ДРЖАВНА
РЕВИЗОРСКА
ИНСТИТУЦИЈА

ИЗВЕШТАЈ
О РЕВИЗИЈИ СВРСИСХОДНОСТИ ПОСЛОВАЊА

Информациони систем за наплату услуга паркинга у Јавном комуналном предузећу за јавне гараже и паркиралишта „Паркинг сервис“, Београд

Број: 400-1058/2024-07/34
Београд, 20. децембар 2024. године

ЈКП „Паркинг сервис“, Београд је кроз унапређене апликативне контроле, мобилну апликацију и нову процедуру за сигурно управљање подацима значајно побољшао транспарентност, доступност и заштиту података корисника, али је потребно развити свеобухватне планове за континуитет пословања у ванредним околностима како би систем био потпуно поуздан.

Информациони системи који се односе на услуге паркирања треба да имају две основне функције: контролу наплате паркинг услуга и контролу доступности и коришћења паркинг места, како би се плаћање вршило у складу са стварном употребом и ефикасношћу пружених услуга. Ови системи се користе за побољшање управљања паркинг простором, као и за информисање грађана о доступности паркинг места у реалном времену. У досадашњем коришћењу ових система, утврђено је да приступ системима и базама података имају и пружаоци услуга, није обезбеђен континуитет пословања у случају раскида сарадње, нису успостављени сви механизми који обезбеђују контролу наплате услуга и управљања паркинг местима.

Слика 1. Тема ревизије

Успостављене мере информационе безбедности обезбеђују основну поузданост система за наплату услуга паркинга, али је неопходно додатно унапређење кроз развој свеобухватних планова за континуитет пословања у ванредним околностима.

Механизам сарадње са корисницима система је успостављен, обезбеђујући основну сигурност и заштиту података, а субјект ревизије је у току ревизије донео процедуру за архивирање, миграцију и уништавање података која омогућава континуитет пословања и безбедан повраћај података у случају раскида сарадње.

Успостављене апликативне контроле обезбеђују ажурну евиденцију и контролу наплате услуга, али и боље информисање грађана кроз употребу мобилне апликације и отворених података, чиме се значајно унапређује транспарентност и доступност информација.

Препоруке

Након спроведене ревизије, Државна ревизорска институција је Јавном комуналном предузећу „Паркинг сервис“, Београд, дала препоруку да развије и имплементира планове континуитета за све критичне сценарије прекида ИТ функција како би се осигурао несметан опоравак у ванредним ситуацијама.

Предузете мере

Током ревизије, ЈКП „Паркинг сервис“, Београд је спровео низ мера усмерених на унапређење информационе безбедности, организације и апликативних контрола како би побољшао сигурност података и ефикасност система.:

- Унапређена је унутрашња организација и систематизација, као и мере за процену и управљање ризицима информационе безбедности.
- Усвојене су процедуре за безбедну предају, миграцију и брисање података у складу са међународним стандардима и законским прописима.
- Уговори са корисницима су допуњени процедурама за сигуран пренос и брисање података, чиме је осигуран континуитет пословања и унапређена заштита података.
- Ограничен је приступ осетљивим подацима и унапређене су апликативне контроле у систему за наплату и контролу паркирања.

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
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 Јавном комуналном предузећу за јавне гараже и паркиралишта „Паркинг сервис“, Београд 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.

За пружање услуга паркинга у граду Београду задужено је Јавно комунално предузеће за јавне гараже и паркиралишта „Паркинг сервис“ (у даљем тексту: ЈКП „Паркинг сервис“, Београд). ЈКП „Паркинг сервис“, Београд је само развило систем за управљање контролом и наплатом паркирања. Систем је имплементиран 2020. године и у досадашњем периоду није спроведена ни интерна, ни екстерна ревизија овог система. Систем се користи за евиденцију издатих дневних, повлашћених и посебних паркинг карата и за евиденцију-контролу доступних паркинга.

Након спроведене ревизије утврдили смо:

ЈКП „Паркинг сервис“, Београд је кроз унапређене апликативне контроле, мобилну апликацију и нову процедуру за сигурно управљање подацима значајно побољшао транспарентност, доступност и заштиту података корисника, али је потребно развити свеобухватне планове за континуитет пословања у ванредним околностима како би систем био потпуно поуздан.

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

1. Успостављене мере информационе безбедности обезбеђују основну поузданост система за наплату услуга паркинга, али је неопходно додатно унапређење кроз развој свеобухватних планова за континуитет пословања у ванредним околностима.
   - ЈКП „Паркинг сервис“, Београд је усвојио нови Правилник о безбедности ИКТ система у складу са организационим променама и припремом за ресертификацију стандарда ISO/IEC 27001:2013. Међутим, утврђено је да Правилник не обухвата све специфичности критичних система, попут система за контролу и наплату паркирања, што указује на непотпуну заштиту ових система у односу на потенцијалне претње информационој безбедности. Као узрок идентификован је изостанак ажурирања одређених одредби у Правилнику које би прецизније обухватиле специфичности

сваког критичног система. Последица овог пропуста је повећан ризик од неовлашћеног приступа и поремећаја у раду система за наплату паркирања, што може негативно утицати на квалитет услуге и ефикасност пословања предузећа. У међувремену, 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. Ажурирања су укључила детаљан Регистар ИКТ подсистема (Прилог 1) и Регистар апликативних подсистема (Прилог 2), који су значајни за управљање и заштиту критичних апликација. Овим изменама смањени су ризици од неовлашћеног приступа и побољшан ниво заштите ИКТ система, чиме је осигурана усклађеност са захтевима стандарда и унапређена информациона безбедност.

- ЈКП „Паркинг сервис“, Београд је успоставило мере физичке заштите и контроле логичког приступа системима, чиме је обезбеђена заштита ИКТ ресурса.
- Иако је предузеће предузело значајне кораке ка континуитету пословања, укључујући процедуре за премештање кључних делова ИКТ система и редовно прављење резервних копија, утврђено је да планови за критичне сценарије, попут прекида напајања или квара на кључним компонентама система, нису у потпуности развијени. Недостају детаљне процедуре за брз и ефикасан опоравак система у ванредним ситуацијама, што представља ризик за континуитет пословања и правовремени опоравак од инцидената. Додатно, предузеће нема јасно дефинисане планове за сценарије који укључују хитне случајеве попут поплава или пожара, и није развило комплетан план континуитета који обухвата све неопходне процедуре и контроле. Овај недостатак оставља простор за могуће прекиде у функционисању у случају већих инцидената, као и повећава ризик за интегритет и безбедност података.
- ЈКП „Паркинг сервис“, Београд је побољшао управљање ризицима у ИКТ систему допуном Правилника о систематизацији послова. Првобитно, Правилник о систематизацији није обухватао прецизно дефинисана радна места и дужности у области превенције и управљања безбедносним ризицима, што је могло довести до нејасноћа у одговорностима и повећаног ризика од безбедносних пропуста. Иако су неке активности, попут надзора комуникационих мрежа, биле део општих задатака, недостатак експлицитних улога у овој области угрозио је поузданост ИКТ система. Током поступка ревизије, ЈКП „Паркинг сервис“, Београд је, 28. октобра 2024. године, ажурирало Правилник о систематизацији, утврђујући да је руководилац Службе за ИТ одговоран за успостављање и примену мера за процену ризика, док су извршни руководилац службе и други одговорни запослени задужени за спровођење мера безбедности. Овим изменама је обезбеђена јаснија подела одговорности и унапређена ефикасност у управљању ризицима, чиме је значајно побољшана информациона безбедност.

2. Механизам сарадње са корисницима система је успостављен, обезбеђујући основну сигурност и заштиту података, а субјект ревизије је у току ревизије донео процедуру за архивирање, миграцију и уништавање података која

омогућава континуитет пословања и безбедан повраћај података у случају раскида сарадње.

- ЈКП „Паркинг сервис“, Београд је правилницима, процедурама и физичком заштитом обезбедио безбедност података корисницима система.
- ЈКП „Паркинг сервис“, Београд је успоставио систем заштите података који обезбеђује сигурност података корисника услуга.
- ЈКП „Паркинг сервис“, Београд није дефинисао адекватне процедуре које би осигурале неометано пословање корисника у случају раскида или истека сарадње, укључујући процедуре за архивирање, миграцију и уништавање података корисника. Уговори са корисницима услуга не садрже одредбе које би омогућиле сигурно извршавање процеса повраћаја или уништавања података у складу са релевантним стандардима и прописима (као што су ISO/IEC 27001, ISO/IEC 27018 и GDPR), чиме се ствара ризик за безбедност и интегритет података корисника. Дефинисан је отказни рок од 60 дана, али активности попут извоза података или преноса криптографских кључева нису прописане, што доводи до могућности прекида у функционисању корисничких система након истека сарадње. Поред тога, недостатак јасних процедура за архивирање и уништавање података оставља простор за неовлашћени приступ или нарушавање интегритета података. У циљу смањења ових ризика, директор ЈКП „Паркинг сервис“, Београд је дана 14. новембра 2024. године одобрио процедуру „Предаја и брисање података са сервера услед престанка уговорних обавеза“ (ПС.П64). Новом процедуром дефинисани су јасни кораци за извоз података, пренос криптографских кључева и пружање техничке подршке у прелазном периоду, као и обавеза трајног уништавања података након истека сарадње. Ове активности су праћене строгим техничким и организационим мерама за осигурање поверљивости, интегритета и усклађености са важећим прописима. Увођењем ове мере, ризици за безбедност и интегритет података корисника су значајно смањени, а континуитет у пословању корисничких система обезбеђен. ЈКП „Паркинг сервис“, Београд је, на иницијативу и засновано на процедури „Предаја и брисање података са сервера услед престанка уговорних обавеза“ од 14. новембра 2024. године, обезбедио да корисници њихових услуга успоставе процедуре за примопредају и брисање података у случају раскида или истека уговора. Ове процедуре су постале саставни део уговора за набавку система за контролу и наплату паркирања путем мобилног видео надзора, чиме је значајно унапређена усклађеност са стандардима и смањени ризици за безбедност и интегритет података корисника.

3. Успостављене апликативне контроле обезбеђују ажурну евиденцију и контролу наплате услуга, али и боље информисање грађана кроз употребу мобилне апликације и отворених података, чиме се значајно унапређује транспарентност и доступност информација.
   - ЈКП „Паркинг сервис“, Београд је унапредио апликативне контроле и ограничио приступ осетљивим подацима након утврђених недостатака.
   - У ЈКП „Паркинг сервис“ Београд апликативне контроле које се користе за продају карата омогућавају ажурну евиденцију дневних пазара и броја продатих паркинг карата, као и извештавање.

- ЈКП „Паркинг сервис“, Београд редовно ажурира податке о паркинг зонама, развило је мобилну апликацију и омогућило коришћење отворених података за боље информисање грађана.

Након спроведене ревизије „Информациони систем за наплату услуга паркинга“, Државна ревизорска институција даје ЈКП „Паркинг сервис“, Београд препоруку 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].

