ДРЖАВНА
РЕВИЗОРСКА
ИНСТИТУЦИЈА

ИЗВЕШТАЈ
О РЕВИЗИЈИ СВРСИСХОДНОСТИ ПОСЛОВАЊА

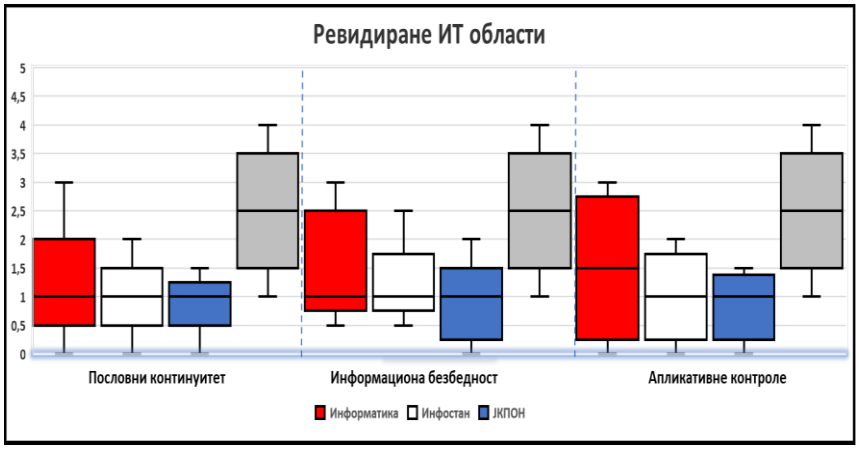
УПРАВЉАЊЕ ИНФОРМАЦИОНИМ СИСТЕМИМА У ЈАВНИМ ПРЕДУЗЕЋИМА ЗА ОБЈЕДИЊЕНУ НАПЛАТУ

Број: 400- 735/2020-03/26
Београд, 23. децембар 2020. године

НЕОПХОДНО УНАПРЕЂЕЊЕ УПРАВЉАЊА ИНФОРМАЦИОНИМ СИСТЕМИМА У ЈКП ЗА ОБЈЕДИЊЕНУ НАПЛАТУ РАДИ СПРЕЧАВАЊА ПОСЛЕДИЦА НЕЖЕЉЕНИХ ДОГАЂАЈА

У претходно спроведеним ревизијама финансијских извештаја и правилности пословања утврђена су неслагања у евиденцијама учесника у систему обједињене наплате. Обједињен обрачун и наплата комуналних услуга заснива се на јединственој обради и наплати неколико стотина различитих услуга за стотине хиљада корисника при чему сваки корисник има сопствени скуп услуга. Контрола појединичног рачуна није могућа без учешћа самог корисника и зато је развијен процес рекламација. Јавна комунална предузећа која учествују у систему треба да усклађују своје евиденције.

Желели смо да оценимо квалитет управљања информационим системом утврђивањем како функционишу контроле и да ли спречавају, откривају и отклањају неефикасности у управљању информационим системима јавних предузећа за обједињену наплату комуналних услуга.



Оцењивање зрелости процеса управљања ИТ ресурсима

Многи послови се обављају на уходан начин који често није документован, тако да поступање зависи од непосредног извршиоца. Тада могу настати разлике у поступању које доводе континуитет пословања предузећа под додатни ризик.

Смањење ризика у пословању које зависи од информационог система, могуће је бољим организовањем управљања безбедношћу, бољом комуникацијом и реаговањем код настанка таквих инцидената.

Иако постоји довољно стручног знања и вишедеценијског искуства, неопходно је иновирање апликативних контрола због растућих потреба корисника као и због нових законских обавеза. Размена података учесника у систему нема све неопходне заштитне механизме и непостојање аутоматизованог усклађивања евиденција ствара простор за честе грешке.

Препоруке

Државна ревизорска институција дала је препоруке ЈКП „Информатика“ Нови Сад, ЈКП „Инфостан технологије“ Београд и ЈКП „Обједињена наплата“ Ниш да:

- донесу План пословног континуитета;
- ИТ ризике уврсте у Регистар;
- врше процену утицаја ризика на пословање;
- израде План за ванредне ситуације;
- израде Планове опоравка од хаварије;
- успоставе процес управљања инцидентима;
- успоставе процес обавештавања и обучавања запослених о сајбер претњама;
- превентивно врше редовни преглед журнала на опреми ИС;
- обезбеде системе за електронско усклађивање евиденција са пружаоцима комуналних услуга;
- обезбеде заштитне хеш механизме за податке који се преносе кроз комуникационе канале;
- обезбеде заштитне механизме који ће осигурати да апликација обрађује само податке унетих употребом апликације;
- да приликом израде извештаја омогуће избор датума последње измене из претходног извештајног периода;
- израде Процену утицаја обраде на личне податке и план имплементације псеудонимизације личних података корисника.

Садржај

Скраћенице и термини

У прегледу су дате скраћенице које су коришћене у извештају:

Пун назив	Скраћеница
Информациони системи у јавним предузећима за обједињену наплату	ИСЈПОН
Јединице локалне самоуправе	ЈЛС
Јавно предузеће за обједињену наплату	ЈПОН
Јавно-комунално предузеће	ЈКП
Јавна комунална предузећа за обједињену наплату- субјекти ревизије	ЈКП за обједињену наплату – субјекти ревизије
Информационо-комуникациони систем	ИКТ систем
Оператор информационо-комуникационог система	Оператор ИКТ система
Информациони систем	ИС
Информационе технологије	ИТ
Дневник активности обраде података (енг. Log за бележење ревизорског трага енг. Audit trail) Ревизорски траг је запис који обезбеђује хронолошко документовање и праћење пословних промена у оквиру пословних процеса, активности или операција од почетка до краја.	Журнал
Закон о заштити података о личности	ЗЗПЛ
ЈКП „Обједињена наплата“ Ниш	ЈКПОН - Ниш

I Резиме и препоруке

Информациони системи у јавним предузећима која врше обједињену наплату комуналних услуга, обједињују податке корисника и пружалаца услуга. ДРИ је у спроведеним ревизијама финансијских извештаја и правилности пословања ЈКП за обједињену наплату у претходним годинама уочила неслагања са евиденцијама јавних комуналних предузећа које пружају комуналне услуге. Поред размене података између ЈКП за обједињену наплату и даваоца (пружалаца) комуналних услуга, план континуитета пословања и информациона безбедност система обједињене наплате су битни део информационог система обједињене наплате. Континуитет пословања и информациона безбедност су важни јер обезбеђују доступност и поузданост података, односно интегритет, комплетност, тачност, конзистентност и очување података које ЈКП за обједињену наплату и даваоци комуналних услуга међусобно размењују.

Државна ревизорска институција је спровела ревизију сврсисходности пословања „Управљање информационим системима у јавним предузећима за обједињену наплату“. Ревизијом су обухваћени субјекти ревизије који врше обједињену наплату комуналних и других услуга на територији града Београда, Новог Сада и Ниша и то: ЈКП „Инфостан технологије“ Београд, ЈКП „Информатика“ Нови Сад и ЈКП „Обједињена наплата“ Ниш. Након спроведене ревизије утврдили смо да је:

НЕОПХОДНО УНАПРЕЂЕЊЕ УПРАВЉАЊА ИНФОРМАЦИОНИМ СИСТЕМИМА У ЈКП ЗА ОБЈЕДИЊЕНУ НАПЛАТУ РАДИ СПРЕЧАВАЊА ПОСЛЕДИЦА НЕЖЕЉНИХ ДОГАЂАЈА.

Наведено смо утврдили на основу закључака, које износимо у наставку, а закључци су донети на основу налаза, који су приказани испод сваког закључка.

ЗАКЉУЧАК 1: ЈКП „Инфостан технологије“ Београд и ЈКПОН-Ниш нису успоставили ефективан план континуитета пословања и план опоравка од хаварије.

- Налаз 1.1: Субјекти ревизије нису препознали и дефинисали значајне ИТ ризике, а што може негативно утицати на управљање информационим системима;
- Налаз 1.2: Субјекти ревизије нису вршили процену утицаја на пословање ни за препознате ризике, а што може негативно утицати на управљање информационим системима;
- Налаз 1.3: Субјекти ревизије немају планове за ванредне ситуације, јер оснивач није својим планом дефинисао задатке и обавезе за ове ЈКП, што може довести до штете и губитака;
- Налаз 1.4: Субјекти ревизије немају свеобухватне планове опоравка од хаварије информационог система којим би дефинисали тај процес, иако поседују знање и искуство у превазилажењу хаваријских догађаја;
- Налаз 1.5: ЈКПОН-Ниш није интерним актом уредила успостављени процес израде резервних копија података што може довести до неадекватног поступања у случају кадровске промене.

ЗАКЉУЧАК 2: Управљање безбедношћу информационих система није потпуно адекватно, јер није успостављено управљање инцидентима.

- Налаз 2.1: Субјекти ревизије поседују Акт којим уређују питања у вези информационе безбедности;
- Налаз 2.2: Субјекти ревизије нису успоставили управљање инцидентима;
- Налаз 2.3: Субјекти ревизије нису донели и спровели план комуникације у вези сајбер претњи;

- Налаз 2.4: У ЈКПОН-Ниш нису документоване изјаве запослених у вези преузимања одговорности;
- Налаз 2.5: Иако субјекти ревизије поседују минималну потребну опрему за онемогућавање неовлашћеног мрежног приступа они не врше редовно преглед покушаја упада у мрежу;

ЗАКЉУЧАК 3: Поред постојећих општих и апликативних контрола улаза, обрачуна и излаза података, неопходно је обезбедити аутоматизовано усаглашавање, као и додатне заштитне механизме.

- Налаз 3.1: ЈКП „Инфостан технологије“ Београд и ЈКПОН-Ниш нису обезбедили усаглашавање података на аутоматизован начин;
- Налаз 3.2: Субјекти ревизије нису применили заштитни механизам који обезбеђује обраду података унетих само употребом апликације;
- Налаз 3.3: ЈКП „Инфостан технологије“ Београд није обезбедио избор датума последње измене као критеријум за извештавање;
- Налаз 3.4: Структура базе података није у довољној мери усклађена са прописаним обавезама мера заштите (псеудонимизације) личних података корисника у информационом систему.

У циљу побољшање управљања информационим системима у јавним предузећима за обједињену наплату, Државна ревизорска институција даје следеће препоруке:

ЈКП Информатика – Нови Сад да:

1. дефинише све значајне ИТ ризике као и потребне елементе на основу којих се у складу са оцењеним утицајем на пословање може одредити адекватна мера у циљу избегавања или умањења негативног утицаја на пословање. (Налаз 1.1.) – Приоритет 1[1].
2. изради Процену утицаја на пословање обухватајући све значајне пословне процесе, информационе системе и услуге, одреди очекивана времена и тачке опоравка за сваки ресурс као и смернице које мере применити. (Налаз 1.2.) – Приоритет 2[2].
3. покрене иницијативу код оснивача да им одреди потребне елементе у оквиру Плана заштите и спасавања, ради израде Плана за рад у ванредним ситуацијама. (Налаз 1.3.) – Приоритет 1.
4. успоставе свеобухватни План опоравка од хаварије и врше његово редовно ажурирање. (Налаз 1.4.) – Приоритет 2.
5. успостави процес управљања инцидентима који ће омогућити благовремен и ефикасан одговор у случају нарушавања безбедности или функционалности информационог система и организује обавештавање надлежног органа електронским путем. (Налаз 2.2.) – Приоритет 2.
6. успоставе процес обавештавања и обучавања запослених чија радна места су изложена сајбер нападима, планира и организује обучавање о новим обавезама која утичу на безбедност информационог система. (Налаз 2.3.) – Приоритет 1.
7. успостави редовно прегледавање ЛОГ датотека (журнала) мрежних уређаја за спречавање упада и свих постојећих система и сачињава о томе записник. (Налаз 2.5.) – Приоритет 2.
8. обезбеди механизам хеш заштите којим би се спречила могућност да апликација обрађује податке који нису комплетни, или обрађени употребом апликације. (Налаз 3.2.) – Приоритет 3[3].

[1] Приоритет 1 - Несврсисходности које је могуће отклонити у року од 90 дана.
[2] Приоритет 2 - Несврсисходности које је могуће отклонити у року до годину дана.
[3] Приоритет 3 – Несврсисходности које је могуће отклонити у року од једне до три године.

9. након израде Процене утицаја обраде на заштиту личних података израде план имплементације псеудонимизације личних података корисника. (Налаз 3.4.) – Приоритет 3.

ЈКП Инфостан технологије – Београд да:

1. донесе План пословног континуитета са потребним елементима, именује тим за спровођење, увежбава, периодично га проверава и иновира. (Налаз 1.) – Приоритет 2.
2. дефинише све значајне ИТ ризике као и потребне елементе на основу којих у складу са оцењеним утицајем на пословање може се одредити адекватна мера у циљу избегавања или умањења негативног утицаја на пословање. (Налаз 1.1.) – Приоритет 1.
3. изради Процену утицаја на пословање обухватајући све значајне пословне процесе, информационе системе и услуге, одреди очекивана времена и тачке опоравка за сваки ресурс као и смернице које мере применити. (Налаз 1.2.) – Приоритет 2.
4. покрене иницијативу код оснивача да им одреди потребне елементе у оквиру Плана заштите и спасавања, ради израде Плана за рад у ванредним ситуацијама. (Налаз 1.3.) – Приоритет 1.
5. успоставе свеобухватни План опоравка од хаварије и врше његово редовно ажурирање. (Налаз 1.4.) – Приоритет 2.
6. успостави процес управљања инцидентима који ће омогућити благовремен и ефикасан одговор у случају нарушавања безбедности или функционалности информационог система и организује обавештавање надлежног органа електронским путем. (Налаз 2.2.) – Приоритет 2.
7. успоставе процес обавештавања и обучавања запослених чија радна места су изложена сајбер нападима, планира и организује обучавање о новим обавезама која утичу на безбедност информационог система. (Налаз 2.3.) – Приоритет 1.
8. успостави редовно прегледавање ЛОГ датотека (журнала) мрежних уређаја за спречавање упада и свих постојећих система и сачињава о томе записник. (Налаз 2.5.) – Приоритет 2.
9. обезбеди електронски начин двосмерног усаглашавања евиденција са предузећима пружаоцима услуга. (Налаз 3.1.) – Приоритет 3.
10. обезбеди механизам хеш заштите којим би се спречила могућност да апликација обрађује податке који нису комплетни, или обрађени употребом апликације. (Налаз 3.2.) – Приоритет 3.
11. да приликом израде извештаја омогуће избор датума последње измене из претходног извештајног периода. (Налаз 3.3.) – Приоритет 3.
12. одреди лице за заштиту личних података и приступи изради Процену утицаја обраде на заштиту личних података, а након тога изради план план имплементације псеудонимизације личних података корисника. (Налаз 3.4.) – Приоритет 3.

ЈКПОН - Ниш да:

1. донесе План пословног континуитета са потребним елементима, именује тим за спровођење, увежбава, периодично га проверава и иновира. (Налаз 1.) – Приоритет 2.
2. дефинише све значајне ИТ ризике као и потребне елементе на основу којих у складу са оцењеним утицајем на пословање може се одредити адекватна мера у циљу избегавања или умањења негативног утицаја на пословање. (Налаз 1.1.) – Приоритет 1.

3. изради Процену утицаја на пословање обухватајући све значајне пословне процесе, информационе системе и услуге, одреди очекивана времена и тачке опоравка за сваки ресурс као и смернице које мере применити. (Налаз 1.2.) – Приоритет 2.
4. покрене иницијативу код оснивача да им одреди потребне елементе у оквиру Плана заштите и спасавања, ради израде Плана за рад у ванредним ситуацијама. (Налаз 1.3.) – Приоритет 1.
5. успоставе свеобухватни План опоравка од хаварије и врше његово редовно ажурирање. (Налаз 1.4.) – Приоритет 2.
6. израде свеобухватни План израде резервних копија података. (Налаз 1.5.) – Приоритет 1
7. успостави процес управљања инцидентима који ће омогућити благовремен и ефикасан одговор у случају нарушавања безбедности или функционалности информационог система и организује обавештавање надлежног органа електронским путем. (Налаз 2.2.) – Приоритет 2.
8. успоставе процес обавештавања и обучавања запослених чија радна места су изложена сајбер нападима, планира и организује обучавање о новим обавезама која утичу на безбедност информационог система. (Налаз 2.3.) – Приоритет 1.
9. обезбеди да сви запослени потпишу изјаву да су упознати са обавезама и одговорностима у вези налога за приступање информационом систему. (Налаз 2.4.) – Приоритет 2.
10. да успостави централизовано управљање лозинкама корисника рачунара и редовно прегледавање ЛОГ датотека (журнала) мрежних уређаја за спречавање упада и свих постојећих система и сачињава о томе записник. (Налаз 2.5.) – Приоритет 2.
11. обезбеди електронски начин двосмерног усаглашавања евиденција са предузећима пружаоцима услуга. (Налаз 3.1.) – Приоритет 3.
12. обезбеди механизам хеш заштите којим би се спречила могућност да апликација обрађује податке који нису комплетни, или обрађени употребом апликације. (Налаз 3.2.) – Приоритет 3.
13. одреди лице за заштиту личних података и приступи изради Процену утицаја обраде на заштиту личних података, а након тога изради план план имплементације псеудонимизације личних података корисника. (Налаз 3.4.) – Приоритет 3.

