ДРЖАВНА
РЕВИЗОРСКА
ИНСТИТУЦИЈА

ИЗВЕШТАЈ
О РЕВИЗИЈИ СВРСИСХОДНОСТИ ПОСЛОВАЊА

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

Број: 400-1058/2024-07/36
Београд, 20. децембар 2024. године

ЈКП „Паркинг сервис“ Чачак управља наплатом паркинг услуга и ажурирањем информација о паркинг зонама, али је потребно унапредити безбедност података, контролу приступа и успоставити механизме за континуитет пружања услуга паркинга

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

Информациона безбедност није адекватно успостављена, јер нису предузете кључне мере заштите, укључујући управљање ИТ ризицима, контролу приступа и планове за континуитет пословања, што значајно угрожава безбедност и поузданост система за наплату услуга паркинга.

Иако је ЈКП „Паркинг сервис“, Чачак обезбедио континуитет пословања у случају раскида сарадње са пружаоцем услуга , недостају кључне процедуре за сарадњу, надзор и контролу заштите података, чиме се угрожава безбедност и поузданост података о корисницима.

Апликативне контроле обезбеђују основну контролу наплате и ажурирање података, али је потребно унапредити управљање корисничким налозима и омогућити коришћење отворених података за бољу доступност информација.

Препоруке

Након спроведене ревизије, Државна ревизорска институција је Јавном комуналном предузећу „Паркинг сервис“, Чачак, између осталих, дала следеће препоруке:

- да ажурира Акт о безбедности ИКТ система како би укључио све специфичности које се односе на информациони систем за наплату паркинг услуга, укључујући јасно дефинисане одредбе о поверавању послова и односу са пружаоцима услуга;
- да развије и усвоји план континуитета пословања у ванредним околностима, који ће обезбедити континуитет пословања и неометано функционисање система;
- да успостави процес управљања ИТ ризицима, укључујући дефинисање послова и одговорности у овој области у Правилнику о систематизацији радних места;
- да усвоји и имплементира процедуре које ће уредити сарадњу са пружаоцима услуга, укључујући јасно дефинисане одговорности за контролу приступа подацима и надзор над извршењем уговорних обавеза;
- да обезбеди механизме за спречавање трајног брисања налога без угрожавања интегритета података, као и да омогући праћење активности корисника како би се осигурао потпуни траг активности у систему;
- да омогући коришћење отворених података и развој мобилне апликације како би се грађанима омогућио лакши приступ информацијама о паркинг услугама.

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“, Чачак	ЈКП „Паркинг сервис“, Чачак
Јединица локалне самоуправе	ЈЛС
Општа регулатива о заштити података о личности (General Data Protection Regulation)	ГДПР
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“, Чачак 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 Чачку, задужено је Јавно комунално предузеће „Паркинг сервис“ (у даљем тексту: ЈКП „Паркинг сервис“, Чачак). Пружалац услуге када је информациони систем у питању је фирма „Synapse tech“ из Београда. Систем је имплементиран 2015. 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“ Чачак управља наплатом паркинг услуга и ажурирањем информација о паркинг зонама, али је потребно унапредити безбедност података, контролу приступа и успоставити механизме за континуитет пружања услуга паркинга.

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

1. Информациона безбедност није адекватно успостављена, јер нису предузете кључне мере заштите, укључујући управљање ИТ ризицима, контролу приступа и планове за континуитет пословања, што значајно угрожава безбедност и поузданост система за наплату услуга паркинга.
   - Организација информационе безбедности у ЈКП „Паркинг сервис“, Чачак није успостављена на адекватан начин због недостатка стратешког планирања, непотпуног Акта о безбедности који не обухвата специфичности односа са пружаоцима услуга, као и недостатка процедура и докумената који би детаљно уредили послове информационе безбедности. Оваква организација оставља простор за нејасну поделу дужности и одговорности, што угрожава контролу и надзор над информационом безбедношћу и повећава ризик од безбедносних инцидената и других претњи информационом систему за наплату паркинг услуга.

- Иако је Актом о безбедности ИКТ система предвиђено да Координатор ИКТ послова контролише приступ ресурсима система и води евиденцију приватних уређаја који приступају систему, ове процедуре нису адекватно примењене у пракси. Лог фајлови активности корисника и администратора се не чувају, што онемогућава праћење и контролу активности на систему. Поред тога, сервери су изнајмљени и налазе се код пружаоца услуга „Synapse tech“, Београд, али ово изнајмљивање и администрирање од стране пружаоца услуга нису адекватно регулисани у Акту о безбедности информационо-комуникационог система, што угрожава физичку и логичку безбедност система.
- ЈКП „Паркинг сервис“, Чачак није успоставило план или процедуру за континуитет пословања у ванредним околностима, иако је Уговором о јавној набавци са пружаоцем услуга „Synapse tech“ Београд дефинисано да комплетна инфраструктура мора обезбедити неометано функционисање система. Недостатак овог плана повећава ризик од прекида у пружању услуга у случају ванредних околности, што може значајно утицати на континуитет пословања и квалитет услуга које субјекат ревизије пружа корисницима. Овај пропуст делом је последица недовољног броја запослених који се баве пословима информационе безбедности, што отежава правовремено планирање и имплементацију мера заштите.
- ЈКП „Паркинг сервис“, Чачак није успоставило процес управљања ИТ ризицима, због недостатка јасно дефинисаних послова у вези са управљањем ризицима у Правилнику о систематизацији радних места. Овај пропуст директно утиче на одсуство запослених који би се бавили управљањем ИТ ризицима, што може довести до повећаног ризика од нежељених догађаја који могу угрозити функционисање ИКТ система, резултирати губитком података или изазвати друге негативне последице по пословање.

2. Иако је ЈКП „Паркинг сервис“, Чачак обезбедило континуитет пословања у случају раскида сарадње са пружаоцем услуга, недостају кључне процедуре за сарадњу, надзор и контролу заштите података, чиме се угрожава безбедност и поузданост података о корисницима.
   - ЈКП „Паркинг сервис“, Чачак није усвојило процедуре које уређују сарадњу са пружаоцима услуга, иако је Актом о безбедности ИКТ система предвиђено да пружаоци услуга могу приступити само одређеним подацима и да је Координатор ИКТ послова одговоран за контролу приступа и надзор над извршењем уговорних обавеза. Међутим, услед тога што је Координатор ИКТ послова једина особа која обавља ове задатке, а уз то постоје други радни задаци које обавља, недостају документи који доказују да се овај надзор адекватно спроводи. Ова ситуација оставља систем изложен ризицима од неадекватног управљања приступом и недовољне заштите података.
   - ЈКП „Паркинг сервис“, Чачак није успоставило механизам за контролу да ли пружалац услуга испуњава услове за заштиту података и није документовао начин праћења извршења уговора у смислу безбедности података. Уговор са пружаоцем услуга не уређује однос у складу са Законом о заштити података о личности, што је резултирало тиме да пружалац услуга има неконтролисан приступ осетљивим личним подацима грађана,

укључујући регистарски број, адресу, контакт телефон и друге личне податке. Такође, подаци који више нису потребни нису адекватно заштићени или уклоњени, што представља озбиљан ризик за безбедност и приватност података.

- ЈКП „Паркинг сервис“, Чачак је обезбедило континуитет пружања услуга паркинга у случају раскида сарадње са пружаоцем услуга.

3. Апликативне контроле обезбеђују основну контролу наплате и ажурирање података, али је потребно унапредити управљање корисничким налозима и омогућити коришћење отворених података за бољу доступност информација.
   - ЈКП „Паркинг сервис“, Чачак није дефинисало процедуре и упутства за управљање апликацијама које се користе за наплату и праћење доступности паркинг места. Непостојање механизама за деактивацију корисника доводи до ризика од неконтролисаног приступа систему. Трајно брисање корисничког налога не онемогућава приступ систему, а преименовање корисничког налога доводи до губитка података и трагова активности претходних запослених, што угрожава интегритет података и поузданост система. Ова ситуација може бити последица недостатка ресурса и техничке подршке за развој и одржавање апликација, као и недовољно дефинисаних одговорности запослених за имплементацију безбедносних мера у систему.
   - У ЈКП „Паркинг сервис“, Чачак апликативне контроле које се користе за продају карата омогућавају ажурну евиденцију дневних пазара и броја продатих паркинг карата, као и извештавање.
   - ЈКП „Паркинг сервис“, Чачак редовно ажурира податке о паркинг зонама, могућностима плаћања и ценама на свом званичном сајту, што доприноси бољем информисању и управљању услугама за грађане. Током поступка ревизије, функционалност модула „Мапа“ за праћење доступности паркинг места у реалном времену, која на почетку ревизије није била у функцији, поново је омогућена, чиме је побољшана доступност информација корисницима. Међутим, модул „Графички приказ“ у систему „Synapse tech“ који такође служи за обавештавање о доступности паркинга, приступачан је само запосленима и не пружа податке у реалном времену. Поред тога, ЈКП „Паркинг сервис“, Чачак није омогућио коришћење отворених података и информисање путем стандардних мобилних апликација, што ограничава потенцијалне кориснике који би иначе могли приступати информацијама преко других дигиталних платформи.