2. Мере предузете у поступку ревизије

У току спровођења ове ревизије:

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

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

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.

3. Захтев за достављање одазивног извештаја

Јавно комунално предузеће за јавне гараже и паркиралишта „Паркинг сервис“, Београд је, на основу члана 40 став 1 Закона о Државној ревизорској институцији, дужно да поднесе Државној ревизорској институцији писани извештај о отклањању откривених несврсисходности (одазивни извештај) у року од 90 дана почев од наредног дана од дана уручења овог извештаја.

Одазивни извештај мора да садржи:

1) навођење ревизије, на коју се он односи;

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

3) приказивање мера исправљања.

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

Субјект ревизије је обавезан да у одазивном извештају искаже мере исправљања по основу откривених несврсисходности односно свих закључака и налаза датих у Извештају о ревизији сврсисходности пословања, као и да поступи по датим препорукама. За мере исправљања Јавно комунално предузеће за јавне гараже и паркиралишта „Паркинг сервис“, Београд је дужно да уз одазивни извештај достави доказе према следећем:

1. За налазе, односно несврсисходности првог приоритета, односно које је могуће отклонити у року од 90 дана Јавно комунално предузеће за јавне гараже и паркиралишта „Паркинг сервис“, Београд је у обавези да достави доказе о отклањању несврсисходности односно предузимању мера исправљања;

2. За налазе, односно несврсисходности другог приоритета, односно које је могуће отклонити у року до годину дана, и трећег приоритета, односно које је могуће отклонити у року до три године, Јавно комунално предузеће за јавне гараже и паркиралишта „Паркинг сервис“, Београд је обавезно да достави акциони план у којем ће описати мере и активности које ће бити предузете ради отклањања несврсисходности или смањења ризика од појављивања несврсисходности у будућем пословању као и планирани период предузимања мера и одговорно лице.

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

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

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

Ако се оцени да одазивни извештај не указује да су откривене несврсисходности отклоњене на задовољавајући начин, сматра се да субјект ревизије крши обавезу доброг пословања. Ако се ради о незадовољавајућем отклањању значајне несврсисходности,

сматра се да постоји тежи облик кршења обавезе доброг пословања. У овим случајевима Државна ревизорска институције је овлашћена да предузима мере сагласно члану 40 ст. 7 до 13 Закона о Државној ревизорској институцији.

Генерални државни ревизор

Душко Пејовић

Digitally signed by Душко Пејовић
Date: 2024.12.20 14:35:20 +01'00'

Др Душко Пејовић
Државна ревизорска институција
Макензијева 41
11000 Београд, Србија
20. децембар 2024. 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[2], Пословником Државне ревизорске институције[3] 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 – грађана, и у којој мери систем омогућава ефикасност контроле наплате и плаћања услуга

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

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 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 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[4]), као и све податке добијене од субјеката. Анализирали смо податке и информације за период од 2021. до 2023. године.

У вези са информационим системом „Паркинг сервис“, Београд, анализиране су области информациона безбедност, успостављање ефективног механизма сарадње са пружаоцима 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. Овај извештај садржи налазе и закључке утврђене у ревизији ЈКП „Паркинг сервис“, Београд.

Детаљнији опис коришћене методологије дат је у Прилогу 1.

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

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[5].

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[6] 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.

[5] Члан 7 став 3 Закона о информационој безбедности.
[6] „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[7].

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.

Одлука о јавним паркиралиштима[8]

Одлуком о јавним паркиралиштима уређују се услови и начин организовања послова у обављању комуналне делатности одржавања јавних простора за паркирање (у даљем тексту: јавна паркиралишта), као и услови коришћења јавних паркиралишта на територији града Београда.

Одлука о промени оснивачког акта Јавног комуналног предузећа за јавне гараже и паркиралишта „Паркинг сервис“, Београд[9]

Предузеће обавља делатност од општег интереса за Град Београд.

Предузеће обавља комуналну делатност управљања јавним паркиралиштима.

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 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 одлуком скупштине јединице локалне самоуправе којом се уређује начин обављања комуналне делатности управљања јавним паркиралиштима, као и вршење наплате ових услуга.

Делатност обухвата и послове у вези с контролом коришћења и наплатом паркирања на посебно обележеним паркинг-местима за снабдевање на ободу пешачких зона кроз јединствени систем електронске контроле коришћења паркинг-места и контроле уласка и изласка возила у пешачким зонама и одржавање система путем јединственог система електронске контроле.

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

[8] „Сл. лист града Београда“, бр. 12/2010 - пречишћен текст, 37/2011, 42/2011 - испр., 11/2014, 30/2014, 34/2014, 89/2014, 96/2016, 36/2017, 118/2018, 26/2019, 52/2019, 65/2020, 152/2020, 9/2021, 111/2021 и 76/2022

[9] "Службени лист града Београда", бр. 14/2024

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.

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:

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

1) примени одговарајуће техничке, организационе и кадровске мере, као што је псеудонимизација, које имају за циљ обезбеђивање делотворне примене начела заштите података о личности, као што је смањење броја података;
2) обезбеди примену неопходних механизама заштите у току обраде, како би се испунили услови за обраду прописани овим законом и заштитила права и слободе лица на која се подаци односе (став 1).

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

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

Члан 45 овог Закона прописује да ако се обрада врши у име руковаоца, руковалац може да одреди као обрађивача само оно лице или орган власти који у потпуности гарантује примену одговарајућих техничких, организационих и кадровских мера, на начин који обезбеђује да се обрада врши у складу са одредбама овог закона и да се обезбеђује заштита права лица на које се подаци односе (став 1).

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

Обрада од стране обрађивача мора бити уређена уговором или другим правно обавезујућим актом, који је закључен, односно усвојен у писменом облику, што обухвата и електронски облик, који обавезује обрађивача према руковаоцу и који уређује предмет и трајање обраде, природу и сврху обраде, врсту података о личности и врсту лица о којима се подаци обрађују, као и права и обавезе руковаоца (став 3).

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

1) обрађује податке о личности само на основу писмених упутстава руковаоца, укључујући и упутство у односу на преношење података о личности у друге државе или међународне организације, осим ако је обрађивач законом обавезан да обрађује податке. У том случају, обрађивач је дужан да обавести руковаоца о тој законској обавези пре започињања обраде, осим ако закон забрањује достављање тих информација због потребе заштите важног јавног интереса;
2) обезбеди да се физичко лице које је овлашћено да обрађује податке о личности обавезало на чување поверљивости података или да то лице подлеже законској обавези чувања поверљивости података;
3) предузме све потребне мере у складу са чланом 50 овог Закона;
4) поштује услове за поверавање обраде другом обрађивачу из 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 је основала 27. децембра 1971. године Скупштина града Београда као Дирекцију за јавне гараже и паркиралишта. У складу са ондашњим саобраћајним потребама, требало је да се обезбеди и уреди простор за паркирање у најфреквентнијим деловима града. Предузеће је назив, али не и делатност, мењало неколико пута, а данашњи облик и име добија 1992. године када је решењем Скупштине града Београда организовано као Јавно комунално предузеће.

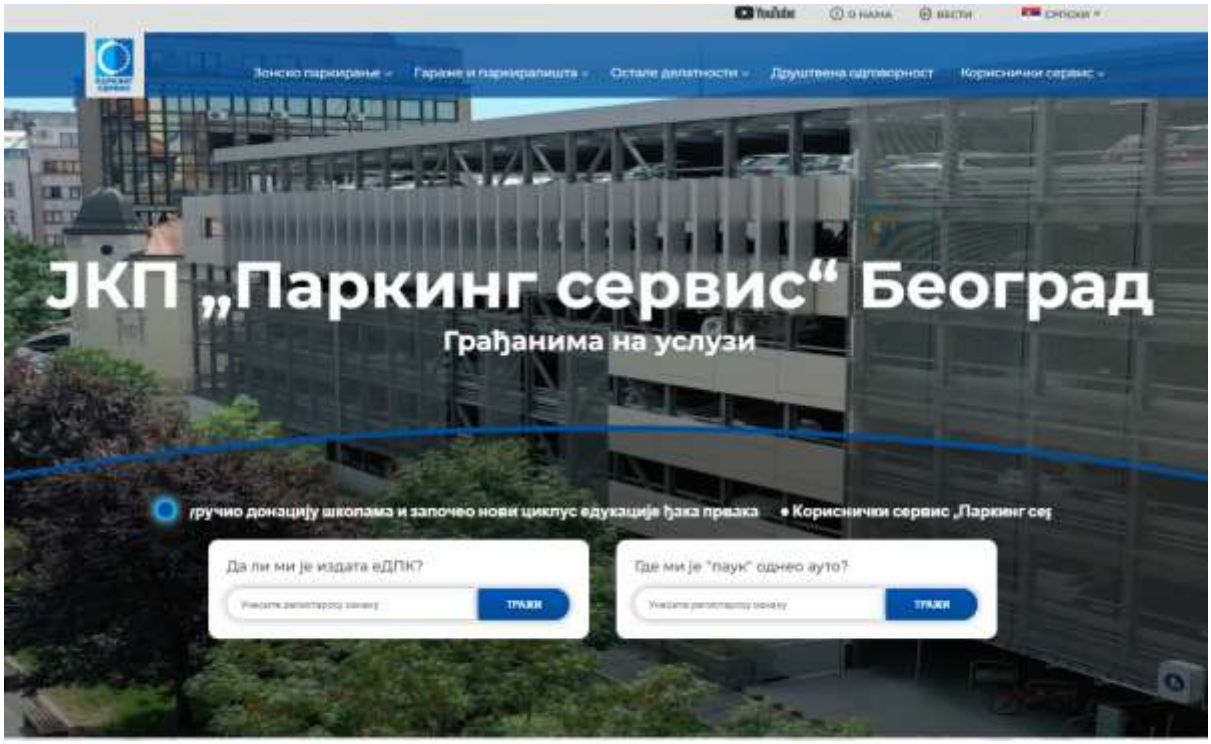
Центар града подељен је на Зону А, црвену, жуту и зелену зону, а паркирање је ограничено на пола сата, један, два или три часа, уз могућност продуженог паркирања: у црвеној зони од 30 минута, у жутој зони од 60 минута и у зеленој зони од 60 минута, те је тиме постигнута добра изменљивост паркираних возила и омогућено паркирање већег броја возила. ЈКП „Паркинг сервис“ користи и одржава више од 42.000 паркинг места. Од овог броја, 33.000 налази се под режимом наплате у зонираном подручју, док се око 9.250 паркинг места налази у гаражама и на паркиралиштима. 2003. године уведен је Зонски систем паркирања. Центар града подељен је на Зону А, црвену, жуту и зелену зону, а паркирање је ограничено на: пола сата, један, два или три часа, уз могућност продуженог паркирања: у црвеној зони од 30 минута, у жутој зони од 60 минута и у зеленој зони од 60 минута, те је тиме постигнута добра изменљивост паркираних возила и омогућено паркирање већег броја возила.

