ДРЖАВНА РЕВИЗОРСКА ИНСТИТУЦИЈА

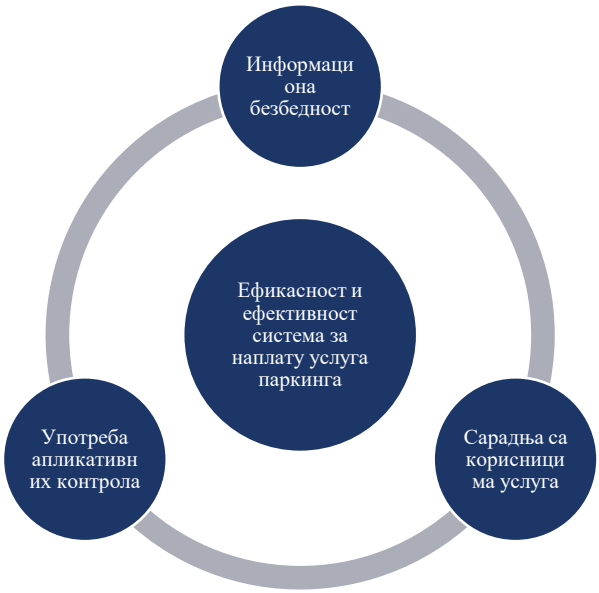
ИЗВЕШТАЈ
О РЕВИЗИЈИ СВРСИСХОДНОСТИ ПОСЛОВАЊА

Информациони систем за наплату услуга паркинга у Јавном комуналном предузећу „Паркинг сервис“, Нови Сад

Број: 400-1058/2024-07/35
Београд, 20. децембар 2024. године

ЈКП „Паркинг сервис“, Нови Сад је успоставило мере безбедности и ефикасне апликативне контроле за наплату услуга паркинга, али је потребно додатно унапредити процедуре за заштиту података својих корисника и интеграцију са стандардним апликацијама.

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, а обрада података о личности није уређена на адекватан начин, јер базе података могу садржати осетљиве личне податке корисника, што изискује примену додатних мера заштите.



Слика 1. Тема ревизије

Успостављене мере информационе безбедности обезбеђују основни ниво поузданости информационих система који се користе за наплату услуга паркинга, а субјект ревизије је ажурирао Правилник о безбедности ИКТ система и у потпуности обухватио специфичности система за контролу и наплату паркирања.

Механизам сарадње са корисницима система делимично је успостављен, због чега је потребно додатно унапредити процедуре које осигуравају поверљивост и поузданост података, као и механизме за миграцију и уништавање података у случају раскида сарадње.

Успостављене апликативне контроле обезбеђују ефикасну наплату и извештавање, али додатна унапређења су потребна у правцу интеграције са стандардним апликацијама и отвореним подацима ради побољшања корисничког искуства и доступности информација.

Препоруке

Након спроведене ревизије, Државна ревизорска институција је Јавном комуналном предузећу „Паркинг сервис“, Нови Сад, дала следеће препоруке:

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

Предузете мере

Током ревизије, ЈКП „Паркинг сервис“, Нови Сад је спровео низ значајних мера за унапређење информационе безбедности, управљања подацима и апликативних контрола, са циљем обезбеђивања сигурности и усклађености са законским и стандардним захтевима:

- Унапређен је Правилник о безбедности ИКТ система и успостављене процедуре за проверу и заштиту система.
- Закључени су уговори који регулишу пренос, брисање и поверљивост података.
- Унапређени су FRIP и SWAT системи са ограниченим приступом и бољом заштитом података.

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 „Паркинг сервис“, Нови Сад	ЈКП „Паркинг сервис“, Нови Сад
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 „Паркинг сервис“, Нови Сад 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 Новом Саду задужено је Јавно комунално предузеће „Паркинг сервис“ (у даљем тексту: ЈКП „Паркинг сервис“, Нови Сад). ЈКП „Паркинг сервис“, Нови Сад је само развило систем за управљање контролом и наплатом паркирања. Систем је имплементиран 2005. 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“, Нови Сад је успоставило мере безбедности и ефикасне апликативне контроле за наплату услуга паркинга, али је потребно додатно унапредити процедуре за заштиту података својих корисника и интеграцију са стандардним апликацијама.

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

1. Успостављене мере информационе безбедности обезбеђују основни ниво поузданости информационих система који се користе за наплату услуга паркинга, а субјект ревизије је ажурирао Правилник о безбедности ИКТ система и у потпуности обухватио специфичности система за контролу и наплату паркирања.
   - ЈКП „Паркинг сервис“, Нови Сад није у потпуности успоставило адекватан систем управљања информационом безбедношћу, нарочито у делу који се односи на специфичности система за контролу и наплату паркирања. Иако су постојећи акти и процедуре у доброј мери усклађени са основним принципима информационе безбедности, Правилник о безбедности ИКТ система није ажуриран тако да обухвати специфичне аспекте информационог система за контролу и наплату паркирања који је у употреби. Ово оставља простор за потенцијалне слабости у безбедности система, посебно у погледу заштите података и безбедносних мера које се

примењују у овом критичном делу ИКТ инфраструктуре. Ипак, у току поступка ревизије, ЈКП „Паркинг сервис“ Нови Сад је предузело кораке ка унапређењу свог система безбедности. Дана 1. октобра 2024. године, донета је Одлука о измени и допуни Правилника о безбедности ИКТ система којом је у члану 35 прецизирана улога Администратора ИКТ система од посебног значаја. Додатно, дана 14. новембра 2024. године, директор ЈКП „Паркинг сервис“, Нови Сад донео је нове измене и допуне Правилника о безбедности ИКТ система. Ове измене обухватиле су унапређење процедура за управљање СМС системом за наплату паркирања, укључујући мониторинг, прављење резервних копија података и одржавање ВПН веза. Такође, ФРИП књиговодствени софтвер и апликација SWAT добили су додатне безбедносне мере, које укључују ограничавање приступа на основу радних задатака и инсталацију безбедносних сертификата. Уведене су и процедуре за размену података са трећим лицима, са посебним акцентом на заштиту података о личности. Овим изменама значајно су побољшане мере заштите критичних подсистема, минимизовани ризици од безбедносних инцидената и обезбеђен је континуитет пословања, чиме је унапређена усклађеност са стандардом ISO/IEC 27001.

- ЈКП „Паркинг сервис“, Нови Сад је успоставило мере физичке заштите и контроле логичког приступа системима.
- ЈКП „Паркинг сервис“, Нови Сад је успоставило мере за континуитет пословања и заштиту података у ванредним околностима.
- ЈКП „Паркинг сервис“, Нови Сад је успоставило систем управљања ризицима у области информационих технологија.

2. Механизам сарадње са корисницима система делимично је успостављен, због чега је потребно додатно унапредити процедуре које осигуравају поверљивост и поузданост података, као и механизме за миграцију и уништавање података у случају раскида сарадње.
   - ЈКП „Паркинг сервис“, Нови Сад је правилницима, процедурама и физичком заштитом обезбедио безбедност података корисницима система.
   - ЈКП „Паркинг сервис“ Нови Сад није имало адекватно успостављене процедуре које би уредиле сарадњу са корисницима услуга у погледу поверљивости и заштите података, нити су подаци били криптовани, што је остављало ризик од нарушавања заштите, интегритета и аутентичности података. Пружаоци услуга имали су приступ личним подацима корисника без довољне контроле, а подаци нису били адекватно заштићени кроз криптографске мере. Овај недостатак је представљао ризик за безбедност личних података грађана и корисника услуга. Међутим, у току ревизије, ЈКП „Паркинг сервис“ Нови Сад је предузело значајне мере, укључујући доношење Уговора о обради података и Уговора о поверљивости, којима су регулисани приступ подацима и обавезе свих учесника у процесу обраде. Приступ осетљивим подацима корисника је уклоњен, а предузеће је обавезало да ће у наредном периоду увести криптовање података и пренос кључева криптовања руковаоцима података. Иако су мере за побољшање већ имплементиране, криптовање података још увек није спроведено, што оставља отворен простор за додатна унапређења у заштити података.
   - ЈКП „Паркинг сервис“, Нови Сад нема успостављене процедуре за архивирање, миграцију и уништавање података у случају раскида сарадње,

нити су уговори са корисницима садржали одредбе које би осигурале пренос података и криптографских кључева. Предузеће је као обрађивач података задржавало корисничке податке и након истека уговора, што је представљало ризик за заштиту и поверљивост података и могло је угрозити континуитет пословања корисника у случају промене пружаоца услуга. Током ревизије, ЈКП „Паркинг сервис“, Нови Сад је у новим уговорима укључило одредбе о преносу података у електронском формату и брисању података по захтеву корисника, у складу са Законом о заштити података о личности. Додатно, обезбеђено је продужење приступа апликацији „SWAT“ до три месеца након раскида сарадње, што омогућава континуитет пословања. Ипак, предузеће и даље треба да успостави потпуне процедуре за уништавање података и миграцију, како би се обезбедила комплетна заштита података и контрола приступа након истека сарадње.