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

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

[1] Приоритет 1 - Несврсисходности које је могуће отклонити у року од 90 дана.

безбедносне инциденте, вођење евиденције о предузетим активностима, као и обавезу извештавања и размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама (Налаз 1.1) – Приоритет 2[2];

3) да јасно дефинише одговорна лица задужена за све аспекте информационе безбедности, укључујући превенцију и реаговање на безбедносне инциденте, како би се обезбедила јасна подела дужности и одговорности и омогућио ефикасан надзор над свим аспектима информационе безбедности (Налаз 1.1) – Приоритет 1;
4) да успостави и имплементира процедуру чувања и контроле активности корисника и администратора кроз лог фајлове, како би се осигурало праћење и надзор над свим активностима на ИКТ систему (Налаз 1.2) – Приоритет 2;
5) да осигура да се у пракси води евиденција и контрола приватних уређаја који приступају ИКТ систему, како би се смањио ризик од неовлашћеног приступа и обезбедила безбедност система (Налаз 1.2) – Приоритет 1;
6) да ажурира Акт о безбедности информационо-комуникационог система како би укључио одредбе о изнајмљивању сервера и администрирању система од стране пружаоца услуга, са јасно дефинисаним мерама заштите и контроле приступа, у складу са важећим прописима и стандардима (Налаз 1.2) – Приоритет 1;
7) да развије и усвоји план континуитета пословања у ванредним околностима, који ће обезбедити континуитет пословања и неометано функционисање система у складу са уговорним обавезама према пружаоцу услуга (Налаз 1.3) – Приоритет 2;
8) да успостави процес управљања ИТ ризицима, укључујући дефинисање послова и одговорности у овој области у Правилнику о систематизацији радних места (Налаз 1.4) – Приоритет 1;
9) да усвоји и имплементира процедуре које ће уредити сарадњу са пружаоцима услуга, укључујући јасно дефинисане одговорности за контролу приступа подацима и надзор над извршењем уговорних обавеза (Налаз 2.1) – Приоритет 2;
10) да документује све активности везане за надзор над пружаоцима услуга, укључујући праћење приступа подацима и извршење уговорних обавеза, како би се обезбедила адекватна заштита података и поузданост система (Налаз 2.1) – Приоритет 2;
11) да успостави механизам за контролу усаглашености пружаоца услуга са условима за заштиту података, укључујући редовне провере и документацију свих активности везаних за безбедност података (Налаз 2.2) – Приоритет 1;
12) да ревидира уговор са пружаоцем услуга како би укључио одредбе о заштити и обради података у складу са Законом о заштити података о личности, са јасно дефинисаним одговорностима и обавезама обе стране (Налаз 2.2) – Приоритет 2;
13) да успостави јасне процедуре за управљање корисничким налозима, укључујући процедуре за деактивацију корисничких налога приликом престанка радног односа или промене радног места (Налаз 3.1) – Приоритет 2;

[2] Приоритет 2 – Несврсисходности које је могуће отклонити у року до годину дана.

14) да обезбеди механизме за спречавање трајног брисања налога без угрожавања интегритета података, као и да омогући праћење активности корисника како би се осигурао потпуни траг активности у систему (Налаз 3.1) – Приоритет 2;
15) да спроведе редовну проверу и ажурирање корисничких налога како би се осигурало да приступ систему имају само овлашћена лица (Налаз 3.1) – Приоритет 1;
16) да омогући коришћење отворених података и развој мобилне апликације како би се грађанима омогућио лакши приступ информацијама о паркинг услугама (Налаз 3.3) – Приоритет 3[3].

2. Мере предузете у поступку ревизије

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

3. Захтев за достављање одазивног извештаја

Јавно комунално предузеће „Паркинг сервис“, Чачак 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“, Чачак 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“, Чачак 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“, Чачак 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

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

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 14:36:58 +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[4], Пословником Државне ревизорске институције[5] и Програмом ревизије Државне ревизорске институције за 2024. годину.

Ревизија је обављена на начин и према поступцима утврђеним Оквиром професионалних стандарда Међународне организације врховних ревизорских институција (INTOSAI), Кодексом професионалне етике државних ревизора и принципима Међународних стандарда врховних ревизорских институција (ISSAI).

1. Проблем

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

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

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

ИТ системи су од кључног значаја за пословање у оквиру јавног сектора и активности постају све скупље, сложеније и као и степен осетљивости података које оне садрже. Осим тога, иницијативе е-управе у Србији имају за циљ унапређење коришћења ИТ и интернета широм јавне управе да би се обезбедиле информације грађанима и привредним друштвима. Институција је кроз своје ревизије ранијих година утврдила да неки субјекти ревизије нису предузели неопходне мере у области безбедности ИТ система - укључујући и право на приступ подацима и поверљивост података. Нису спровели неопходне процене ризика, нити су усвојили стратегије које регулишу развој ИТ технологија. Ово неадекватно планирање ИТ развоја довело је до кашњења у реализацији пројеката укључујући и нови интегрисани пословни ИТ систем и резултирало је у додатним трошковима.

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

2. Циљ ревизије

Циљ ревизије је био да се оцени ефективност и ефикасност информационог система у ЈКП „Паркинг сервис“, Чачак 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

[4] „Службени гласник РС“, бр. 101/05, 54/07, 36/10 и 44/18-др.закон
[5] „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 пружаоцима услуга испунио све неопходне циљеве, укључујући и поузданост података?

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

3. У којој мери успостављене апликативне контроле обезбеђују контролу наплате карата и 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 пружаоцима услуга. Као и у случају претходна два питања, најпре се анализирају правила и процедуре које се односе на сарадњу са пружаоцима услуга, а посебно када је у питању ИТ безбедност, тј. заштита података. Такође, потребно је анализирати механизам за контролу спровођења уговора, нарочито у погледу поверљивости. У том смислу потребно је анализирати обавезе субјекта и судова у вези Закона о заштити података о личности.

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

У вези са информационим системом „Synapse tech“ doo из Београда, анализиране су области: информациона безбедност, успостављање ефективног механизма сарадње са пружаоцима услуга и апликативне контроле.

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

Током поступка ревизије спроведена је ревизија код пет субјеката, а извештаји су објављени на сајту Државне ревизорске институције. Овај извештај садржи налазе и закључке утврђене у ревизији ЈКП „Паркинг сервис“, Чачак.

Детаљнији опис коришћене методологије дат је у Прилогу 1.

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

III Опис предмета ревизије

Информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост и аутентичност тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица[7].

Успостављање ефективног механизма сарадње са пружаоцима услуга кључно је како би се осигурало да се услуге пружају у складу са очекивањима и потребама субјекта.. . Субјект ревизије треба да има процесе у циљу обезбеђивања периодичног праћења статуса пројекта, квалитета услуге и тестирања производа пре увођења у оперативно окружење. Осим тога, као део процеса праћења извршења обавеза пружаоца услуга, субјект ревизије може да врши и ревизију интерног процеса осигурања квалитета пружених услуга, како би се обезбедило да кадар пружаоца услуга прати уговорно одобрену политику и планове за све своје послове[8].

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 прописа и у наставку дајемо преглед најважнијих одредби према надлежностима.

Закон о локалној самоуправи

Законом је експлицитно дата општини надлежност[9] да, преко својих органа, у складу са Уставом и законом, уређује и обезбеђује обављање комуналних делатности. У том циљу, у складу са законом, јединица локалне самоуправе за остваривање својих права и дужности и за задовољавање потреба локалног становништва може основати предузећа, установе и друге организације које врше јавну службу, али и уговором, у складу са начелима конкуренције и јавности, поверити правном или физичком лицу обављање својих послова.