Од септембра 2020. године мултифункционална возила са специјалном надоградњом (Scan Car), популарно названа „Око соколово“, контролишу наплату паркирања на подручју примене зонског система. Прописно паркираним возилима, за која паркирање није плаћено или је истекло дозвољено време паркирања систем аутоматски креира електронску дневну паркинг карту.

ЈКП „Паркинг сервис“, Београд пружа и услуге преноса возила, у сарадњи са Саобраћајном полицијом, Комуналном милицијом и Комуналном инспекцијом. Специјализованим дизалицама „Паркинг сервис” уклања непрописно паркирана, хаварисана и нерегистрована возила. Покретне дизалице, тзв. „паук“, 24 сата дневно, сваког дана у години, налазе се у приправности за ванредне ситуације, као што су саобраћајне незгоде, елементарне непогоде, ватрогасне и хитне медицинске интервенције. „Паркинг сервис“ активно учествује и у свим градским манифестацијама и прославама, обезбеђујући проходност улица, због безбедности и комфора учесника и гостију Београда.

Само комунално предузеће је развило информациони систем за наплату паркирања. Прилагођавајући своје пословање модерним технологијама, 2020. године уведен је тзв. еПаркинг. У склопу ове иновације, пуштена је у рад апликација за плаћање паркирања и навођење до најближег слободног паркинг места. Возачима је пружена могућност да паркирање на подручју примене зонског система, у гаражама и на паркиралиштима плате електронски - платним картицама, средствима депонованим у самој апликацији или слањем СМС поруке (зонско паркирање).

Слика 3. Организациона шема ЈКП „Паркинг сервис“, Београд



Слика 4. Сајт ЈКП „Паркинг сервис“, Београд

- ***СМС:***

  Унети регистарску ознаку возила великим словима и без размака у тело поруке;

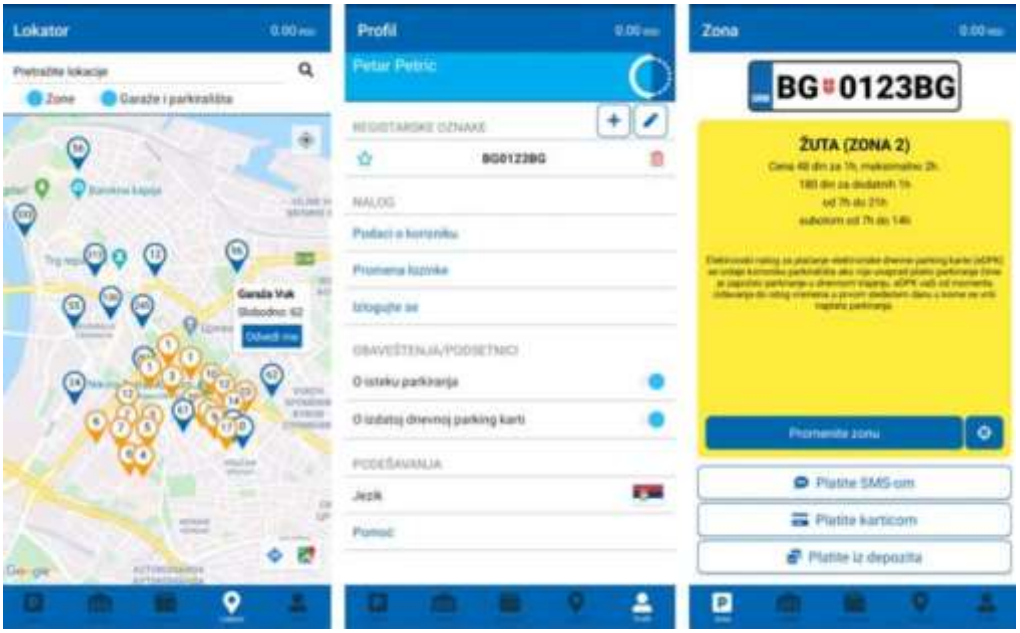
  У зависности од паркинг зоне пошаље се порука на кратки број

  Добија се повратна порука са информацијом о успешној уплати паркирања

  Неколико минута пре истека паркинг услуге добија се порука, која подсећа када истиче време паркирања, како би се могло продужити паркинг или благовремено уклонити возило.

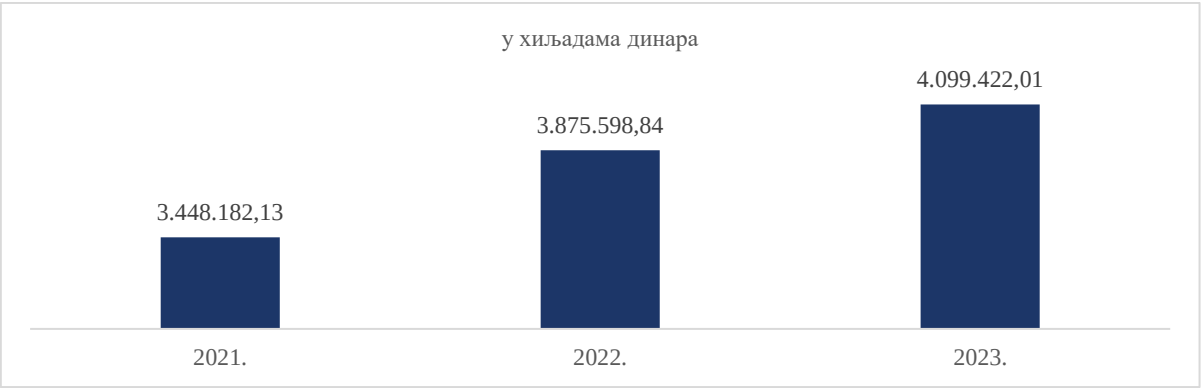
- ***Плаћање код контролора:*** ***куповином електронске паркинг карте код контролора, који контролише и наплаћује коришћење паркинг места***

Слика 5. Начин наплате ЈКП „Паркинг сервис“, Београд



Слика 6. Апликација за плаћање и навођење до најближег паркинг места

На основу анализе доступне документације и података које је доставило ЈКП „Паркинг сервис“, Београд, као и других извора информација, посебну пажњу посвећена је разматрању прихода од паркирања и њиховој структури током ревидираног периода. У наставку следе графикони који приказују укупне приходе и структуру прихода од паркирања за протекли период, пружајући преглед финансијског учинка у оквиру овог сегмента пословања.



Графикон 1. Укупни приходи од паркирања у ревидираном периоду

Графикон 2. Структура прихода од паркирања у ревидираном периоду

Укупни приходи ЈКП „Паркинг сервис“, Београд бележе константан раст током ревидираног периода, као што је приказано на графикону 1. Највећи део прихода потиче од сатних и дневних паркинг карата, што указује на доминацију краткорочног паркирања у приходној структури. Месечне карте и други извори прихода, као што су накнаде за опомене и административне услуге, чине мањи, али значајан удео. Ови подаци сугеришу да је основа финансијског учинка заснована на дневној коришћењу паркинга од стране грађана, док дугорочне претплате и административни трошкови играју мању улогу.

Након анализе прихода који су остварени у области наплате паркинг услуга, важно је размотрити и кретање потраживања по основу дневних карата за паркирање. Дневне карте за паркирање се односе на паркинг карте које се издају корисницима у случајевима непрописног паркирања, где се наплаћује додатна накнада за цео дан паркирања. Потраживања по овом основу представљају значајан фактор у финансијском пословању, јер указују на ефикасност наплате ових услуга и управљање обавезама корисника. У наставку је приказано кретање потраживања по основу дневних карата за паркирање, што омогућава детаљнији увид у овај аспект пословања.

Графикон 3. Потраживања за дневне карте за паркирање у ревидираном периоду[16]

Потраживања по основу дневних карата за паркирање показују осцилације током анализираног периода, као што је приказано на графикону 3. Овде наглашавамо да је просечан период наплате ових потраживања 23 дана. Иако постоји константан ниво потраживања, висина ових дуговања указује на потребу за побољшањем ефикасности наплате ових услуга. Повећање напора у праћењу обавеза корисника и унапређење механизама наплате могло би довести до смањења дуговања и допринети бољој финансијској стабилности предузећа.

[16] Износ директног отписа потраживања за дневне карте на крају године представља износ директног отписа након протека 3 године, односно наступања апсолутног рока застарелости потраживања; износ на крају 2021. године представља износ отписаних потраживања из 2018. године итд.

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.

IV Закључци

На основу анализе података и документације достављене од стране ЈКП „Паркинг сервис“, Београд, 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. Успостављене мере информационе безбедности обезбеђују основну поузданост система за наплату услуга паркинга, али је неопходно додатно унапређење кроз развој свеобухватних планова за континуитет пословања у ванредним околностима.
2. Механизам сарадње са корисницима система је успостављен, обезбеђујући основну сигурност и заштиту података, а субјект ревизије је у току ревизије донео процедуру за архивирање, миграцију и уништавање података која омогућава континуитет пословања и безбедан повраћај података у случају раскида сарадње.
3. Успостављене апликативне контроле обезбеђују ажурну евиденцију и контролу наплате услуга, али и боље информисање грађана кроз употребу мобилне апликације и отворених података, чиме се значајно унапређује транспарентност и доступност информација.

У наставку извештаја наводимо закључке са одговарајућим налазима.

ЗАКЉУЧАК 1: Успостављене мере информационе безбедности обезбеђују основну поузданост система за наплату услуга паркинга, али је неопходно додатно унапређење кроз развој свеобухватних планова за континуитет пословања у ванредним околностима

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 7. 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: ЈКП „Паркинг сервис“, Београд није у ревидираном периоду у потпуности ажурирао Правилник о безбедности ИКТ система у складу са специфичностима система за контролу и наплату паркирања

ЈКП „Паркинг сервис“, Београд је усвојио нови Правилник о безбедности ИКТ система у складу са организационим променама и припремом за ресертификацију стандарда ISO/IEC 27001:2013. Међутим, утврђено је да Правилник не обухвата све специфичности критичних система, попут система за контролу и наплату паркирања, што указује на непотпуну заштиту ових система у односу на потенцијалне претње информационој безбедности.

Као узрок идентификован је изостанак ажурирања одређених одредби у Правилнику које би прецизније обухватиле специфичности сваког критичног система. Последица овог пропуста је повећан ризик од неовлашћеног приступа и поремећаја у раду система за наплату паркирања, што може негативно утицати на квалитет услуге и ефикасност пословања предузећа.

У међувремену, 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. Ажурирања су укључила детаљан Регистар ИКТ подсистема (Прилог 1) и Регистар апликативних подсистема (Прилог 2), који су значајни за управљање и заштиту критичних апликација. Овим изменама смањени су ризици од неовлашћеног приступа и побољшан ниво заштите ИКТ система, чиме је осигурана усклађеност са захтевима стандарда и унапређена информациона безбедност.

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

ЈКП „Паркинг сервис“, Београд 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.