3. Успостављене апликативне контроле обезбеђују ефикасну наплату и извештавање, али додатна унапређења су потребна у правцу интеграције са стандардним апликацијама и отвореним подацима ради побољшања корисничког искуства и доступности информација.
   - ЈКП „Паркинг сервис“, Нови Сад је предузео мере за ограничавање приступа осетљивим подацима у софтверима за наплату и контролу паркирања, уз побољшање апликативних контрола.
   - У ЈКП „Паркинг сервис“, Нови Сад апликативне контроле које се користе за продају карата омогућавају ажурну евиденцију дневних пазара и броја продатих паркинг карата, као и извештавање.
   - ЈКП „Паркинг сервис“, Нови Сад редовно објављује информације о паркинг зонама, доступности паркинг места, као и могућностима плаћања преко свог сајта и инфо-табли. Такође, предузеће је развило мобилну апликацију која олакшава начин плаћања и пружа корисне информације грађанима. Ипак, систем за обраду и објаву отворених података још увек није успостављен, а информације о доступности паркинг места нису интегрисане у стандардне апликације попут Google Maps. Ово представља потенцијалну слабост у информисању грађана и смањује могућност корисницима да лакше управљају паркирањем, што би било могуће уз коришћење шире доступних апликација. Недостатак система за отворене податке и интеграције са мобилним апликацијама ограничава обим доступности информација и пружање услуга у модернијем, дигиталном формату.

Након спроведене ревизије „Информациони систем за наплату услуга паркинга“, Државна ревизорска институција даје ЈКП „Паркинг сервис“, Нови Сад следеће препоруке:

1) да спроведе криптовање осетљивих података корисника система и осигура да управљање криптографским кључевима буде у надлежности руковаоца података, уз редовну проверу сигурности овог процеса (Налаз 2.2) – Приоритет 2[1];
2) да усвоји правилник и процедуре које ће регулисати архивирање, уништавање и миграцију података у случају раскида сарадње са корисницима услуга,

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

укључујући извоз података и пренос криптографских кључева (Налаз 2.3) – Приоритет 2;

3) да омогући коришћење отворених података и даљи развој мобилне апликације, како би побољшао доступност информација о паркинг местима и унапредио услуге за грађане (Налаз 3.3) – Приоритет 3[2].

2. Мере предузете у поступку ревизије

У току спровођења ове ревизије:

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

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

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

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

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

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

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

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

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

3. Захтев за достављање одазивног извештаја

Јавно комунално предузеће „Паркинг сервис“, Нови Сад 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 „Паркинг сервис“, Нови Сад 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 „Паркинг сервис“, Нови Сад 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 „Паркинг сервис“, Нови Сад 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 14:36:21 +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[3], Пословником Државне ревизорске институције[4] 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“, Нови Сад 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

[3] „Службени гласник РС“, бр. 101/05, 54/07, 36/10 и 44/18-др.закон
[4] „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[5]), 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“, Нови Сад, 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.

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

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“, Нови Сад.

Детаљнији опис коришћене методологије дат је у Прилогу 1.

III Опис предмета ревизије

Информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост и аутентичност тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица[6].

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[7] 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.

[6] Члан 7 став 3 Закона о информационој безбедности.
[7] „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[8].

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 управљању јавним паркиралиштима на територији Града Новог Сада[9]

Одлуком се уређује начин организовања послова у обављању комуналне делатности управљања јавним паркиралиштима на територији Града Новог Сада.

Управљање јавним паркиралиштима је одржавање јавних паркиралишта и простора за паркирање на обележеним местима, организација и вршење контроле и наплате паркирања, услуга уклањања непрописно паркираних, одбачених или остављених возила, премештање возила под условима прописаним законом, постављање уређаја којима се по налогу надлежног органа спречава одвожење возила, у случајевима предвиђеним овом одлуком, као и вршење наплате ових услуга.

Одлука о усклађивању одлуке о оснивању јавног комуналног предузећа „Паркинг сервис“ Нови Сад[10]

Предузеће обавља делатност од општег интереса за Град Нови Сад.

Претежна делатност је: Услужне делатности у копненом саобраћају. Изградња стамбених и нестамбених зграда (паркинг гаража, укључујући и подземне гараже).

Изградња путева и аутопутева (постављање ограда и саобраћајних ознака и сл, бојење и обележавање ознака на путевима). Припремна градилишта (земљане радове: ископавање, насипање, нивелисање терена, ископ канала, уклањање стена, минирање и др.) Друмски превоз терета (превоз аутомобила, изнајмљивање теретног возила с возачем). Рачунарско програмирање (писање, мењање, тестирање, документовање и одржавање софтвера; укључује и писање програма на основу упутства корисника и друге делатности и послове утврђене Статутом Јавног предузећа. Предузеће обавља комуналну делатност управљања јавним паркиралиштима. Управљање јавним паркиралиштима врши се на основу Програма коришћења саобраћајних површина и посебних простора одређених за паркирање моторних возила, као и управљање и

[8] „Службени гласник РС“, бр. 88/11, 104/16 и 95/18, члан 2 став 1
[9] „Сл. лист Града Новог Сада“, бр. 20/2023, 35/2023 - аутентично тумачење и 18/2024
[10] „Сл. лист Града Новог Сада“, бр. 47/2016 и 57/2016 - испр.

премештање паркираних возила и постављање уређаја којима се спречава одвожење возила по налогу надлежног органа.

Закон о информационој безбедности[11]

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[12]

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[13]

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[14]

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

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

ризика за права и слободе физичких лица који произилазе из обраде, руковалац је приликом одређивања начина обраде, као и у току обраде, дужан да:

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

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

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

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

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

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

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

1) обрађује податке о личности само на основу писмених упутстава руковаоца, укључујући и упутство у односу на преношење података о личности у друге државе или међународне организације, осим ако је обрађивач законом обавезан да обрађује податке. У том случају, обрађивач је дужан да обавести руковаоца о тој законској обавези пре започињања обраде, осим ако закон забрањује достављање тих информација због потребе заштите важног јавног интереса;
2) обезбеди да се физичко лице које је овлашћено да обрађује податке о личности обавезало на чување поверљивости података или да то лице подлеже законској обавези чувања поверљивости података;
3) предузме све потребне мере у складу са чланом 50 овог Закона;
4) поштује услове за поверавање обраде другом обрађивачу из 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[15]

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[16]

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.

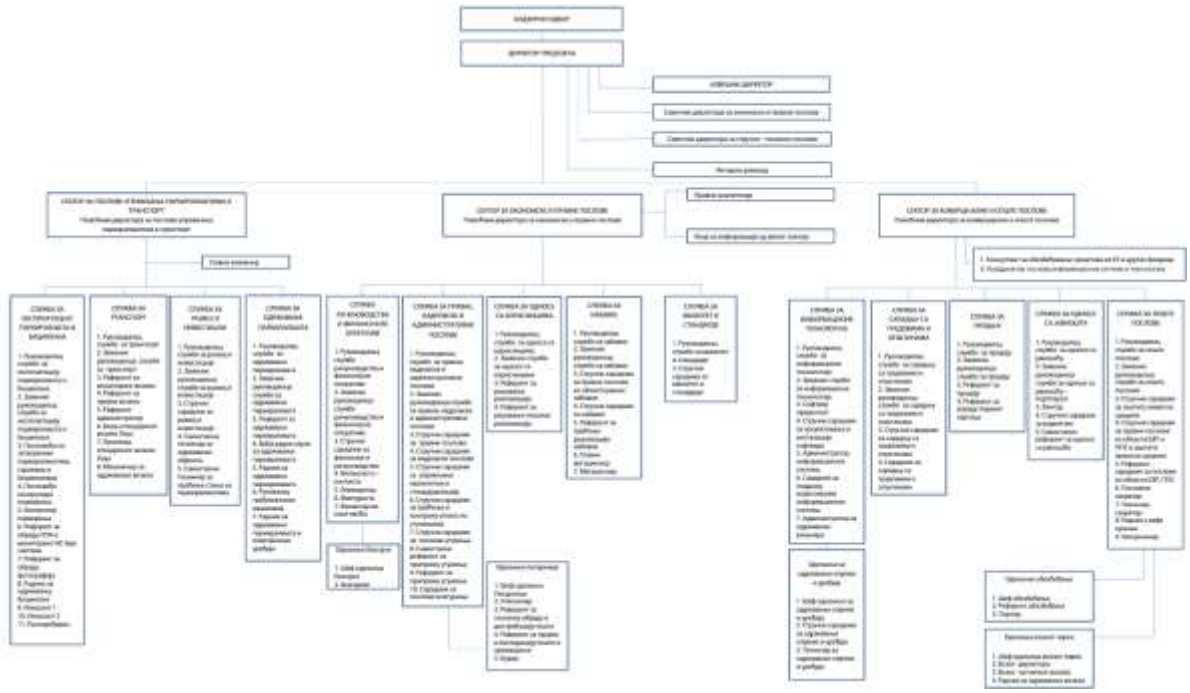
[15] „Службени гласник РС“, број 94/17 и 52/21
[16] „Службени гласник РС“, број 27/2018

Институционални оквир

ЈКП „Паркинг сервис” Нови Сад основала је Скупштина Града Новог Сада, 16. децембра 2004. године, како би се све већи проблеми паркирања у Новом Саду решавали на озбиљан и систематичан начин. Делатност предузећа је одржавање, уређење и коришћење јавних паркиралишта и гаража, као и услуге у друмском саобраћају. Циљ „Паркинг сервиса” је модернизација и унапређење културе паркирања у граду. То подразумева организацију паркиралишта, њихово уређење, видно и прописно обележавање вертикалном и хоризонталном сигнализацијом, како би грађани ову врсту услуге могли да користе на најбољи и најквалитетнији начин.