Генерални државни ревизор

_____

Др Душко Пејовић
Државна ревизорска институција
Макензијева 41
11000 Београд, Србија
23. децембар 2020. године

II Увод

Државна ревизорска институција спровела је ревизију сврсисходности пословања „Управљање информационим системима у јавним предузећима за обједињену наплату" у периоду од јуна до октобра 2020. године[4]. Ревизија сврсисходности пословања је спроведена у складу са Законом о Државној ревизорској институцији[5], Пословником Државне ревизорске институције[6] и Програмом ревизије Државне ревизорске институције за 2020. годину.

Ревизија је обављена на начин и према поступцима утврђеним оквиром ревизорских стандарда Међународне организације врховних ревизорских институција (INTOSAI), Кодексом професионалне етике државних ревизора, принципима Међународних стандарда врховних ревизорских институција (ISSAI), Методолошким правилима и смерницама за ревизију сврсисходности пословања и Методолошким правилима и смерницама за ИТ ревизију Државне ревизорске институције.

1. Проблем

ДРИ је у спроведеним ревизијама финансијских извештаја и правилности пословања ЈКП за обједињену наплату у претходним годинама уочила неслагања са евиденцијама јавних комуналних предузећа које пружају комуналне услуге. Поред тога информациони системи у јавним предузећима који врше обједињену наплату, и у предузећима која врше комуналне услуге (даваоци услуга) нису ажурирани и усклађени. Неажурност база података за последицу може имати мање приходе, више трошкове наплате, али и могуће судске процесе (трошкове) због притужби грађана на ажурност евиденција. Такође, безбедност ових система треба да буде на нивоу који обезбеђује поузданост података, а то подразумева интегритет, комплетност, тачност, конзистентност и очување података, безбедност информационог система и континуитет пословања, уважавајући сврху за коју се ти подаци и системи користе.

2. Циљ ревизије

Кључни циљ ревизије је оцена да ли опште ИТ контроле и апликативне контроле спречавају, откривају и отклањају неефикасности у управљању информационим системима јавних предузећа за обједињену наплату комуналних услуга.

3. Ревизорска питања

За остварење циља ревизије формулисали смо главно питање и ревизорска питања. Имајући у виду значај који информациони системи јавних предузећа за обједињену наплату имају, Државна ревизорска институција се определила да главно питање ревизије буде:

Да ли се на адекватан начин управља информационим системом јавног предузећа за обједињену наплату комуналних услуга?

Примењујући Методолошка правила и смернице за ревизију сврсисходности пословања извршили смо декомпозицију главног питања на три аспекта и три ревизорска питања. Одређивање најризичнијих аспеката главног ревизијског питања урађено је процењивањем ризика у складу са Методолошким правилама и смерницама за ИТ ревизију Државне ревизорске

[4] Број ревизије 400-1118/2019-03.
[5] „Службени гласник РС", бр. 101/05, 54/07, 36/10 и 44/18-др.закон.
[6] „Службени гласник РС", број 9/09.

институције, која поставља квантитативне и квалитативне критеријуме, што је детаљније разрађено у Прилогу 1 - Методологија у поступку рада.

Да бисмо одговорили на главно питање, испитивали смо:

1. Да ли се постоји ефективан план континуитета пословања и план опоравка од хаварије?
   1.1. Да ли предузеће врши периодичну процену ризика узимајући у обзир значајне промене у пословном окружењу?
   1.2. Да ли предузеће врши периодичну процену утицаја на пословање?
   1.3. Да ли предузеће има план за ванредне ситуације?
   1.4. Да ли предузеће има ефективан план опоравка од хаварије?
   1.5. Да ли предузеће има и спроводи план за резервне копије?
2. Да ли се на адекватан начин управља безбедношћу информационих система јавних предузећа за обједињену наплату?
   2.1. Да ли предузеће поседује ефективне акта, процедуре и/или правила за обезбеђење информација?
   2.2. У којој мери су значајни ризици избегнути или ублажени?
   2.3. Да ли су правила и процедуре ефикасне и ефективне за безбедну интерну и екстерну комуникацију?
   2.4. Како предузеће обезбеђује да запослени буду упознати са својим улогама и одговорностима у погледу заштите ИСЈПОН?
   2.5. Како предузеће открива и спречава приступ информатичкој инфраструктури неовлашћеним особама?
3. У којој мери се примењују опште и апликативне контроле улаза, обрачуна и излаза података у информационим системима јавних предузећа за обједињену наплату?
   3.1. У којој мери информациони систем у јавним предузећима за обједињену наплату поседује адекватне контроле улаза података у информациони систем?
   3.2. У којој мери апликативне контроле омогућавају интегритет и потпуност свих трансакција које се обављају у информационом систему?
   3.3. У којој мери се примењују контроле које осигуравају потпуност и тачност излазних података из информационих система јавних предузећа за обједињену наплату?
   3.4. У којој мери је структура базе података усклађена са прописаним обавезама псеудонимизације личних података корисника?

4. Обим и ограничења ревизије

Ревизијом смо обухватили три ИТ области у три јавна комунална предузећа која су основана искључиво за вршење обједињене наплате комуналних услуга у градовима Београд, Нови Сад и Ниш за период 2018-2019. година, а за поједине анализе смо користили и податке из 2020. године.

Предмет испитивања је био:

- Опште ИТ контроле које треба да обезбеде ефективно спровођење континуитета пословања у ванредним условима, у условима непредвиђених догађаја, посебно када је реч о хаваријским догађајима (догађаји са материјално значајним последицама по информациону имовину);
- Опште ИТ контроле и активности у обезбеђивању информационе безбедности целокупног информационог система, посебно за информационе системе који размењују података са другим информационим системима;
- Процена адекватности и поузданости апликативних контрола рачунарске апликације која обухвата интерне акте (стратегије, планове, политике, процедуре, обрасце итд.) процесе, људе и системе сва три субјекта ревизије у складу са дефинисаним циљем.

У поступку ревизије нисмо испитивали:

- Да ли финансијски извештаји субјеката ревизије истинито и објективно приказују њихово финансијско стање, резултате пословања и новчане токове, у складу са прихваћеним рачуноводственим начелима и стандардима;
- Финансијске трансакције и одлуке у вези са примањима и приходима и расходима и издацима, ради утврђивања да ли су односне трансакције извршене у складу са законом, другим прописима и за планиране сврхе;
- Међусобне обавезе и потраживања комуналних предузећа која учествују у систему обједињене наплате.

У циљу потврђивања информација из документације и прикупљања података који нису доступни у документима, обавили смо интервјуе, послали упитнике субјектима ревизије.

Ограничења ове ревизије, у смислу давања оцене адекватности начина управља информационим системима у јавним предузећима за обједињену наплату комуналних услуга није било.

Ревизијом нисмо обухватили анализу да ли сва физичка лица плаћају комуналне услуге преко система обједињене наплате, односно да ли постоје лица којима се не врши обрачун и наплата комуналних услуга преко система обједињене наплате или директно преко даваоца комуналних услуга.

На основу тражених података од девет (9) даваоца комуналних услуга са територије града Новог Сада, Београда и Ниша (топлана, чистоћа, водовод) о броју корисника комуналних услуга (физичких и правних лица) са стањем на 31.12.2018. и 31.12.2019. године којима се директно наплаћују комуналне услуге (а не преко система обједињене наплате), добили смо следеће одговоре од ЈКП:

Табела 1. Преглед броја корисника који директно плаћају пружаоцима комуналних услуга

Назив ЈКП	31.12.2018.		31.12.2019.	
	Физичка лица	Правна лица	Физичка лица	Правна лица
Град Београд				
Београдски водовод и канализација	96.559	43.699	97.761	43.949
Градска чистоћа		16.253		16.655
Београдске електране	8.162	7.137	8.002	7.053
Град Нови Сад				
Новосадска топлана	3.336	2.582	3.394	2.541
Чистоћа		13.442		15.824
Водовод и канализација	9018	7624	9003	7572
Град Ниш				
Наисус (водовод и канализација)	51.410	7.643	52.730	7.752
Медиана (чистоћа)		1.940		1.959
Градска топлана	1.233	891	1.192	928

5. Методологија у поступку рада

Да бисмо остварили циљ ревизије и одговорили на ревизорска питања, анализирали смо законску и подзаконску регулативу, користили стручну литературу (WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions), као и све податке добијене од субјеката ревизије и других субјеката, (јавна комунална предузећа у градовима и општинама Републике Србије и јавна комунална предузећа која учествују у систему обједињене наплате). Анализирали смо податке и информације за период од 2018. до 2019. године. Такође смо за поједине анализе користили и податке из 2020. године.

Управљање информационим системом подразумева успостављање низа пословних процеса, посебно зато што је реч о техничко-технолошком систему који обухвата опрему, софтвер, комуникацију и друге погодности које се користе у сврху евидентирања, чувања, обраде, преноса података у било ком облику.

Које пословне процесе треба да успостави организација чије пословање није могуће без употребе рачунарских система, дефинишу међународни стандарди чији се захтеви налазе и у основама наших прописа. Специфичност јавних комуналних предузећа за обједињену наплату у односу на друга комунална предузећа огледа се у томе да своју делатност не може да обавља без рачунарских система.

У фази планирања ревизије прикупљени су подаци и документација на основу које је извршена процена ризика у циљу одређивања обима ревизије.

У ревизији информационих система/технологија обим[7] се одређује из једног или више домена и то:

- Организациона политика за ИТ;
- Организациона управљачка структура за ИТ;
- Опште контроле у оквиру пословања које су аутоматизоване;
- Управљање имовином;
- Развој, набавка и одржавање информационих система, укључујући и мапирање пословних процеса и повезане програмске логике;
- Управљање ИТ операцијама;
- Управљање физичким окружењем;
- Управљању људским ресурсима;
- Управљање комуникацијама;
- Управљање информатичком безбедношћу;
- Управљање усклађеношћу са прописима;
- Пословни континуитет и управљање опоравком након елементарних непогода/хаварије;
- Управљање контролама апликација.

Приручником[8] је предвиђена оцена сложености информационог система и могућност избора области за испитивање и то: ИТ управљање, развој и набавка, ИТ операције, ангажовање добављача, планови континуитета пословања и опоравка од хаварије, информациона безбедност и апликативне контроле.

Проценили смо ревизијски ризик и одабрали домене: планови континуитета пословања и опоравка од хаварије, информациона безбедност и апликативне контроле.

[7] Методолошка правила и смернице за ИТ ревизију Државне ревизорске институције.
[8] WGITA – IDI Приручник за ИТ ревизију врховних ревизорских институција (енг. WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions).

Табела 2. Преглед ризичних области

Област/домени	Ниво ризика	Напомена
ИТ управљање	Средњи	У фази планирања утврђено непостојање стратешких планова остварења пословних циљева и излагању ризику за безбедност информација.
Развој и набавка	Низак	Самостални развој апликације дуже од 40 година, унапређење и усклађивање апликације са прописима и другим захтевима.
ИТ операције	Средњи	Вишегодишње искуство у организованом решавању рекламација из облигационог домена довело је до недостатка процене утицаја на пословање и многи елементи оперативног управљања пате од недостатака.
Ангажовање добављача	Низак	Кључне процесе организују ангажовањем запослених у предузећу и пословно знање остаје у пословној организацији са обавезом подмлађивања развојног тима.
Планови континуитета пословања и опоравка од хаварије	Висок	Учестали прекиди у пословању услед дејства природних узрока и више силе погубно делује на пословне резултате. Услуге обрачуна и наплате су оне које се морају испоручити како би се осигурао континуитет пословања, избегло изазивање губитка и испуњавање законских или других обавеза. Ако ове услуге буду прекинуте у дужем временском периоду, то ће довести до финансијских и других губитака. Ако је опоравак од хаварије критичних функција компромитован, континуитет пословања ће бити угрожен. Ако улоге и одговорности нису јасне и разумљиве од стране одговарајућег кадра, добар план такође може постати неефикасан. Планови морају бити спроводљиви са расположивим ресурсима, периодично тестирани и сви недостаци документовани и отклоњени.
Информациона безбедност	Висок	Корисници комуналних услуга поред правних лица, бројчано најзначајнија су физичка лица чији се лични подаци обрађују у инфо-рмационом систему. Изложеност следећим ризицима: неовлашћено откривање информација; неовлашћена модификација или уништење информација; угроженост ИС од хакерског напада; уништавање инфраструктуре; ометање приступа; поремећај обраде података у ИС; и ризик да подаци буду украдени, поставља читав низ безбедносних захтева.
Апликативне контроле	Висок	Ризици су повезани са улазним подацима који се обрађују у апликацији и могу довести недозвољеног модификовања/брисања података и дати погрешан резултат без обзира што постоји обрада рекламација. Непостојање контрола обраде настају услед погрешног мапирања пословних правила, неадекватних тестирања кода програма, или лоших контрола над различитим верзијама програма за враћање интегритета обраде након неочекиваног прекида. Непостојање контрола излазних података доводе до ризика стварања погрешних извештаја о управљању и кршења поверљивости података. Сталне грешке у подацима имају далекосежне последице по апликацију, с обзиром да подаци могу да се користе за велики обим трансакција у апликацији.

Детаљнији опис коришћене методологије дат је у Прилогу 1.

III Опис предмета ревизије

1. Законодавни и институционални оквир

Законом о комуналним делатностима дефинисано је 14 делатности[9] пружања комуналних услуга од општег интереса, од значаја за остварење животних потреба физичких и правних лица код којих је ЈЛС дужна да створи услове за обезбеђење одговарајућег квалитета, обима, доступности и континуитета, као и надзор над њиховим вршењем.

ЈЛС дужна је да створи услове за обезбеђење одговарајућег квалитета, обима, доступности и континуитета комуналних услуга, тако што оснива јавна комунална предузећа за обављање ових делатности, вршећи надзор над њиховим пословањем.

Комуналне делатности су делатности од општег интереса и то су[10]:

1. Снабдевање водом за пиће,
2. Пречишћавање и одвођење атмосферских и отпадних вода,
3. Производња, дистрибуција и снабдевање топлотном енергијом,
4. Управљање комуналним отпадом,
5. Градски и приградски превоз путника,
6. Управљање гробљима и сахрањивање и погребна делатност,
7. Управљање јавним паркиралиштима,
8. Обезбеђивање јавног осветљења,
9. Управљање пијацама,
10. Одржавање улица и путева,
11. Одржавање чистоће на површинама јавне намене,
12. Одржавање јавних зелених површина,
13. Димничарске услуге,
14. Делатност зоохигијене.

Скупштина ЈЛС може као комуналне делатности одредити и друге делатности од локалног интереса и прописати услове и начин њиховог обављања.[11]

ЈКП „Информатика“ Нови Сад

Одлуком о одређивању комуналних делатности од локалног интереса и поверавању обављања комуналне делатности од локалног интереса[12] за град Нови Сад одређене су комуналне делатности од локалног интереса и поверавање обављање комуналних делатности од локалног интереса.

Комуналне делатности од локалног интереса су:

- сузбијање и уништавање коровске биљке амброзије,
- картирање терена под коровском биљком амброзијом и другим алергогеним биљкама, лабораторијска и теренска истраживања и мониторинг,
- декорација Града Новог Сада,
- одржавање елемената визуелних комуникација, опреме за оглашавање и плакатних места,

[9] Члан 2 став 1 Закона о комуналним делатностима (Службени гласник РС, бр. 88/2011, 104/2016 и 95/2018).
[10] Члан 2 став 2 и 3 Закона о комуналним делатностима (Службени гласник РС, бр. 88/2011, 104/2016 и 95/2018).
[11] Члан 2 став 5 Закона о комуналним делатностима (Службени гласник РС, бр. 88/2011, 104/2016 и 95/2018).
[12] „Сл. лист Града Новог Сада“, бр . 69/2013.

- одржавање урбаног мобилијара,
- чишћење јавних површина некатегоризованих на другом месту (фасаде јавних зграда, споменици, вештачке подлоге, бехатон и сличне површине),
- обједињена обрада података и наплата комуналних услуга,
- обезбеђивање карантина за животиње,
- обрада података у вези са накнадом за коришћење грађевинског земљишта,
- изградња и одржавање Општег информационог система Града Новог Сада,
- телекомуникациони систем - оптичка, кабловска и друга телекомуникациона инфраструктура (изградња, одржавање и пружање услуга),
- обележавање и одржавање простора за извођење паса,
- прогнозно - извештајни послови у вези са заштитом здравља биљака,
- услуге одржавања и поправке стамбених и пословних зграда, установа и других облика организовања за које се средства планирају у буџету Града Новог Сада,
- одржавање отворених канала и насипа за одвођење воде са површина јавне намене, и
- утврђивање и праћење квалитета воде за пиће.

ЈКП „Информатика“ Нови Сад под тим именом постоји од 10. априла 2009. године, а почеци сежу до 1971. године када је основан рачунарски центар при тадашњем Заводу за изградњу Града са циљем организовања и развијања послова информатике за потребе Општине Нови Сад[13].

Прва одлука о обједињеној наплати Град Нови Сад је донео 1994. године, затим је та одлука допуњавана и мењана 1995. и 1997. године. Одлуком о обједињеној наплати комунално-стамбених и других услуга[14], у циљу економичније и ефикасније наплате одређених комунално-стамбених и других услуга, уређен:

- је систем обједињене обраде података и наплате комунално-стамбених и других услуга
- су питања у вези са начином вршења послова обједињене наплате, накнадном за извршене послове и правима и обавезама правних и физичких лица-корисника комунално-стамбених и других услуга.