ЈКП „Паркинг сервис“, Београд је 28. септембра 2020. године усвојио Правилник о безбедности информационо–комуникационог система ЈКП „Паркинг сервис“, Београд. Овим Правилником биле су утврђене мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационог система. Наведени Правилник о безбедности информационо-комуникационог система

ЈКП „Паркинг сервис“ Београд усвојен је ради усклађивања са изменама и допунама Закона о информационој безбедности и стицања сертификата ISO 27001, чиме је измењен Правилник из 2017. године. Овај Правилник обезбеђује ажурирање процедура и појмова у складу са законском регулативом и захтевима за заштиту података и безбедност ИКТ система.

Нови Правилник о безбедности информационо-комуникационог система ЈКП „Паркинг сервис“ Београд (у даљем тексту: Правилник о безбедности ИКТ система) донет је 27. септембра 2023. године као припрема за ресертификацију стандарда ISO/IEC 27001:2013, који потврђује усаглашеност система управљања безбедношћу информација и чија валидност истиче 30. новембра 2023. године. Измене у Правилнику о безбедности ИКТ система биле су неопходне услед организационих промена унутар предузећа, које су уследиле након доношења Одлуке о измени и допуни Правилника о унутрашњој организацији и систематизацији послова. Ова Одлука, која је ступила на снагу 26. октобра 2022. године, довела је до промене назива „Служба за информатику и аутоматику“ у „Служба за информационе технологије“ и брисања Одељења за развој и управљање аутоматиком и систематизовања Одељења за развој паркирања и управљање аутоматским паркинг системима у оквиру Службе за заједничке послове. Новим Правилником о безбедности ИКТ система је прецизно дефинисана и разграничена надлежност између Службе за информационе технологије и Службе за заједничке послове у погледу одговорности за одржавање и функционисање информационо-комуникационог система предузећа, како би се осигурало његово несметано функционисање у складу са новим организационим оквиром.

Међутим, и нови Правилник о безбедности ИКТ система се односи на све системе у предузећу и није ажуриран у складу са информационим системом за контролу и наплату паркирања који је у употреби. Пошто ЈКП „Паркинг сервис“, Београд користи више различитих информационих система, у Правилнику о безбедности ИКТ система треба предвидети тачне дефиниције на који се информациони систем који део Правилника о безбедности ИКТ система односи.

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.

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

Директор ЈКП „Паркинг сервис“, Београд је јула 2020. године донео Одлуку о имплементацији система менаџмента безбедношћу информација према међународном стандарду ISO/IEC 27001. У складу са предвиђеном активношћу израде системске документације система менаџмента безбедношћу информација, ЈКП „Паркинг сервис“, Београд је усвојило низ процедура и упутстава којима су уређени послови из области информационе безбедности а у смислу праћења активности, ревизије и надзора у оквиру управљања информационом безбедношћу. Ове процедуре су:

- Управљање ризицима по безбедност информација из домена Службе за ИТ;
- Безбедносне политике и поступци за администраторе ИТ система у Служби за ИТ;
- Безбедносне политике и поступци за кориснике ИТ система у домену Службе за ИТ;
- Управљање инцидентима нарушавања безбедности информација из домена Службе за ИТ;
- Израда плана пословног континуитета из домена Службе за ИТ;
- Управљање ИТ услугама и ИТ аутсорсом из домена Службе за ИТ.

ЈКП „Паркинг сервис“, Београд је успоставило и примењује систем менаџмента квалитетом у сагласности са захтевима стандарда ISO 9001:2015. У складу са наведеним стандардом развијена је и усвојена Процедура Развој и управљање системима из области информационе технологије. У поглављима 6.1.25. и 6.1.26. наведене Процедуре предвиђено је праћење примене Правилника о безбедности ИКТ система и интерне провере усаглашености са Правилником о безбедности ИКТ система. Праћење активности, ревизија и надзор у оквиру управљања информационом безбедношћу у ЈКП „Паркинг сервис“ одвија се кроз низ строго дефинисаних процедура и одговорности. Служба за информационе технологије задужена је за праћење примене Правилника о безбедности ИКТ система, посебно у делу који се односи на делокруг њених активности. Сваки запослени корисник ИКТ ресурса упознат је са својим одговорностима кроз потписивање изјаве о прихватању правила, што потврђује њихову обавезу поштовања прописаних безбедносних мера. Кључну улогу у надзору имају главни администратор база података, систем администратор и администратор КОЦ-а, који су одговорни за контролу приступа ресурсима ИКТ система. Системска интерна ревизија, коју спроводи Служба за информационе технологије, осигурава да је ИКТ систем усклађен са важећим правилницима. Тим за проверу израђује извештај о усаглашености који се доставља руководству предузећа, чиме се осигурава континуирано праћење и унапређивање система информационе безбедности.

ЈКП „Паркинг сервис“, Београд је Правилником о унутрашњој организацији и систематизацији послова (у даљем тексту: Правилник о систематизацији) одредио две службе задужене за аспекте информационе безбедности у предузећу: Служба за информационе технологије и Служба за заједничке послове – Одељење за развој паркирања и управљање аутоматским паркинг системима. У оквиру Службе за информационе технологије систематизовано је 18 радних места са 38 извршилаца у два одељења. Тренутно је запослено 26 лица. У оквиру Одељења за развој паркирања и управљање аутоматским паркинг системима систематизовано је 9 радних места са 25

извршилаца. Тренутно је запослено 17 лица. У наставку су дати називи радног места, као и информација о попуњености радних места из области информационих технологија и безбедности:

Табела број 2. Систематизована и попуњена радна места у Служби за информационе технологије и Одељењу за развој паркирања и управљање аутоматским паркинг системима

Назив радног места	Број систематизованих места	Број запослених лица
Служба за информационе технологије		
Руководилац Службе за информационе технологије	1	1
Извршни руководилац Службе за информационе технологије	1	1
Координатор за послове унапређења информационог система	1	-
Главни организатор информационогсистема	1	1
Стручни сарадник за правне послове из области информационих технологија	1	1
Пословни секретар у служби	1	1
Одељење за информатику		
Шеф одељења за информатику	1	-
Систем инжењер	2	2
Главни администратор база података	1	1
Администратор за апликативни развој и подршку информационом систему	2	2
Пословођа информационих технологија	1	-
Организатор информационог система	1	1
Систем администратор и администратор базе података	5	4
Техничар информатичке опреме	5	4
Одељење Контролно-оперативни центар (КОЦ)		
Шеф одељења контролно-оперативног центра (КОЦ)	1	-
Главни администратор контролно-оперативног центра (КОЦ)	2	2
Администратор контролно-оперативног центра (КОЦ)	5	1
Техничар одељења контролно-оперативног центра (КОЦ)	6	4
Служба за заједничке послове – Одељење за развој паркирања и управљање аутоматским паркинг системима		
Шеф одељења за развој паркирања и управљања аутоматским паркинг системима	1	1
Водећи стручни сарадник одељења	1	-
Инжењер развоја и унапређења стационарног саобраћаја	2	1
Главни администратор аутоматских система	1	1
Организатор реализације пројеката и активности развоја	1	-
Организатор послова аутоматских система	2	2
Администратор аутоматских система	3	3
Водећи техничар аутоматских система	4	2
Техничар аутоматских система	10	7

Пословима информационе безбедности се у највећој мери баве запослени из Службе за информационе технологије. Запослени на радном месту Систем

администратор и администратор база података имају кључну улогу у одржавању безбедности ИКТ система. Њихове дужности укључују свакодневну контролу приступа ресурсима система и проверавају да ли се врше приступи са непознатих уређаја. Они су такође одговорни за подешавање приватних уређаја који приступају систему, за бекап података са уређаја пре слања на сервис, као и за одржавање система за спречавање упада у ИКТ систем са интернета. Систем администратор и администратор база података редовно ажурирају и подешавају системску опрему, врше анализу активности у циљу идентификације слабости система и усклађују корисничке налоге у складу са променама радних места и привилегија корисника.

Стручни сарадник за правне послове из области информационих технологија системски прати прописе, судску праксу и стручну литературу, са посебним освртом на прописе о информационој безбедности, приватном обезбеђењу и заштити података о личности, стара се о њиховој примени, припрема извештаје о стању у овој области и редовно извештава извршног руководиоца и руководиоца Службе за ИТ; такође, учествује у сачињавању упутстава о раду запослених, процедура и других аката из делокруга свог рада и рада Службе за ИТ, проверавајући њихову усклађеност са Законом о информационој безбедности, Законом о приватном обезбеђењу и Законом о заштити података о личности.

Запослени из Службе за информационе технологије редовно учествују на семинарима и саветовањима како би се упознали са најновијим трендовима и праксама у области информационих технологија и безбедности. Поред тога, у оквиру предузећа се организују и интерне обуке, где запослени стичу нова знања и унапређују своје вештине кроз размену искустава и интерне едукације, што доприноси сталном развоју и побољшању ефикасности рада ИТ службе.

Чланом 32 Правилника о безбедности ИКТ система је предвиђено да у случају било каквог инцидента који би могао угрозити безбедност ресурса ИКТ система, запослени-корисник има обавезу да одмах обавести Систем администратора и администратора база података из Службе за информационе технологије или главног администратора аутоматских система из Службе за заједничке послове, Одељења за развој паркирања и управљања аутоматским паркинг системима. Након пријема пријаве, запослени су дужни да одмах обавесте надлежне руководиоце и администратора ИКТ система, који ће у складу са Правилником о безбедности ИКТ система предузети потребне мере како би заштитили ИКТ ресурсе и спречили даље угрожавање система.

ЈКП „Паркинг сервис“, Београд је дана 31. јула 2020. године донело процедуру Управљање инцидентима нарушавања безбедности информација из домена Службе за ИТ, а последњи пут ју је ажурирало 13. септембра 2023. године. Овом процедуром дефинишу се активности управљања инцидентима нарушавања безбедности информација, техничким рањивостима и слабостима ИТ система у домену Службе за ИТ, са циљем ефикасног одзива и минимизирања ризика. Процедура укључује дефинисање шта се сматра инцидентом нарушавања безбедности, формирање тима за одзив на инциденте, као и систем за пријављивање, евидентирање, прикупљање података и решавање инцидената. При томе, велики акценат ставља се на прикупљање и чување доказа, што омогућава дубљу анализу и учење из претходних инцидената, као и периодично извештавање о инцидентима који су утицали на процену ризика у оквиру ИТ система. Централизован систем за управљање инцидентима у оквиру ISMS-а осигурава да сваки инцидент буде адекватно пријављен, анализиран и решен, уз стално праћење ефикасности примењених безбедносних мера. Имплементација различитих контрола, у складу са ISO/IEC 27001 стандардом, омогућава ЈКП „Паркинг сервис“,

Београд да смањи ризик по ИКТ системе и заштићене податке, обезбеђујући континуирану безбедност и интегритет пословних процеса.

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[17].

