћање паркирања путем мобилних апликација (Android/iOS)**

Овај модул омогућава корисницима да на згодан начин плате паркирање користећи мобилне апликације на Android и iOS платформама. Корисници могу уносити своје податке, као што су регистарски број возила и изабрана паркинг зона, директно у апликацију, која је повезана са системом за наплату. Плаћање се врши путем електронских средстава, а апликација пружа могућност праћења времена преосталог за паркирање, као и опцију да продужи трајање паркирања. Апликација је дизајнирана са фокусом на једноставност коришћења, што омогућава корисницима да брзо и ефикасно изврше плаћање, док истовремено оператор добија податке у реалном времену о уплатама.

5. Web сервис за информисање корисника о неплаћеним налозима

Овај модул омогућава корисницима да преко јавног веб сервиса провере да ли имају неплаћене налоге за паркирање. Корисници уносе потребне податке, као што су регистарски број возила или други идентификатори, а систем им омогућава преглед неплаћених налога у року од 24 сата од издавања. Осим основних информација о дуговањима, модул пружа опцију генерисања QR кода који корисници могу користити за директно плаћање. Овај сервис је дизајниран да буде једноставан за употребу и приступачан свима, пружајући брз начин за проверу и регулисање дуговања, што побољшава транспарентност и ефикасност система наплате паркирања.

6. Минисајт апликација

Минисајт апликација је дизајнирана као лако доступна платформа која корисницима пружа кључне информације о паркинг услугама. Ова апликација омогућава корисницима да приступе информацијама о локацијама паркинг места, тарифама, радном времену и периодима наплате. Поред основних информација, минисајт такође садржи детаље о додатним услугама које нуди оператор, као што су резервације паркинг места или опције за дугорочне претплате.

Ово је основна структура модула који чине софтвер за контролу и наплату паркирања, а сваки од њих игра важну улогу у ефикасном управљању системом паркирања.