[7] Члан 7 став 3 Закона о информационој безбедности.
[8] WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions.
[9] „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[10].

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 комуналној делатности управљања јавним паркиралиштима[11]

Одлуком се одређују услови и начин обављања комуналне делатности управљања јавним паркиралиштима на територији Града Чачка, права и обавезе вршиоца комуналне делатности, обим и квалитет комуналних услуга, финансирање, начин вршења надзора над обављањем делатности управљања јавним паркиралиштима и друга питања која су од значаја за обављање делатности.

Одлука о усклађивању оснивачког акта јавног комуналног предузећа „Паркинг сервис“ Чачак са Законом о јавним предузећима[12]

Предузеће обавља делатност од општег интереса за Град Чачак.

Претежна делатност предузећа је пружање услужне делатности у копненом саобраћају. Поред претежне делатности, Јавно предузеће ће обављати и делатност изградња путева и аутопутева. Јавно предузеће може без уписа у регистар да врши и друге делатности које служе обављању претежне делатности, уколико за те делатности испуњава услове предвиђене Законом. Предузеће обавља комуналну делатност управљања јавним паркиралиштима и уредног задовољавања потреба крајњих корисника услуга.

Закон о информационој безбедности[13]

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

[10] „Службени гласник РС“, бр. 88/11, 104/16 и 95/18, члан 2 став 1
[11] „Службени лист Града Чачка“, бр. 23/21 и 10/22
[12] „Службени лист Града Чачка“, бр. 22/16, 8/19, 5/22 и 22/22
[13] „Службени гласник РС“, бр. 6/16, 94/17 и 77/19

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[14]

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[15]

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[16]

Уређује право на заштиту физичких лица у вези са обрадом података о личности и слободни проток таквих података, начела обраде, права лица на које се подаци односе, обавезе руковалаца и обрађивача података о личности, кодекс поступања, пренос података о личности у друге државе и међународне организације, надзор над спровођењем овог закона, правна средства, одговорност и казне у случају повреде права физичких лица у вези са обрадом података о личности, као и посебни случајеви обраде.

Чланом 42 Закона о заштити података о личности прописано је да се мере заштите уређују узимајући у обзир ниво технолошких достигнућа и трошкове њихове примене, природу, обим, околности и сврху обраде, као и вероватноћу наступања ризика и ниво ризика за права и слободе физичких лица који произилазе из обраде, руковалац је приликом одређивања начина обраде, као и у току обраде, дужан да:

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

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

[14] „Службени гласник РС“, број 94/16
[15] „Службени гласник РС“, број 94/16
[16] „Службени гласник РС“, број 87/18

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[17]

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.

[17] „Службени гласник РС“, број 94/17 и 52/21

Закон о електронској управи[18]

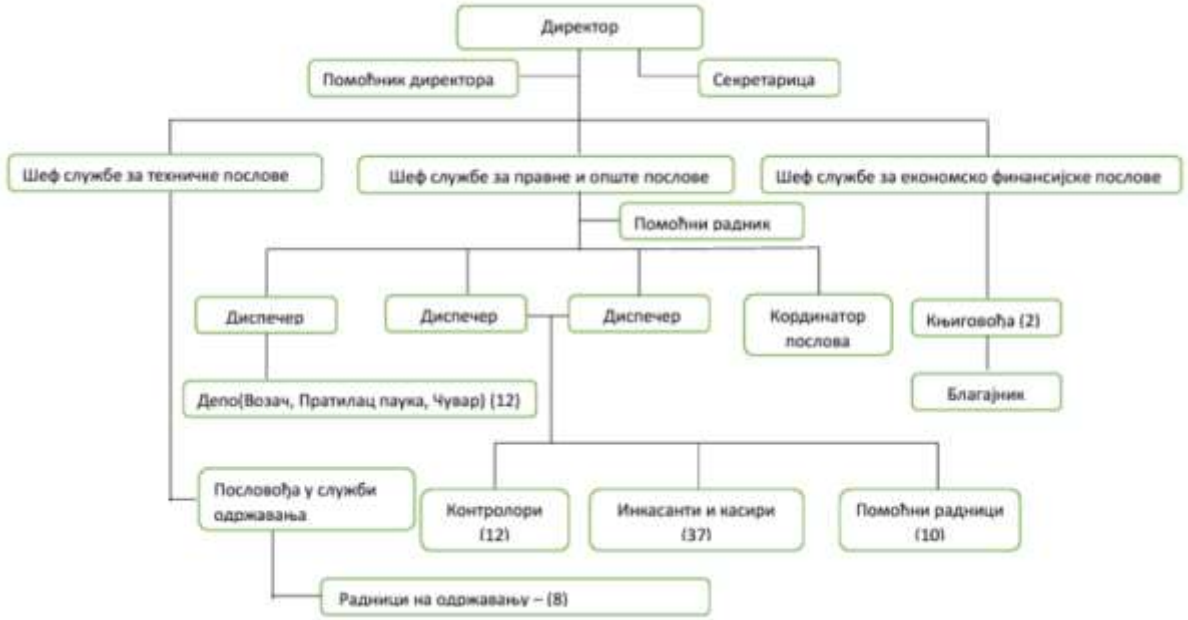
Као једно од начела наводи управо ефикасност управљања опремом, где прописује да је орган дужан да ефикасно управља опремом којом располаже тако да омогући њено правилно и економично коришћење.

[18] „Службени гласник РС“, број 27/2018

Институционални оквир

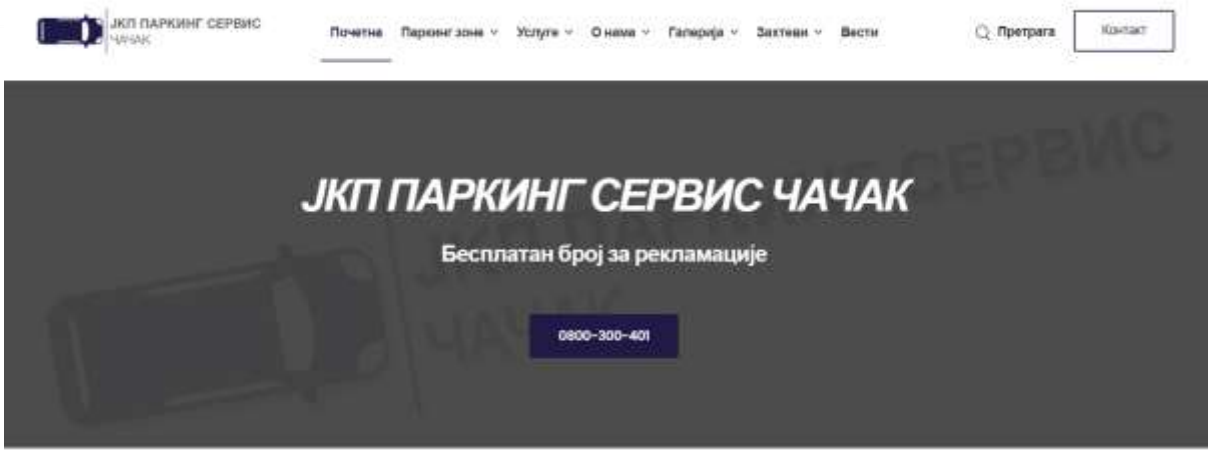
ЈКП „Паркинг сервис“, Чачак основано је Одлуком о оснивању Јавног комуналног предузећа „Паркинг сервис“ Чачак од 15. децембра 2008. године[19]. Основна делатност предузећа је услужна делатност у копненом саобраћају, што подразумева регулисање стационарног саобраћаја у граду Чачку. Поред претежне делатности предузеће обавља и делатност изградњу путева и аутопутева и то бојење и обележавање ознака на путевима, постављање ограда и саобраћајних ознака и сл, односно означавање општинских путева и улица вертикалном и хоризонталном сигнализацијом, односно постављање сигнализације у редовним и привременим условима. Предузеће врши и наплаћује услуге паркирања моторних возила на отвореним и затвореним паркиралиштима, као и услуге одношења неправилно паркираних и напуштених моторних возила. У надлежности предузећа су одржавање и обележавање паркиралишта.