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 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

[17] IT Audit Handbook

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: ЈКП „Паркинг сервис“, Београд је успоставило мере физичке заштите и контроле логичког приступа системима, чиме је обезбеђена заштита ИКТ ресурса

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

Чланом 13 Правилника о безбедности ИКТ система дефинисана су ограничења приступа подацима и средствима за обраду података. Приступ ресурсима ИКТ система

је строго дефинисан врстом корисничког налога који запослени поседује. Администраторски налог омогућава пун приступ свим ресурсима система у сврху инсталације, одржавања и управљања, док кориснички налог даје ограничена права искључиво за коришћење додељеног профила. Запосленима је забрањено да деле своје корисничке податке са другим лицима, осим са администраторима у случајевима подешавања. Сви корисници ИКТ система су у обавези да поштују прописане мере безбедности, као што су коришћење ресурса искључиво у пословне сврхе, заштита поверљивих података и лозинки, као и редовно архивирање података у складу са утврђеним процедурама. Додатно, запослени морају осигурати да се сви приступи информационим ресурсима одвијају на основу експлицитно додељених права, те да се користе техничке мере сигурности, попут антивирусних програма и заштитних зидова (firewall), како би се спречиле потенцијалне претње по систем.

Чланом 14 Правилника о безбедности ИКТ система дефинисано је одобравање овлашћеног и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа. Право приступа ресурсима ИКТ система у Предузећу имају искључиво запослени који поседују администраторске или корисничке налоге. Администраторски налог омогућава пун приступ и управљање свим ИКТ ресурсима, укључујући сервере, мрежну инфраструктуру и техничке системе, док је његова употреба ограничена на запослене у одређеним улогама као што су систем администратори, администратори база података и техничари из контролно-оперативног центра (КОЦ), као и на трећа лица која имају уговорно дефинисана права приступа. Кориснички налог, који се састоји од корисничког имена и лозинке, додељује се на основу захтева одељења за људске ресурсе и омогућава запосленима приступ ресурсима неопходним за обављање њихових радних задатака. Администратори воде евиденцију о свим корисничким налозима, контролишу њихово коришћење, мењају права приступа и по потреби укидају налоге у складу са захтевима.

Процедуром Безбедоносне политике и поступци за администраторе ИТ система у Служби за ИТ детаљно је описано поступање приликом доделе права приступа, промене и укидање права коришћења информационе имовине. Политика контроле приступа информационој имовини поставља јасне смернице за доделу, промену и укидање права приступа у складу са пословним потребама и безбедносним захтевима. Процес доделе права приступа почиње одобрењем захтева за доделу приступа ИТ систему, након чега се отвара кориснички налог и евидентира у Регистру приступних права. Сваком кориснику се додељује јединствено корисничко име, осим у посебним случајевима када су одобрени групни налози из пословних разлога. Сви кориснички налози и права се редовно преиспитују како би се осигурало да одговарају актуелним потребама радних задатака. Приликом промене радног места или задатка, права приступа се ревидирају и прилагођавају новим обавезама запосленог. У случају раскида радног односа, приступни подаци и права се одмах укидају како би се спречио неовлашћени приступ информационој имовини предузећа. Систем је такође подешен тако да бележи све неуспешне покушаје пријављивања и ограничава број дозвољених покушаја, како би се спречиле злоупотребе. Редовна ревизија приступних права и активности корисника обезбеђује висок ниво безбедности и контроле над приступом информационим ресурсима.

Чланом 17 Правилника о безбедности ИКТ система уређена је физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему. Простор у коме се налазе сервери, мрежна и комуникациона опрема ИКТ система организован је као административна зона са контролисаним приступом. Ова зона је физички обезбеђена механичком бравом и/или

електронском контролом приступа, уз видљиво означавање. Простор је заштићен од компромитујућег електромагнетног зрачења (КЕМП), пожара и других елементарних непогода, а такође је климатизован ради одржавања одговарајуће температуре. Сервер је заштићен УПС уређајима, а додатну сигурност обезбеђују два агрегата за напајање, што осигурава континуиран рад у случају нестанка електричне енергије. Евиденција о уласку у административну зону води се у Служби за информационе технологије и Одељењу за развој паркирања и управљање аутоматским паркинг системима у оквиру Службе за заједничке послове.

Чување података о догађајима који могу бити од значаја за безбедност ИКТ система регулисано је чланом 22 Правилника о безбедности ИКТ система. Активности администратора и запослених-корисника у ИКТ систему прате се кроз дневнике активности као што су activitylog, history, securitylog, и transactionlog. Сваког последњег радног дана у недељи, ови дневници се архивирају у складу са процедуром за израду резервних копија података, према члану 20 Правилника. Систем администратор и администратор база података су дужни да најмање једном месечно, или по потреби чешће, врше анализу ових дневника како би идентификовали потенцијалне слабости у ИКТ систему.

Чланом 7 Правилника о безбедности ИКТ система прописана су поступања у вези безбедности рада на даљину и употребе мобилних уређаја. Наведено је да је приступ ресурсима ИКТ система за нерегистроване кориснике омогућен само за делове мреже који су конфигурисани за приступ Интернету, док је приступ службеној мрежи забрањен. Запослени који користе мобилне уређаје у власништву предузећа могу приступати ресурсима ИКТ система само у оквиру својих радних задатака, уз писану сагласност руководиоца Службе за информационе технологије. Мобилни уређаји морају бити подешени са VPN мрежом и заштитним софтвером како би се осигурала безбедност приступа. Запосленима је забрањено самостално инсталирање софтвера, као и уступање уређаја трећим лицима. Систем администратори и администратори база података свакодневно контролишу приступ и евидентирају уређаје, док је приступ са приватних уређаја дозвољен само уз одобрење и под строгим условима.

Рад са удаљености је уређен одељком 6.14. процедуре Безбедоносне политике и поступци за администраторе ИТ система у Служби за ИТ. Рад са удаљености представља осетљиву категорију приступа, која захтева пажљиву контролу. Администратори приступа морају редовно проверавати и управљати додељеним правима, нарочито након измена система или промена у особљу. Неактивне сесије морају бити прекинуте након 15 минута ради безбедности. Ако је неопходно, аутсорсинг партнерима се може дозволити удаљени приступ уз строго ограничене ресурсе и одобрење руководства, уз обавезу евидентирања свих активности. Физичка и комуникациона безбедност морају бити приоритет при раду са удаљености, а приватни уређаји морају бити контролисани и осигурани. Овлашћења и права приступа се укидају чим више нису потребна. Контрола мрежних активности спроводи се преко „Firewall“ и „Proxy“ сервера, осигуравајући безбедан приступ интернету и интерним системима.

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 раздвајања 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: ЈКП „Паркинг сервис“, Београд није у потпуности успоставило мере за континуитет пословања и заштиту података у ванредним околностима

Иако је предузеће предузело значајне кораке ка континуитету пословања, укључујући процедуре за премештање кључних делова ИКТ система и редовно прављење резервних копија, утврђено је да планови за критичне сценарије, попут прекида напајања или квара на кључним компонентама система, нису у потпуности развијени. Недостају детаљне процедуре за брз и ефикасан опоравак система у ванредним ситуацијама, што представља ризик за континуитет пословања и правовремени опоравак од инцидената.

Додатно, предузеће нема јасно дефинисане планове за сценарије који укључују хитне случајеве попут поплава или пожара, и није развило комплетан план континуитета који обухвата све неопходне процедуре и контроле. Овај недостатак оставља простор за могуће прекиде у функционисању у случају већих инцидената, као и повећава ризик за интегритет и безбедност података.

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

Чланом 33 Правилника о безбедности ИКТ система, ЈКП „Паркинг сервис“, Београд је прописао мере које обезбеђују континуитет обављања посла у ванредним околностима. У случају ванредних околности које могу захтевати премештање ИКТ система из просторија предузећа, Служба за информационе технологије и Служба за заједничке послове, посебно Одељење за развој паркирања и управљање аутоматским паркинг системима, имају обавезу да у најкраћем року обезбеде пренос кључних делова ИКТ система на резервну локацију или активирају редундантне компоненте ако постоје. Овај процес се спроводи у складу са планом реаговања у ванредним и кризним ситуацијама. Спецификација неопходних делова система за функционисање у таквим ситуацијама израђује се у три примерка од стране шефова Службе за информационе технологије и Одељења за развој паркирања, при чему се један примерак чува код запосленог, други код лица задуженог за послове одбране и ванредних ситуација, а трећи код руководиоца службе. Делови система који нису неопходни за рад у ванредним ситуацијама складиште се на резервној локацији коју одређују руководиоци релевантних служби. Процес складиштења мора бити организован тако да опрема буде безбедна, обележена и евидентирана у складу са важећим процедурама.

ЈКП „Паркинг сервис“, Београд је дана 31. јула 2020. године донео процедуру Израда плана пословног континуитета из домена Службе за ИТ, а последњи пут ју је ажурирало 13. септембра 2023. године. План континуитета пословања (BCP) из домена службе за ИТ има кључну улогу у обезбеђивању непрекидне испоруке производа и услуга организације, чак и у случају значајног прекида ИТ функција, као што су прекиди у напајању, комуникационим линковима или кључним сервисима. Овај план, заснован на процени претњи и ризика, идентификује критичне ресурсе, претње и рањивости, и предлаже мере које имају за циљ спречавање озбиљних прекида у раду. Кроз активности као што су израда, покретање, преиспитивање и одржавање плана, обезбеђује се спремност предузећа за брз и ефикасан опоравак ИТ функција. Тим за одзив на инциденте и опоравак игра кључну улогу у имплементацији превентивних мера, као и у брзом реаговању на инциденте, чиме се минимизирају оперативни поремећаји. План такође садржи важне процедуре које служе као водич за опоравак критичних система, указује на локације кључних података и ресурса, и обезбеђује комуникацију са добављачима и корисницима у случају прекида. Поред тога, документује алтернативне изворе за набавку добара и ресурса, као и процедуре за архивирање и чување важних записа, чиме осигурава несметан опоравак пословних активности.

Процедура предвиђа развијање планова за следеће сценарије прекида ИТ функција:

- Прекид снабдевања електричном енергијом;
- Прекид рада услед поплаве;
- Прекид рада услед пожара;
- Прекид приступа интернету на главном оптичком линку;
- Прекид рада/квар на серверу са подацима и сервисима;
- Прекид рада/квар на главном рутеру за интернет;
- Прекид рада/квар на једном од два мрежна свича;

- Прекид рада/квар на УПС уређају;
- Прекид рада/квар на агрегату.

Међутим, планови континуитета за наведене сценарије још увек нису развијени.