Одлуком о усклађивању одлуке о организовању јавног предузећа „Информатика“ Нови Сад [15] је извршено усклађивање Одлуке са Законом о јавним предузећима. ЈКП „Информатика“ Нови Сад је основана за послове из области телекомуникација, информатике и наплате комунално-стамбених производа и услуга. Оснивач Јавног предузећа је Град Нови Сад, Жарка Зрењанина број 2, матични број 08179115. Град Нови Сад је власник 100% удела у основном капиталу ЈКП „Информатика“ Нови Сад. Пословно име под којим послује: Јавно комунално предузеће „Информатика“ за послове из области телекомуникација, информатике и наплате комунално-стамбених производа и услуга, Нови Сад. Скраћено пословно име: ЈКП „Информатика“ Нови Сад. Седиште је у Новом Саду, Булевар цара Лазара број 3[16].

ЈКП „Инфостан технологије“ Београд

На територији Града Београда Одлуком о одређивању комуналних делатности[17], поред комуналних делатности одређених Законом о комуналним делатностима[18], као комуналне делатности, одређене су и следеће делатности од локалног интереса:

- одржавање јавних WЦ-а;

[13] https://www.nsinfo.co.rs/cyr/istorijat
[14] Одлука о обједињеној наплати комунално стамбених и других услуга Нови Сад ("Сл. лист Града Новог Сада", бр. 8/94, 12/95 и 9/97 - одлука УСРС)
[15] Сл. лист Града Новог Сада 47/2016.
[16] Чланови 2, 3 и 4 Одлуке о усклађивању одлуке о организовању јавног предузећа „Информатика“ Нови Сад.
[17] „Сл. лист Београда“, 2/2017, 109/2018 и 52/2019.
[18] „Службени гласник РС“, бр. 88/11 и 104/16.

- одржавање јавних купатила;
- одржавање јавних часовника;
- обједињена обрада и наплата комуналних услуга;
- обезбеђивање услова за уређивање, употребу, унапређење и заштиту грађевинског земљишта, припрема и реализација средњорочних и годишњих програма уређивања грађевинског земљишта;
- обезбеђивање услова за уређивање, употребу, унапређење и заштиту Комплекса Београдске тврђаве и парка Калемегдан;
- чишћење (уклањање) графита са објеката видљивих са површина јавне намене и обезбеђивање заштите од њиховог наношења.

"Инфостан" је основала Скупштина града Београда 1. фебруара 1977 . године. Од 21. децембра 1989. године послује под именом Јавно комунално предузеће "Инфостан". Систем обједињене наплате (СОН) комуналних услуга у Београду формиран је и у оперативној је експлоатацији од 1. јануара 1977 . године у циљу економичне и рационалне обраде података и наплате комуналних и других услуга и накнада. Скупштина града Београда је 07.12.2015. године донела Одлуку о промени оснивачког акта Јавног комуналног предузећа „Инфостан“. Пословно име предузећа промењено је из ЈКП „Инфостан“ у ЈКП „Инфостан технологије“[19] .

Јавно комунално предузеће „Инфостан технологије“ Београд. Скраћено пословно име: ЈКП „Инфостан технологије“ Београд. Седиште: Данијелова 33, 11010 Београд. Општина Вождовац. Матични број: 07048971. ПИБ: 100383967. Шифра делатности: 6311 - обрада података, хостинг и сл. Град Београд је власник 100% удела у основном капиталу ЈКП „Инфостан технологије“ Београд.

ЈКП „Обједињена наплата“ Ниш

Одлуком о одређивању комуналних делатности од локалног интереса[20] за град Ниш као комуналне делатности од локалног интереса одређене су:

- одржавање бунара,
- превоз посмртних остатака у саобраћајним несрећама и другим незгодама,
- декорација града,
- обједињена обрада и наплата комуналних услуга (обрада података, рачуноводствени и књиговодствени послови),
- израда урбанистичких планова и урбанистичко-техничких услова из Програма уређивања грађевинског земљишта, који у себи садрже комуналну инфраструктуру,
- организација, контрола и реализација интегрисаног тарифног система превоза путника у градском и приградском саобраћају на територији Града Ниша,
- израда идејних и главних пројеката и остале техничке документације за изградњу, реконструкцију и одржавање водоводне и канализационе мреже и објеката за водоснабдевање и каналисање на територији Града Ниша,
- израда идејних и главних пројеката и остале техничке документације за изградњу, реконструкцију и одржавање
- објеката система даљинског грејања на територији Града Ниша,
- пре везивање и замена прикључних веза, реконструкција водоводних и канализационих мрежа и поновно повезивање приликом периодичног, редовног и ургентног одржавања и реконструкције јавних саобраћајница.

Предузеће за заједничку наплату комуналних услуга на једном, заједничком рачуну, под називом „Комуналац“ Ниш основано је крајем 1983. године. Предузеће ЈКП „Медиана“ Ниш у чијем саставу је био и „Комуналац“ са системом обједињене наплате је основано 1990. године. Од 1992.

[19] https://www.infostan.rs/sr/istorija.
[20] „Сл. лист града Ниша“, бр. 5/2014, 92/2016 и 139/2017.

године „Водовод“ наплату утрошене воде поверава сектору „Обједињена наплата“ у оквиру ЈКП „Медиана“ Ниш, али Скупштина града две године касније доноси „Одлуку о начину и роковима плаћања комуналних услуга“ којом „Водовод“ излази из система обједињене наплате. Дана 26.12.2003. године поменута одлука је иновирана, тако да се наплата свих комуналних услуга, а тиме и утрошене воде, поверава новоформираном ЈКП „Обједињена наплата“ Ниш. Систем обједињене наплате и новоформирано ЈКП „Обједињена наплата“ Ниш, потпуно су заживели осамостаљењем предузећа 01.01.2009. године. Одлука о оснивању "Јавног комуналног предузећа за обједињену наплату комуналних, стамбених и других услуга и накнада" - Ниш донета је 26.12.2003. године. Предузеће је регистровано 16.01.2006. године, са седиштем у нишу у улици Наде Томић 7, а самостално отпочело са радом 01.01.2009. године[21]. Пословно име: Јавно комунално предузеће за обједињену наплату комуналних, стамбених и других услуга и накнада Ниш. Скраћено пословно име: ЈКП „Обједињена наплата“ Ниш. Матични број: 20116803. ПИБ: 104244673. Шифра и назив делатности: 6311- Обрада података, хостинг и сл. Град Ниш је власник 100% удела у основном капиталу ЈКП „Обједињена наплата“ Ниш.

2. *Информациони системи јавних предузећа за обједињену наплату*

Рачунарска апликација за обједињену наплату

Информациони систем је сложен скуп технологије, процеса и људи који заједно функционишу ради процесирања, складиштења и преношења информација и података, како би се подржала мисија организације и њене пословне функције.

Рачунарска апликација за обједињену наплату је веома специфична у односу на друге књиговодствене апликације због тога што предузеће које обавља делатност обједињене наплате не мора бити и најчешће није власник услуга за које врши фактурисање и наплату. Из тог разлога апликације имају могућност да се у систем обједињене наплате осим локалних комуналних предузећа укључе и друга привредна друштва која пружају комуналне и друге услуге, које имају уговорни однос са корисницима система обједињене наплате.

Рачунарска апликација за обједињену наплату поседује системске функционалности које обезбеђују:

- рачуноводственим пословима обрачуна, евидентирања, обједињује процесе фактурисања, сторнирања и књижења, пријем и евидентирање рекламација на рачун;
- преглед и извештавање о дуговањима и потраживањима (задужењима и раздужењима) корисника;
- обрачун утрошка воде или неке друге услуге која има мерни инструмент, које је могуће вршити на више начина, аконтативно уз коначне обрачуне или пријемом готовог обрачуна из ЈКП за воду и канализацију или другог даваоца услуге;
- управљање банковним изводима или благајном, када се евидентирање уплата може вршити и баркода на обрачуну као и читача, преузимање електронског извода од пословне банке итд;
- аналитичко и синтетичко рачуноводство према потребама даваоца услуга укључених у систем обједињене наплате;
- штампање, ковертирање и експедиција обрачуна са приказом комплетних елемената који учествују у обрачуну;
- управљање дуговањем корисника, кроз репрограме дугова и праћење наплате по репрограмима, обрачун камата у жељеном периоду, праћење старости дуговања и праћење наплате по утужењима;

[21] http://www.jkponnis.rs/o-nama.

- размена података са пружаоцима услуга који учествују у систему обједињене наплате, приступање подацима за своје кориснике услуга;
- управљање некретнинама, власницима, корисницима, техничким подацима о непокретностима, врстама услуга које се пружају сходно врсту намени непокретности;
- веб/интернет апликација за кориснике и њихов приступ својим финансијским и осталим подацима.

Веб/интернет верзија апликације за обједињену наплату омогућава корисницима да путем интернета приступе свим својим рачунима и уплатама. Корисници у сваком тренутку могу, преко интернета да виде следеће податке:

- Преглед услуга које им се фактуришу;
- Преглед финансијског стања по услугама;
- Преглед свих обрачуна са детаљима:
- Преглед свих уплата са детаљима;
- Преглед свих налога за књижење са детаљима;
- Преглед мерних инструмената и њихових стања.

На овај начин је потрошачима омогућено да без одласка на шалтере обједињене наплате прегледају и одштампају своје податке и на тај начин уштеде своје време. Са овим сервисом се у потпуности заокружује систем обједињене наплате обухватајући све аспекте пословања. Такође је на овај начин испуњена обавеза транспарентности рада система с обзиром на значај целокупног система за кориснике комуналних услуга.

Ова врста апликације и података којима приступа излаже систем посебним ризицима од недозвољеног објављивања личних података и поред апликативних контрола значајна је и са становишта информационе безбедности.

У претходно спроведеним ревизијама[22] је наведено да су многи проблеми у пословању настали услед неадекватног управљања информационим системом у целини. Дефинисање потребних функционалности софтверске апликације директно одређује квалитет техничке спецификације у процесу јавне набавке новог информационог система.

Разноврсност учесника у систему обједињене наплате уважавајући све специфичности које носе ЈЛС по својој природи има најмање два аспекта. Даваоци комуналних услуга воде сопствене евиденције и често поред корисника својих услуга који плаћају преко система обједињене наплате имају и кориснике са којима остварују директан пословни однос[23]. Са друге стране, разноврсност корисника комуналних услуга поред физичких и правних лица у стамбеним и пословним објектима често доводе до комбиноване наплате комуналних услуга[24].

Информациони системи у јавним предузећима за обједињену наплату (даље у тексту: ИСЈПОН) прикупљају и обрађују податке од корисника или их преузимају из информационих системима јавних комуналних предузећа која их поседују.

Одређен број ЈЛС своје ИСЈПОН су формирали на постојећим информационим системима, најчешће јавних предузећа која се баве пословима одржавања стамбених зграда.

Други случај је да су ИСЈПОН самостално развијана софтверска решења која уважавају све специфичности ових послова, код великог броја правних лица пружалаца услуга и када се услуге

[22] Извештај о ревизији финансијских извештаја и правилности пословања јавног комуналног предузећа „Инфостан“ Београд за 2012. годину.

[23] Јавно комунално предузеће своје услуге изношења смећа у стамбеним зградама наплаћује преко система обједињене наплате, а корисницима који поседују приватне објекте – куће, своје услуге наплаћују испостављањем сопствених рачуна.

[24] Правно лице (привредно друштво) може неке услуге плаћати путем система обједињене наплате и притом да поједине услуге уговори посебним уговором са јавним комуналним предузећем.

обрачунавају на веома различите начине, по квадрату стана, броју чланова породице, учешћу у укупној грађевинској површини итд.

Слика број 1 Скупови података у систему обједињене наплате

ИСЈПОН је самостално развијена апликација која поседује трослојну архитектуру чија база података обрађује: податке о непокретностима, личне податке грађана, подаци о пружаоцима услуга, подаци о комуналним услугама, прописани елементи обрачуна и др.

Циљеви обједињене наплате комуналних услуга

ЈЛС су у својим одлукама о начину плаћања комуналних услуга дефинисале и саме циљеве које та јавна предузећа за обављање послова наплате комуналних услуга треба да остваре. Тиме се у суштини дефинишу циљеви информационих система да обједињену наплату комуналних услуга свих јавних предузећа обављају на економичан и ефикасан начин.

Да би се ови циљеви остварили дефинишу се даваоци (јавна комунална предузећа) и корисници услуга у систему обједињене наплате, уређују се њихова права и обавезе, начини организовања и вршења послова из делатности обједињене наплате услуга и накнада, начини обрачуна износа, као и многа друга питања.

Економичност и ефикасност обједињене наплате комуналних услуга огледа се кроз:

- смањење трошкова пословања (трошкови обрачуна, утужења, опомена, штампе и доставе фактура) на нивоу ЈЛС (за све учеснике у систему обједињене наплате);
- смањење броја запослених укључених у систем обрачуна и наплате;
- повећање процента наплате у распону од 20-100% у односу на време пре увођења система обједињене наплате и у зависности од даваоца услуга укључених у систем;
- устаљеност у приливу наплаћених средстава и њихово одржавање на високом нивоу;
- ажурирање базе података путем рекламација грађана који пријављују промене власништва, односно укључивање или искључивање неке комуналне услуге, промене површине итд;
- анализу базе података кроз стално “упаривање” података из база свих даваоца услуга, чиме се откривају корисници који користе услуге, а нису обухваћени процесом наплате;
- смањење трошкова за кориснике/домаћинства јер плаћају услуге једном уплатницом на једном месту које је најближе месту боравка.

3. Начини наплате комуналних услуга

У циљу прикупљања података о броју јавних предузећа за обједињену наплату у Републици Србији (начину наплате комуналних услуга), послато је питање свим ЈЛС:

Да ли се наплата комуналних производа и услуга у вашој општини/граду врши преко обједињене наплате?[25]

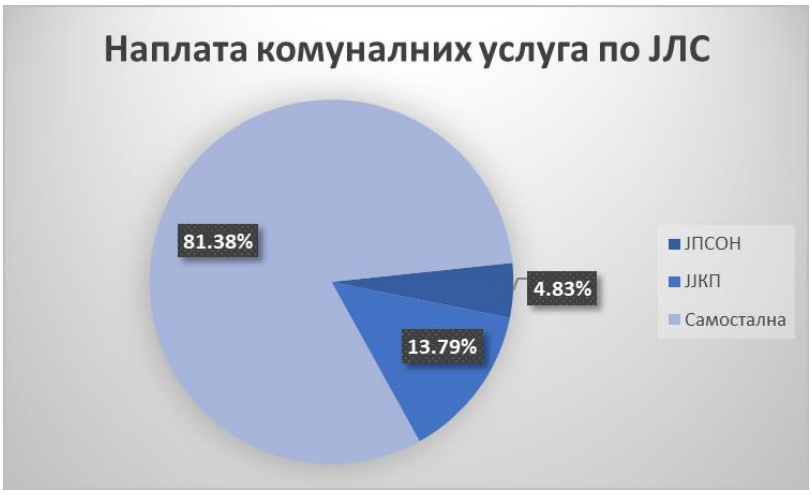
Постоје три начина наплате комуналних услуга и то:

ЈЛС су основале јавно предузеће за обједињену наплату комуналних услуга (даље у тексту: ЈПОН) и послове наплате комуналних услуга врши обједињено на једном обрачуну (преко једног рачуна). Овај начин наплате примењује 4,83% ЈЛС.

ЈЛС су одлуком одредиле једно ЈКП, најчешће за одржавање стамбених зграда да врши наплату и за остала комунална предузећа обједињујући све обавезе корисника на једном обрачуну. Овај начин наплате примењује 13,79% ЈЛС.

Комунална предузећа самостално наплаћују пружене услуге у 81,38% ЈЛС.

Ако погледамо ЈЛС према броју корисника (домаћинства) којима пружају комуналне услуге видимо да 53,67% корисника плаћа појединачно комуналне услуге, док више комуналних услуга на једном обједињеном рачуну плаћа 46,33% корисника.