Пружалац услуге информационог система је „Synapse tech“ doo из Београда. Систем је имплементиран 2015. године



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

[19] „Службени лист Града Чачка бр.12/08 и 15/13



Слика 4. Сајт ЈКП „Паркинг сервис“, Чачак

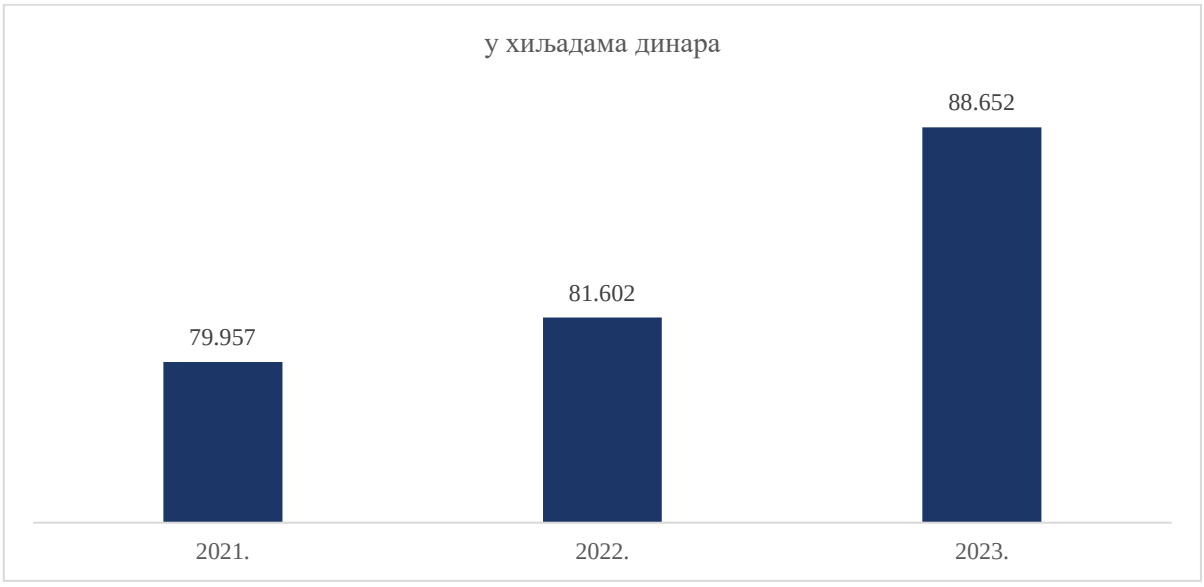
- *СМС:*
  Унети регистарску ознаку возила великим словима и без размака у тело поруке;
  У зависности од паркинг зоне пошаље се порука на кратки број
  Добија се повратна порука са информацијом о успешној уплати паркирања
  Неколико минута пре истека паркинг услуге добија се порука, која подсећа када истиче време паркирања, како би се могло продужити паркинг или благовремено уклонити возило.

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

Слика 5. Начини наплате паркирања у ЈКП „Паркинг сервис“, Чачак

Слика 6. Информација о доступности паркинг места

На основу анализе доступне документације и података које је доставило ЈКП „Паркинг сервис“, Чачак, 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.

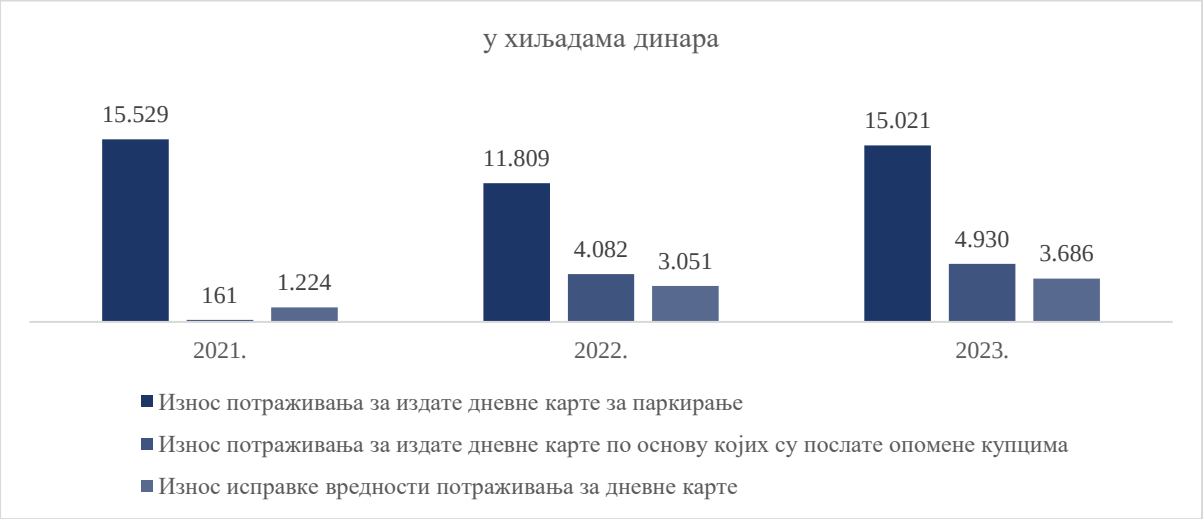


Графикон 1. Укупни приходи од паркирања у ревидираном периоду

Графикон 2. Структура прихода од паркирања у ревидираном периоду

На основу приказаних података, приходи ЈКП „Паркинг сервис“ Чачак показују умерен раст током анализираног периода, с највећим порастом у последњој години. Највећи удео прихода долази од сатних и дневних карата, што указује на доминацију краткорочног паркирања. Такође, постоји стабилан пораст прихода од месечних претплатних карата, док су приходи од посебних дневних карата варирали. Ова структура прихода указује на зависност од краткорочних услуга, али и на потенцијал за унапређење наплате услуга путем претплатних карата и других видова паркинг услуга.

Након анализе прихода који су остварени у области наплате паркинг услуга, важно је размотрити и кретање потраживања по основу посебних дневних карата. Посебне дневне карте 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 посебних дневних карата, што омогућава детаљнији увид у овај аспект пословања.



Графикон 3. Потраживања за посебне дневне карте у ревидираном периоду

На основу приказаних података о потраживањима по основу издатих дневних карата за паркирање, приметно је да се потраживања разликују током анализираних година. Потраживања за дневне карте су у једном периоду значајно расла, што указује на потребу за унапређењем механизама наплате. Иако су предузете одређене мере, висок ниво потраживања и даље представља изазов за предузеће. Неопходно је додатно појачати активности у циљу смањења потраживања, кроз боље праћење корисничких обавеза и правовремено реаговање на дуговања.

2. Информациони систем „Synapse tech“ doo из Београда

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

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

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

IV Закључци

На основу анализе података и документације достављене од стране ЈКП „Паркинг сервис“, Чачак, 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. Информациона безбедност није адекватно успостављена, јер нису предузете кључне мере заштите, укључујући управљање ИТ ризицима, контролу приступа и планове за континуитет пословања, што значајно угрожава безбедност и поузданост система за наплату услуга паркинга.
2. Иако је ЈКП „Паркинг сервис“, Чачак обезбедило континуитет пословања у случају раскида сарадње са пружаоцем услуга, недостају кључне процедуре за сарадњу, надзор и контролу заштите података, чиме се угрожава безбедност и поузданост података о корисницима.
3. Апликативне контроле обезбеђују основну контролу наплате и ажурирање података, али је потребно унапредити управљање корисничким налозима и омогућити коришћење отворених података за бољу доступност информација.

У наставку извештаја наводимо закључке са одговарајућим налазима.

ЗАКЉУЧАК 1: Информациона безбедност није адекватно успостављена, јер нису предузете кључне мере заштите, укључујући управљање ИТ ризицима, контролу приступа и планове за континуитет пословања, што значајно угрожава безбедност и поузданост система за наплату услуга паркинга

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“, Чачак није успоставило адекватну организацију и управљање информационом безбедношћу

Организација информационе безбедности у ЈКП „Паркинг сервис“, Чачак није успостављена на адекватан начин због недостатка стратешког планирања, непотпуног Акта о безбедности који не обухвата специфичности односа са пружаоцима услуга, као и недостатка процедура и докумената који би детаљно уредили послове информационе безбедности. Оваква организација оставља простор за нејасну поделу дужности и одговорности, што угрожава контролу и надзор над информационом безбедношћу и повећава ризик од безбедносних инцидената и других претњи информационом систему за наплату паркинг услуга.