ЈКП „Паркинг сервис” примењује систем паркирања који подразумева организацију паркиралишта у четири зоне: екстра, црвена, плава и бела. Осим по цени, ове зоне се разликују и по ограничењу времена задржавања у њима. Екстра зона, као последње уведена, ограничила је задржавање на сат времена, а све у циљу повећања фреквенције измене возила на највише оптерећеним паркиралиштима у градском језгру. У црвеној зони време задржавања возила ограничено је на два сата, док у плавој и белој зони ограничење не постоји. Такође, постоје и паркиралишта са контролом уласка и изласка, као и повремена паркиралишта. Паркирање је могуће платити куповином паркинг карте на киоску и мобилним телефоном (слањем СМС-а са регистарском ознаком аутомобила), као и паушалном претплатом која подразумева куповину месечних карата, које су сврстане у три категорије: станарске, предузетничке и „златне” карте. Сама категоризација карата подразумева њихово ценовно разликовање, као и различите могућности коришћења паркиралишта.

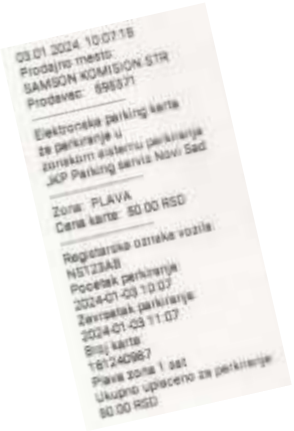
Само комунално предузеће је развило информациони систем за наплату паркирања. Систем је имплементиран 2005. године.



Слика 3. Организациона шема ЈКП „Паркинг сервис“, Нови Сад

Слика 4. Сајт ЈКП „Паркинг сервис“, Нови Сад

- *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.

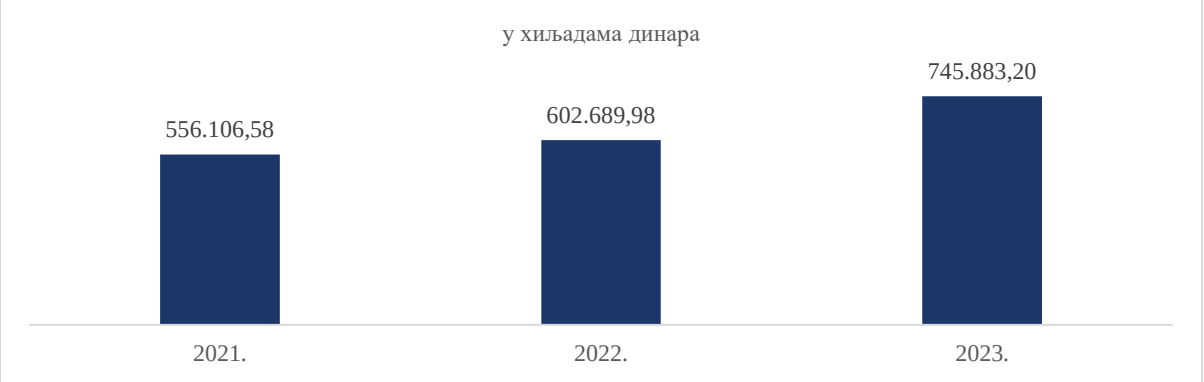


- *еПК:*
  Паркирање се може платити куповином електронске паркинг карте (еПК),
  на више продајних места у граду.

Слика 5. Начини наплате карата за паркирање

Слика 6. Апликација nSpark

На основу анализе доступне документације и података које је доставило ЈКП „Паркинг сервис“, Нови Сад, 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“, Нови Сад показују позитиван тренд са постепеним растом током анализираног периода. Графикон 1 показује да је највећи део прихода остварен од сатних и дневних паркинг карата, што указује на значај краткорочног паркирања у структури прихода. Поред тога, приходи од месечних карата и других услуга, попут опомена, чине мањи, али и даље значајан део укупних прихода. Ови подаци сугеришу да се највећи део прихода генерише од директних корисника паркинг услуга кроз краткорочно коришћење, док дугорочне претплате и опомене играју секундарну улогу у финансијској структури.

Након анализе прихода који су остварени у области наплате паркинг услуга, важно је размотрити и кретање потраживања по основу опомена - дневних карата за паркирање. Опомене - 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 опомена - дневних карата за паркирање, што омогућава детаљнији увид у овај аспект пословања.

Графикон 3. Потраживања за опомене - дневне карте за паркирање у ревидираном периоду[17]

Потраживања по основу опомена - дневних карата за паркирање показују одређене флуктуације током анализираног периода, што је приказано на графикону 3. Висок ниво ових потраживања сугерише да ЈКП „Паркинг сервис“, Нови Сад и даље има простора за побољшање у ефикасности наплате ових услуга. Управљање потраживањима кроз боље праћење обавеза корисника и унапређење механизама наплате може значајно допринети смањењу ових дуговања и повећању финансијске стабилности предузећа.

[17] 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“, Нови Сад

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

Подсистеми у оквиру система за контролу и наплату паркирања:

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

1) СМС систем за наплату паркирања.

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

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

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

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

2) Књиговодствени софтвер FRIP.

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

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

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

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

3) Апликација SWAT за анализу и праћење активности.

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

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

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

IV Закључци

На основу анализе података и документације достављене од стране ЈКП „Паркинг сервис“, Нови Сад, 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 основни ниво поузданости информационих система који се користе за наплату услуга паркинга, а субјект ревизије је ажурирао Правилник о безбедности ИКТ система и у потпуности обухватио специфичности система за контролу и наплату паркирања.
2. Механизам сарадње са корисницима система делимично је успостављен, због чега је потребно додатно унапредити процедуре које осигуравају поверљивост и поузданост података, као и механизме за миграцију и уништавање података у случају раскида сарадње.
3. Успостављене апликативне контроле обезбеђују ефикасну наплату и извештавање, али додатна унапређења су потребна у правцу интеграције са стандардним апликацијама и отвореним подацима ради побољшања корисничког искуства и доступности информација.

У наставку извештаја наводимо закључке са одговарајућим налазима.

ЗАКЉУЧАК 1: Успостављене мере информационе безбедности обезбеђују основни ниво поузданости информационих система који се користе за наплату услуга паркинга, а субјект ревизије је ажурирао Правилник о безбедности ИКТ система и у потпуности обухватио специфичности система за контролу и наплату паркирања

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“ Нови Сад је делимично ажурирало управљање информационом безбедношћу, јер у ревидираном периоду Правилник о безбедности ИКТ система није обухватао све специфичности система за контролу и наплату паркирања

ЈКП „Паркинг сервис“, Нови Сад није у потпуности успоставило адекватан систем управљања информационом безбедношћу, нарочито у делу који се односи на специфичности система за контролу и наплату паркирања. Иако су постојећи акти и процедуре у доброј мери усклађени са основним принципима информационе безбедности, Правилник о безбедности ИКТ система није ажуриран тако да обухвати специфичне аспекте информационог система за контролу и наплату паркирања који је у употреби. Ово оставља простор за потенцијалне слабости у безбедности система, посебно у погледу заштите података и безбедносних мера које се примењују у овом критичном делу ИКТ инфраструктуре.

Ипак, у току поступка ревизије, ЈКП „Паркинг сервис“ Нови Сад је предузело кораке ка унапређењу свог система безбедности. Дана 1. октобра 2024. године, донета је Одлука о измени и допуни Правилника о безбедности ИКТ система којом је у члану 35 прецизирана улога Администратора ИКТ система од посебног значаја. Овом изменом усклађене су радне дужности Администратора ИКТ система са Правилником о систематизацији, чиме је део претходних недостатака исправљен.

Додатно, дана 14. новембра 2024. године, директор ЈКП „Паркинг сервис“, Нови Сад донео је нове измене и допуне Правилника о безбедности ИКТ система. Ове измене обухватиле су унапређење процедура за управљање СМС системом за наплату паркирања, укључујући мониторинг, прављење резервних копија података и одржавање ВПН веза. Такође, ФРИП књиговодствени софтвер и апликација SWAT добили су додатне безбедносне мере, које укључују ограничавање приступа на основу радних задатака и инсталацију безбедносних сертификата. Уведене су и процедуре за размену података са трећим лицима, са посебним акцентом на заштиту података о личности.

Овим изменама значајно су побољшане мере заштите критичних подсистема, минимизовани ризици од безбедносних инцидената и обезбеђен је континуитет пословања, чиме је унапређена усклађеност са стандардом ISO/IEC 27001.

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

ЈКП „Паркинг сервис“, Нови Сад 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“, Нови Сад је јануара 2019. године донело Правилник о безбедности информационо-комуникационог система Јавно комуналног предузећа „Паркинг сервис“, Нови Сад (у даљем тексту: Правилник о безбедности ИКТ система), али се тај документ 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“, Нови Сад 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.

Чланом 2 Правилника о безбедности ИКТ система је наведено да се за праћење примене Правилника обавезује запослени на радном месту Координатор послова информационих система и технологија, док је у Правилнику о унутрашњој организацији и систематизацији послова у ЈКП „Паркинг сервис“, Нови Сад (у даљем тексту: Правилник о систематизацији) за поменуто радно место у области информационе безбедности наведено само да учествује у дефинисању политике безбедности у информационом систему. Са друге стране, Правилником о систематизацији је запосленом на радном месту Администратор ИКТ система од посебног значаја одређено да управља ИКТ системом Предузећа, проверава безбедност и уређује мере заштите ИКТ система од посебног значаја, као и да врши проверу усклађености примењених мера заштите ИКТ система са актом о безбедности ИКТ система. Ова неусклађеност између одредби два правилника ствара ризик од нејасноћа у вези са надлежностима и одговорностима запослених. Уколико није јасно дефинисано који је запослени задужен за спровођење одређених активности у области информационе безбедности, може доћи до пропуста у примени мера заштите ИКТ система, као и до недовољно ефикасног надзора над применом ових мера.