Слика број 2 Начин наплате комуналних услуга у Републици Србији према броју ЈЛС

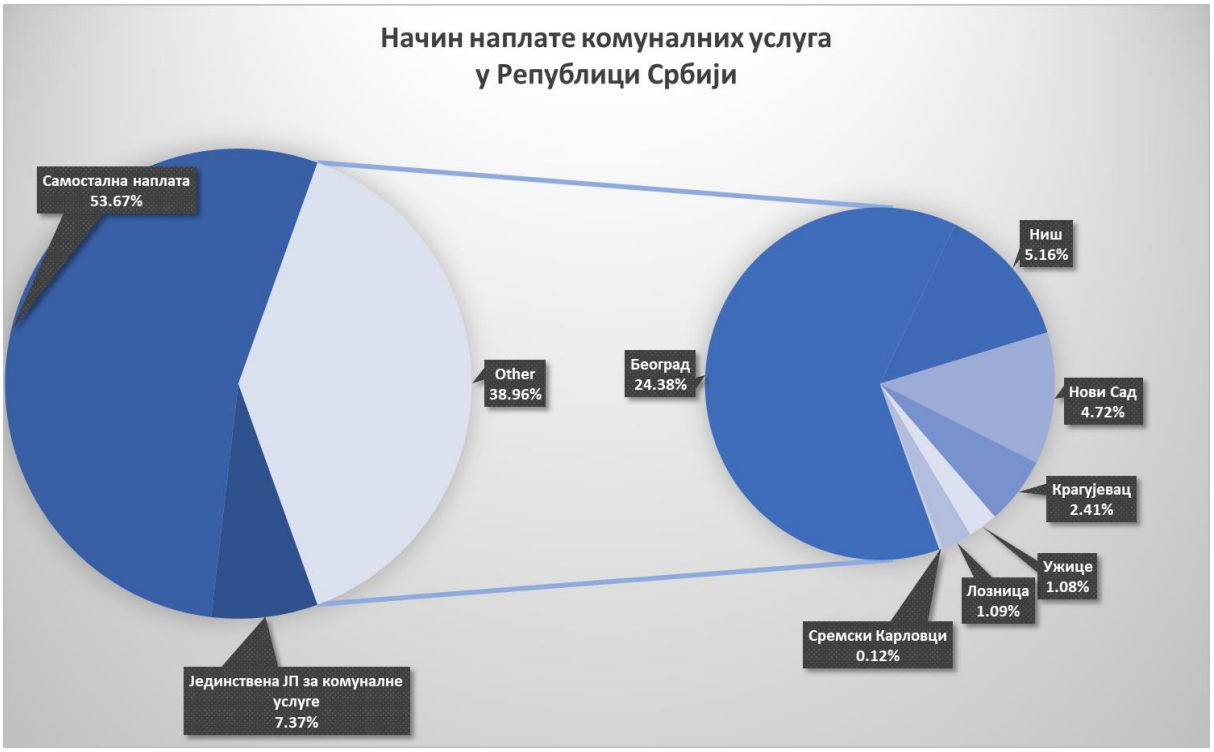
За ове послове обједињавања више комуналних услуга на једном рачуну седам ЈЛС је основало посебна јавна комунална предузећа за обједињену наплату и то: градови Београд, Нови Сад, Ниш, Крагујевац, Лозница, Ужице и општина Сремски Карловци. Оваквим начином наплате обухваћено је 38,96% корисника у Републици Србији.

Обрачунавање и наплата услуга се врши једном месечно[26], тако да на пример једна ЈЛС са 100.000 корисника, ако једном месечно обрачуна у просеку четири комуналне услуге, евидентира претходно стање дуговања, просечно једну уплату у претходном месецу, обрачуна порез на опорезоване услуге, обрачуна износ за уплату, попуст на редовно измирење итд. годишње у бази података најмање евидентира преко 10 милиона трансакција. Ако се узме у обзир да у пракси због начина утврђивања дуга информациони системи чувају историјат свих промена

[25] Појашњење: Под обједињеном наплатом подразумевамо скуп одређених послова ради наплате комуналних и других услуга путем јединствене уплатнице и да је град/општина основала/поверила одређеном јавном предузећу обављање делатности обједињене наплате.

[26] Одлука о начину плаћања комуналних услуга на територији града Београда.

од увођења у рад или најмање 10 година као рок апсолутне застарелости, многи системи обрађују базе са преко 100 милиона записа.



Слика број 3 Начин наплате комуналних услуга у Републици Србији по корисницима

Комуналне услуге које се обједињено наплаћују су најчешће: одржавање стамбених зграда, испорука топлотне енергије (грејање станова), испорука воде, одвођење отпадних вода, одржавање чистоће (одношење смећа) итд.

IV Закључци

На основу анализе података и документације достављених од стране субјеката ревизије, као и обављених интервјуа (представници субјеката ревизије и извора информација), донели смо следеће закључке:

1. ЈКП „Инфостан технологије“ Београд и ЈКПОН-Ниш нису успоставили ефективан план континуитета пословања и план опоравка од хаварије.
2. Управљање безбедношћу информационих система није потпуно адекватно, јер није успостављено управљање инцидентима.
3. Поред постојећих општих и апликативних контрола улаза, обрачуна и излаза података, неопходно је обезбедити аутоматизовано усаглашавање, као и додатне заштитне механизме.

У наставку Извештаја, наводимо закључке са одговарајућим налазима, које илуструјемо примерима.

ЗАКЉУЧАК 1: ЈКП „Инфостан технологије“ Београд и ЈКПОН-Ниш нису успоставили ефективан план континуитета пословања и план опоравка од хаварије.

Наш циљ у овом делу извештаја, био је да одговоримо на прво ревизијско питање, односно да ли је успостављен ефективан план континуитета пословања и план опоравка од хаварије.

Законом о информационој безбедности[27] се уређују мере заштите од безбедносних ризика у ИКТ системима и одговорностима правних лица приликом управљања и коришћење ИКТ система. Приликом планирања и примене мера заштите ИКТ система треба се руководити следећим начелима:

1. Начело управљања ризиком,
2. Начело свеобухватне заштите,
3. Начело стручности и добре праксе,
4. Начело свести и оспособљености.

Када су у питању план континуитета пословања и план опоравка од хаварије, они се понекад користе као синоними, али су заправо два различита и комплементарна појма. Оба су важна, јер заједно обезбеђују да организација може да функционише на одређеном капацитету након природне катастрофе или хаварије.

Кључни елементи континуитета пословања су: план и политика континуитета пословања, организација функције континуитета пословања, процена утицаја на пословање, управљање ризицима, превентивне контроле, план опоравка у случају хаварије, документација за план континуитета пословања, план тренинга и тестирања, информациона безбедност и резервне копије и план опоравка када су послови додељени добављачу услуга.[28]

На основу постављеног питања, формулисали смо и следећа потпитања:

- Да ли предузеће врши периодичну процену ризика узимајући у обзир значајне промене у пословном окружењу?
- Да ли предузеће врши периодичну процену утицаја на пословање?
- Да ли предузеће има план за ванредне ситуације?
- Да ли предузеће има ефективан план опоравка од хаварије?
- Да ли предузеће има и спроводи план за резервне копије?

Табела 3. Планови и процедуре за обезбеђење пословног континуитета код ЈКП субјеката ревизије

Опис-субјекти ревизије	ЈКП Информатика Нови Сад	ЈКП Инфостан технологије Београд	ЈКП Обједињена наплата Ниш
Стратегија процене ризика	број 16899-4/19 од 30.12.2019.	број 10475/4 од 29.10.2018.	број 00-7640 од 29.12.2017.
Регистар ризика	Да	Да	Да
План континуитета пословања	БЦП -1002 од 30.5.2018.	„backup“ и „restore“ података за систем СОН-а	није усвојен акт, планирано усвајање акта у 2021. години
План за резервне копије	Да, план "back-up" за Оракл базе, процедура 1010.5 од 30.5.2018.	Правилник безбедности ИКТ система и Процедура за инфраструктуру и сервисе	није усвојен појединачни акт, неформална процедура за спровођење "back-up"-а

[27] Члан 1 Закона о информационој безбедности.

28 WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions.

Опис-субјекти ревизије	ЈКП Информатика Нови Сад	ЈКП Инфостан технологије Београд	ЈКП Обједињена наплата Ниш
План за ванредне ситуације	НЕ	НЕ	НЕ
План опоравка од хаварије	НЕ	НЕ	НЕ

План континуитета пословања (Business Continuity Planning-BCP) подразумева активности које организација спроводи у циљу опоравка пословних процеса након хаварије. У пракси је то план како организација наставља да послује након што се деси хаварија (природне катастрофе или друге врсте хаварије).

План континуитета пословања треба да садржи:

1) процедуре у случају прекида пословања,
2) списак ресурса неопходних за поновно успостављање континуитета пословања
3) податке о тимовима и члановима тимова који ће бити одговорни за поновно успостављање пословања, њихове дужности и одговорности,
4) резервну локацију у случају прекида пословања и немогућности поновног успостављања пословних процеса на примарној локацији.

Према одредбама Закона о информационој безбедности (члан 7) и према члану 29 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја[29] оператор ИКТ система[30] 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.

Такође је прописано да оператор ИКТ система треба да успостави, документује, имплементира и одржава процесе, процедуре и контроле да би осигурао захтевани ниво континуитета пословања током ванредне ситуације (члан 29 став 2 Уредбе)[31].

Задатак оператора ИКТ система је да верификује успостављене и имплементиране контроле континуитета пословања у редовним условима рада, како би оне биле важеће и ефективне током ванредне ситуације (члан 29 став 3 Уредбе).

ЈКП Информатика – Нови Сад

ЈКП „Информатика“ Нови Сад је усвојила План континуитета пословања[32] као документован скуп поступака и информација које су развијене, сакупљене и обрађене тако да су спремне за употребу у случају инцидента и које омогућавају наставак кључних активности на одређеном прихватљивом нивоу.

План континуитета пословања садржи део за опште информације (сврха, циљеви, принципи, будуће промене у ЈКП) и део за критичне процесе у ЈКП (напајање електричном енергијом, пожар, мрежа електронских комуникација, услуга штампе, доступност хардвера и софтвера). Примарни циљ управљања континуитетом пословања за ЈКП „Информатика“ Нови Сад је одржавање минимума прихватљивих сервиса пословања у продуженом временском периоду у

[29] „Службени гласник РС“ бр. 94/2016.
[30] Оператор ИКТ система – правно лице, орган власти или организациона јединице органа власти који користи информационо-комуникациони систем у оквиру обављања своје делатности, односно послова из своје надлежности.
[31] Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја.
32 План континуитета пословања.

случајевима прекида нормалног пословања[33]. Важна компонента Плана континуитета пословања ЈКП „Информатика“ Нови Сад је постојање резервне локације на адреси која је различита од седишта правног лица. Друга битна компонента Плана континуитета пословања је постојање тима за дефинисање и примену Плана. У ЈКП „Информатика“ Нови Сад за Кризног менаџера је именован Самостални сарадник за послове заштите на раду и техничку безбедност објеката који координира рад Тима за управљање ванредним ситуацијама и има одговорност да говори у име организације у случају прекида континуитета пословања[34]. Тим за управљање ванредним ситуацијама чине помоћници директора, руководилац људских ресурса и организатор послова система квалитета.

Критични процеси ЈКП „Информатика“ Нови Сад су, сходно Плану континуитета пословања:

1. Напајање електричном енергијом;
2. Пожар;
3. Мрежа електронских комуникација;
4. Услуге штампе и дораде хартије;
5. Доступност ИТ сервисима (софтвер);
6. Доступност ИТ опреми (хардвер).

Почетком марта 2020. године ЈКП „Информатика“ Нови Сад је доживела хакерски „ransomware“ напад. Том приликом криптовани су сви „word“, „excel“ и други документи чиме је запосленима онемогућен нормалан рад.

ЈКП Инфостан технологије – Београд

ЈКП „Инфостан технологије“ Београд није усвојио План континуитета пословања, односно није документовао процесе, процедуре и контроле да би осигурао захтевани ниво континуитета пословања током ванредне ситуације. ЈКП „Инфостан технологије“ Београд је доставио одговор да се процедуре које се односе на континуитет пословања и опоравак система у случају катастрофалног отказа своде на „backup“ и „restore“ података за систем СОН-а (система обједињене наплате)[35]. ЈКП „Инфостан технологије“ Београд зависно од типа прекида односно да ли је у питању делимични или потпуни прекид у раду пословних процеса примењује следећа решења:

- у случају делимичног отказа система за рад пословних сервиса њихову улогу преузимају редундантни системи како би се минимизовао планирани прекид у раду система. То значи да за све кључне тачке у систему, чији би отказ значио дужи прекид у раду, постоји удвајање ресурса. Ово се реализује кроз обнављање постојећих система рачунарске мреже, система за складиштење података и других инфраструктурних ресурса.
- у случају потпуног, хаваријског отказа користи се „Disaster Recovery“ локација[36].

У Правилнику о безбедности информационо-комуникационог система ЈКП „Инфостан технологије“ Београд наведено је да у случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде, Сектор за пословне операције и сервисе, је дужан да у најкраћем року пренесе делове ИКТ система (или обезбеди функционисање редундантних компоненти на резервној локацији уколико постоје) неопходне за функционисање у ванредној

[33] Ibid.
[34] Ibid.
[35] BCP и DRP.
[36] Одговор на Захтев за доставу документације и податке ЈКП Инфостан технологије Београд.

ситуацији на резервну локацију, у складу са планом реаговања у ванредним и кризним ситуацијама.

Препорука: Препоручујемо ЈКП Инфостан технологије – Београд да донесе План пословног континуитета са потребним елементима, именује тим за спровођење, увежбава, периодично га проверава и иновира.

ЈКПОН – Ниш

ЈКП „Обједињена наплата“ Ниш није усвојио План континуитета пословања, односно није документовао процесе, процедуре и контроле да би осигурао захтевани ниво континуитета пословања током ванредне ситуације. ЈКП „Обједињена наплата“ Ниш је планирао увођење Стандарда ИСО 22301-Систем менаџмента континуитетом пословања, Планом набавки за 2021. годину.[37]

Препорука: Препоручујемо ЈКПОН - Ниш да донесе План пословног континуитета са потребним елементима, именује тим за спровођење, увежбава, периодично га проверава и иновира.

Налаз 1.1: Субјекти ревизије нису препознали и дефинисали значајне ИТ ризике, а што може негативно утицати на управљање информационим системима.

Економско, друштвено и политичко окружење се убрзано мења тако да руководство јавног комуналног предузећа мора бити спремно на промене, измену приоритета и важност појединих делова пословања. Руководилац ЈКП сноси крајњу одговорност за управљање ризицима. У овој улози процес управљања ризицима је алат који помаже руководству да што прецизније предвиди промену околности и да на њих адекватно реагује.

Управљање ризицима омогућава да се:

- предвиде неповољне околности или догађаји који би могли спречити остварење пословних циљева;
- усмери управљање, контрола и ресурси према кључним подручјима делатности и с њима повезаним ризицима.

Ризици повезани са ИТ управљањем појављују се због непостојања стратешког документа којим се дефинишу смернице, како остварити стратешке циљеве. Неуспостављени орган или управљачко тело које се бави овим питањима стратешког управљања синергично делује на недовољно квалитетно испуњење сврхе оснивања ЈКП за обједињену наплату. Обзиром да је реч о јавном комуналном предузећу које чини важан део комуналног система ЈЛС, стратешки документи управљачких органа ЈЛС уопште не дефинишу питања дигитализације комуналних услуга, и све се заснива на спорадичним напорима без дефинисања јасних циљева и њихове усклађености са стратешким циљевима ЈЛС.

ЈКП за обједињену наплату – субјекти ревизије су основани ради обављања делатности из области информационих технологија (обраду података и хостинг и кабловске телекомуникације) и зато је управљање информационим системом важан део ЈКП за обједињену наплату.

ЈКП за обједињену наплату – субјекти ревизије су усвојили стратегије управљања ризицима и усвојили регистар ризика.

[37] 7 - Политика пословног континуитета.

Стандардима ИСО 27005-Управљање ИТ ризицима дефинисани су типови претњи (ризика):

- Физичка оштећења (пожар, уништење водом, загађење, хемијски акциденти, уништавање опреме или медија, корозија, хладноћа, прашина);
- Природне катастрофе (климатски промене, сеизмички догађаји, поплаве);
- Пандемије и епидемије;
- прекид у пружању кључних услуга (грешка система за одржавање температуре, губитак напона напајања, квар телекомуникационе опреме);
- прекид због радијације (термичка и друга зрачења);
- компромитовање информација (пресретање сигнала и ометања сигнала, шпијунирање, крађа медија или докумената, крађа опреме, недозвољено објављивање докумената, индустријска шпијунажа, инсајдери, саботажа).

У табели број 4 дат је преглед ИТ ризика који су препознали субјекти ревизије у Регистру ризика. Субјекти ревизије нису препознали, дефинисали и предвидели одговоре на ИТ ризике који су наведени у ИСО стандарду 27005-Управљање ИТ ризицима.

Табела 4. Преглед евидентираних ИТ ризика у Регистру ризика

ЈКП Информатика Нови Сад	ЈКП Инфостан технологије Београд	ЈКП Обједињена наплата Ниш
Губитак расположивости услуге	Достављање Извештаја служби књиговодства СОН-а само у штампаној форми, на основу кога наведена служба даље прекуцава све податке ручно, успорава Процес израде извештаја о задужењу и наплати на месечном нивоу и може да услови појаву грешака због великог утицаја људског фактора	Покушај пљачке (безбедност)
Пожар	Непостојање континуираног извештавања о пријему, роковима, ангажованим ресурсима и реализацији Захтева за информатичку подршку, потенцијално онемогућава ефикасно управљање захтевима и последично успорава остале пословне процесе који зависе од информатичке подршке	Проневера (спречавање губитка)
Квар компоненте/оштећење опреме	Непостојање плана континуитета пословања која има за циљ да успостави мере опоравка у случају катастрофа, може утицати да критични пословни процеси нису заштићени од већих катастрофа које би могле да утичу на благовремено настављање процеса пословања	Погрешан обрачун и пренос пазара удружи оцима
		Грешке при уносу и анализи података у матичну евиденцију

Када је у питању Стратегија процене ризика, субјекти ревизије су усвојили документ, који поседују типску-формалну структуру која се захтева при доношењу Стратегије управљања ризицима. Према достављеним подацима Регистар ризика су усвојили сви субјекти ревизије (ЈКП Информатика Нови Сад, ЈКП Инфостан технологије Београд и ЈКП Обједињена наплата Ниш). Од посебне важности је процена, попис и управљање ИТ ризицима јер субјекти ревизије управљају сложеним ИТ системима и обављају послове из информатичке делатности. Анализом стратегије процене ризика и регистра ризика субјеката ревизије утврђено је да исти не садрже критеријуме за евидентирање и извештавање о свим ИТ ризицима који су карактеристични за овај информациони систем. Поред тога што нису обухваћени карактеристични ИТ ризици

(дефинисани стандардима ИСО 27005) субјектима ревизије недостаје процена утицаја на пословање и припадајуће мере које требају да избегну или умање негативни утицај на пословање.