Заштита од губитка података и израда резервних копија је предвиђена чланом 21 Правилника о безбедности ИКТ система. Чување резервних копија података у предузећу је организовано кроз редовне процедуре архивирања на преносиве медије (CD-ROM, DVD, USB, екстерни хард диск), које се обављају на дневном, недељном, месечном и годишњем нивоу, у циљу осигурања обнове података у случају потребе. Дневне копије се креирају сваког радног дана у 20 часова, док се недељне израђују последњег радног дана у недељи. Месечне и годишње копије настају последњег радног дана у месецу, односно у години. Годишње копије се чувају у два примерка – један у просторији предвиђеној за архивирање дневних и недељних копија, а други у дислоцираном, обезбеђеном објекту. Исправност резервних копија проверава се сваких шест месеци, осигуравајући да су подаци исправни и спремни за употребу. Одговорна лица из ЈКП „Паркинг сервис“, Београд су нам потврдила да су резервне копије смештене у безбедан простор за одлагање ван објекта.

У поглављу 6.8. Израда резервних копија („backup“ процедуре) за телекомуникационе системе из домена службе за ИТ у оквиру процедуре Безбедоносне политике и поступци за администраторе ИТ система у Служби за ИТ наведено је да се резервне копије информација и софтвера редовно израђују, испитују и проверавају у складу са Упуством за израду резервних копија службе за ИТ, а користе се за опоравак система у складу са процедуром за израду плана пословног континуитета службе за ИТ.

Препоручујемо ЈКП „Паркинг сервис“, Београд да развије и имплементира планове континуитета за све критичне сценарије прекида ИТ функција како би се осигурао несметан опоравак у ванредним ситуацијама.

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: ЈКП „Паркинг сервис“, Београд је унапредио управљање ризицима у ИКТ систему допуном Правилника о систематизацији послова

ЈКП „Паркинг сервис“, Београд је побољшао управљање ризицима у ИКТ систему допуном Правилника о систематизацији послова. Првобитно, Правилник о систематизацији није обухватао прецизно дефинисана радна места и дужности у области превенције и управљања безбедносним ризицима, што је могло довести до нејасноћа у одговорностима и повећаног ризика од безбедносних пропуста. Иако су неке активности, попут надзора комуникационих мрежа, биле део општих задатака, недостатак експлицитних улога у овој области угрозио је поузданост ИКТ система.

Током поступка ревизије, ЈКП „Паркинг сервис“, Београд је, 28. октобра 2024. године, ажурирало Правилник о систематизацији, утврђујући да је руководилац Службе за ИТ одговоран за успостављање и примену мера за процену ризика, док су извршни руководилац службе и други одговорни запослени задужени за спровођење мера безбедности. Овим изменама је

обезбеђена јаснија подела одговорности и унапређена ефикасност у управљању ризицима, чиме је значајно побољшана информациона безбедност.

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

У опису послова у Служби за информационе технологије ниједно радно место није експлицитно задужено за послове превенције и заштите од безбедносних ризика у ИКТ систему. Иако су неке дужности, попут управљања системима заштите и надзора комуникационих мрежа, наведене као делови општих задатака, не постоји посебно дефинисано радно место или специфичне дужности које би се искључиво односиле на превенцију и управљање безбедносним ризицима у ИКТ систему. Овај недостатак може утицати на ефикасност управљања безбедношћу информационог система и захтева додатно прецизирање у Правилнику о систематизацији.

Чланом 6 Правилника о безбедности ИКТ система наведено је између осталог да се под пословима из области безбедности ресурса ИКТ система сматрају и послови управљања ризицима у области информационе безбедности, као и послови предвиђени процедурама у области информационе безбедности.

ЈКП „Паркинг сервис“, Београд је дана 31. јула 2020. године донело процедуру Управљање ризицима по безбедност информација из домена Службе за ИТ, а последњи пут ју је ажурирало 13. септембра 2023. године. Овом процедуром се дефинишу одговорности и методологија за процену ризика по безбедност информација у оквиру Службе за ИТ, као и неопходни процеси за управљање тим ризицима у складу са захтевима стандарда ISO/IEC 27001. Управљање ризицима по информациону безбедност обухвата: идентификацију информационе имовине и њених власника, процену вредности те имовине, идентификацију потенцијалних претњи и рањивости, као и утврђивање вероватноће појаве тих претњи и њиховог утицаја на безбедност. На основу ових анализа, израчунава се ниво ризика пре и после примене мера заштите, а руководство доноси одлуке о прихватљивом нивоу ризика. Процес укључује и третман ризика кроз избор адекватних мера заштите, израду Изјаве о применљивости, као и континуирани надзор, преиспитивање и унапређивање управљања ризицима ради осигурања потпуне безбедности информација.

Из ове процедуре произлазе следећи записи:

1) Регистар информацине имовине, електронска форма;
2) Регистар ризика, електронска форма;
3) План поступања са ризицима, електронска форма;
4) Изјава о применљивости (SoA), електронска форма.

За успостављање, примену и одржавање ове процедуре одговоран је руководилац Службе за информационе технологије, а њену реализацију спроводе извршни руководилац службе, координатор за послове унапређења информационог система, шеф одељења за информатику, шеф контролно оперативног центра и главни организатор информационог система, међутим ове дужности нису наведене у Правилнику о систематизацији.

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.

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: Механизам сарадње са корисницима система је успостављен, обезбеђујући основну сигурност и заштиту података, а субјект ревизије је у току ревизије донео процедуру за архивирање, миграцију и уништавање података која омогућава континуитет пословања и безбедан повраћај података у случају раскида сарадње

Циљ овог дела извештаја био је да оцени степен до којег је ЈКП „Паркинг сервис“, Београд успоставио 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.

ЈКП „Паркинг сервис“, Београд на дан објављивања извештаја о ревизији, заједно са предузећем „Прокомсофт“ доо из Новог Сада, пружа услуге система за контролу и наплату паркирања путем мобилног видео надзора код два јавно комунална предузећа на територији Републике Србије. Та јавно комунална предузећа су:

1) Јавно комунално предузеће „Паркинг сервис“, Ниш;
2) Комунално јавно предузеће „Златибор“, Чајетина.

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 је правилницима, процедурама и физичком заштитом обезбедио 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 је усвојио скуп документа – правилнике, процедуре и упутства којима се уређује безбедност података ИКТ система и то:

- Правилник о безбедности ИКТ система;
- Управљање ризицима по безбедност информација из домена Службе за ИТ;
- Безбедносне политике и поступци за администраторе ИТ система у Служби за ИТ;
- Безбедносне политике и поступци за кориснике ИТ система у домену Службе за ИТ;
- Управљање инцидентима нарушавања безбедности информација из домена Службе за ИТ.

ЈКП „Паркинг сервис“, Београд је обезбедио физичку заштиту објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему. Простор у коме се налазе сервери, мрежна и комуникациона опрема ИКТ система организован је као административна зона са контролисаним приступом. Ова зона је физички обезбеђена механичком бравом и електронском контролом приступа, уз видљиво означавање. Простор је заштићен од компромитујућег електромагнетног зрачења (КЕМП), пожара и других елементарних непогода, а такође је климатизован ради одржавања одговарајуће температуре. Сервер је заштићен УПС уређајима, а додатну сигурност обезбеђују два агрегата за напајање, што осигурава континуиран рад у случају нестанка електричне енергије. Евиденција о уласку у административну зону води се у Служби за информационе технологије и Одељењу за развој паркирања и управљање аутоматским паркинг системима у оквиру Службе за заједничке послове.

Чување резервних копија како својих, тако и података корисника услуга у предузећу је организовано кроз редовне процедуре архивирања на преносиве медије (CD-ROM, DVD, USB, екстерни хард диск), које се обављају на дневном, недељном, месечном и годишњем нивоу, у циљу осигурања обнове података у случају потребе. Дневне копије се креирају сваког радног дана у 20 часова, док се недељне израђују последњег радног дана у недељи. Месечне и годишње копије настају последњег радног дана у месецу, односно у години. Годишње копије се чувају у два примерка – један у просторији предвиђеној за архивирање дневних и недељних копија, а други у дислоцираном, обезбеђеном објекту[18]. Исправност резервних копија проверава се сваких шест месеци, осигуравајући да су подаци исправни и спремни за употребу. Одговорна лица из ЈКП „Паркинг сервис“, Београд су нам потврдила да су резервне копије смештене у безбедан простор за одлагање ван објекта.

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.

[18] Члан 21 Правилника о безбедности ИКТ система.

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

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

У члану 11 Правилника о безбедности информационо-комуникационог система ЈКП „Паркинг сервис“, Београд наводи се да подаци у ИКТ систему предузећа могу бити означени као тајни у складу са Законом о заштити података о личности, Законом о тајности података и другим релевантним прописима. Овакви подаци морају бити заштићени у складу са Законом о тајности података и Правилником о пословној тајни предузећа. Члан 43 наглашава да се обрада података о личности врши у складу са Законом о заштити података о личности и Правилником о заштити података о личности предузећа, уз поштовање начела интегритета и поверљивости.

У систему заштите података о личности у ЈКП „Паркинг сервис“, Београд, јасно су дефинисане улоге руковаоца, обрађивача и подобрађивача података, што омогућава прецизно управљање и одговорност у процесу обраде података о личности. ЈКП „Паркинг сервис“, Београд је постављен као обрађивач података, док је корисник услуга, који користи услуге овог система, дефинисан као руковалац података. Поред тога, компанија „Prokomsoft“ д.о.о. је ангажована као подобрађивач, задужена за специфичне аспекте обраде података у складу са уговореним обавезама. Ова структура омогућава управљање безбедношћу података, при чему се свака страна придржава јасно дефинисаних обавеза и процедура које се односе на заштиту података о личности.

Корисник услуга, као руковалац, дефинише сврху и начин обраде података, док је ЈКП „Паркинг сервис“ Београд одговоран за извршење тих активности у складу са уговором и правним оквиром који регулише заштиту података о личности.

Сарадња између ових субјеката регулисана је кроз стандардне уговорне клаузуле (СУК), као и путем додатних уговора и овлашћења за ангажовање подобрађивача. Ови документи садрже све потребне мере које обрађивач мора да спроведе у складу са налозима руковаоца, обезбеђујући усклађеност са Законом о заштити података о личности и правилном обрадом података. Уговори обавезују обрађивача да прати активности подобрађивача, посебно у делу који се односи на безбедност података, како би се осигурала контрола и одржала поверљивост.

Документи попут овлашћења за ангажовање подобрађивача, процене ризика и изјава о поверљивости детаљно дефинишу одговорности свих страна у погледу заштите података о личности. Овлашћења за ангажовање подобрађивача прецизирају на који начин обрађивач може ангажовати треће стране у процесу обраде података, уз обавезу да све активности буду усклађене са налозима руковаоца и важећим правним прописима.

Овај документ такође обухвата контролне механизме којима руковалац осигурава да се сви стандарди безбедности одржавају на највишем нивоу.

Процена ризика је кључни документ који предвиђа потенцијалне претње и рањивости у процесу обраде података, као и мере за смањење тих ризика. Овај документ је од великог значаја јер омогућава свим учесницима да благовремено идентификују и реагују на безбедносне ризике, чиме се смањује вероватноћа повреде података.