Такође, чланом 35 Правилника о безбедности ИКТ система је наведено да проверу ИКТ система ЈКП „Паркинг сервис“, Нови Сад врши Координатор имплементација нових технологија. Међутим наведено радно место се не спомиње у Правилнику о систематизацији, што такође ствара ризик од нејасноћа у вези са надлежностима и одговорностима запослених.

ЈКП „Паркинг сервис“, Нови Сад је у јануару 2022. године као додатни документ донело и Правилник о начину евидентирања, заштите и коришћења електронских докумената, којим се регулише начин евидентирања, заштите и коришћења електронских докумената у информационим системима ЈКП „Паркинг сервис“, Нови Сад.

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

ЈКП „Паркинг сервис“, Нови Сад 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:

– Процедура рада Службе за информационе технологије;
– Процедура управљања ИТ ресурсима;
– Процедура за управљање инцидентима информационе безбедности;
– Процедура за континуитет безбедности информација;
– Процедура ризици и прилике;
– Упутство за рад Одељења за одржавање опреме;
– Упутство за рад са уређајима за контролу наплате услуге паркирања.

У Процедури рада Службе за информационе технологије у делу Развој, тестирање, примена и надзор над радом софтверских решења наведени су и поступци који се односе на надзор над радом софтверских решења. Надзор над радом софтверских решења у предузећу спроводи се кроз захтеве које иницирају или одобравају руководиоци служби путем е-маил комуникације. За мање послове, детаљи се договарају тимски, док се за веће ангажује подизвођач уз састанке и пратеће белешке које воде запослени задужени за надзор. Администратор ИКТ система је одговоран за праћење квалитета извршења и, по потреби, дефинише фазе рада. Сва документација се чува у електронској или писаној форми, а након завршетка и тестирања, подносилац захтева добија повратну информацију о реализацији.

ЈКП „Паркинг сервис“, Нови Сад је Правилником о систематизацији дефинисао два радна места која се односе на ИТ послове ван Службе за информационе технологије, а запослено је троје извршилаца, седам радних места у оквиру Службе за информационе технологије са петоро запослених и три радна места у оквиру Одељења за одржавање опреме и уређаја са седам запослених лица. У наставку су дати називи радног места, као и информација о попуњености радних места из области информационих технологија:

Табела 2. Запослени у области информационих технологија

Назив радног места	Број запослених
Администратор ИКТ система од посебног значаја	1
Координатор послова информационих система и технологија	2
Служба за информационе технологије	
Руководилац Службе за информационе технологије	1
Самостални стручни сарадник за информационе технологије	2
Софтвер пројектант	-
Стручни сарадник за пројектовање и инсталацију софтвера	-
Администратор информационих система	2
Сарадник за подршку корисницима информационих система	-
Администратор за одржавање рачунара	-
Одељење за одржавање опреме и уређаја	
Шеф одељења за одржавање опреме и уређаја	1
Стручни сарадник за одржавање опреме и уређаја	1
Техничар за одржавање опреме и уређаја	5

Пословима информационе безбедности се у највећој мери баве: Администратор ИКТ система од посебног значаја, Координатор послова информационих система и технологија, Руководилац Службе за информационе технологије и Самостални стручни сарадник за информационе технологије. Администратор ИКТ система од посебног значаја управља ИКТ системом Предузећа, проверава безбедност и уређује мере заштите

ИКТ система од посебног значаја; врши проверу усклађености примењених мера заштите ИКТ система са актом о безбедности ИКТ система; обавља послове везано за спречавање и ублажавање последица инцидента којим се угрожава или нарушава безбедност информације; учествује у прописивању мера везано за безбедност ИКТ система; обавља превенцију и заштиту од безбедносних ризика у ИКТ систему; доноси мере и спроводи поступке за постизање и одржавање адекватног нивоа система безбедности; унапређује информациону безбедност и проверава усклађености примене мера заштите; учествује и уређује односе са трећим лицима на начин који обезбеђује предузимање мера заштите тог ИКТ система у складу са законом, уколико поверава активности у вези са ИКТ системом од посебног значаја трећим лицима; учествује у подизању свести код запослених о значају информационе безбедности, предлаже и учествује у прописивању овлашћења и одговорности запослених у вези са сигурношћу и ресурсима ИКТ система; пријављује националном ЦЕРТ-у инциденте који значајно угрожавају информациону безбедност ИКТ система. Координатор послова информационих система и технологија учествује у дефинисању политике безбедности у информационом систему. Руководилац Службе за информационе технологије координира са Администратором ИКТ система од посебног значаја у вези са пословима везаним за безбедност ИКТ система, израде и реализације информационог система, ажурирања постојећег и имплементације новог софтвера. Самостални стручни сарадник за информационе технологије координира са Администратором ИКТ система од посебног значаја у вези са пословима везаним за безбедност ИКТ система, израде и реализације информационог система, ажурирања постојећег и имплементације новог софтвера. Сва наведена радна места су попуњена.

Запослени из Службе за информационе технологије, као и из других служби и одељења предузећа, редовно учествују на обукама и семинарима ван предузећа, где стичу знања о најновијим технолошким решењима и стандардима у области информационе безбедности и других релевантних области. Ово доприноси континуираном унапређењу њихових вештина и стручности у свакодневном раду.

Чланом 32 Правилника о безбедности ИКТ система је предвиђено да у случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени-корисник је дужан да одмах обавести Службу за ИТ. Уколико се ради о инциденту који је дефинисан у складу са Уредбом о поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, руководилац Службе за ИТ је дужан/а да обавести директора Предузећа и надлежни орган. Служба за ИТ води евиденцију о свим инцидентима, као и пријавама инцидената, у складу са Уредбом, на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

ЈКП „Паркинг сервис“, Нови Сад је дана 6. априла 2023. године утврдио Процедуру за управљање инцидентима информационе безбедности. Ова процедура дефинише начин идентификовања, обавештавања, истраживања и анализе инцидената безбедности информација, осигурава брзу детекцију безбедносних претњи и слабости те брзу реакцију и одговор на безбедносне инциденте те предузимање мера за спречавање његовог понављања и идентификовање потреба и подручја за елиминисање потенцијалних узрока инцидента нарушавања безбедности информација, техничким рањивостима и слабостима система безбедности. Процедура се примењује ради откривања и пријава инцидента, класификацију инцидента, одговор на инцидент, континуирано унапређење мера које се предузимају у предузећу за ванредне ситуације које могу настати у зони деловања предузећа или су одговорност предузећа, а односи се

на све људе (запослене, привремене раднике, особље уговарача, посетиоце и сво остало особље на радном месту). Процедура описује поступања запослених и служби: приликом пријављивања инцидената по информациону безбедност од стране Администратора ИКТ система од посебног значаја; поступак пријаве и управљања инцидентом, анализе узрока инцидента, и затварања инцидента и корективних мера. У процедури су јасно наведене улоге и одговорности запослених приликом појаве инцидената.

У току поступка ревизије, директор ЈКП „Паркинг сервис“, Нови Сад је дана 1. октобра 2024. године донео Одлуку о измени и допуни Правилника о безбедности информационо-комуникационог система Јавног комуналног предузећа „Паркинг сервис“, Нови Сад број 2024-0-1164/1, којом је предвиђено у члану 35 да Администратор ИКТ система од посебног значаја врши проверу ИКТ система предузећа. Проверу спроводи кроз три основна корака: прво, утврђује се усклађеност Правилника о безбедности ИКТ система са прописаним условима и мерама заштите, овлашћењима и процедурама; друго, проверава се примена тих мера у оперативном раду кроз интервјуе, симулације и преглед документације; и треће, врши се техничка провера безбедносних слабости у ИКТ систему кроз анализу конфигурација, техничких података и тестирање познатих слабости. На овај начин, радне дужности Администратора ИКТ система од посебног значаја усклађене су у Правилнику о безбедности ИКТ система са радним дужностима дефинисаним за ово радно место у Правилнику о систематизацији.

Директор ЈКП „Паркинг сервис“, Нови Сад је дана 14. новембра 2024. године донео измене и допуне Правилника о безбедности ИКТ система, са циљем да унапреди безбедност и функционалност информационих система, укључујући и систем за контролу и наплату паркирања. Ове измене су резултирале прецизним дефинисањем одговорности, процедура и мера заштите, како би се осигурали интегритет, поверљивост и доступност података. СМС систем за наплату паркирања је додатно регулисан кроз детаљне процедуре које обухватају праћење, надзор и измене сервера, мониторинг СМС центара и подршку корисницима. Уведене су и мере за прављење резервних копија података и одржавање ВПН веза, чиме је обезбеђена стабилност и безбедност система. ФРИП књиговодствени софтвер је организован на начин који омогућава да корисници имају приступ искључиво оним модулима који су неопходни за њихове радне задатке. На овај начин су ограничене потенцијалне злоупотребе и унапређена је контрола приступа. Апликација SWAT, која се користи за анализу и праћење активности, добила је додатне безбедносне мере. Приступ овој апликацији сада захтева инсталацију безбедносног сертификата и коришћење јединствених корисничких налога са строго дефинисаним правима приступа, што знатно повећава ниво заштите. Додатно, уређене су процедуре за размену података са државним органима и трећим лицима. Уговорима су дефинисане обавезе у вези са заштитом података о личности и поверљивости, као и услови под којима се врши размена података, у складу са Законом о заштити података о личности.

Овим изменама, ЈКП „Паркинг сервис“, Нови Сад је унапредио усклађеност са стандардом ISO/IEC 27001, побољшао заштиту критичних подсистема и минимизовао ризике од безбедносних инцидената, обезбеђујући стабилност и континуитет пословања.

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[18].