ЈКП Информатика – Нови Сад

Иако је успостављен Регистар ризика нису обухваћени значајни ИТ ризици који могу изазвати поремећаје у пословању, делимичним, краткотрајним као и дужим прекидима у пружању услуга. То може довести до умањења поверења корисника у способност ЈКП да обављају додељене послове због којих су основани.

Препорука: Препоручујемо ЈКП Информатика – Нови Сад да дефинише све значајне ИТ ризике као и потребне елементе на основу којих у складу са оцењеним утицајем на пословање може одредити адекватна мера у циљу избегавања или умањења негативног утицаја на пословање.

ЈКП Инфостан технологије – Београд

Иако је успостављен Регистар ризика нису обухваћени значајни ИТ ризици који могу изазвати поремећаје у пословању, делимичним, краткотрајним као и дужим прекидима у пружању услуга. То може довести до умањења поверења корисника у способност ЈКП да обављају додељене послове због којих су основани.

Препорука: Препоручујемо ЈКП Инфостан технологије – Београд да дефинише све значајне ИТ ризике као и потребне елементе на основу којих у складу са оцењеним утицајем на пословање може одредити адекватна мера у циљу избегавања или умањења негативног утицаја на пословање.

ЈКПОН – Ниш

Иако је успостављен Регистар ризика нису обухваћени значајни ИТ ризици који могу изазвати поремећаје у пословању, делимичним, краткотрајним као и дужим прекидима у пружању услуга. То може довести до умањења поверења корисника у способност ЈКП да обављају додељене послове због којих су основани.

Препорука: Препоручујемо ЈКПОН – Ниш да дефинише све значајне ИТ ризике као и потребне елементе на основу којих у складу са оцењеним утицајем на пословање може одредити адекватна мера у циљу избегавања или умањења негативног утицаја на пословање.

Налаз 1.2: Субјекти ревизије нису вршили процену утицаја на пословање ни за препознате ризике, а што може негативно утицати на управљање информационим системима.

Процена пословног утицаја је поступак утврђивања које су активности у пословању су критичне по остварење циљева, од којих ресурса зависе постизање резултата, зависи и избор примењених мера које треба да обезбеде отпорност према ризику и јачање континуитета пословања. Које мере ће организација применити зависи од процењеног значаја и утицаја критичног процеса и/или ресурса.

Сваки информациони систем и/или информациона услуга коју користе запослени у свом раду, пословни партнери, корисници итд, а у овом случају то је целокупни систем комуналних услуга са свим становницима, може се заштити на различите начине. Колико једна информациона услуга, електронска пошта, интернет презентација, портал за увид у комуналне рачуне, систем за обрачун услуга, интернет веза, итд. је важна за пословање ЈКП одредиће избор начина обезбеђења наставка рада у случају остварења ризика.

Ако се комуникација између запослених, додела радних задатака, извештавање итд. обавља употребом електронске поште, онда је веома важно да сервер електронске поште (Mail server) функционише без прекида. Ако се процени да је рад сервера електронске поште пресудан за функционисање ЈКП, неопходно је документовати:

- Попис свих пословних активности и ресурса како би се утврдило шта треба заштитити и/или опоравити након појаве поремећаја у пословању;
- Одредити приоритете процесима и услугама, који морају бити заштићени од последица поремећаја у пословању;
- Одредити времена опоравка (РТО) и тачку опоравка (РПО), колико брзо се мора наставити пословање након поремећаја и колику штету (нпр. губитак података итд.) може приуштити ЈКП;
- Утврдити мере које треба применити за умањење ризика и последица поремећаја пословања у складу са претходним захтевима.

ЈКП Информатика – Нови Сад

ЈКП Информатика – Нови Сад нема документовану процену утицаја на пословање, а приоритете у опоравку одређује на основу стручне процене и искуства тренутно запослених на ИТ пословима.

Препорука: Препоручујемо ЈКП Информатика – Нови Сад да изради Процену утицаја на пословање обухватајући све значајне пословне процесе, информационе системе и услуге, одреди очекивана времена и тачке опоравка за сваки ресурс као и смернице које мере применити.

ЈКП Инфостан технологије – Београд

ЈКП Инфостан технологије – Београд нема документовану процену утицаја на пословање, а приоритете у опоравку одређује на основу стручне процене и искуства тренутно запослених на ИТ пословима.

Препорука: Препоручујемо ЈКП Инфостан технологије – Београд да изради Процену утицаја на пословање обухватајући све значајне пословне процесе, информационе системе и услуге, одреди очекивана времена и тачке опоравка за сваки ресурс као и смернице које мере применити.

ЈКПОН – Ниш

ЈКПОН – Ниш нема документовану процену утицаја на пословање, а приоритете у опоравку одређује на основу стручне процене и искуства тренутно запослених на ИТ пословима.

Препорука: Препоручујемо ЈКПОН – Ниш да изради Процену утицаја на пословање обухватајући све значајне пословне процесе, информационе системе и услуге, одреди очекивана времена и тачке опоравка за сваки ресурс као и смернице које мере применити.

Налаз 1.3: Субјекти ревизије немају планове за ванредне ситуације, јер оснивач није својим планом дефинисао задатке и обавезе за ове ЈКП, што може довести до штете и губитака.

Законом о информационој безбедности[38] се одређују мере заштите од безбедносних ризика у ИКТ системима и одговорностима правних лица приликом управљања и коришћење ИКТ система. Под редним бројем 28 се одређује мера која обезбеђује континуитет обављања посла у ванредним околностима. У уредби о ближем уређењу мера заштите информационо-комуникационих система[39] од посебног значаја се одређује да ЈКП треба да:

[38] Члан 7 Закона о информационој безбедности.
[39] "Сл. Гласник РС", бр. 94/2016.

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

Законом о смањењу ризика од катастрофа и управљању ванредним ситуацијама[40] су утврђене бројне обавезе органа локалне самоуправе, са циљем да се, уз њихов незаменљив допринос и кроз сарадњу са другим субјектима, смањи ризик од катастрофа и делотворније управља ванредним ситуацијама у Републици Србији.
Законом је омогућено да привредни субјекти који су овлашћени да се баве израдом Процене угрожености од катастрофа и Плана заштите и спасавања, могу бити ангажовани на изради планова, и дефинисати задатке за свако комунално предузеће, које и како треба да обезбеде континуитет пословања у ванредним ситуацијама.
Орган локалне самоуправе као оснивач ЈКП треба да одреди степен безбедности и отпорности свих ЈКП, према ризицима који прете услед природних или техничко - технолошких несрећа.

ЈКП Информатика – Нови Сад

Оснивач Град Нови Сад није обавестио ЈКП које мере и активности за спречавање и умањење последица катастрофа треба да планира и шта се од ЈКП очекује у ванредним ситуацијама.

Као последицу ЈКП Информатика – Нови Сад нема документован План континуитета пословања у ванредним ситуацијама, и досадашње поступање је одређено на основу стручне процене и искуства тренутно одговорних запослених лица.

Препорука: Препоручујемо ЈКП Информатика – Нови Сад да покрене иницијативу код оснивача да им одреди потребне елементе у оквиру Плана заштите и спасавања, ради израде Плана за рад у ванредним ситуацијама.

ЈКП Инфостан технологије – Београд

У Правилнику о безбедности информационо-комуникационог система ЈКП „Инфостан технологије“ Београд наведено је да се у случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде, Сектор за пословне операције и сервисе, је дужан да у најкраћем року пренесе делове ИКТ система (или обезбеди функционисање редундантних компоненти на резервној локацији уколико постоје) неопходне за функционисање у ванредној ситуацији на резервну локацију, у складу са планом реаговања у ванредним и кризним ситуацијама.
ЈКП Инфостан технологије – Београд није тестирао измештање ИКТ система из зграде, расположивост редундантних компоненти и система за функционисање на резервној локацији и нема План реаговања у ванредним и кризним ситуацијама.

[40] "Сл. гласник РС", бр. 87/2018.

Препорука: Препоручујемо ЈКП Инфостан технологије – Београд да покрене иницијативу код оснивача да им одреди потребне елементе у оквиру Плана заштите и спасавања, ради израде Плана за рад у ванредним ситуацијама.

ЈКПОН – Ниш

Оснивач Град Ниш није обавестио ЈКП које мере и активности за спречавање и умањење последица катастрофа треба да планира и шта се од ЈКП очекује у ванредним ситуацијама.

ЈКПОН – Ниш нема документован План континуитета пословања у ванредним ситуацијама, и досадашње поступање је одређено на основу стручне процене и искуства тренутно одговорних запослених лица.

Препорука: Препоручујемо ЈКПОН – Ниш да покрене иницијативу код оснивача да им одреди потребне елементе у оквиру Плана заштите и спасавања, ради израде Плана за рад у ванредним ситуацијама.

Налаз 1.4: Субјекти ревизије немају свеобухватне планове опоравка од хаварије информационог система којим би дефинисали тај процес, иако поседују знање и искуство у превазилажењу хаваријских догађаја.

План опоравка од хаварије[41] подразумева процес планирања и тестирања опоравка информационог система (хардвера и софтвера) након што се деси хаварија[42].

План опоравка од хаварије треба да садржи:

- процедуре за опоравак информационог система кад наступе катастрофални догађаји;
- приоритете опоравка ресурса информационог система;
- податке о тимовима и члановима тимова који ће бити одговорни за опоравак информационог система, њихове дужности и одговорности;
- резервну локацију за опоравак информационог система, односно локацију резервног рачунарског центра.

План опоравка од хаварије омогућава ЈКП да настави да функционише након што се деси хаварија.

Субјекти ревизије нису доставили доказе да су усвојили и примењују План опоравка од хаварије.

ЈКП Информатика – Нови Сад

ЈКП „Информатика“ Нови Сад је за потребе опоравка ИС у случају хаварије имплементирала решење „VMware Site Recovery Manager“ или скраћено „CPM“. „Site Recovery Manager“ (CPM) инфраструктура се састоји из два подсистема.

ЈКП „Информатика“ Нови Сад није доставила доказе да су усвојили и примењују План опоравка од хаварије.

Препорука: Препоручујемо ЈКП Информатика – Нови Сад да успоставе свеобухватни План опоравка од хаварије и врше његово редовно ажурирање.

ЈКП Инфостан технологије – Београд

ЈКП „Инфостан технологије“ Београд је навео да се као план опоравка од хаварије у случају делимичног отказа система за рад пословних сервиса користе редундантни системи како би се минимизовао планирани прекид у раду система.

[41] Енг. Disaster Recovery Planning-DRP.

[42] Хаварија је поремећај у техничко-технолошком систему који доводи до потпуног отказа у дужем временском периоду.

ЈКП „Инфостан технологије“ Београд наводи да у случају отказа свих делова одређене компоненте система могуће да се сервисирање кроз услугу одржавања, које је дефинисано за све кључне тачке у систему. Ова услуга одржавања је за одређене делове дефинисана кроз „CLA“ услове. То је случај са инфраструктуром одређеној за рад СОН-а (Unisys систем за обраду података за СОН).
Такође, представници ЈКП „Инфостан технологије“ Београд у случају потпуног отказа система када није могуће успоставити на оригиналној локацији функционисање система СОН-а, у том случају користила би се резервна локација.
ЈКП Инфостан технологије – Београд није доставио доказе да су усвојили и примењују План опоравка од хаварије.

Препорука: Препоручујемо ЈКП Инфостан технологије – Београд да успоставе свеобухватни План опоравка од хаварије и врше његово редовно ажурирање.

ЈКПОН – Ниш

ЈКП „Обједињена наплата“ Ниш нема усвојен План опоравка од хаварија, али су навели да је то питање регулисано члановима 16, 17, 20 и 21. Правилника о безбедности ИКТ система. Наведеним члановима Правилника о безбедности ИКТ система је уопштено дефинисана:

- физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему,
- заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава који чине ИКТ систем,
- заштита од губитака података и
- чување података о догађајима који могу бити од значаја за безбедност ИКТ система.

Препорука: Препоручујемо ЈКПОН – Ниш да успоставе свеобухватни План опоравка од хаварије и врше његово редовно ажурирање.

Налаз 1.5: ЈКПОН-Ниш није интерним актом уредила успостављени процес израде резервних копија података што може довести до неадекватног поступања у случају кадровске промене.

Управљање резервним копијама података треба да обухвати поступке израде, чувања и тестирања ових копија, као и опоравка података и софтверских компонената, како би се омогућило поновно успостављање пословних процеса у оквиру циљног времена опоравка.
ЈКП за обједињену наплату – субјекти ревизије треба да обезбеди да су резервне копије података ажурне и адекватно заштићене, а поступци опоравка тестирани и успешни.

ЈКП Информатика – Нови Сад

ЈКП „Информатика“ Нови Сад је усвојила Процедуру за израду резервних копија (back-up) број ПРО-1010.5 дана 30. маја 2018. године[43]. Усвојена Процедура је типског карактера према ИСО стандарду 27002:2013. ЈКП „Информатика“ Нови Сад спроводи План „back-up“-а за „Oracle“ базе сходно Уговору о редовном одржавању „Oracle“ базе. У оквиру Уговора налазе се и услуге планирања „back-up“-а као и ажурирање „back-up“ процедура у зависности од хардверско-софтверских или пословних промена[44]. „Back-up“ база се врши једном недељно, док се тестирање опоравка врши по редовној процедури квартално, по захтеву ЈКП „Информатика“ Нови Сад и након ажурирања „back-up“ процедура.
ЈКП „Информатика“ Нови Сад поседује две различите платформе за виртуализацију, једну базирану на „VMware Enterprise“ технологији и другу базирану на „Hyper-V“ технологији. За

[43] PRO-1012 1_вер_3_22 05 2017.
[44] План бекапа за Оракл базе.

чување резервних копија виртуелних сервера изграђен је систем за „back-up" који подржава заштиту за обе платформе.

ЈКП Инфостан технологије – Београд

План за резервне копије у ЈКП „Инфостан технологије" Београд је дефинисан Правилником о виртуализацији безбедности информационо-комуникационог система[45], Процедуром за инфраструктуру и сервисе[46] и Списку идентификованих пословних процеса Сектора за пословне операције и сервисе „Процеси СПОС"[47]. Базе података обавезно се архивирају на преносиве медије најмање једном дневно, недељно, месечно и годишње за потребе обнове базе података[48]. Исправност копија-архива проверава се најмање на шест месеци и то тако што се изврши повраћај база података које се налазе на медију, при чему враћени подаци након повраћаја треба да буду исправни и спремни за употребу[49].
ЈКП „Инфостан технологије" Београд сходно Списку идентификованих пословних процеса у оквиру Плана за резервне копије спроводи:

- Редовни „dump" базе-свакодневни,
- Копирање „Audit" датотека базе, backup
- Комплетно копирање дискова,
- „Garbage collection",
- „Back-up" система,
- Мониторинг (бекап, логови, стање дискова, перформансе).

ЈКПОН – Ниш

ЈКП „Обједињена наплата" Ниш нема усвојен појединачни акт везан за резервне копије. ЈКП „Обједињена наплата" Ниш нас је обавестио да постоји неформална процедура за спровођење "back-up" података.
У оквиру Правилника о безбедности ИКТ система у ЈКП „Обједињена наплата" Ниш наведено је да се базе података обавезно архивирају на преносиве медије најмање једном недељно, за потребе обнове базе података. Исправност копија-архива проверава се најмање на шест месеци и то тако што се изврши повраћај база података које се налазе на медију, при чему враћени подаци након повраћаја треба да буду исправни и спремни за употребу[50].
Субјект ревизије ЈКП „Обједињена наплата" Ниш је на питање везано за План за резервне копије навео да свакога радног дана (понедељак-субота) радници Службе за системску подршку и развој ИС по затварању шалтера пуштају апликацију за „back-up" базе, затим да се наредног јутра бекап „зип"-ује. Даљи корак је да се „зип"-овани „back-up" снима на ДВД и на екстерни хард диск. На крају се диск одлаже на посебно означено место. У плану је обезбеђивање још једне додатне локације где би се једном недељно чувао диск са копијом базе података[51]. ЈКП „Обједињена наплата" Ниш према достављеном одговору једном месечно, викендом, по завршетку рада, а после формирања и слања свих месечних извештаја и рачуна, гаси главни сервер и формира копију базе података. Копија се снима на Тест сервер који служи за све врсте тестирања и за брже откривање промена у бази[52].

Препорука: Препоручујемо ЈКП „Обједињена наплата" Ниш да израде свеобухватни План израде резервних копија података.

[45] Инфостан Акт о безбедности.
[46] ПР-СПОС-СЛИС-01 В2-20170922.
[47] 15.1 Процеси_СПОС.
[48] Инфостан Акт о безбедности (члан 21.)
[49] Инфостан Акт о безбедности (члан 21.)
[50] Правилник о безбедности.
[51] 8. прављење копије базе на диску и екстеном хард диску.
[52] 8. прављење копије базе на тест сервер.

ЗАКЉУЧАК 2: Управљање безбедношћу информационих система није потпуно адекватно, јер није успостављено управљање инцидентима.

Наш циљ у овом делу извештаја, био је да одговоримо на друго ревизијско питање, односно да ли се на адекватан начин управља безбедношћу информационих система јавних предузећа за обједињену наплату.