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

ЈКП „Паркинг сервис“, Чачак 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“, Чачак није имало Акт о безбедности информационо-комуникационог система у периоду обухваћеним ревизијом, али је донео Акт о безбедности информационо-комуникационог система дана 25.3.2024. године. Наведени документ се односи на све информационе системе у предузећу, дакле не искључиво на информациони систем за наплату паркинг услуга. Између осталог, не садржи одредбе које се односе на поверавање послова, тј. однос са пружаоцима услуга, у конкретном случају то је фирма „Synapse tech“ доо, Београд.

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“, Чачак нема усвојене процедуре или слична документа које на детаљан начин уређују послове из области информационе безбедности, а у смислу праћења активности, ревизије и надзора у оквиру управљања информационом безбедношћу.

ЈКП „Паркинг сервис“, Чачак није документовало да је другим актима послове информационе безбедности уредило на начин који омогућава јасну поделу дужности и одговорности, али и контролу свих тих послова.

ЈКП „Паркинг сервис“, Чачак у Правилнику о систематизацији радних места дефинисао је два радна места које се односе на ИТ послове – помоћник директора предузећа који обавља и посао контроле рада СМС система и место координатор послова који сарађује са техничком службом у предузећу у делу који се односи на видео надзор и рад уређаја и опреме за систем СМС наплате паркирања. Од два предвиђена радна места попуњено је само место координатора послова.

Када су у питању послови који се односе на наплату паркинг услуга, шест запослених обавља послове контроле правилног коришћења и плаћања паркиралишта. Код двоје запослених у опису посла је наведена безбедност и заштита на раду, као и да евидентира пропусте и проблеме у раду наплате паркинга и рада „паук“ возила и настоји да их отклони.

ЈКП „Паркинг сервис“, Чачак није утврдило процедуре нити дефинисало 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.

Препоручујемо ЈКП „Паркинг сервис“, Чачак да ажурира Акт о безбедности информационо-комуникационог система како би уредили све специфичности које се односе на информациони систем за наплату паркинг услуга, укључујући јасно дефинисане одредбе о поверавању послова и односу са пружаоцима услуга.

Препоручујемо ЈКП „Паркинг сервис“, Чачак да усвоји и имплементира процедуре које детаљно уређују послове из области информационе безбедности, укључујући превенцију и реаговање на безбедносне инциденте, вођење евиденције о предузетим активностима, као и обавезу извештавања и размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама.

Препоручујемо ЈКП „Паркинг сервис“, Чачак да јасно дефинише одговорна лица задужена за све аспекте информационе безбедности, укључујући превенцију и реаговање на безбедносне инциденте, како би се обезбедила јасна подела дужности и одговорности и омогућио ефикасан надзор над свим аспектима информационе безбедности.

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[20].

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

[20] 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“, Чачак није успоставило адекватан процес управљања и контроле приступа софтверу за паркирање

Иако је Актом о безбедности ИКТ система предвиђено да Координатор ИКТ послова контролише приступ ресурсима система и води евиденцију приватних уређаја који приступају систему, ове процедуре нису адекватно примењене у пракси. Лог фајлови активности корисника и администратора се не чувају, што онемогућава праћење и контролу активности на систему. Поред тога, сервери су изнајмљени и налазе се код пружаоца услуга „Synapse tech“, Београд, али ово изнајмљивање и администрирање од стране пружаоца услуга нису адекватно регулисани у Акту о безбедности информационо-комуникационог система, што угрожава физичку и логичку безбедност система.

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

Корисничке налоге додељује Координатор ИКТ послова, у складу са чланом 16 Акта о безбедности ИКТ система ЈКП „Паркинг сервис“, Чачак.

Чланом 8 је дефинисано између осталог да је за контролу и надзор над обављањем послова корисника, у циљу заштите и безбедности ИКТ система надлежан Координатор ИКТ послова.

Чланом 10 је дефинисано да је Координатор ИКТ послова дужно да контролише приступ ресурсима ИКТ система предузећа и проверава да ли има приступа са непознатих уређаја. Није међутим успостављена процедура о чувању и контроли активности корисника и администратора (лог фајлови). Лог фајлови се не чувају у ЈКП „Паркинг сервис“, Чачак.

Чланом 7 је дефинисано да Координатор ИКТ послова води евиденцију приватних уређаја са којих ће бити омогућен приступ ИКТ систему. Ови уређаји морају бити подешени од стране одговорног лица за надзор спровођења VPN процедуре и могу се користити само за обављање послова у надлежности корисника и то у периоду када није могуће користити уређај у власништву предузећа. У пракси, не врши се евиденција нити контрола уређаја са којих се приступа систему.

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

Чланом 17 је дефинисано да се у циљу физичке сигурности информатичких ресурса морају обезбедити следећи услови: да сервери морају бити смештени у посебној просторији, тј. сервер соби, да приступ соби, поред лица која су задужена за одржавање ИКТ система, могу имати и друга лица, уз претходно одобрење директора предузећа, односно овлашћеног лица – Координатора ИКТ послова, такође, дефинисано је и да приступ медијима са поверљивим подацима морају бити заштићени од неауторизованог приступа и прегледа. Међутим, сервер рачунари се како је то наведено у техничкој спецификацији налазе код пружаоца услуга „Synapse tech“, Београд у складу са Уговорима о јавној набавци[21].

Како су навела одговорна лица у ЈКП „Паркинг сервис“, Чачак, администраторски налог има и фирма „Synapse tech“, Београд.

Актом о информационој безбедности није дефинисано и предвиђено изнајмљивање сервера нити администрирање које обавља пружалац услуга.

Препоручујемо ЈКП „Паркинг сервис“, Чачак да успостави и имплементира процедуру чувања и контроле активности корисника и администратора кроз лог фајлове, како би се осигурало праћење и надзор над свим активностима на ИКТ систему.

[21] Уговор број 255/6 од 25.4.2024. године

Препоручујемо ЈКП „Паркинг сервис“, Чачак да осигура да се у пракси води евиденција и контрола приватних уређаја који приступају ИКТ систему, како би се смањио ризик од неовлашћеног приступа и обезбедила безбедност система.

Препоручујемо ЈКП „Паркинг сервис“, Чачак да ажурира Акт о безбедности информационо-комуникационог система како би укључио одредбе о изнајмљивању сервера и администрирању система од стране пружаоца услуга, са јасно дефинисаним мерама заштите и контроле приступа, у складу са важећим прописима и стандардима.

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“, Чачак није успоставило план континуитета пружања услуге паркинга у ванредним околностима

ЈКП „Паркинг сервис“, Чачак није успоставило план или процедуру за континуитет пословања у ванредним околностима, иако је Уговором о јавној набавци са пружаоцем услуга „Synapse tech“ Београд дефинисано да комплетна инфраструктура мора обезбедити неометано функционисање система. Недостатак овог плана повећава ризик од прекида у пружању услуга у случају ванредних околности, што може значајно утицати на континуитет пословања и квалитет услуга које субјекат ревизије пружа корисницима. Овај пропуст делом је последица недовољног броја запослених који се баве пословима информационе безбедности, што отежава правовремено планирање и имплементацију мера заштите.

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

ЈКП „Паркинг сервис“, Чачак није успоставило план/процедуру континуитета пословања у ванредним околностима. Уговором о јавној набавци ЈН 64/12 – Одржавање СМС система са модулом за контролу и наплату паркирања са фирмом „Synapse tech“ Београд дефинисано је да комплетна инфраструктура мора имати неометано функционисање система.

Препоручујемо ЈКП „Паркинг сервис“, Чачак да развије и усвоји план континуитета пословања у ванредним околностима, који ће обезбедити континуитет пословања и неометано функционисање система у складу са уговорним обавезама према пружаоцу услуга.

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

Влада Републике Србије је обавезе оператора ИКТ система детаљније уредила Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја. Члан 29 наведене Уредбе уређује мере које обезбеђују континуитет обављања посла у ванредним околностима и то:

- Оператор ИКТ система треба да предвиди мере којима се обезбеђује обављање послова у ванредним околностима, а које подразумевају одржавање информационе безбедности на задовољавајућем нивоу, дефинисање

одговорности, планова, поступака у случају ванредних догађаја и процедура за опоравак ИКТ система, у оквиру редовних процедура за одржавање информационе безбедности или доношењем посебних процедура.