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 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

[18] IT Audit Handbook

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“, Нови Сад је успоставило мере физичке заштите и контроле логичког приступа системима

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 у предузећу одређен је врстом корисничког налога и додељеним правима приступа. Администратори имају пун приступ свим ресурсима ИКТ система, док запослени-корисници могу користити само своје налоге, без могућности њиховог дељења са другима, осим са администраторима ради подешавања. Свако кршење ових правила подлеже дисциплинској и кривичној одговорности. Запослени су обавезни да користе ресурсе искључиво у пословне сврхе, да чувају поверљиве податке и лозинке, да се одјављују са система када нису присутни и да захтевају одобрење за инсталацију новог

софтвера или хардвера. Коришћење интернета, електронске поште и складиштење података мора бити у складу са прописаним правилима, а сви приступи и интервенције на систему морају бити засновани на принципу минималне неопходности.

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 ИКТ систему имају искључиво запослени који поседују администраторске или корисничке налоге. Администраторски налог омогућава потпун приступ и управљање свим ресурсима ИКТ система, као и отварање нових или измену постојећих налога. Овај налог отвара руководилац Службе за ИТ или овлашћено лице. Кориснички налог се састоји од корисничког имена и лозинке или електронског сертификата и служи за аутентификацију и ауторизацију приступа ресурсима система. Администратор додељује кориснички налог на основу захтева запосленог задуженог за управљање људским ресурсима, након уноса података у систем за управљање људским ресурсима, у складу са пословним потребама запосленог. Администратор води евиденцију корисничких налога, контролише њихово коришћење, мења права приступа и укида налоге по потреби. Увидом у администраторски модул утврђено је да постоји троје корисника система који имају статус администратора, и то Администратор ИКТ система од посебног значаја и двоје Самосталних стручних сарадника за информационе технологије.

Процедуром управљања ИТ ресурсима детаљно је описано поступање приликом доделе права приступа, промене и укидање права коришћења информационе имовине. Процедура уређује следеће аспекте:

- **Додела права кориснику информационог система**: Права се додељују на основу докумената који се достављају ИТ служби након распоређивања запосленог на радно место. То укључује доделу права за електронску пошту, приступ локалној мрежи, контролорске системе и специфичне фолдере на серверима.
- **Промена нивоа права приступа**: Права се мењају при промени радног места или на основу захтева руководиоца. У случају промене задужења, врши се раздуживање или ново задуживање информационе имовине.
- **Трајно укидање права**: При престанку радног односа или на захтев директора, врши се укидање права коришћења приступа системима, које евидентира администратор ИКТ система.
- **Параметри приступа и евиденција**: Кориснички налози и лозинке се додељују и ажурирају од стране администратора, уз посебне мере безбедности за лозинке.
- **Провера логова**: Лог фајлови се проверавају на захтев ревизије или по налогу директора предузећа.
- **Инсталација софтвера**: Софтвер се инсталира уз одобрење ИТ службе, а запослени немају право самосталне инсталације.
- **Заштита рачунара**: Укључује заштитне зидове (firewall), антивирусне програме и друге безбедносне мере на радним станицама.
- **Одржавање сервера**: Приступ сервер сали и одржавање опреме омогућени су само овлашћеним лицима, уз евиденцију уласка у сервер салу.
- **Рад са удаљености и BYOD**: Приватни уређаји могу се користити за приступ електронској пошти, а даљински приступ се обезбеђује за хитне интервенције и мониторинг ИТ система уз поштовање правила безбедног рада.

Чланом 17 Правилника о безбедности ИКТ система уређена је техничка заштита просторија односно у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему. Просторија у којој се налазе сервери и мрежна опрема организована је као административна зона, са контролисаним приступом, механичком бравом и видео надзором. Простор мора бити заштићен од електромагнетног зрачења, пожара и других непогода, уз одржавање одговарајуће температуре. Приступ омогућава и надзире Руководилац службе за ИТ или овлашћено лице, а осим администратора, трећа лица могу улазити ради инсталације и одржавања опреме уз претходно одобрење.

Чување података о догађајима који могу бити од значаја за безбедност ИКТ система регулисано је чланом 22 Правилника о безбедности ИКТ система. Дневници активности администратора и запослених (activitylog, history, securitylog, transactionlog) се воде и архивирају сваког последњег радног дана у недељи према процедурама за израду копија података у ИКТ систему. Систем за контролу и дојаву о грешкама мора бити подешен да одмах обавештава администратора и Руководиоца службе за ИТ о свим нерегуларним активностима, покушајима упада и упадима у систем.

Чланом 7 Правилника о безбедности ИКТ система прописана су поступања у вези безбедности рада на даљину и употребе мобилних уређаја. Наведено је да запослени-корисници ресурса ИКТ система, могу путем мобилних уређаја, који су у власништву ЈКП „Паркинг сервис“, Нови Сад, и који су подешени од стране Службе за ИТ да приступају само оним деловима ИКТ система који им омогућавају обављање радних задатака у оквиру њихове надлежности, а на основу писане сагласности непосредног руководиоца. Мобилни уређаји морају бити подешени тако да омогуће сигуран и безбедан приступ, коришћењем VPN мреже ИКТ система и листе MAC адреса уређаја путем којих је дозвољен приступ, уз активан одговарајући софтвер за заштиту од вируса и другог злонамерног софтвера. Приступ ресурсима ИКТ система ЈКП „Паркинг сервис“, Нови Сад са удаљених локација, од стране запослених-корисника, у циљу обављања радних задатака, омогућен је путем заштићене VPN/интернет конекције. Запосленом-кориснику, забрањена је самостална инсталација софтвера и подешавање мобилног уређаја, као и давање уређаја другим неовлашћеним лицима (на услугу, сервисирање и сл.). Руководилац службе за ИТ контролише приступ ресурсима ИКТ система и проверава да ли има приступа са непознатих уређаја (са непознатих MAC адреса), те уколико се установи неовлашћен приступ предузима потребне мере. Приступ ресурсима ИКТ система, са приватног уређаја, није дозвољен.

Рад са удаљености је уређен одељком 5.4.8. Процедуре управљања ИТ ресурсима. Администратор ИКТ система, руководилац Службе за ИТ и овлашћено лице предузећа које је задужено за одржавање сервера и локалне рачунарске мреже имају омогућен даљински приступ информационом систему ради мониторинга информационог система и хитних интервенција у случају потребе. Директор предузећа и администратор ИКТ система имају право да у ЈКП „Паркинг сервис“ Нови Сад ауторизују по потреби рад са удаљености за запосленог путем ВПН–а/лиценцног програма за даљински приступ и у том случају запослени попуњавају и шаљу захтев Q2.ИТ.12.04-01 Захтев за приступ локалној рачунарској мрежи предузећа лиценцним програмом за даљински приступ.

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“, Нови Сад је успоставило мере за континуитет пословања и заштиту података у ванредним околностима

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“, Нови Сад је прописао мере које обезбеђују континуитет обављања посла у ванредним околностима. У случају ванредних околности које захтевају измештање ИКТ система из зграде предузећа, руководилац Службе за ИТ је задужен да у најкраћем року пренесе делове ИКТ система неопходне за наставак функционисања на резервну локацију, у складу са планом реаговања у ванредним и кризним ситуацијама. Спецификацију делова ИКТ система неопходних за функционисање у таквим околностима израђује руководилац Службе за ИТ у три примерка, који се налазе код њега, запосленог

надлежног за послове одбране и ванредних ситуација, као и код директора ЈКП „Паркинг сервис“, Нови Сад. Ови делови система који нису неопходни за непосредно функционисање у ванредним ситуацијама складиште се на одређену резервну локацију, коју одређује директор. Процес складиштења мора бити спроведен тако да опрема буде безбедна, означена и евидентирана у складу са званичном евиденцијом која се о њој води.

ЈКП „Паркинг сервис“, Нови Сад је дана 6. априла 2023. године донео Процедуру за континуитет безбедности информација. Ова процедура описује кораке које примењују запослени у ЈКП „Паркинг сервис“, Нови Сад код израде плана за континуитет безбедности информација да би се обезбедила спремност организације да осигура све предуслове за наставак пословања у случајевима када дође до хаварије или изненадног прекида пословања. План континуитета безбедности информација у ЈКП „Паркинг сервис“, Нови Сад развија се како би се осигурао наставак пословних активности након прекида или инцидента. Он дефинише кораке за опоравак пословних процеса и управљање операцијама током рестаурације безбедности информација, коју спроводи тим за континуитет одређен од стране Менаџера за информациону безбедност. План укључује све активности организације и обезбеђује ресурсе неопходне за континуитет рада, као и заштиту запослених и опреме. У том смислу развијени су:

- План континуитета у случају прекида снабдевања електричне енергије;
- План континуитета у случају пожара;
- План континуитета у случају изненадног отказа критичног ресурса ИКТ система.

План континуитета безбедности информација подлеже тестирању, где год је могуће, најмање једном годишње кроз обуке и вежбе. Резултати тестирања се документују, а могућа побољшања се идентификују. Сви појединци који су укључени у тестиране делове плана морају учествовати у тестирању. Менаџер за информациону безбедност води евиденцију о присуству и трајању теста кроз извештај о тестирању плана континуитета безбедности информација.

Заштита од губитка података и израда резервних копија је предвиђена чланом 21 Правилника о безбедности ИКТ система. Базе података се архивирају најмање једном недељно и годишње ради обнове, док се остали документи архивирају једном месечно и годишње. Архивирање се обавља у периоду када не омета рад система. Годишње копије се чувају у два примерка, од којих један остаје у просторији са месечним копијама, а други у архиви предузећа на другој локацији. Исправност архива проверава се сваких пет година, а тестирање се обавља без утицаја на рад ИКТ система. Одговорна лица из ЈКП „Паркинг сервис“, Нови Сад су нам потврдила да се врше периодичне превентивне провере креирања резервних копија података.