Изјаве о поверљивости обавезују све стране да информације које обрађују или имају на располагању третирају као поверљиве, уз посебан фокус на заштиту од неовлашћеног приступа и злоупотребе. Ови документи дефинишу детаљне процедуре у случају да дође до повреде података, укључујући обавештавање надлежних органа и руковаоца, предузимање корективних мера и спровођење додатних безбедносних провера како би се спречило поновно угрожавање података.

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 на који начин би обезбедио архивирање података, уништавање или повраћај података у случају да корисник система промени пружаоца услуга

ЈКП „Паркинг сервис“, Београд није дефинисао адекватне процедуре које би осигурале неометано пословање корисника у случају раскида или истека сарадње, укључујући процедуре за архивирање, миграцију и уништавање података корисника. Уговори са корисницима услуга не садрже одредбе које би омогућиле сигурно извршавање процеса повраћаја или уништавања података у складу са релевантним стандардима и прописима (као што су ISO/IEC 27001, ISO/IEC 27018 и GDPR), чиме се ствара ризик за безбедност и интегритет података корисника. Дефинисан је отказни рок од 60 дана, али активности попут извоза података или преноса криптографских кључева нису прописане, што доводи до могућности прекида у функционисању корисничких система након истека сарадње. Поред тога, недостатак јасних процедура за архивирање и уништавање података оставља простор за неовлашћени приступ или нарушавање интегритета података.

У циљу смањења ових ризика, директор ЈКП „Паркинг сервис“, Београд је дана 14. новембра 2024. године одобрио процедуру „Предаја и брисање података са сервера услед престанка уговорних обавеза“ (ПС.П64). Новом процедуром дефинисани су јасни кораци за извоз података, пренос криптографских кључева и пружање техничке подршке у прелазном периоду, као и обавеза трајног уништавања података након истека сарадње. Ове активности су праћене строгим техничким и организационим мерама за осигурање поверљивости, интегритета и усклађености са важећим прописима. Увођењем ове мере, ризици за безбедност и интегритет података корисника су значајно смањени, а континуитет у пословању корисничких система обезбеђен.

ЈКП „Паркинг сервис“, Београд је, на иницијативу и засновано на процедури „Предаја и брисање података са сервера услед престанка уговорних обавеза“ од 14. новембра 2024. године, обезбедио да корисници њихових услуга успоставе процедуре за примопредају и брисање података у случају раскида или истека уговора. Ове процедуре су постале саставни део уговора за набавку система за контролу и наплату паркирања путем мобилног видео надзора, чиме је значајно унапређена усклађеност са стандардима и смањени ризици за безбедност и интегритет података корисника.

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

ЈКП „Паркинг сервис“, Београд није дефинисао адекватне процедуре или механизме који би осигурали неометано пословање својих корисника у случају раскида или истека сарадње. У случају прекида сарадње са корисницима услуга, не постоје прописане активности које би омогућиле корисницима да наставе са радом без прекида. Овај недостатак односи се на изостанак процедура за извоз података, пренос

криптографских кључева, као и на могућност пружања техничке подршке у прелазном периоду док корисници не пронађу новог пружаоца услуга. Такође, не постоји правилник ни процедура о архивирању података или уништавању истих у случају да корисник система промени пружаоца услуга. ЈКП „Паркинг сервис“, Београд исте податке чува иако је он обрађивач података, а не руковалац.

У уговорима са корисницима софтвера за наплату и контролу паркирања чланом 14 је дефинисано да је у случају раскида сарадња отказни рок 60 дана, у којем су оба уговарача дужна да извршавају своје уговорене обавезе до истека отказног рока, тако да је ЈКП „Паркинг сервис“, Београд омогућило пружање техничке подршке у прелазном периоду док корисници не пронађу новог пружаоца услуга. Али у уговору нису дефинисане активности за извоз података (миграција података) и пренос криптографских кључева.

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.

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.

Ове мере унапређују усклађеност са релевантним стандардима и прописима (попут ISO/IEC 27001, ISO/IEC 27018 и GDPR) и минимизују ризик за безбедност и интегритет података корисника, истовремено осигуравајући континуитет пословања и заштиту података у случају раскида или истека уговора.

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: Успостављене апликативне контроле обезбеђују ажурну евиденцију и контролу наплате услуга, али и боље информисање грађана кроз употребу мобилне апликације и отворених података, чиме се значајно унапређује транспарентност и доступност информација

Циљ овог дела извештаја био је да оцени у којој мери успостављене апликативне контроле обезбеђују ефикасну контролу наплате и тачност пружених услуга у ЈКП „Паркинг сервис“, Београд. 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 3.1: ЈКП „Паркинг сервис“, Београд је унапредио апликативне контроле и ограничио приступ осетљивим подацима након утврђених недостатака

ЈКП „Паркинг сервис“, Београд је развио информациони систем Scan Car за наплату и контролу услуга паркинга, али у почетној фази ревизије утврђено је да систем нема успостављене апликативне контроле за управљање корисничким налозима и приступом осетљивим подацима. Током тестирања права корисника, установљено је да су запослени на позицијама благајника и шефа одељења имали неограничен приступ личним подацима грађана и могућност експорта података у xlsx формату, што није било у складу са њиховим радним обавезама. Такође, корисници са улогом у Call Centru имали су приступ осетљивим подацима, иако им је опис посла захтевао приступ само општим информацијама.

Међутим, након указивања на ове недостатке, ЈКП „Паркинг сервис“, Београд је брзо реаговао и предузео мере за унапређење апликативних контрола. Ограничен је приступ личним подацима за кориснике којима исти нису неопходни за обављање радних задатака, а могућност експорта података из табела у XLSX формат је укинута. Такође, уведена је измена у систему која онемогућава промену корисничког имена након његовог уноса, чиме се обезбеђује већа сигурност и интегритет података.

ЈКП „Паркинг сервис“, Београд, је развило информациони систем Scan Car који служи за наплату и контролу услуга паркинга у Београду. За приступ Scan Car потребна је VPN конекција у оквиру самог ЈКП „Паркинг сервис“, Београд, док је за приступ Scan Car код корисника услуга потребан сертификат који се обнавља сваке године.

ЈКП „Паркинг сервис“ Београд је успоставио процедуре и упутства за управљање пословним процесима који се користе за софтвер за наплату паркинга.

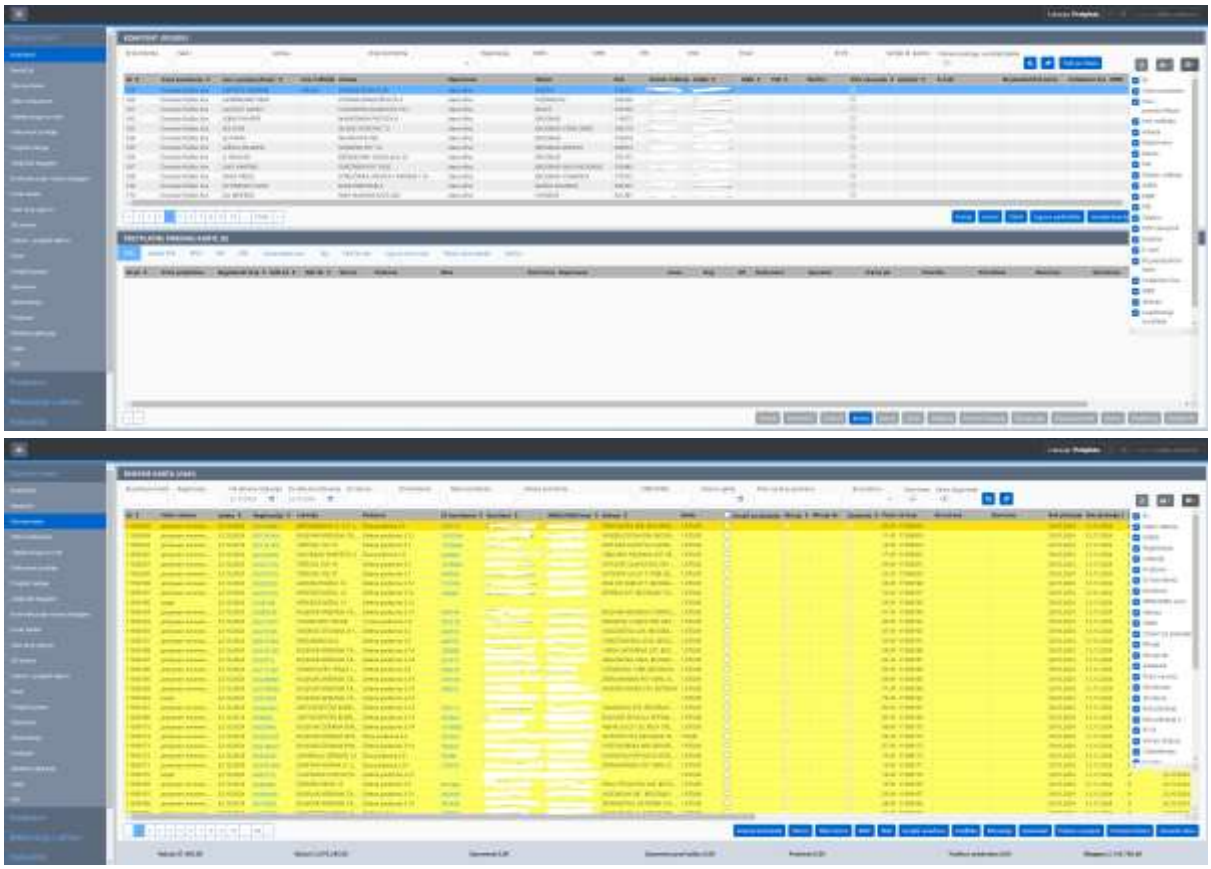
Иако постоје процедуре и упутства, није успостављен механизам апликативне контроле, јер смо у ревизији утврдили да не постоји контрола када је у питању

преименовање налога, па долази до губитка података унетих од стране претходног корисника.

У ревизији смо тестирали апликативну контролу права корисника система, а као налоге смо користили запослене на месту Благајника, Call Centar и шефа одељења.

Запослени ЈКП „Паркинг сервис“, Београду на месту Благајника и шефа одељења могу да види личне податке грађана, иако им по опису посла који обављају, исти нису потребни. Исте те податке могу да експортују у xlsx формату. USB портови на рачунарима су затворени и само по захтеву шефова одељења могу бити откључани.

Запослени ЈКП „Паркинг сервис“, Београд на месту Call Centar имају приступ осетљивим подацима иако би по опису посла требало да имају само опште информације за грађане када им се обрате, као што су: да ли је извршена наплата, да ли је возило на депоу и сл.



Слика 8. Виде се осетљиви подаци у информационом систему

Упутства за употребу апликација су доступна свим запосленима тако да су обезбедили примену правила и процедура за управљање корисничким налозима и приступом.