У оквиру одговора на друго ревизијско питање разматрали смо стратегије развоја ИТ у ЈКП за обједињену наплату, процедуре везане за информациону безбедност, политике управљања инцидентима, листе корисника ИС обједињене наплате и на који начин су запослени (корисници ИС) упознати са улогама и одговорностима у погледу коришћења и заштите ИС и података.

На основу постављеног питања, формулисали смо и следећа потпитања:

- Да ли предузеће поседује ефективна акта, процедуре и/или правила за обезбеђење информација?
- У којој мери су значајни ризици избегнути или ублажени?
- Да ли су правила и процедуре ефикасне и ефективне за безбедну интерну и екстерну комуникацију?
- Како предузеће обезбеђује да запослени буду упознати са својим улогама и одговорностима у погледу заштите ИСЈПОН?
- Како предузеће открива и спречава приступ информатичкој инфраструктури неовлашћеним особама?

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, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица[53].

Информациона безбедност подразумева способност система (софтвера) да обезбеди поверљивост, интегритет и заштиту података и информационог система. Информациона безбедност укључује мере откривања, документовања и решавање проблема неовлашћеног приступа или измене података на серверима, обради и преносу података и омогућавању рада овлашћеним корисницима. Информациона безбедност обухвата безбедност система и безбедност комуникација. Кључне ставке информационе безбедности су доступност, поверљивост и интегритет података и система[54].

Према одредбама члана 7 Закона о информационој безбедности оператор ИКТ система од посебног значаја (у нашем случају-субјекти ревизије) одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система. Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидента, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима[55]. Мере заштите ИКТ система су у Закону о информационој безбедности подељене на 28 мера заштите [56]. Према одредбама члана 8 Закона о информационој безбедности оператор ИКТ система од посебног значаја дужан је да донесе акт о безбедности ИКТ система. Такође је дужан да самостално или уз ангажовање спољних експерата врши проверу усклађености примењених мера ИКТ система са актом о безбедности ИКТ система и то најмање једном годишње и да о томе сачини извештај[57].

[53] Члан 2 став 1 тачка 3 Закона о информационој безбедности.
[54] WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions.
[55] Члан 7 став 2 Закона о информационој безбедности.
[56] Члан 7 став 3 Закона о информационој безбедности.
[57] Члан 8 став 4 Закона о информационој безбедности.

Табела 5. Преглед донешених аката којима се уређују питања информационе безбедности

Опис-субјекти ревизије	ЈКП Информатика Нови Сад	ЈКП Инфостан технологије Београд	ЈКП Обједињена наплата Ниш
Акт о информационој безбедности	Да, број 5499/17 од 1.3.2017. године	Да, број 1432/2 од 6.3.2017. године	Да, Правилник о безбедности ИКТ система, број 3055 од 15.6.2020. године
Политика управљања инцидентима	Немају усвојену политику управљања. *	Немају усвојену политику	Немају усвојену политику

*усвојена процедура извештавања о инцидентима.

Стратегија развоја ИТ у ЈКП за обједињену наплату – субјектима ревизије

Стратегија развоја информационих технологија у ЈКП за обједињену наплату не постоји као обавезан документ и код већине јавних предузећа се планира на годишњем нивоу кроз циљеве програма пословања.

ЈКП „Информатика“ Нови Сад поседује Петогодишњи план развоја ИТ инфраструктуре, из маја 2020. године. Петогодишњи план развоја ИТ инфраструктуре је израдио консултант према техничкој спецификацији ЈКП „Информатика“ Нови Сад. Петогодишњи план развоја ИТ инфраструктуре садржи преглед постојеће инфраструктуре, принципе нове ИТ инфраструктуре и архитектуре, предлог неопходне ИТ документације, креирање ИТ инфраструктурних докумената, анализа постојећих система подршке, предлог новог модела подршке[58].

ЈКП „Инфостан технологије“ Београд нема усвојену стратегију развоја информационих технологија као посебан документ, али се планирање ИТ ресурса ради у оквиру програма пословања, који се доноси на годишњем нивоу. У оквиру програма пословања су дефинисани различити циљеви који су заједнички на нивоу ЈКП-а и захтевају учешће ИТ сектора у остваривању истих. Главни циљеви у области рада ИТ службе су: обезбеђивање континуитета функционисања пословних сервиса, повећање безбедности у раду рачунских мрежа и повећање перформанси основних и пратећих пословних сервиса[59].

ЈКП „Обједињена наплата“ Ниш нема усвојену стратегију развоја информационих технологија као посебан документ, али поседује Средњорочни план пословне стратегије и развоја за период 2017-2021. годину. У Средњорочном плану су као кључне области дефинисане следеће области: база података, информациона технологија и увођење стандарда[60].

Налаз 2.1: Субјекти ревизије поседују Акт којим уређују питања у вези информационе безбедности.

Законом о информационој безбедности[61] се одређују мере заштите од безбедносних ризика у ИКТ системима и одговорностима правних лица приликом управљања и коришћење ИКТ система. Чланом 8 Закона прописана је обавеза да ЈКП донесе Акт о безбедности ИКТ система од посебног значаја којом се уређују мере заштите, а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система од посебног значаја. Посебна Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја детаљније дефинише садржај акта који се мора редовно усклађивати с променама у окружењу и у самом ИКТ систему.

[58] Петогодишњи план развоја ИТ инфраструктуре.
[59] Одговор на Захтев за доставу документације и податке ЈКП Инфостан технологије Београд.
[60] Средњорочни план, ЈКП Обједињена наплата.
[61] Члан 7 Закона о информационој безбедности.

ЈКП је дужан да самостално или уз ангажовање спољних експерата врши проверу усклађености примењених мера ИКТ система са актом и то најмање једном годишње и да о томе сачини извештај.

ЈКП Информатика – Нови Сад

ЈКП „Информатика“ Нови Сад је донела Акт о безбедности ИКТ система дана 1. марта 2017. године. ЈКП „Информатика“ Нови Сад је имплементирала и сертификовала пословни систем према захтевима међународних стандарда ИСО 9001:2008 и ИСО/ИЕС 2700:2013. У Акту о безбедности ИКТ система мере заштите упућују на процедуре које су усвојене у складу са захтевима имплементираног стандарда ИСО 27001:2013[62]. ЈКП је доставила и извештај о провери усклађености примењених мера ИКТ система из децембра 2019. године.

ЈКП Инфостан технологије – Београд

ЈКП „Инфостан технологије“ Београд је донео Правилник о безбедности ИКТ система дана 6. марта 2017. године. Правилником су утврђене мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система. ЈКП „Инфостан технологије“ Београд поседује сертификате следећих стандарда: СРПС ИСО 9001:2015 Систем менаџмента квалитетом, СРПС ИОС/ИЕЦ 27001:2014 Систем меџамента безбедношћу информација и СРПС ИСО 31000:2015 Система менаџмента ризиком[63].

ЈКПОН – Ниш

ЈКП „Обједињена наплата“ Ниш је донела Правилник о безбедности ИКТ система дана 15. јуна 2020. године. Правилником су одређене мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система од посебног значаја[64]. У периоду обухвата ревизије 2018-2019. године ЈКП „Обједињена наплата“ Ниш није имала усвојен Правилник о безбедности ИКТ система што је била обавеза у складу са Законом о информационој безбедности.

ЈКП „Обједињена наплата“ Ниш је донела Правилник о безбедности ИКТ система дана 15. јуна 2020. године.

Налаз 2.2: Субјекти ревизије нису успоставили управљање инцидентима.

Руководилац ЈКП сноси крајњу одговорност за управљање ризицима, стога је поред обухватања свих ИТ ризика неопходно проценити значај и утицај могућег остварења у виду поремећаја у пословању и припремити мере које ће се применити у циљу спречавања штете или умањења последица по људе и имовину. ЈКП у складу с обимом и сложеношћу пословања је успоставила информациони систем. Последично ЈКП треба да надзире, контролише и унапређује процес управљања овим системом ради смањења изложености ризицима и очувања безбедности и функционалности тог система.

У којој мери су значајни ризици избегнути или ублажени пре свега зависи од примењених мера код појаве ризика, када наступи поремећај у пословању. ЈКП за обједињену наплату које пружа услуге обрачуна и наплате комуналних услуга чији је рад уређен прописима има успостављен систем рекламација за обраду насталих грешака, утврђивања свих потребних елемената које настају у том процесу. Унапређење рада на пружању услуга се заснива на утврђивању узрока настале грешке или проблема. Природу, трајање, узрока или инцидента који је изазвао грешку или проблем, можемо утврдити ако анализирамо све евидентиране инциденте.

[62] Акт о безбедности ИКТ система ЈКП Информатика Нови Сад 5499 01.03.2017.
[63] Инфостан Акт о безбедности.
[64] Правилник о безбедности.

Законом о информационој безбедности[65] је инцидент дефинисан као сваки догађај који има стваран негативан утицај на безбедност мрежних и информационих система.

Тако је предвиђено и успостављање јединственог система за пријем обавештења о инцидентима као информациони систем у који се уносе подаци о инцидентима у ИКТ системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности, а које је успоставило регулаторно тело РАТЕЛ.

Обавеза сваког ЈКП да о инцидентима у ИКТ систему обавештава је уређена Уредбом[66] којом су одређени сви неопходни елементи инцидената, који се достављају електронским путем.

ЈКП Информатика – Нови Сад

Иако је успостављен процес управљања рекламацијама, до сада нису успоставили електронску евиденцију са свим елементима инцидената на начин који би омогућио електронско достављање обавештења надлежном органу.

Препорука: Препоручујемо ЈКП Информатика – Нови Сад да успостави процес управљања инцидентима који ће омогућити благовремен и ефикасан одговор у случају нарушавања безбедности или функционалности информационог система и организује обавештавање надлежног органа електронским путем.

ЈКП Инфостан технологије – Београд

Иако је успостављен процес управљања рекламацијама, до сада нису успоставили електронску евиденцију са свим елементима инцидената на начин који би омогућио електронско достављање обавештења надлежном органу.

Препорука: Препоручујемо ЈКП Инфостан технологије – Београд успостави процес управљања инцидентима који ће омогућити благовремен и ефикасан одговор у случају нарушавања безбедности или функционалности информационог система и организује обавештавање надлежног органа електронским путем.

ЈКПОН – Ниш

Иако је успостављен процес управљања рекламацијама, до сада нису успоставили електронску евиденцију са свим елементима инцидената на начин који би омогућио електронско достављање обавештења надлежном органу.

Препорука: Препоручујемо ЈКПОН – Ниш успостави процес управљања инцидентима који ће омогућити благовремен и ефикасан одговор у случају нарушавања безбедности или функционалности информационог система и организује обавештавање надлежног органа електронским путем.

Налаз 2.3: Субјекти ревизије нису донели и спровели план комуникације у вези сајбер претњи.

Законом о информационој безбедности[67] као прве мере заштите одређено је успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу. У Уредби о ближем уређењу мера заштите

[65] Члан 2 Закона о информационој безбедности.

[66] Уредба о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја ("Сл. гласник РС", бр. 11/2020) и претходна Уредба о поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у ИКТ системима од посебног значаја („Сл. Гласник РС“ бр. 94/2016).

[67] Члан 7 Закона о информационој безбедности.

информационо-комуникационих система[68] дефинише се да ЈКП треба да обезбеди да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност.

Како би лица која користе ИКТ систем односно управљају ИКТ системом разумели своје одговорности, оператор ИКТ система обучава запослене о важности информационе безбедности ИКТ система, мерама и процедурама за заштиту ИКТ система и њиховим обавезама.

Оператор ИКТ система је дужан да покрене одговарајући поступак против лица одговорних за нарушавање безбедности информационог система.

Све веће претње по безбедност информационог система долази из сајбер простора путем електронских порука са злонамерним садржајем. Зато је неопходно редовно обавештавати запослене о најновијим покушајима да буду преварени лажном поруком које нападачи користе како би преузели управљање над појединим деловима или целокупним системом. У том процесу унутрашње комуникације треба обухватити и друге такве догађаје као што су злоупотреба лозинке за приступ систему, итд.

Поред обавештавања потребно је и организовати интерно обучавање о новим обавезама, прописима и другим важним догађајима који утичу на безбедност информационог система.

ЈКП Информатика – Нови Сад

Корисници информационог система нису редовно обавештавани нити обучавани како да препознају претње из сајбер простора.

Препорука: Препоручујемо ЈКП Информатика – Нови Сад да успоставе процес обавештавања и обучавања запослених чија радна места су изложена сајбер нападима, планира и организује обучавање о новим обавезама која утичу на безбедност информационог система.

ЈКП Инфостан технологије – Београд

Корисници информационог система нису редовно обавештавани нити обучавани како да препознају претње из сајбер простора.

Препорука: Препоручујемо ЈКП Инфостан технологије – Београд да успоставе процес обавештавања и обучавања запослених чија радна места су изложена сајбер нападима, планира и организује обучавање о новим обавезама која утичу на безбедност информационог система.

ЈКПОН – Ниш

Корисници информационог система нису редовно обавештавани нити обучавани како да препознају претње из сајбер простора.

Препорука: Препоручујемо ЈКПОН – Ниш да успоставе процес обавештавања и обучавања запослених чија радна места су изложена сајбер нападима, планира и организује обучавање о новим обавезама која утичу на безбедност информационог система.

[68] "Сл. Гласник РС", бр. 94/2016.

Налаз 2.4: У ЈКПОН-Ниш нису документоване изјаве запослених у вези преузимања одговорности.

У Уредби о ближем уређењу мера заштите информационо-комуникационих система[69] дефинише се да ЈКП треба да обезбеди да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност.

Сваки запослени приликом добијања налога за приступ информационим ресурсима потписује сагласност о последицама одавања лозинке за приступ информационим ресурсима.

Обрасци обухватају и параметре приступа систему и као такви интерни акти се придружују персоналном досијеу запосленог над којима се морају примењивати заштитне мере јер поседују осетљиве податке о личности.

ЈКП Информатика – Нови Сад

ЈКП „Информатика“ Нови Сад је обезбедио да запослени буду упознати са својим улогама и одговорностима у погледу заштите ИСЈПОН на такав начин да приликом преузимања корисничких креденцијала за рад у ИС корисници добијају списак правила и препорука, и својим потписом потврђују да су упознати са правилима.

ЈКП Инфостан технологије – Београд

ЈКП „Инфостан технологије“ Београд је обезбедио да запослени буду упознати са својим улогама и одговорностима у погледу заштите ИСЈПОН на такав начин да приликом преузимања корисничких креденцијала за рад у ИС корисници добијају списак правила и препорука, и својим потписом потврђују да су упознати са правилима.

ЈКПОН – Ниш

Иако је донет Правилник о безбедности информационо комуникационог система којим се одређују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационог система од посебног значаја који је усвојен дана 15.06.2020. (зав.бр. 00-3055) са којим су запослени упознати путем јавно доступне адресе, и она садржи одредбе које су запослени у обавези да поштују, а односе се на улоге и одговорности у погледу заштите информационог система, нису обезбедили личне изјаве да су запослени упознати са личном одговорношћу.

Препорука: Препоручујемо ЈКПОН – Ниш да обезбеди да сви запослени потпишу изјаву да су упознати са обавезама и одговорностима у вези налога за приступање информационом систему.

Налаз 2.5: Иако субјекти ревизије поседују минималну потребну опрему за онемогућавање неовлашћеног мрежног приступа они не врше редовно преглед покушаја упада у мрежу.

Законом о информационој безбедности[70] дефинише да је информационо-комуникациони систем (ИКТ систем) технолошко-организациона целина која обухвата: електронске комуникационе мреже у смислу закона који уређује електронске комуникације; уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарског програма; податке који се воде, чувају, обрађују, претражују или преносе помоћу средстава у сврху њиховог рада, употребе, заштите или одржавања; организациону структуру путем које се управља ИКТ системом; и све типове системског и апликативног софтвера и софтверске развојне алате.

[69] "Сл. Гласник РС", бр. 94/2016.
[70] Члан 7 Закона о информационој безбедности.

Пошто је ИКТ систем повезан на интернет мрежу, неопходно је обезбедити мрежне уређаје који ће спречавати неовлашћени приступ информационим ресурсима.

ЈКП Информатика – Нови Сад

ЈКП „Информатика“ Нови Сад користи системе заштите откривања и спречавања недозвољеног приступа ИТ инфраструктури на два нивоа: логички ниво и физички ниво.

У оквиру логичког нивоа заштите употребљава се заштитни уређај у кластерском режиму реализације на примарној локацији и софтверско решење као систем за филтрирање корисничког приступа интернету. ЈКП „Информатика“ Нови Сад сада користи антивирусно решење које обухвата и заштиту од рансомвера.
У оквиру физичког нивоа заштите, подаци и критични ИТ системи се налазе у дата центрима, у које је могућ приступ само уз овлашћено лице. Постоји 24 часовни систем видео надзора уз стално присуство физичког обезбеђења. Улаз у главну сервер собу је заштићен вратима са електронским закључавањем. Такође при уласку у сервер салу се користе безбедносне процедуре као аутентификацију преко PIN кодова и читача ID картица[71].
Све активности у анализи ЛОГ датотека се догађају по захтеву надлежних органа или у циљу спровођења контроле настале грешке у систему и не врше се редовно.

Препорука: Препоручујемо ЈКП Информатика – Нови Сад да успостави редовно прегледавање ЛОГ датотека (журнала) мрежних уређаја за спречавање упада и свих постојећих система и сачињава о томе записник.