Израда резервне копије података (backup) је уређена одељком 5.11. Процедуре рада Службе за информационе технологије. Према овој процедури, подешавање и праћење резервних копија (backup) свих база података, укључујући фотографије возила у прекршају које генеришу контролори и Видео паук апликација, као и резервне копије апликација и фајл система свих сервера, врши се у складу са Планом континуитета безбедности информација (документ Q2.ИТ.12.01-01). Приликом ових активности води се рачуна о свим релевантним факторима како би се осигурало да рад предузећа не буде прекинут. За израду резервних копија података задужен је пословни партнер са којим је склопљен уговор о текућем одржавању СМС система наплате. Администратор ИКТ система и Руководилац службе за ИТ надзиру овај процес и одговарају за квалитет извршења послова.

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).

Налаз 1.4: ЈКП „Паркинг сервис“, Нови Сад је успоставило систем управљања ризицима у области информационих технологија

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

У Правилнику о систематизацији код Администратора ИКТ система је наведено да обавља превенцију и заштиту од безбедносних ризика у ИКТ систему.

ЈКП „Паркинг сервис“, Нови Сад је дана 18. августа 2023. године донело Стратегију управљања ризицима у ЈКП „Паркинг сервис“, Нови Сад. Стратегија управљања ризицима обухвата идентификацију, процену и контролу потенцијалних догађаја који могу имати негативан утицај на остваривање циљева предузећа. Основни циљ Стратегије је успостављање ефикасног система управљања ризицима који ће омогућити постизање планираних резултата и осигурање континуитета пословања. Ризици се евидентирају у Регистру ризика (Образац број 2), који је успостављен на нивоу предузећа и представља саставни део Стратегије управљања ризицима.

Регистар ризика обухвата четири ризика која се односе на област информационих технологија, односно у оквиру Службе за ИТ. За сваки ризик наведени су процена преосталог ризика, одговор на ризик и метод управљања ризиком, као и мере за његово управљање, рокови за спровођење мера, одговорна лица за њихово извршење, и датум контроле примене тих мера.

У октобру 2023. године, ЈКП „Паркинг сервис“, Нови Сад је спровео поступак процене ризика који је обухватио и ризике у оквиру информационо-комуникационих и телекомуникационих система. Приликом анализе седам идентификованих ризика, утврђено је да су четири ризика минимална, два мала, а један ризик значајан. Препоруке укључују развој правилника и процедура за осигурање континуитета и безбедности рада ИКТ система у ванредним ситуацијама, наставак обуке запослених о безбедносним ризицима, те подизање нивоа безбедносне културе. Такође, предложена је имплементација новог стандарда SRPS ISO/IEC 27001:2022 ради боље припреме за будуће изазове у овој области.

ЈКП „Паркинг сервис“, Нови Сад је дана 8. децембра 2023. године донело Процедуру ризици и прилике. Сврха процедуре је да предузеће идентификује ризике и прилике који произлазе из пословних активности, циљева и захтева заинтересованих страна у области заштите животне средине, безбедности и здравља на раду, информационе безбедности и борбе против мита. Процедура дефинише елементе управљања ризицима, укључујући методологију оцењивања, третман и прихватање ризика, као и комуникацију о ризицима.

Предузеће, приликом планирања система менаџмента безбедности информација, утврђује ризике и прилике како би осигурало постизање предвиђених резултата, повећање жељених ефеката, спречавање или смањење нежељених ефеката и побољшање система. Мере које се односе на ризике и прилике интегришу се у систем менаџмента. Процес оцењивања ризика обухвата:

1) успостављање критеријума за ризике,
2) идентификацију ризика,
3) анализу ризика,
4) вредновање ризика по безбедност информација.

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.

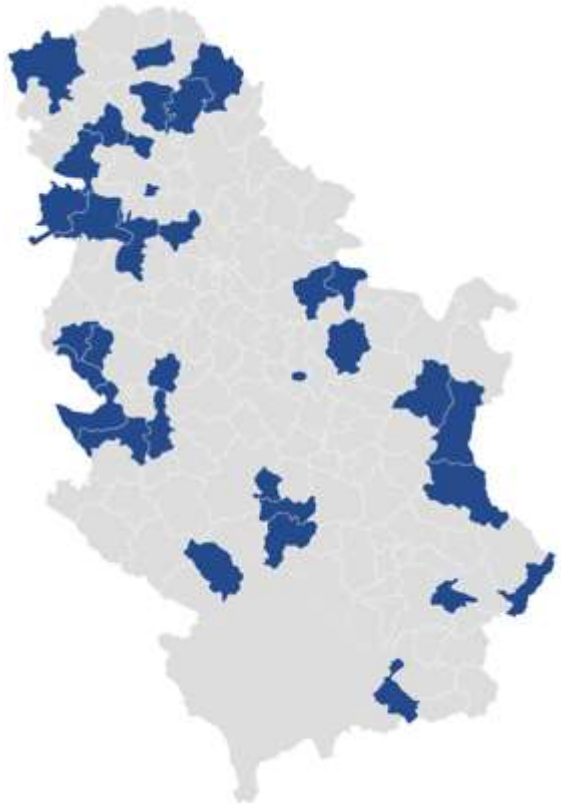
Када су у питању ИТ ризици, у пракси се примењује тзв. 3Д приступ (претња, рањивост, последица) или 2Д приступ (вероватноћа, утицај). Сама класификација ризика се најчешће врши према утицају, а кораци који обично следе обухватају анализу ризика (вероватноћа појављивања сваког ризика понаособ и процена 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 делимично је успостављен, због чега је потребно додатно унапредити процедуре које осигуравају поверљивост и поузданост података, као и механизме за миграцију и уништавање података у случају раскида сарадње

Циљ овог дела извештаја био је да оцени степен до којег је ЈКП „Паркинг сервис“, Нови Сад 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“, Новог Сада на дан објављивања извештаја о ревизији, заједно са предузећем „Proapp“ doo из Новог Сада, пружа услуге система за контролу и наплату паркирања путем мобилног видео надзора код 34 јавно комунална предузећа на територији Републике Србије. Та јавно комунална предузећа су:



ЈКП „Стандард“, Књажевац
ЈКСП „Сента“
ЈКП „Паркинг сервис“, Сомбор
ЈКП „Темерин“
ЈКП „Паркинг сервис“, Петровац на Млави
ЈКП „Биоктош“, Ужице
ЈКП „Комуналије“, Сремска Митровица
ЈКП „Чистоћа“, Стара Пазова
ЈКП „Стандард“, Шид
ЈП „Нови аутопревозник“, Врњачка Бања
ЈП „Кикинда“
ЈП „Пословни центар“, Александровац - Жупа
ЈКП „Паркинг сервис“, Нови Пазар
ЈП „Комуналац“, Бечеј
ЈКП „Дунав“, Велико Градиште
ЈКП „1.мај“, Крупањ
ЈКП „Осечина“
ЈКП „Наш дом“, Пожега
ЈП „Комуналац“, Димитровград
ЈП „Комуналац“, Бујановац
ЈКП „Белило“, Сремски Карловци
ЈКП „Комуналпројект“, Бачка Паланка
ЈП „ББ ТЕРМ“, Бајина Башта
ЈКП „Водовод Мионица“, Мионица
ЈКП „Комуналац“, Власотинце
ЈКП „Комуналац“, Рума
ЈКП „Паркинг сервис“, Зајечар
ЈКП „Комуналац“, Врбас
ЈКП „Стандард“, Љубовија
ЈКП „Паркинг сервис“, Пожаревац
ЈКП „Морава“, Лапово
ЈКП за стамбене услуге „Бор“
ЈКП „Расина“, Брус

Слика 8. Списак ЈП којима ЈКП „Паркинг сервис“, Нови Сад пружа услуге Информационог система за наплату услуга паркинга

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“, Нови Сад 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“ Нови Сад је усвојио скуп документа - правилнике, процедуре и упутства којима се уређује безбедност података ИКТ система и то:

- Правилник о начину евидентирања, заштите и коришћења електронских докумената;
- Процедура управљања ИТ ресурсима;
- Процедура за континуитет безбедности информација;
- Упутство за рад одељења за одржавање опреме.

ЈКП „Паркинг сервис“ Нови Сад је обезбедило просторије у којима се налазе средства и документи ИКТ система. Правилник о безбедности ИКТ система у члану 17 дефинише да Просторија у којој се налазе сервери, мрежна или комуникациона опрема ИКТ система буде видљиво означена просторија која је обезбеђена механичком бравом и видео надзором. Такође просторија мора да буде обезбеђена од компромитујућег електромагнетног зрачења, пожара и других елементарних непогода и у њој треба да буде одговарајућа температура. Улазак у просторију омогућава и надзире Руковалац службе за ИТ или од њега овлашћено лице. води се евиденција о приступу просторије. Што је и на терену потврђено, а сваки улазак у просторију се евидентира. Сервер соба је обезбеђена и додатним напајањем у виду УПС-ева, тако да и у случају нестанка електричне мреже систем може несметано да функционише. У току ревизије ЈКП „Паркинг сервис“ Нови Сад је у фази постављања и секундарног сервера који ће бити на другој локацији.

ЈКП „Паркинг сервис“ Нови Сад свакодневно врши backup како својих тако и корисничких података и исте чувају у посебној просторији, како је и дефинисано интерним актом[19].

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.

[19] Правилник о начину евидентирања, заштите и коришћења електронских документима.