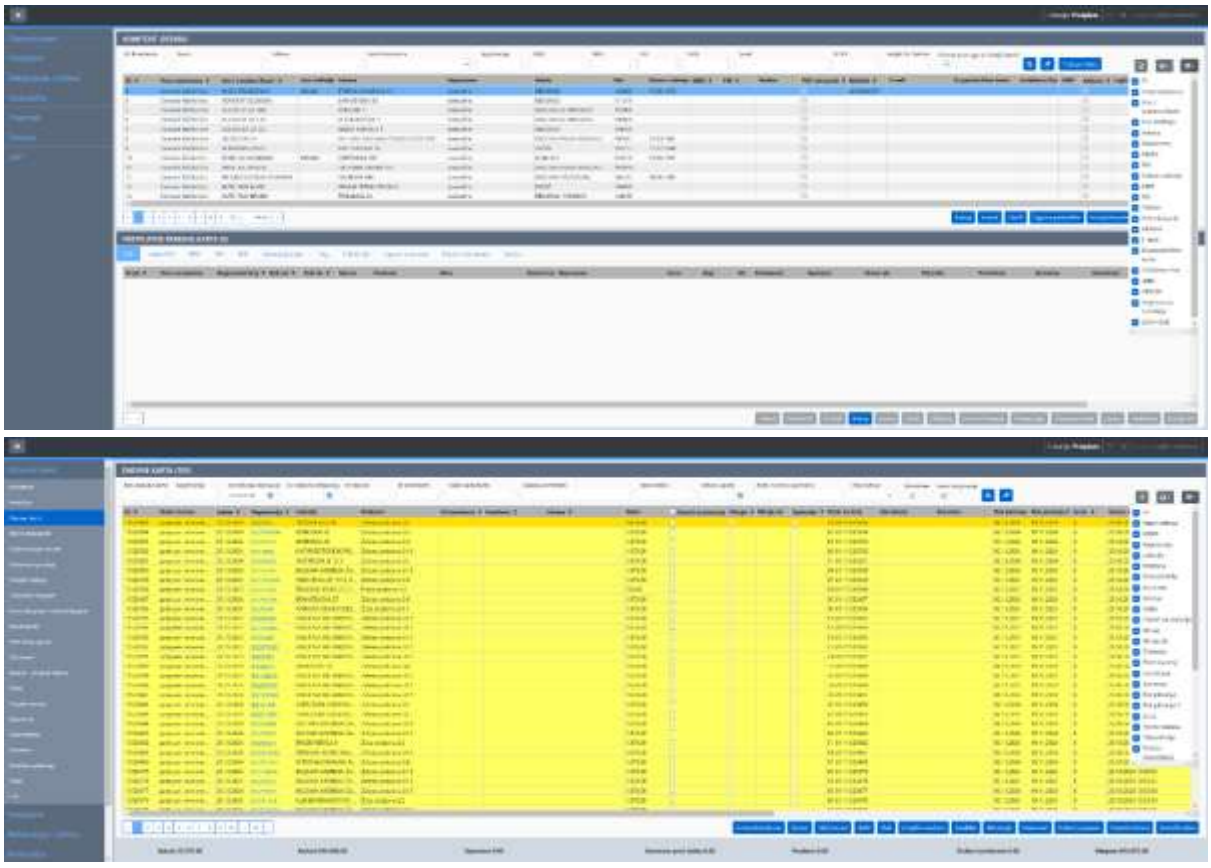
Управљање корисничким налозима у апликацији за наплату и контролу паркинг места требало би да обухвати успостављање јасних и дефинисаних процедура које регулишу сваки аспект управљања корисничким правима, приступом и деактивацијом налога. Процедуре би требало да укључе механизме за безбедно деактивирање 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.

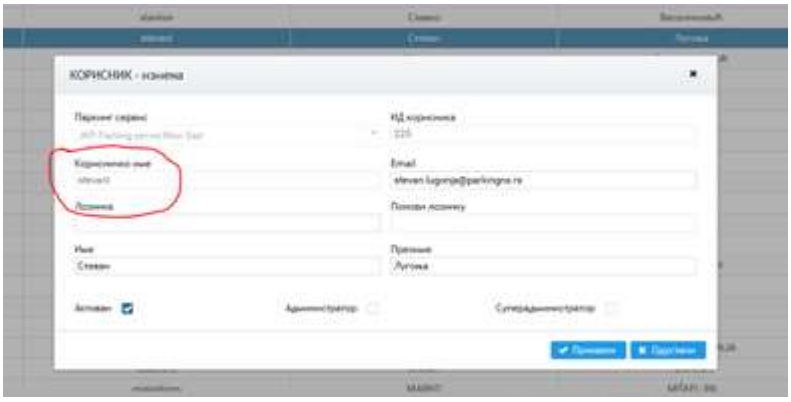
Након спроведене анализе и тестирања апликација од стране Државне ревизорске институције ЈКП „Паркинг сервис“, Београд је предузео следеће мере.

У Информационом систему укинули су 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.



Слика 9. Уклоњене колоне са осетљивим подацима који се налазе у информационом систему

У Back office апликацији за наплату и контролу паркирања укинута је могућност измене корисничког имена. Сада је при измени података username "бледо" и само приказано без могућности за изменом.



Слика 10. Онемогућено је брисање и измена Username у Back office апликацији

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 3.2: У ЈКП „Паркинг сервис“ Београд апликативне контроле које се користе за продају карата омогућавају ажурну евиденцију дневних пазара и броја продатих паркинг карата, као и извештавање

ЈКП „Паркинг сервис“ Београд продају карата врши у својим објектима (месечне карте), путем СМС порука (сатне карте) или преко мобилне апликације (плаћање паркирања СМС поруком, платном картицом или депозитом на самој апликацији), саму продају обављају запослени на тим пословима у предузећу, а апликативни софтвер се користи ради евиденције пазара, и прегледа броја карата по врстама.

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 3.3: ЈКП „Паркинг сервис“, Београд редовно ажурира податке о паркинг зонама, развило је мобилну апликацију и омогућило коришћење отворених података за боље информисање грађана

ЈКП „Паркинг сервис“ Београд редовно ажурира информације о паркинг зонама, ценама и могућностима плаћања на свом званичном сајту и путем мобилне апликације „Паркинг Сервис“, омогућено је коришћење отворених података тако да су корисници сајта и мобилне апликације информисани о доступности паркинг места у реалном времену.

ЈКП „Паркинг сервис“, Београд путем свог официјелног сајта[19] објављује обавештења о паркинг зонама, да ли је возило на депоу или је издата е-ППК, могућност плаћања и ценовник редовно ажурирају, што доводи до бољег управљања и информисања грађана. ЈКП „Паркинг сервис“ Београд је развио и мобилну апликацију[20] која олакшава начин плаћања као и пружање корисних информација грађанима. Такође је развијена и могућност наплате преко QR баркода, као на бензинским пумпама.

Што се тиче доступности паркинга она је омогућена преко инфо-табли које обавештавају возаче о броју слободних места како у оближњим јавним гаражама тако и у улицама. Доступност паркинга може се пратити и преко мобилне апликације у реалном времену.

Када је у питању употреба отворених података, како је наведено на Порталу отворених података[21]: „Отворени подаци су подаци у машински читљивом и отвореном облику доступни за поновну употребу. Подаци морају бити у облику који је погодан за рачунарску обраду, односно облику који омогућава лак приступ и манипулацију подацима помоћу рачунарских програма (машински читљиви). Подаци морају бити доступни у форматима записа чија је употреба могућа без плаћања накнаде или других ограничења, као и за чију обраду је доступан најмање један алат слободног софтвера (отворени облик).“

Отворени подаци могу укључивати информације и тренутна обавештења о паркинг зонама, доступности паркинга, ценама карата, могућност плаћања, привременој обустави паркинг места (услед реновирања улице), информације о томе која су паркинг места прилагођена инвалидима итд.

[19] https://www.parking-servis.co.rs/
[20] Мобилна апликација Паркинг Сервис
[21] https://data.gov.rs/sr/

Овако структуране податке могу користити и физичка и правна лица, за израду апликација, што може бити корисно нарочито код лица која не користе званичну апликацију градских предузећа или градских управа.

У граду Београду, омогућено је информисање путем стандардних апликација на мобилним утрећајима, као што је то Google Maps или слична.

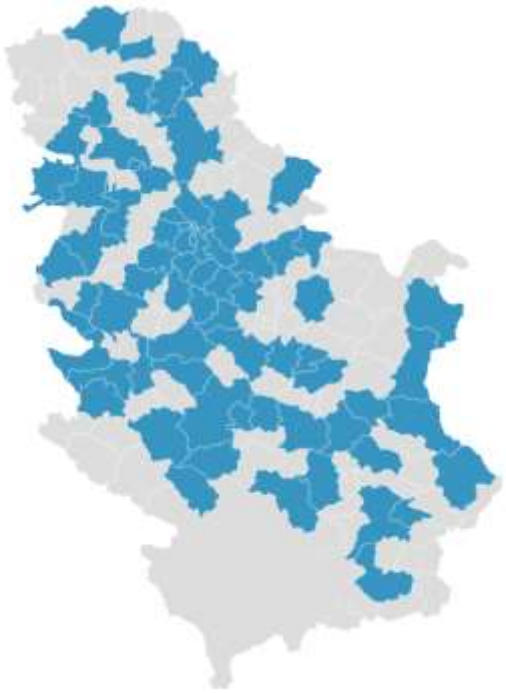
Јавна комунална предузећа треба да настоје да редовно ажурирају податке о паркинг зонама, ценама, доступности паркинг места и могућностима плаћања у реалном времену. Пожељно је да ти подаци буду доступни не само путем званичних веб сајтова, већ и у формату отворених података који омогућавају лакшу интеграцију 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

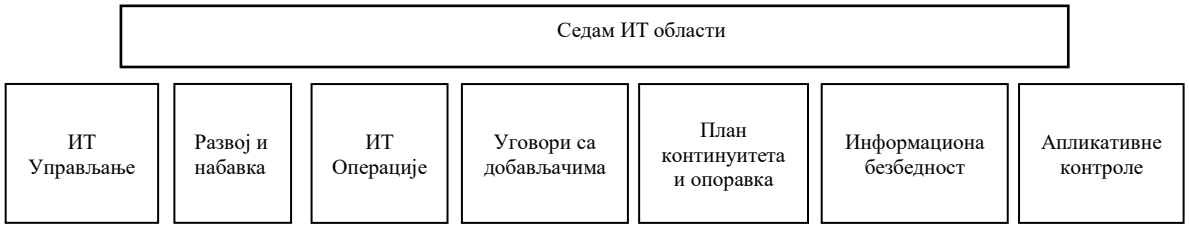
Прилог 1. Методологија у поступку рада

У току предстудије послали смо упитник[22] свим јединицама локалне самоуправе које на својој територији имају јавно предузеће које се бави наплатом услуга паркирања.



Слика 11. 61 ЈЛС које имају информациони систем прекога 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 12. 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.

[22] 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[23]:

- 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;

[23] 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.