ЈКП Инфостан технологије – Београд

ЈКП „Инфостан технологије“ Београд користи системе заштите откривања и спречавања недозвољеног приступа ИТ инфраструктури зависно од типа приступа. Постоји приступ надгледања спољног и унутрашњег мрежног саобраћаја.

Спољни приступ се надгледа и контролише на нивоу Firewall заштитног уређаја који детектује и спречава неауторизовани спољни приступ и омогућава ауторизовани приступ, при чему постоје лог-ови за сваки покушај приступа на самом Firewall уређају за ограничени временски период. Ове логове је неопходно архивирати за историјат битних догађаја. Архивирање и „Log Management“ се врши „Log Management“ системом. Поред надгледања приступа контролише се долазни и одлазни интернет саобраћај, детекција злонамерног садржаја у мејл саобраћају тј. превенција „zero day“ напада итд.

Унутрашњи саобраћај се контролише заштитним уређајима: у питању је осигурани начин приступа серверима – дефинисана су правила која омогућавају међусобну комуникацију дефинисаних сервера односно сервера и група корисничких рачунара. Приступ се дефинише и надзире по одређеном порту односно изабраном протоколу чиме се постиже виши ниво безбедности у односу на класичне заштитне уређаје. Такође се користи и NPMD систем за праћење и управљање перформансама и стањима мреже и апликација тј. праћење мрежног саобраћаја који у својим логовима може да пружи податке о могућим покушајима неауторизованог приступа.

Додатни уређај за лакше управљање подацима је уређај „Log Management“ који омогућава централизовано прикупљање, обраду и поједностављену нотификацију и давање упозорења/алармирање у случају неуобичајених или инцидентних догађања у мрежи.

Посебан део заштите је физичка заштита приступа сервер сали, просторијама ИТ службе на главној локацији и локацијама радних јединица. Заштита се постиже постојањем службе за контролу приступа просторијама као и системом електронске заштите врата. За улазак је

[71] Приступ ИТ инфраструктури.

неопходно поседовати ауторизовану картицу или токен за приступ заштићеним просторијама. Такође се врши и видео надзор свих битних просторија[72].

Све активности у анализи ЛОГ датотека се догађају по захтеву надлежних органа или у циљу спровођења контроле настале грешке у систему и не врше се редовно.

Препорука: Препоручујемо ЈКП Инфостан технологије – Београд да успостави редовно прегледавање ЛОГ датотека (журнала) мрежних уређаја за спречавање упада и свих постојећих система и сачињава о томе записник.

ЈКПОН – Ниш

ЈКП „Обједињена наплата“ Ниш користи системе заштите откривања и спречавања недозвољеног приступа ИТ инфраструктури које је прописао Правилником о безбедности ИКТ система. Предмет заштите су: хардверске и софтверске компоненте ИКТ система, подаци који се обрађују или чувају на компонентама ИКТ система и кориснички налози и други подаци о корисницима информатичких ресурса ИКТ система. Приступ ресурсима ИКТ система одређен је врстом налога, односно додељеном улогом коју запослени-корисник има. Право приступа имају само запослени/корисници који имају администраторске или корисничке налоге, међутим управљање налозима није централизовано. ЈКПОН-Ниш не поседује сервер за контролу домена или активни директоријум и на тај начин је отежана контрола ажурности лозинке корисника. Физичка заштита се обезбеђује тако што се простор у коме се налазе сервери, мрежна или комуникациона опрема ИКТ система организује као административна зона. Простор где се налазе сервери, мрежна или комуникациона опрема ИКТ система мора садржати противпожарну опрему, прозори и врата морају бити увек затворени. Сервери и активна мрежна опрема, су стално прикључени на уређаје за непрекидно напајање-УПС[73]. У периоду обухвата ревизије (2018-2019.година) ЈКПОН није имала усвојен Правилник о безбедности ИКТ система и формализоване поступке заштите, откривања и спречавања недозвољеног приступа ИТ инфраструктури.

Све активности у анализи ЛОГ датотека се догађају по захтеву надлежних органа или у циљу спровођења контроле настале грешке у систему и не врше се редовно.

Препорука: Препоручујемо ЈКПОН – Ниш да успостави централизовано управљање лозинкама корисника рачунара и редовно прегледавање ЛОГ датотека (журнала) мрежних уређаја за спречавање упада и свих постојећих система и сачињава о томе записник.

[72] Одговор на Захтев за доставу документације и податке ЈКП Инфостан технологије Београд.
[73] Правилник о безбедности.

ЗАКЉУЧАК 3: Поред постојећих општих и апликативних контрола улаза, обрачуна и излаза података, неопходно је обезбедити аутоматизовано усаглашавање, као и додатне заштитне механизме.

Наш циљ у овом делу извештаја, био је да одговоримо на треће ревизијско питање, односно да у којој мери се примењују опште и апликативне контроле улаза, обрачуна и излаза података у информационим системима јавних предузећа за обједињену наплату.

На основу постављеног питања, формулисали смо и следећа потпитања:

1. У којој мери информациони систем у јавним предузећима за обједињену наплату поседује адекватне контроле улаза података у информациони систем?
2. У којој мери апликативне контроле омогућавају интегритет и потпуност свих трансакција које се обављају у информационом систему?
3. У којој мери се примењују контроле које осигуравају потпуност и тачност излазних података из информационих система јавних предузећа за обједињену наплату?
4. У којој мери је структура базе података усклађена са прописаним обавезама псеудонимизације личних података корисника?

Информациони системи су критични за многе пословне организације јер подржавају кључне процесе пословања. Са собом носе и значајне пословне ризике, погрешне одлуке због погрешне евиденције услед ненамерних или намерних грешака, губитак података, неовлашћено објављивање података, укључујући и повећане претње по сајбер безбедност услед све већег пословања преко интернета и на крају нерентабилног одржавања.

Прегледи апликативних контрола омогућавају руководству независну процену ефикасности и ефективности дизајна и деловања интерних контрола и процедура у информационом систему, а које се односе на аутоматизовање пословних процеса, идентификацију проблема који се односе на апликацију, а који заврђују додатну пажњу. [74]

С обзиром да су апликативне контроле уско повезане са појединачним трансакцијама у овом случају обрачуна и наплате комуналних услуга, једноставно је увидети због чега ће тестирање контрола пружити ревизору уверавање о тачности одређених функционалности боље него тестирање општих контрола.

Подаци и информације које се евидентирају и обрађују у ИСЈПОН се чувају у системима за управљање базама података (сервери базе података). Омогућавајући вишекориснички рад са значајним бројем корисника и обраду значајног броја трансакција уједно постављају питање интегритета тих података у суштини питање поверења у такве евиденције. Сама рачунарска апликација омогућава значајан број начина обрачуна комуналних услуга, а многе комуналне услуге се по одлуци корисника стављају/скидају на рачун обједињене наплате.

У градовима где је организовано јавно комунално предузеће за послове обрачуна и наплате комуналних услуга за рачун предузећа које пружају те услуге доносе се одлуке о начину и обухвату грађана који су корисници тих услуга.

У наставку је дат преглед укупног броја корисника услуга (домаћинстава која су у систему обједињене наплате) и броја даваоца комуналних услуга (ЈКП и друга предузећа чије услуге се наплаћује преко обједињене наплате) са стањем на дан 31.12.2019. године и 20.5.2020. године.

[74] Приручник за ИТ ревизију врховних ревизорских институција WGITA – IDI/INTOSAI, 2013.

Табела 6. Преглед броја корисника

Опис	ЈКП Информатика Нови Сад	ЈКП Инфостан технологије	ЈКП Обједињена наплата Ниш
Број корисника на 31.12.2019.	176.968	1.414.524	99.215
Број корисника на 20.5.2020.	177.488	1.414.524[75]	99.862
Број давалаца услуга на 31.12.2019.	4.260	594	127
Број давалаца услуга на 20.5.2020.	4.353	738	128

Сваки корисник комуналних услуга има обавезу плаћања тих услуга у складу са важећим прописима.

Налаз 3.1: ЈКП „Инфостан технологије“ Београд и ЈКПОН-Ниш нису обезбедили усаглашавање података на аутоматизован начин.

Циљ контрола улазних података је провера да ли унос врше овлашћене особе, да ли врше унос из валидних извора података, да ли су подаци тачни и комплетни, а да када то нису апликација не изврши обраду таквих података, што се потврђује од стране интерне контроле валидацијом података.

Валидација је поступак утврђивања или проверавања ваљаности тј. утврђивања веродостојности[76], тачности[77] и комплетности[78] неког податка и/или документа из којег се подаци преузимају или преписују. Валидација може имати и за циљ испитивање законитости документа или податка. Циљ валидације је доказивање да неки податак нема само привидну ваљаност, нпр. податак постоји (унет је у евиденцију), него његова вредност припада очекиваном скупу вредности. Утврђивање да ли податак припада очекиваном скупу (законит, истинит и да ли се налази у дефинисаним границама, могућих вредности) изводи се на неколико различитих узорака, чиме се ствара могућност упоређивања резултата и извођења поузданих закључака о валидности унетог податка.[79]

Сви подаци који се уносе у информациони систем морају бити засновани на проверљивим изворним документима. Документи које корисник прилаже и даје на увид приликом уноса података су личне карте, уговор о купопродаји итд. Када је реч о корисницима који станују у заједничким објектима, податке који утичу на обрачун путем образаца достављају управници стамбених јединица. Податке очитаних вредности са мерних инструмената или износе од предузећа које пружају комуналне услуге достављају се путем електронске поште или успостављеним електронским сервисима за размену података.

Улазни подаци треба да се контролишу на могућност појаве грешке или омашке.

[75] У истој табели су евидентирани сви корисници на чије је име израђиван рачун, утврђивање старости је могуће тек из накнадне анализе.
[76] **Веродостојност** подразумева да су трансакције истините и да се заснивају на оригиналним документима.
[77] **Тачност** подразумева да су трансакције исправне и у складу са изворним подацима који се евидентирају.
[78] **Комплетност, потпуност** – подразумева да ниједна исправна трансакција није изостављена из евиденција.
[79] ISSAI 5300 – Смернице за ИТ ревизију, INTOSAI 2016.

ЈКП Информатика – Нови Сад

Унос података се врши на основу документације коју доставља корисник комуналних услуга и присуством на шалтеру предузећа даје сагласност да му се услуге обрачунавају и наплаћују.

Комунална предузећа пружаоци услуге очитане вредности са мерних инструмената директно уносе у базу података ЈКП „Информатика“ Нови Сад. Због директног уноса у базу података није потребно вршити усаглашавање евиденција.

Исправке података и рачуна путем рекламација се обавља на шалтерима ЈКП „Информатика“ Нови Сад. Запослени у финансијама и рачуноводству ЈКП „Информатика“ Нови Сад обављају и све пратеће рачуноводствене активности, обрачуна камата, опомене, утужења итд.

Пословима обрачуна и наплате се баве од 1971. године, а ову платформу сопствене апликације развијају од 1994. године на овој технолошкој платформи поседује развојни систем на којем се врши тестирање нових функционалности и након примопредаје врши се трансфер на продукциони систем.

ЈКП Инфостан технологије – Београд

Унос података за нове кориснике се врши на основу документације коју доставља корисник комуналних услуга и присуством на шалтеру предузећа даје сагласност да му се услуге обрачунавају и наплаћују.

Комунална предузећа пружаоци услуге очитане вредности са мерних инструмената прво евидентирају у својим информационим системима, а потом употребом СФТП сервиса датотеке у XLSX и CSV формату који је дефинисан протоколима за свако појединачно предузеће пружаоца услуге.

Табела 7. Преглед размене података са ЈКП пружаоцима услуга

Пружалац услуге	Начин повезивања потрошње
ЈП ЕПС	Пренос идентификатора и личних података
ЈП Сурчин	Није дефинисан протокол
ДДОР Нови Сад	Пренос идентификатора и личних података
Дунав осигурање	Пренос идентификатора и личних података
ЈКП Градска чистоћа	Пренос идентификатора и личних података
ЈКП Београдске електране	Пренос идентификатора и личних података
ЈКП Водовод и канализација	Пренос идентификатора

Након пријема и електронске потврде да су достављени сви подаци ЈКП приступа се увозу података без логичке контроле примљених вредности. У случају постојања грешке или омашке она ће бити видљива тек након уручења рачуна кориснику који може упутити рекламацију.

У размени података са пружаоцима услуге преноси се ИДЕНТ корисника као и његови лични подаци што није неопходно, у посебним датотекама се размењују подаци о текућим задужењима корисника, корисницима којима престаје услуга, новим корисницима, прешифрираним корисницима, рекламације као и спорним корисницима (утужење итд.).

Размена ових података се не одвија уживо (енг. on-line) и одвија се у једном смеру од пружаоца услуге до ЈКП Инфостан технологије, а обзиром да се грешке и омашке догађају на обе стране неопходна је двосмерна комуникација (уживо).

Препорука: Препоручујемо ЈКП Инфостан технологије – Београд да обезбеди електронски начин двосмерног усаглашавања евиденција са предузећима пружаоцима услуга.

Број рекламација на податке који се тичу корисника, корисника и даваоца услуге и елемената за обрачун услуга није значајан у односу на укупан број трансакција. Такође, корисници услуга (грађани) врше контролу података при самом пријему рачуна и елемената за обрачун услуга.

Исправке података и рачуна путем рекламација се обавља на шалтерима предузећа. Запослени у финансијама и рачуноводству обавља и све пратеће рачуноводствене активности, обрачуна камата, опомене, утужења итд.

Табела 8. Преглед рекламација на податке који се налазе у систему

Година	промена датума доспећа	уговор 1470	ажурирање назива корисника	ажурирање назива за гашење	корекција имена за опомену	име власника СТР-а	евиденција умрлих	адреса пребивалишта	ажурирање јмбг-а	споразум - 2010	Укупно
2010							36		124	791	951
2011						219	66	740	58	197	1280
2012		67				1025	404	1914	49		3459
2013	34		687	44	30	464	954	6390	154426		163029
2014	929	39	7321	1043		1	237	46	584		10200
2015	385		982	64	152	3	147	1962	65		3760
2016	350		1069	26			6442	3	63		7953
2017	275		1478	42			342	1	45		2183
2018	1020		2530	71			421	3	64		4109
2019	248		8465	137		1	439	3	223		9516
2020	108		1210	22			65		77		1482
Укупно	**3349**	**106**	**23742**	**1449**	**182**	**1713**	**9553**	**11062**	**155778**	**988**	**207922**

Највећи број рекламација је евидентиран 2013. године када је извршено ажурирање јединственог матичног броја грађана корисника комуналнних услуга.

Пословима обрачуна и наплате се баве од 1977. године, а ову платформу сопствене апликације развијају од 1993. године на овој технолошкој платформи поседује развојни систем на којем се врши тестирање нових функционалности и након примопредаје врши се трансфер на продукциони систем.

ЈКПОН – Ниш

Унос података се врши на основу документације коју доставља корисник комуналних услуга и присуством на шалтеру предузећа даје сагласност да му се услуге обрачунавају и наплаћују.

Исправке података и рачуна путем рекламација се обавља на шалтерима предузећа. Запослени у финансијама и рачуноводству обавља и све пратеће рачуноводствене активности, обрачуна камата, опомене, утужења итд.

Пословима обрачуна и наплате се баве од 1983. године, а ову платформу сопствене апликације развијају од 2003. године на овој технолошкој платформи поседује развојни систем на којем се врши тестирање нових функционалности и након примопредаје врши се трансфер на продукциони систем.

Комунална предузећа пружаоци услуге очитане вредности са мерних инструмената прво евидентирају у својим информационим системима, а потом употребом сервиса електронске поште достављају датотеке у XLSX и CSV формату за које није дефинисан протокол.

Размена ових података се не одвија уживо (енг. on-line) и одвија се у једном смеру од пружаоца услуге до ЈКПОН Ниш, а обзиром да се грешке и омашке догађају неопходна је двосмерна комуникација (уживо).

Препорука: Препоручујемо ЈКПОН – Ниш да обезбеди електронски начин двосмерног усаглашавања евиденција са предузећима пружаоцима услуга.

Налаз 3.2: Субјекти ревизије нису применили заштитни механизам који обезбеђује обраду података унетих само употребом апликације.

Интегритет подразумева очуваност изворног садржаја и комплетност података[80]. Ово питање је детаљније разрадила Народна банка Србије у својој Одлуци о минималним стандардима управљања информационим системом финансијске институције[81] која под интегритетом означава да су подаци, информације и процеси заштићени од неовлашћеног или непредвиђеног мењања, односно да евентуалне такве промене не остају неопажене.

Код система за управљање базама података (IBM DB2, UNISYS DBSII, Microsoft SQL, Oracle RDBMS, и др.) очекује се да неовлашћени корисник не може вршити измене, као што ни овлашћени корисник не може вршити неовлашћене измене. Имајући у виду да је проблем интегритета вишеслојан, а обухвата: оперативни систем, сервер за управљање базама података, табеле и колоне у базама посебно смо дали значај кориснички дефинисаном интегритету.

Интегритет оперативног система у овој ревизији је испитиван у оквиру питања о адекватности управљања информационом безбедности ИСЈПОН.

Произвођачи су у својим спецификацијама дефинисали и обезбедили команде за проверу и верификацију интегритета целокупног система и обезбедили су софтверске алате за поправке оштећених датотека.

Интегритет података се у систему база података обично спроводи низом ограничења интегритета или правила. Три врсте ограничења интегритета су својствени део модела релационих података: интегритет ентитета, интегритет домена и референцијални интегритет. И посебно важан је кориснички дефинисани интегритет који се спроводи кроз апликативне контроле у самој апликацији.