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

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

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

Налаз 2.2: ЈКП „Паркинг сервис“, Нови Сад је предузело значајне мере за заштиту података, , међутим постоји потреба за увођењем криптовања података

ЈКП „Паркинг сервис“ Нови Сад није имало адекватно успостављене процедуре које би уредиле сарадњу са корисницима услуга у погледу поверљивости и заштите података, нити су подаци били криптовани, што је остављало ризик од нарушавања заштите, интегритета и аутентичности података. Пружаоци услуга имали су приступ личним подацима корисника без довољне контроле, а подаци нису били адекватно заштићени кроз криптографске мере. Овај недостатак је представљао ризик за безбедност личних података грађана и корисника услуга.

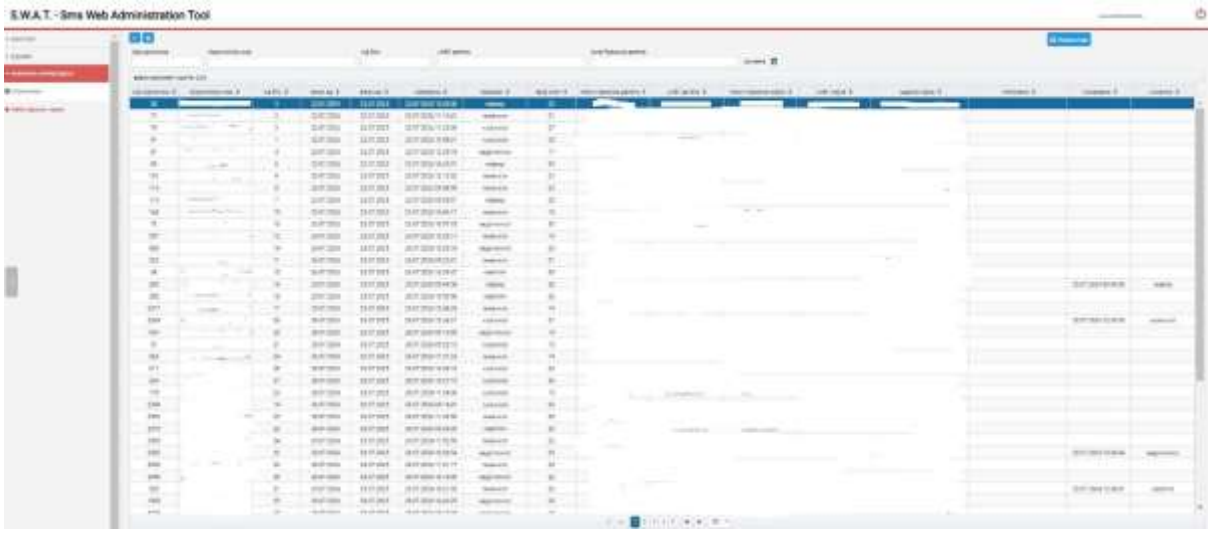
Међутим, у току ревизије, ЈКП „Паркинг сервис“ Нови Сад је предузело значајне мере, укључујући доношење Уговора о обради података и Уговора о поверљивости, којима су регулисани приступ подацима и обавезе свих учесника у процесу обраде. Приступ осетљивим подацима корисника је уклоњен, а предузеће је обавезало да ће у наредном периоду увести криптовање података и пренос кључева криптовања руковаоцима података. Иако су мере за побољшање већ имплементиране, криптовање података још увек није спроведено, што оставља отворен простор за додатна унапређења у заштити података.

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

ЈКП „Паркинг сервис“, Нови Сад у периоду ревидирања није имао процедуре које уређују сарадњу са корисницима услуга у делу поверљивости података као и приступу

подацима од стране подобрађивача. Подаци нису криптовани тако да постоји ризик о нарушавању заштите, аутентичности односно интегритету података. Правилник о безбедности ИКТ система у члану 30 дефинише да пружаоци услуга могу приступити само оним подацима који се налазе у базама података које су део софтвера који су они израдили, односно за које постоји уговором дефинисан приступ. ЈКП „Паркинг сервис“ Нови Сад има потписан уговор са фирмом „Proapp“ DOO око одржавања једног дела система, а нису предвидели приступ подацима од стране подобрађивача (outsourcing фирме), док се лог фајлови система такође чувају и код фирме „Proapp“ DOO.

У базама података, чувају се лични подаци о грађанима којима су издате дневне карте односно претплатници (име и презиме, ЈМБГ, адреса, контакт телефон), и у те податке пружалац услуга (ЈКП „Паркинг сервис“ Нови Сад) има увек увид, тачније може да врши обраду података без контроле од стране руковаоца. Приликом подношења захтева за добијање претплатних карата, грађани се на посебним формуларима сагласе са тиме да се може вршити обрада њихових података. Међутим, након завршеног процеса издавања претплатне карте, подаци не треба да буду доступни пружаоцу услуга чак ни на увид, било да их треба обрисати или криптовати, при чему би кључ био код руковаоца. То сада, као што је наведено, није случај.



Слика 9. Подаци грађана који су били видљиви корисницима информационог система

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

У Уговору о обради података ЈКП „Паркинг сервис“, Нови Сад је обрађивач и детаљно су дефинисана права и обавезе руковаоца и обрађивача у вези са обрадом личних података коју врши обрађивач у име руковаоца, у циљу заштите права лица на која се подаци односе. Такође у уговору су дефинисана права и подобрађивача као и да обрађивач може да ангажује подобрађивача само уз писмену сагласност руковаоца. Пренос података о личности може се вршити у државе потписнице Конвенције о заштити лица у односу на аутоматску обраду личних података Савета Европе - бр.108[20]. односно у државе за које је Влада Републике Србије утврдила да обезбеђују примерени ниво заштите.

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

[20] (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - No.108)

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

Препоручујемо ЈКП „Паркинг сервис“, Нови Сад да спроведе криптовање осетљивих података корисника система и осигура да управљање криптографским кључевима буде у надлежности руковаоца података, уз редовну проверу сигурности овог процеса.

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“, Нови Сад није успоставило процедуре за архивирање, уништавање и миграцију података у случају раскида сарадње са корисницима

ЈКП „Паркинг сервис“, Нови Сад нема успостављене процедуре за архивирање, миграцију и уништавање података у случају раскида сарадње, нити су уговори са корисницима садржали одредбе које би осигурале пренос података и криптографских кључева. Предузеће је као обрађивач података задржавало корисничке податке и након истека уговора, што је представљало ризик за заштиту и поверљивост података и могло је угрозити континуитет пословања корисника у случају промене пружаоца услуга.

Током ревизије, ЈКП „Паркинг сервис“, Нови Сад је у новим уговорима укључило одредбе о преносу података у електронском формату и брисању података по захтеву корисника, у складу са Законом о заштити података о личности. Додатно, обезбеђено је продужење приступа апликацији „SWAT“ до три месеца након раскида сарадње, што омогућава континуитет пословања. Ипак, предузеће и даље треба да успостави потпуне процедуре за уништавање података и миграцију, како би се обезбедила комплетна заштита података и контрола приступа након истека сарадње.

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

Не постоји правилник ни процедура о архивирању података или уништавању истих у случају да корисник система (34 корисника) промени пружаоца услуга. Уговорима није предвиђена ниједна активност или обавеза ЈКП „Паркинг сервис“, Нови Сад у случају раскида уговора. ЈКП „Паркинг сервис“, Нови Сад исте податке чува иако је он обрађивач податка, а не руковалац.

ЈКП „Паркинг сервис“, Нови Сад 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.

У уговорима са корисницима софтвера за наплату и контролу паркирања чланом 15 је дефинисано да је у случају раскида сарадња отказни рок 90 дана тако да је ЈКП „Паркинг сервис“, Нови Сад 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.

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

Препоручујемо ЈКП „Паркинг сервис“, Нови Сад да усвоји правилник и процедуре које ће регулисати архивирање, уништавање и миграцију података у случају раскида сарадње са корисницима услуга, укључујући извоз података и пренос криптографских кључева.

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 ефикасну наплату и извештавање, али додатна унапређења су потребна у правцу интеграције са стандардним апликацијама и отвореним подацима ради побољшања корисничког искуства и доступности 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“, Нови Сад. 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“, Нови Сад је предузело мере за ограничавање приступа осетљивим подацима у софтверима за наплату и контролу паркирања, уз побољшање апликативних контрола

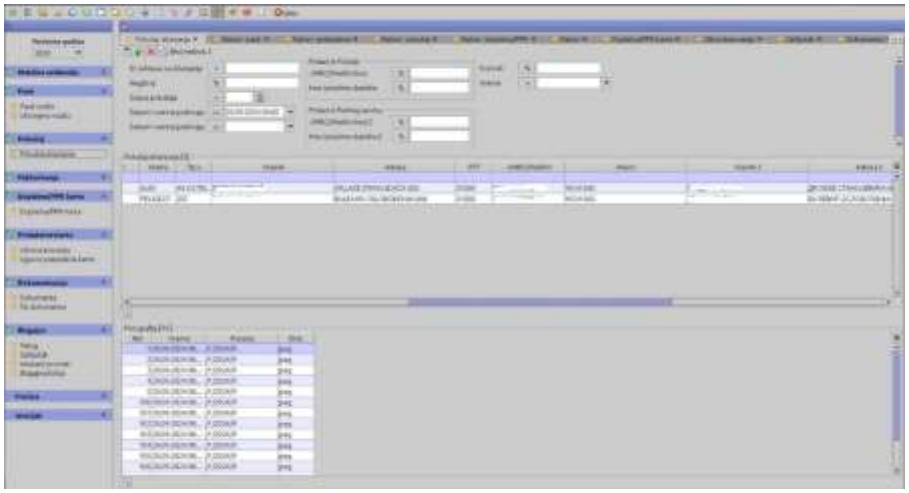
ЈКП „Паркинг сервис“, Нови Сад, користи два софтвера који служи за наплату и контролу услуга паркинга у Новом Саду и то су FRIP и SWAT. За приступ FRIP систему потребна је VPN конекција у оквиру самог ЈКП „Паркинг сервис“, Нови Сад, док је за приступ SWAT систему потребан сертификат који се обнавља сваке године.