- Оператор ИКТ система треба да успостави, документује, имплементира и одржава процесе, процедуре и контроле да би осигурао захтевани ниво континуитета пословања током ванредне ситуације.
- Оператор ИКТ система треба да верификује успостављене и имплементиране контроле континуитета пословања у редовним условима рада, како би оне биле важеће и ефективне током ванредне ситуације.
- Оператор ИКТ система треба да идентификује захтеве за доступност ИКТ система. Редундантне компоненте треба размотрити онда када се доступност не може гарантовати коришћењем постојећих архитектура система.

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

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

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

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

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

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

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

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

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

Нестанак електричне енергије, нарочито у дужем периоду, поплава, земљотрес, пожар, па чак и крађа или намерно оштећење опреме су догађаји које се не могу предвидети, а који могу систем или део система оштетити у толиком проценту да је онемогућено његово функционисање. Ово се чак може односити и на саму зграду у којој се систем налази.

План опоравка од катастрофе, када су ови ризици у питању, садржи мере које су усмерене на опремање и употребу секундарне (резервне) локације у оваквим случајевима. Та локација се успоставља на удаљености која треба да обезбеди њено

функционисање у случају неких од наведених догађаја (наравно, у зависности од природе послова, њиховог обима и важности, величине система итд). На резервној локацији се поставља неопходна опрема за функционисање система: електрично напајање, мрежна инфраструктура, секундарни сервери – апликативни и за складиштење података итд.

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

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

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

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

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

Налаз 1.4: ЈКП „Паркинг сервис“, Чачак није успоставило управљање ИТ ризицима

ЈКП „Паркинг сервис“, Чачак није успоставило процес управљања ИТ ризицима, због недостатка јасно дефинисаних послова у вези са управљањем ризицима у Правилнику о систематизацији радних места. Овај пропуст директно утиче на одсуство запослених који би се бавили управљањем ИТ ризицима, што може довести до повећаног ризика од нежељених догађаја који могу угрозити функционисање ИКТ система, резултирати губитком података или изазвати друге негативне последице по пословање.

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

ЈКП „Паркинг сервис“, Чачак није успоставило управљање ИТ ризицима. У Правилнику о систематизацији радних места нису дефинисани послови који се односе на управљање ризицима, а самим тим у предузећу не постоје запослени који се баве наведеним послом.

Препоручујемо ЈКП „Паркинг сервис“, Чачак да успостави процес управљања ИТ ризицима, укључујући дефинисање послова и одговорности у овој области у Правилнику о систематизацији радних места.

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.

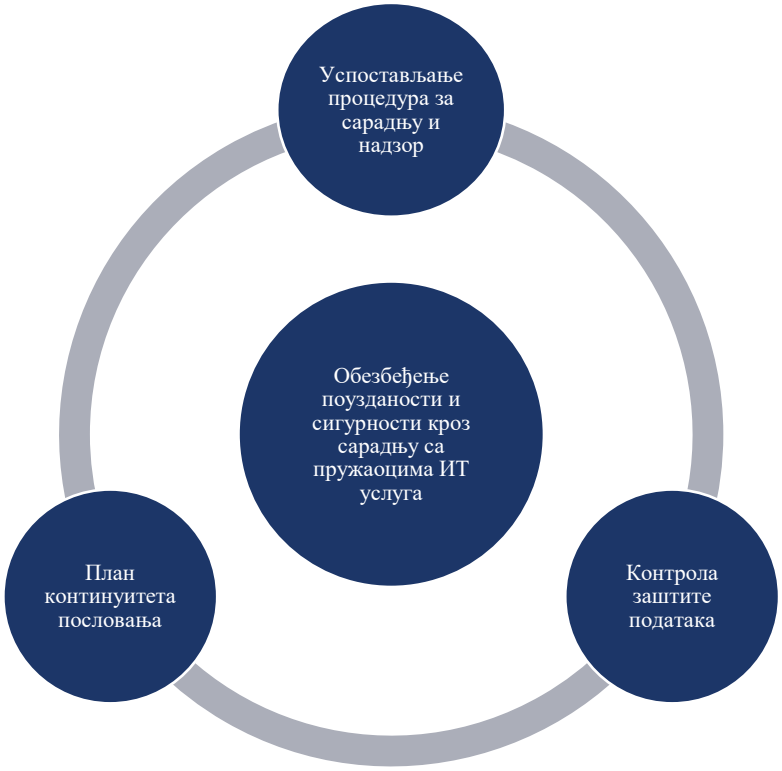
Уколико се жели поуздан, али истовремено и ефикасан систем, без процене ризика то се не може постићи. На пример, могуће је све елементе система дуплирати, и тако постићи скоро 100% поуздан систем. Али због цене дуплирања, такав систем се не може сматрати ефикасним, јер се можда исти циљ (поузданост) 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: Иако је ЈКП „Паркинг сервис“, Чачак обезбедило континуитет пословања у случају раскида сарадње са пружаоцем услуга, недостају кључне процедуре за сарадњу, надзор и контролу заштите података, чиме се угрожава безбедност и поузданост података о корисницима

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



Слика 8. Графички приказ обезбеђења поузданости и сигурности кроз сарадњу са пружаоцима ИТ услуга

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

Налаз 2.1: ЈКП „Паркинг сервис“, Чачак није успоставило процедуре за сарадњу и надзор над пружаоцима услуга

ЈКП „Паркинг сервис“, Чачак није усвојило процедуре које уређују сарадњу са пружаоцима услуга, иако је Актом о безбедности ИКТ система предвиђено да пружаоци услуга могу приступити само одређеним подацима и да је

Координатор ИКТ послова одговоран за контролу приступа и надзор над извршењем уговорних обавеза. Међутим, услед тога што је Координатор ИКТ послова једина особа која обавља ове задатке, а уз то постоје други радни задаци које обавља, недостају документи који доказују да се овај надзор адекватно спроводи. Ова ситуација оставља систем изложен ризицима од неадекватног управљања приступом и недовољне заштите података.

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

Нису усвојене процедуре које уређују сарадњу са пружаоцем услуга. Акт о безбедности ИКТ система у ЈКП „Паркинг сервис“, Чачак, 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. Дефинисано је да је Координатор ИКТ послова одговоран за контролу приступа и надзор над извршењем уговорних обавеза. ЈКП „Паркинг сервис“, Чачак није документовало да се овај надзор обавља, и на који начин.

Препоручујемо ЈКП „Паркинг сервис“, Чачак да усвоји и имплементира процедуре које ће уредити сарадњу са пружаоцима услуга, укључујући јасно дефинисане одговорности за контролу приступа подацима и надзор над извршењем уговорних обавеза.

Препоручујемо ЈКП „Паркинг сервис“, Чачак да документује све активности везане за надзор над пружаоцима услуга, укључујући праћење приступа подацима и извршење уговорних обавеза, како би се обезбедила адекватна заштита података и поузданост система.

ИТ послове из области информационе безбедности када је у питању сарадња са пружаоцима услуга је неопходно детаљно уредити у смислу примене правила и процедуре које се односе на безбедност података, праћења активности, ревизије и надзора у оквиру управљања информационом безбедношћу. На тај начин се са једне стране пружа могућност за контролу квалитета рада на тим пословима, а са друге стране омогућава да у случајевима кадровских промена, новозапослена лица могу веома брзо и лако наставити са свим пословима, што би у случају да процедура нема било скоро немогуће, или немогуће у неком краћем временском периоду. Како би биле функционалне, неопходно је да процедуре буду довољно детаљне и свеобухватне, да поред описа свих процеса садрже и податке ко ради на којој активности (не у смислу имена него у смислу одређеног радног места), као и податке о изменама итд.

Уредбом о ближем уређењу мера заштите ИКТ система од посебног значаја предвиђена је заштита средстава оператора ИКТ система која су доступна пружаоцима услуга тако да оператор ИКТ система у својим процедурама предвиђа ниво доступности и врсту информација и средства којима могу да приступе пружаоци услуга, начине

приступа информацијама и средствима и надзор над приступом. Оператор ИКТ система треба да идентификује и успостави процедуре безбедности информација које се конкретно баве приступом информацијама пружаоца услуга унутар организације. Обавезе пружаоца услуга у вези са информацијама и средствима која су доступна пружаоцима услуга оператора ИКТ система регулишу се споразумом између оператора ИКТ система и пружаоца услуга, чијим одредбама се обезбеђује адекватан ниво заштите информација и средстава, у складу са прописима и техничким стандардима. Оператор ИКТ система дужан је да обезбеди да пружалац услуга обавља поверене активности у складу са актом о безбедности ИКТ система, односно другим актима којима се уређује безбедност његовог информационог система (члан 26).

Налаз 2.2: ЈКП „Паркинг сервис“, Чачак није успоставило механизам за контролу заштите података од стране пружаоца услуга

ЈКП „Паркинг сервис“, Чачак није успоставило механизам за контролу да ли пружалац услуга испуњава услове за заштиту података и није документовао начин праћења извршења уговора у смислу безбедности података. Уговор са пружаоцем услуга не уређује однос у складу са Законом о заштити података о личности, што је резултирало тиме да пружалац услуга има неконтролисан приступ осетљивим личним подацима грађана, укључујући регистарски број, адресу, контакт телефон и друге личне податке. Такође, подаци који више нису потребни нису адекватно заштићени или уклоњени, што представља озбиљан ризик за безбедност и приватност података.

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

Није успостављен механизам када је у питању сарадња са пружаоцем услуга и контрола да ли је пружалац услуге усвојио услове за заштиту података, и да ли их спроводи. Такође, није документован начин на који се прати извршење уговора у делу безбедности података. ЈКП „Паркинг сервис“, Чачак је у смислу Закона о заштити података о личности, руковалац подацима. Пружалац услуге, фирма „Synapse tech“ доо, Београд у овом случају је обрађивач података. Уговором није уређен однос у смислу примене одредаба Закона о заштити података. Правилником о ИКТ систему је дефинисано 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. Уговором није дефинисана заштита и обрада података.

Што се тиче корисника система јасно су дефинисана корисничка права корисника у складу са послом којим је дефинисано у систематизацији радног места.

Приликом подношења захтева за добијање претплатних карата, грађани се на посебним формуларима сагласе са тиме да се може вршити обрада њихових података. Након завршеног процеса издавања месечне паркинг карте, подаци као што су ЈМБГ и број личне карте се не уносе у систем, па је ризик на осетљиве податке мали, међутим у базама података, чувају се лични подаци о грађанима којима су издате дневне карте

односно претплатници (име и презиме, регистарски број, адреса, контакт телефон), и у те податке пружалац услуга има увек увид, тачније може да врши обраду података без контроле од стране руковаоца, тачније ЈКП „Паркинг сервис“, Чачак.

Препоручујемо ЈКП „Паркинг сервис“, Чачак да успостави механизам за контролу усаглашености пружаоца услуга са условима за заштиту података, укључујући редовне провере и документацију свих активности везаних за безбедност података.

Препоручујемо ЈКП „Паркинг сервис“, Чачак да ревидира уговор са пружаоцем услуга како би укључио одредбе о заштити и обради података у складу са Законом о заштити података о личности, са јасно дефинисаним одговорностима и обавезама обе стране.

Механизам сарадње са пружаоцима ИТ услуга може да обухвати скуп политика, процедура, упутстава, докумената, али и активности које су усмерене на идентификацију циљева и послова за чије остварење, тј. обављање се користе информациони системи, израду специфичних захтева у смислу потреба за хардверским, софтверским и људским ресурсима, али и примене стандарда, начине на које се ангажују пружаоци услуга, стандардизацију уговора који се потписују са пружаоцима услуга, а који подразумевају и делове који се односе на информациону безбедност, начин на који се прате пружене услуге, осигурава законитост у раду, обезбеђује континуирана сарадња и комуникација, евидентирање будућих потреба, припрему и имплементацију нових захтева, одређивање лица која су задужена за сарадњу са пружаоцима услуга итд. ИТ послове из области информационе безбедности када је у питању сарадња са пружаоцима услуга је неопходно детаљно уредити у смислу примене правила и процедура које се односе на безбедност података, праћења активности, ревизије и надзора у оквиру управљања информационом безбедношћу. Када су у питању информациони системи у јавним предузећима за наплату услуга паркинга, предузећа су руковаоци подацима, док су у случају ангажовања пружаоца услуга, они обрађивачи. Законом о заштити података о личности, прописане су обавезе и однос руковаоца и обрађивача, нарочито када су у питању безбедносне мере. Ако се обрада врши у име руковаоца, руковалац може да одреди као обрађивача само оно лице или орган власти који у потпуности гарантује примену одговарајућих техничких, организационих и кадровских мера, на начин који обезбеђује да се обрада врши у складу са одредбама овог закона и да се обезбеђује заштита права лица на које се подаци односе (став 1). Анализом мера заштите, може се закључити да ли су све неопходне мере прописане и примењене. Законом о информационој безбедности уређују се мере заштите ИКТ система од посебног значаја.

Када су у питању пружаоци услуга, треба истаћи неке од најважнијих чланова закона који уређују питања заштите информационих система и поверљивости података.

Закон о информационој безбедности, у члану 7 уређује мере заштите ИКТ система од посебног значаја и то:

Оператор ИКТ система од посебног значаја одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система. Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

Мере заштите ИКТ система се, између осталог, односе на: заштиту средстава оператора ИКТ система која су доступна пружаоцима услуга (став 3 тачка 25) и одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга (став 3 тачка 26).

Уредбом о ближем уређењу мера заштите ИКТ система од посебног значаја прописано је у члану 26 да оператор ИКТ система у својим процедурама предвиђа ниво доступности и врсту информација и средства којима могу да приступе пружаоци услуга, начине приступа информацијама и средствима и надзор над приступом. Оператор ИКТ система треба да идентификује и успостави процедуре безбедности информација које се конкретно баве приступом информацијама пружаоца услуга унутар организације. Обавезе пружаоца услуга у вези са информацијама и средствима која су доступна пружаоцима услуга оператора ИКТ система регулишу се споразумом између оператора ИКТ система и пружаоца услуга, чијим одредбама се обезбеђује адекватан ниво заштите информација и средстава, у складу са прописима и техничким стандардима. Оператор ИКТ система дужан је да обезбеди да пружалац услуга обавља поверене активности у складу са актом о безбедности ИКТ система, односно другим актима којима се уређује безбедност његовог информационог система. У члану 27 је прописано да у циљу одржавања уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга, оператор ИКТ система успоставља механизме надзора над пружањем услуга, именује лице које је задужено за праћење реализације пружања услуга и контролу испуњености нивоа информационе безбедности, применом одговарајућих процедура и успоставом надзора.

Налаз 2.3: ЈКП „Паркинг сервис“, Чачак је обезбедило континуитет пружања услуга паркинга у случају раскида сарадње са пружаоцем услуга

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

У постојећим уговорима са пружаоцем услуга је предвиђена активност или обавеза пружаоца услуга у случају раскида сарадње, или непродужења уговора. У систему које је тренутно у употреби, у случају раскида сарадње било би омогућено праћење слободних паркинг места па самим тим и омогућено информисање грађана о временском интервалу паркирања као и продаја паркинг карата, контрола паркираних возила итд.

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

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

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

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

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

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

Влада Републике Србије је обавезе оператора ИКТ система детаљније уредила Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја. Члан 29 наведене Уредбе уређује мере које обезбеђују континуитет обављања посла у ванредним околностима и то:

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

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

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

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

ЗАКЉУЧАК 3: Апликативне контроле обезбеђују основну контролу наплате и ажурирање података, али је потребно унапредити управљање корисничким налозима и омогућити коришћење отворених података за бољу доступност информација

Циљ овог дела извештаја био је да оцени у којој мери успостављене апликативне контроле обезбеђују ефикасну контролу наплате и тачност пружених услуга у ЈКП „Паркинг сервис“, Чачак. 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“, Чачак није успоставило процедуре и контроле за управљање корисничким налозима у апликацији за наплату и доступност паркинг места

ЈКП „Паркинг сервис“, Чачак није дефинисало процедуре и упутства за управљање апликацијама које се користе за наплату и праћење доступности паркинг места. Непостојање механизама за деактивацију корисника доводи до ризика од неконтролисаног приступа систему. Трајно брисање корисничког налога не онемогућава приступ систему, а преименовање корисничког налога доводи до губитка података и трагова активности претходних запослених, што угрожава интегритет података и поузданост система. Ова ситуација може бити последица недостатка ресурса и техничке подршке за развој и одржавање апликација, као и недовољно дефинисаних одговорности запослених за имплементацију безбедносних мера у систему.