ЈКП „Паркинг сервис“ Нови Сад 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 FRIP система.

Запослени ЈКП „Паркинг сервис“, Нови Сад на месту Благајника може да приступи и мења податке која му нису у опису послова. Благајник може да види личне податке грађана иако му за опис посла који обавља нису потребни. Има приступ матичној евиденцији где поред података грађана може да види и податке запослених и свих који имају приступ систему које користи ЈКП „Паркинг сервис“, Нови Сад.



Слика 10. Видели се осетљиви подаци у FRIP систему

Запослени ЈКП „Паркинг сервис“, Нови Сад на месту Call Centar имали су у посматраном периоду у моделу „Покушај уклањања“ приступ осетљивим подацима и приступ измени, односно брисању података, 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.

Приликом тестирања SWAT система установили смо да генерисани извештаји садрже осетљиве податке грађана, иако они нису потребни.

Слика 11. Видели се осетљиви подаци у SWAT систему

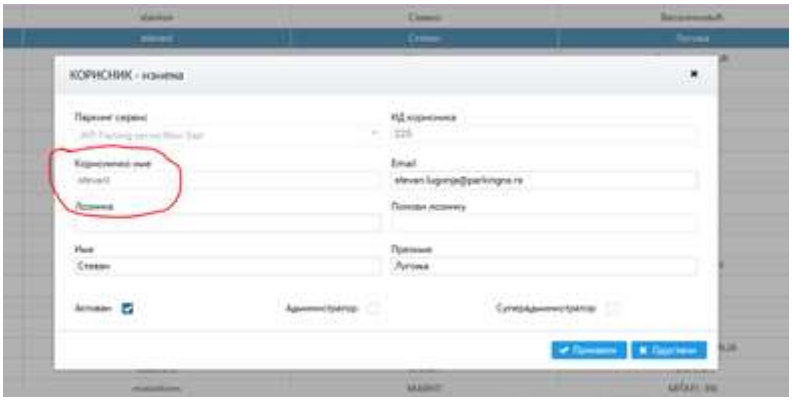
Упутства за употребу апликација су доступна свим запосленима тако да су обезбедили примену правила и процедура за управљање корисничким налозима и приступом.

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

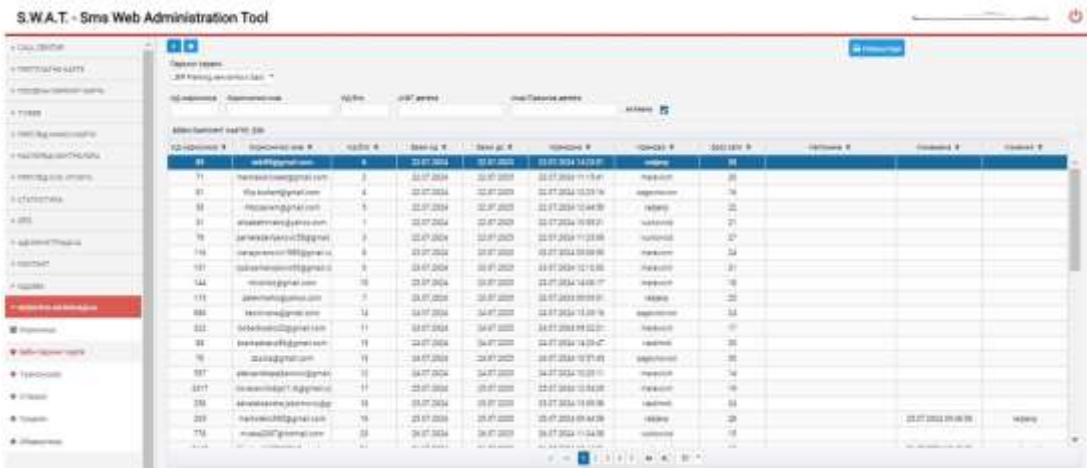
Слика 12. Уклоњене колоне са осетљивим подацима који се налазе у FRIP систему

Слика 13. Укинут експорт података у CSV и XLSX (на десни клик из табеле)

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



Слика 14. Онемогућено је брисање и измена Username у SWAT систему



Слика 15. Уклоњене колоне са ЈМБГ, именом и презименом мајке и детета у SWAT систему

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“, Нови Сад апликативне контроле које се користе за продају карата омогућавају ажурну евиденцију дневних пазара и броја продатих паркинг карата, као и извештавање

ЈКП „Паркинг сервис“ Нови Сад продају карата врши у својим објектима (месечне карте), или путем СМС порука (сатне карте) и греб карте, 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“, Нови Сад редовно објављује информације о паркинг зонама и развио је сопствену мобилну апликацију, али није омогућио приступ отвореним подацима и интеграцију са стандардним апликацијама

ЈКП „Паркинг сервис“, Нови Сад редовно објављује информације о паркинг зонама, доступности паркинг места, као и могућностима плаћања преко свог сајта и инфо-табли. Такође, предузеће је развило мобилну апликацију која олакшава начин плаћања и пружа корисне информације грађанима. Ипак, систем за обраду и објаву отворених података још увек није успостављен, а информације о доступности паркинг места нису интегрисане у стандардне апликације попут Google Maps. Ово представља потенцијалну слабост у информисању грађана и смањује могућност корисницима да лакше управљају паркирањем, што би било могуће уз коришћење шире доступних апликација. Недостатак система за отворене податке и интеграције са мобилним апликацијама ограничава обим доступности информација и пружање услуга у модернијем, дигиталном формату.

ЈКП „Паркинг сервис“ Нови Сад путем свог официјелног сајта[21] 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“ Нови Сад је развио и мобилну апликацију[22] која олакшава начин плаћања као и пружање корисних информација грађанима. Такође у фази развоја је и могућност наплате преко QR баркода, као на бензинским пумпама.

Што се тиче доступности паркинга она је тренутно омогућена само преко инфо-табли које обавештавају возаче о броју слободних места у оближњим паркиралиштима са контролом уласка и изласка.

Када је у питању употреба отворених података, како је наведено на Порталу отворених података[23]: „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.

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 Новом Саду, није омогућено информисање путем стандардних апликација на мобилним утрећајима, као што је то Google Maps или слична.

[21] https://parkingns.rs/
[22] Мобилна апликација nSpark
[23] https://data.gov.rs/sr/

Препоручујемо ЈКП „Паркинг сервис“, Нови Сад да омогући коришћење отворених података и даљи развој мобилне апликације, како би побољшао доступност информација о паркинг местима и унапредио услуге за грађане.

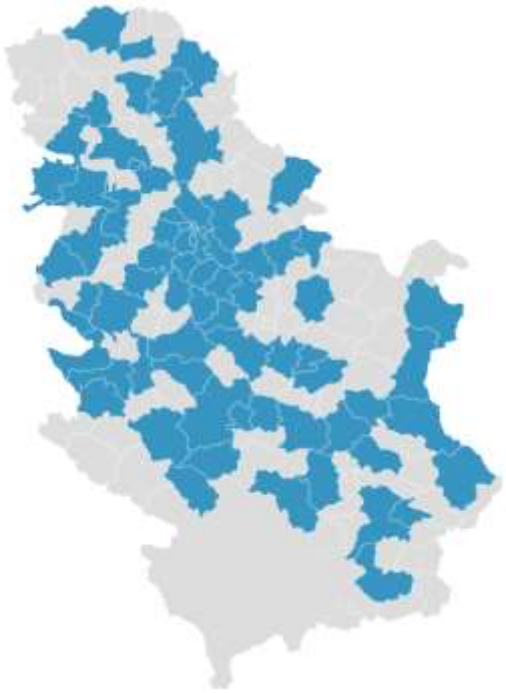
Јавна комунална предузећа треба да настоје да редовно ажурирају податке о паркинг зонама, ценама, доступности паркинг места и могућностима плаћања у реалном времену. Пожељно је да ти подаци буду доступни не само путем званичних веб сајтова, већ и у формату отворених података који омогућавају лакшу интеграцију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

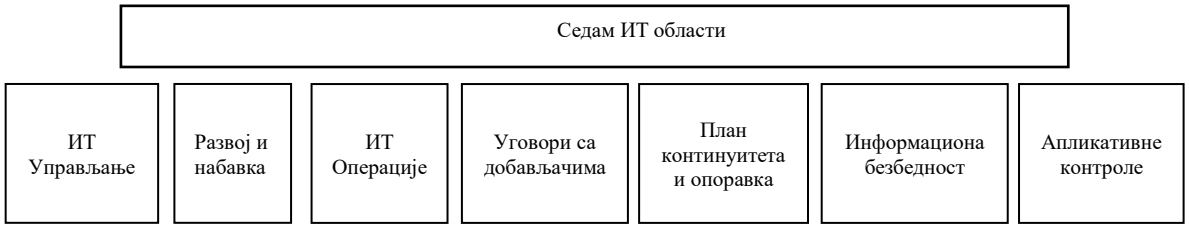
Прилог 1. Методологија у поступку рада

У току предстудије послали смо упитник[24] свим јединицама локалне самоуправе које на својој територији имају јавно предузеће које се бави наплатом услуга паркирања.



Слика 16. 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 17. 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.

[24] 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[25]:

- 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;

[25] 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.