ЈКП „Паркинг сервис“, Чачак није успоставио процедуре и упутстава којима се уређују пословни процеси РЈ Паркинг сервиса а који се користе за употребу апликације за наплату и апликације за доступност паркинг места.

Није успостављен механизам приликом деактивације корисника, у систему је омогућено да се „деактивација корисника“ врши на два начина:

- Трајно брисање из система
- Преименовање налога на ново запосленог

Приликом трајног брисања из система апликативна контрола није функционисала јер корисник је и даље могао да се улогује, а брисањем из базе довело би да се бришу подаци које би унео тај корисник, а у случају преименовања корисника долази да претходни запослени није ни радио у предузећу и не постоји траг његових уноса података.

Препоручујемо ЈКП „Паркинг сервис“, Чачак да успостави јасне процедуре за управљање корисничким налозима, укључујући процедуре за деактивацију корисничких налога приликом престанка радног односа или промене радног места.

Препоручујемо ЈКП „Паркинг сервис“, Чачак да обезбеди механизме за спречавање трајног брисања налога без угрожавања интегритета података, као и да омогући праћење активности корисника како би се осигурао потпуни траг активности у систему.

Препоручујемо ЈКП „Паркинг сервис“, Чачак да спроведе редовну проверу и ажурирање корисничких налога како би се осигурало да приступ систему имају само овлашћена лица.

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.

Поред тога, упутства за употребу апликација морају бити доступна свим запосленима како би се обезбедила доследна примена правила и процедура за управљање корисничким налозима и приступом.

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

ЈКП „Паркинг сервис“, Чачак 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“, Чачак успешно ажурира податке о паркинг зонама, али није омогућило коришћење отворених података и информисање путем мобилних апликација

ЈКП „Паркинг сервис“, Чачак редовно ажурира податке о паркинг зонама, могућностима плаћања и ценама на свом званичном сајту, што доприноси бољем информисању и управљању услугама за грађане. Током поступка ревизије, функционалност модула „Мапа“ за праћење доступности паркинг места у реалном времену, која на почетку ревизије није била у функцији, поново је омогућена, чиме је побољшана доступност информација корисницима. Међутим, модул „Графички приказ“ у систему „Synapse tech“ који такође служи за обавештавање о доступности паркинга, приступачан је само запосленима и не пружа податке у реалном времену. Поред тога, ЈКП „Паркинг сервис“, Чачак није омогућио коришћење отворених података и информисање путем стандардних мобилних апликација, што ограничава потенцијалне кориснике који би иначе могли приступати информацијама преко других дигиталних платформи.

ЈКП „Паркинг сервис“, Чачак паркинг услуге обавља путем свог официјалног сајта[22] обавештења о паркинг зонама, депо, могућност плаћања и ценовник се редовно ажурирају, што доводи до бољег управљања и информисања грађана.

Како нам је објашњено ти подаци се добијају од стране контролора па доступност паркинг места није у реалном времену. Али на сајту имају посебан одељак „Мапа“ која обавештава грађане о доступност паркинг места на територији града Чачка у реалном времену, али у току ревизије није функционисало.

[22] https://parkingcacak.co.rs/

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 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 о тренутној 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 јавних комуналних предузећа.

У граду Чачку, није омогућено информисање путем стандардних апликација на мобилним уређајима.

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

Препоручујемо ЈКП „Паркинг сервис“, Чачак да омогући коришћење отворених података и развој мобилне апликације како би се грађанима омогућио лакши приступ информацијама о паркинг услугама.

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.

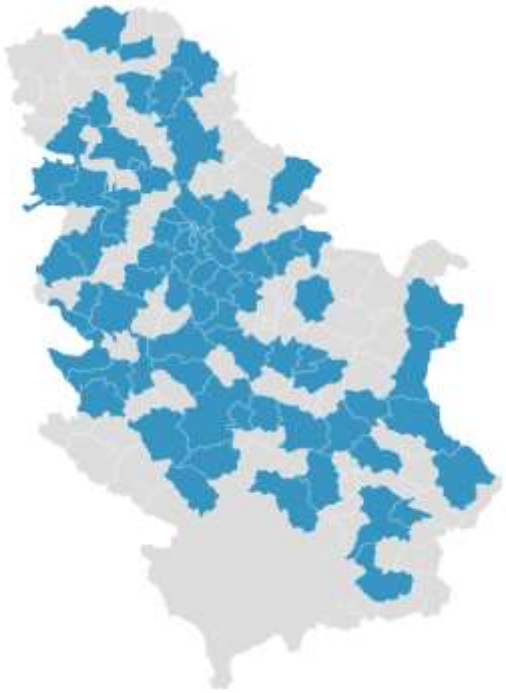
Пожељно је да подаци буду у машински читљивом формату, што би омогућило њихову лакшу употребу од стране физичких и правних лица, без додатних трошкова. Уз примену отворених података, предузећа би могла значајно побољшати транспарентност и приступачност својих услуга, омогућавајући корисницима да информације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

[23] https://data.gov.rs/sr/

V Прилози

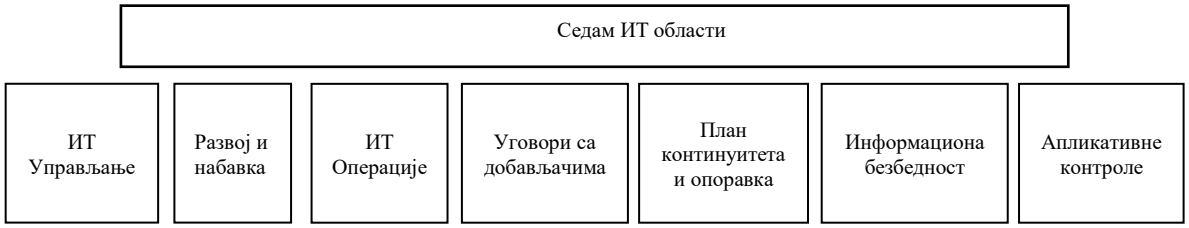
Прилог 1. Методологија у поступку рада

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 9. 61 ЈЛС које имају информациони систем преког које врше паркинг сервис услуге

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



Слика 10. 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:

- Анализа како је уређен приступ пружаоца услуге информационим системима и серверима, као и другим потребним ресурсима и да ли се то евидентира и где;
- Провера да ли се прати извршење обавеза пружаоца услуге када су у питању нивои услуга дефинисани уговором;
- Провера извештаја о безбедносним инцидентима и докумената за праћење како би се утврдило које активности субјект предузима када пружалац услуге крши безбедносна правила и процедуре;
- Провера процедура које је субјекат предузео а које се односе на питања поверљивости;
- Провера да ли уговорни услови и обавезе дефинишу безбедносна ограничења и обавезе које контролишу како ће пружаоц услуге користити имовину организације и приступати информационим системима и услугама;
- Провера да ли су пружаоци услуга извршили повреде безбедности информација. Провера активности руководства у погледу таквих кршења;
- Анализа шта су примарне контроле физичке безбедности система. Провера да ли одговарају најновијој анализи ризика;
- Прегледање локацијских и физичких мера предострожности у смислу кључних елемената ИТ инфраструктуре. Провера какве су контроле за заштиту животне средине успостављене (апарат за гашење пожара, аларм, системи за напајање, итд.);
- Провера процедура у циљу утврђивања колико често се прегледају различити приступи и привилегије које запослени код пружаоца услуга имају;
- Провера да ли постоје документоване процедуре за обележавање осетљивих излазних информација апликација и, где је то потребно, слање осетљивих излазних информација на посебне уређаје са контролом приступа;

- Добијање документације и процена пројекта, имплементације, приступа и прегледање;
- Провера да ли је, уз нулте или минималне трошкове, могуће из постојећег система добити додатне услуге, превасходно у области услуга ка грађанима;
- Да ли постоје капацитети да се услуге које сада обезбеђује пружалац услуга реализују унутар субјеката;
- Да ли је однос између субјеката и пружаоца услуга у складу 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.