- **Интегритет ентитета** односи се на концепт примарног кључа и огледа се у томе да свака табела мора имати примарни кључ и да колона примарног кључа треба бити јединствена, и не сме бити NULL дефиниције. На овај начин се могу спречавати дупликати на нивоу релационе базе података али не у потпуности без додатних механизама.
- **Интегритет домена** одређује да све колоне у релационој бази података морају бити декларисане по типу. Тако се спречавају погрешни уноси у којем није могуће унети текстуални опис у колони где су новчани износи или датум документа. Честа грешка се појављује у декларисању колона за датуме типа стринг/текст/char, која се радила због

[80] Закон о информационој безбедности ("Сл. гласник РС", бр. 6/2016, 94/2017 і 77/2019)

[81] Одлука о минималним стандардима управљања информационим системом финансијске институције ("Сл. гласник РС", бр. 23/2013, 113/2013, 2/2017 и 88/2019)

правописних посебности. Тада се у евиденцијама услед слабих апликативних контрола појављују непостојећи датуми нпр. 30. фебруар, 31. септембар итд.

- **Референцијални интегритет** односи се на концепт страног кључа. Када су две или више табела повезане, морамо осигурати да вредност страног кључа у сваком тренутку одговара вредности примарног кључа. У противном када не постоји референцијално ограничење долази до појаве неповезаних редова тзв. сирочади. Референтни интегритет ће спречити кориснике да: додају комуналне услуге на рачун непостојећим корисницима и исто тако неће дозволити брисање корисника са списка ако постоје евидентиране његове обавезе у повезаној табели.

Ако база података не подржава ове врсте интегритета или се оне не користе приликом моделовања базе података за евидентирање, обрачун и наплату комуналних услуга, одговорност је рачунарске апликације да осигурају интегритет података док база података подржава једино модел доследности за складиштење и преузимање података.

Постојање јединственог, добро контролисаног и добро дефинисаног система интегритета података се утиче на:

- стабилност (један централизовани систем врши све операције интегритета података);
- перформансе (све операције интегритета података изводе се у истом нивоу као и модел доследности);
- поновна употреба (све апликације имају користи од једног централизованог система интегритета података);
- одрживост (један централизовани систем за управљање интегритетом свих података).

Све савремене базе података (IBM DB2, UNISYS DBSII, Microsoft SQL, Oracle RDBMS, и др.) подржавају ове карактеристике и системи за управљање базе података омогућавају интегритет података.

Кориснички дефинисани интегритет односи се на скуп правила која је одредио дизајнер апликације, а која не спадају ју претходно наведеним врстама интегритета. Када се врши обрада рачуна по појединачним аналитичким ставкама укупни збирови по новчаним износима се евидентирају у повезаној табели заглавља рачуна. Кориснички дефинисан интегритет подразумева да било која исправка или измена износа појединачне ставке се аутоматски обрачунава и у повезаној табели заглавља рачуна. Ова врста интегритета се може постићи и програмирањем тригера над табелом или покретањем складиштене процедуре за обрачун. Интегритет података мора бити обухваћен целом обрадом трансакције узимајући у обзир и евидентирање заставица за контролу/верификацију евидентираних података.

ЈКП Информатика – Нови Сад

Обрачун се обавља након добијања потврде да су комунална предузећа ажурирала све податке за претходни месец и након пријема и увоза података о субвенцијама из градске управе, врши се пробни обрачун. У контролом износа увидом у извештај референти могу да провере ако неки рачун "пробије" максимални износ.

Обрачун воде се врши на основу стања мерних места и везе простора и мерних уређаја. Један простор може бити на више водомера, те се за сваки водомер обрачунава просечан утрошак по "прикаченим" члановима, па када збир просечних утрошака по водомерима пређе лимит (5 м3) узима се скупља цена.

Неке од услуга имају и субвенције (нпр услуге ЈКП вода, грејање и смеће), па врста субвенције корисника одређује и јединичну цену услуге (углавном је то 50% редовне цене, осим за субвенције по броју деце где је то 30, 40 и 50% редовне цене). Одговарајућа Градска управа нам доставља спискове ових корисника.

Након пробног обрачуна употребом извештаја „очитано - обрачунато на мерним уређајима“, „нови налози за наплату“ у процесу контроле установљавају се "неочекивани" резултати. А конкретни разлози преко функције "Увид у обрачуне" када се евентуалне грешке исправљају (измена начина обрачуна, цене, особине за обрачун), тако да се обрачун пушта поново само за ту услугу или налог за наплату.

Тек када се отклоне сви неочекивани резултати, извлаче се рекапитулације. Исправност рекапитулација потврђују главни референти обраде и руководилац службе. Закључењем обрачуна, који се копира из привремене у трајне обрачунске табеле.

Након тога се ради формирање рачуна, групе по доставним поштама и реонима, формира инфо блок, награђивање редовних платиша итд.

Исправке података и рачуна путем рекламација се обавља на шалтерима предузећа. Запослени у финансијама и рачуноводству обавља и све пратеће рачуноводствене активности, обрачуна камата, опомене, утужења итд.

Систем за управљање базама података је Oracle RDBMS верзија 11 за коју је произвођач обуставио подршку и последње отклањање неусклађености је било августа 2013. године[82]. Систем је инсталиран на „Linux“ оперативном систему и рачунарски сервер је виртуелизован чиме се битно смањује рањивост од делимичног отказа и недоступности.

Модел базе података је обухватио механизме који обезбеђују све наведене врсте интегритета, док се директно из сваког записа може очитати ко и када је креирао запис и индиректно из журнала базе података измене појединих ентитета записа. Колоне са датумима су правилно декларисане као и постојање релација између повезаних табела.

Недостаје механизам хеш заштите[83] који обезбеђује комплетност преузетих података од комуналних предузећа пружалаца услуге као и комплетност измене података која спречава да апликација не обрађује податке исправљене од стране администратора базе, мада се подаци о овим изменама могу очитати индиректно у журналу базе података.

Препорука: Препоручујемо ЈКП Информатика – Нови Сад да обезбеди механизам хеш заштите којим би се спречила могућност да апликација обрађује податке који нису комплетни, или обрађени употребом апликације.

ЈКП Инфостан технологије – Београд

Главни систем за управљање базама података је UNISYS DBSII за коју је произвођач обуставио подршку али се врши аутоматизована репликација базе на Microsoft SQL верзија 2012 и последње отклањање неусклађености је било августа 2019. године.

Главни систем је инсталиран на UNISYS ClearPath MCP оперативном систему за који постоје свега три познате рањивости које су отклоњене 26.02.2018. године, док је репликациона база на Windows оперативном систему.

Реплицирани модел базе података не садржи релације (ограничења на табелама) које би омогућиле референцијални интегритет, и ова врста интегритета се обезбеђује на нивоу апликације. Ко и када је евидентирао запис није могуће у свакој табели очитати из записа али је могуће индиректно из журнала базе података измене појединих ентитета записа. Колоне са датумима су декларисане као текстуалне и систем за управљање базама података не може обезбедити интегритет ентитета.

Недостаје механизам хеш заштите који обезбеђује комплетност преузетих података од комуналних предузећа пружалаца услуге као и комплетност измене података која спречава да

[82]https://docs.oracle.com/en/database/oracle/oracle-database/12.2/cncpt/introduction-to-oracle-database.html#GUID-A42A6EF0-20F8-4F4B-AFF7-09C100AE581E

[83]Смернице за ревизију информационог система јавног дуга (GUID 5259 Public Debt Information Systems)

апликација не обрађује податке исправљене од стране администратора базе, мада се подаци о овим изменама могу очитати индиректно у журналу базе података.

Могуће грешке у рачунима могу настати као последица погрешно очитаних и/или унетих података у систем чије се исправке обављају успостављеним процедурама рекламације.

Препорука: Препоручујемо ЈКП Инфостан технологије – Београд обезбеди механизам хеш заштите којим би се спречила могућност да апликација обрађује податке који нису комплетни, или обрађени употребом апликације.

ЈКПОН – Ниш

Систем за управљање базама података је Oracle RDBMS верзија 9 за коју је произвођач обуставио подршку и последње отклањање неусклађености је било априла 2007. године. Систем је инсталиран на „Linux“ оперативном систему и рачунарски сервер је виртуелизован чиме се битно смањује рањивост од делимичног отказа и недоступности.

Модел базе података не садржи релације (ограничења на табелама) које би омогућиле референцијални интегритет, и ова врста интегритета се обезбеђује на нивоу апликације. Ко и када је евидентирао запис није могуће у свакој табели очитати из записа али је могуће индиректно из журнала базе података измене појединих ентитета записа. Колоне са датумима су декларисане као текстуално и систем за управљање базама података не може обезбедити интегритет ентитета.

Недостаје механизам хеш заштите који обезбеђује комплетност преузетих података од комуналних предузећа пружалаца услуге као и комплетност измене података која спречава да апликација не обрађује податке исправљене од стране администратора базе, мада се подаци о овим изменама могу очитати индиректно у журналу базе података.

Могуће грешке у рачунима могу настати као последица погрешно (очитаних и) унетих података у систем чије се исправке обављају успостављеним процедурама рекламације.

Препорука: Препоручујемо ЈКПОН – Ниш да обезбеди механизам хеш заштите којим би се спречила могућност да апликација обрађује податке који нису комплетни, или обрађени употребом апликације.

Налаз 3.3: ЈКП „Инфостан технологије“ Београд није обезбедио избор датума последње измене као критеријум за извештавање.

Излазне контроле имају за циљ да пруже уверавање да ће подаци који се достављају корисницима бити тачни, презентовани, форматирани и испоручени на доследан и сигуран начин.

Излазне контроле укључују:

- **Евидентирање и чување дефинисаних образаца, докумената и рачуна на сигурном месту** – Обрасци, докумената и рачуни треба да буду правилно евидентирани и похрањени како би се обезбедиле одговарајуће мере заштите од уништења, неовлашћене измене садржаја или неовлашћеног обелодањивања. Архиву треба рутински ускладити да увек буде доступна и евентуална одступања од ових правила треба правилно утврдити и отклонити.

- **Рачунарски генерисана документа и/или рачуни** – Сва документа овог типа треба архивирати и третирати као и физичка (папирна) документа. На генерисаним документима поставити обавештење о лицу одговорном за садржај, а на рачунима поставити обавештење о условима пуноважности у виду идентификационе ознаке одговорног лица овлашћеног за издавање рачуноводствене исправе.

- **Дистрибуција рачуна и других излазних докумената** - Излазни документи и рачуни треба да се дистрибуирају према одобреним параметрима дистрибуције, који могу бити аутоматизовани или ручни. Оперативно особље треба да верификује да ли су излазни извештаји комплетни и испоручени према распореду. Сви излазни документи и рачуни треба да се евидентирају пре дистрибуције. Неконтролисани приступ дистрибуирању излазних докумената и рачуна може угрозити поверљивост и зато је неопходна адекватна физичка контрола дистрибуције. Излазна документа и рачуни који садрже осетљиве податке требало би да се штампају у сигурним, контролисаним условима. Такође би требало обезбедити адекватно одлагање таквих докумената како би се осигурало да не може доћи до неовлашћеног приступа. Излазна документа и рачуни који се дистрибуирају електронским путем преко званичне интернет презентације или рачунарског система, треба обухватити провером логичког приступа и начина доделе налога. Код излазних докумената са осетљивим подацима (тужба итд.) укључује се евиденција да и примаоц је потписао пријем као доказ о пријему документа.

- **Билансирање и усаглашавање излаза** апликационог програма за обраду података треба рутински контролнисати. Требало би обезбедити трагове ревизије како би се олакшало праћење обраде трансакција и усаглашавање података.

- **Руковање излазним грешкама** - Морају се успоставити процедуре за пријављивање и контролу грешака која се јављаају у рачунима и другим документима. Извештај о грешци треба да буде благовремен и достављен оном одељењу на преглед које је одговорно за садржај и могућу грешку.

- **Чување записа о грешкама у рачунима и другим излазним документима** – Хронолошка евиденција свих насталих грешака и рад на утврђивању разлога, као и отклањање истих. На основу прописа морају се донети интерна правила и процедуре за ову врсту рекламација.

- **Верификација пријема рачуна и других излазних докумената** - Да би се обезбедило да се осетљиви извештаји правилно дистрибуирају, прималац треба да евидентира дневник као доказ о пријему резултата.

ЈКП Информатика – Нови Сад

Након тога се ради формирање рачуна, групе по доставним поштама и реонима, формира инфо блок, награђивање редовних платиша итд.

Штампа се случајни узорак неколико рачуна којег парафира/одобрава руководилац службе обраде. Главни референт обраде закључује генерацију рачуна – књигу излазних рачуна, и од тог момента су рачуни доступни принтинг центру за штампу. Паковање по рејонима (експозитурама поште) достављање у пошту која је одговорна за уручивање и повраћај у случају не уручивања. У наредних пар сати су доступни корисницима портала на званичној презентацији.

Исправке података и рачуна путем рекламација се обавља на шалтерима предузећа. Запослени у финансијама и рачуноводству обавља и све пратеће рачуноводствене активности, обрачуна камата, опомене, утужења итд.

ЈКП Инфостан технологије – Београд

Приликом израда интерних извештаја, увида у стање, рекапитулација о обрачунатим износима, међусобним дуговањима, рачунарска апликација нема могућност одређивања обраде последњег датума прихватања измене. На овај начин се приликом израде извештаја обухватају сва стања која су евидентирана до тог тренутка у систему. Протоком времена, исправљају се грешке из претходног извештајног периода, измене и допуне, рекламације, итд. које утичу на стање у

претходном извештајном периоду и када поново израђујемо извештај за претходни период он више не даје иста финансијска стања као ни друге елементе битне за пословно одлучивање.

Непосредно пред штампање рачуна којег одобрава руководилац службе обраде штампају се контролни примерци.

Исправке података и рачуна путем рекламација се обавља на шалтерима предузећа. Запослени у финансијама и рачуноводству обавља и све пратеће рачуноводствене активности, обрачуна камата, опомене, утужења итд.

Препорука: Препоручујемо ЈКП Инфостан технологије – Београд да приликом израде извештаја омогуће избор датума последње измене из претходног извештајног периода.

ЈКПОН – Ниш

Непосредно пред штампање рачуна којег одобрава руководилац службе обраде штампају се репрезентативни узорци ради провере исправности. Исправке података и рачуна путем рекламација се обавља на шалтерима предузећа. Запослени у финансијама и рачуноводству обавља и све пратеће рачуноводствене активности, обрачуна камата, опомене, утужења итд.

Налаз 3.4: Структура базе података није у довољној мери усклађена са прописаним обавезама мера заштите (псеудонимизације) личних података корисника у информационом систему.

Као последица процеса придруживања Републике Србије Европској унији, хармонизације права и директне примене права ЕУ, али и потребе, тј. недостатака старог законског решења, Србија је донела нови Закон о заштити података о личности (“Сл. гласнику РС”, број 87/2018), који се примењује од 21. августа 2019. године.
Нови Закон о заштити података о личности је производ пре свега Уредбе 2016/679 Европског парламента и Директиве 2016/680 Европског парламента и Савета, чије су одредбе у великој мери преузете и уграђене у сам Закон.
Комунална предузећа која обрађују личне податке грађана могу имати одређене додатне трошкове који могу да настану због обраде података о личности која није у складу са законом, а посебно због обраде личних података странаца који могу поседовати некретнине или потенцијално због преноса података о личности у другу државу или међународну организацију.
Први задатак јавног предузећа, органа управе као и других правних лица је да именују лице задужено за заштиту података. Следећи корак је да лице задужено за заштиту података у сарадњи са другим запосленима изради процену утицаја обраде на заштиту личних података. Одговорно лице руковаоца података треба да уговорно уреди однос са обрађивачем личних података.
Прописане су бројне обавезе руковалаца. У зависности да ли се обавезе односе на све или само поједине руковаоце, можемо их поделите на опште и посебне обавезе. Опште обавезе се односе на све руковаоце, независно од специфичности руковаоца, као што је то случај са органима власти, каи и независно од обима обраде или броја запослених код руковаоца као послодавца. Поједини руковаоци имају посебне обавезе које су последица било врсте руковаоца, било података који се обрађују или начина њихове обраде[84].

Посебно важна питања из Закона о заштити података о личности која те тичу имплементације у информациони систем у ком се обрађују подаци о личности су:

1. Пристанак лица на обраду података (чл. 15);
2. Обрада посебних врста података о личности (чл. 17);

[84] Званична презентација Повереника за информације од јавног значаја и заштиту података о личности **https://www.poverenik.rs/sr-yu/za%C5%A1tita-podataka/obaveze-rukovalaca-podatacima.html**

3. Информисање и начини остваривања права лица на које се односе подаци ако обраду врше надлежни органи у посебне сврхе (чл. 22);
4. Право на исправку и допуну (чл. 29);
5. Право на брисање података о личности (чл. 30);
6. Право на ограничење обраде (чл. 31);
7. Право на преносивост података (чл. 36);
8. Мере заштите (чл. 42);
9. Евиденција радњи обраде (чл. 47);
10. Безбедност обраде (чл. 50);
11. Процена утицаја на заштиту података о личности (чл. 54);
12. Обавезе у погледу преноса података о личности у друге државе и међународне организације (чл. 63-72).

Приликом процене утицаја обраде на заштиту личних података процењују се ризици и одређују мере које се предузимају за обраду података у информационом систему када наведена техничка питања треба обрадити и у смислу избора начина решавања ових питања.

Псеудонимизација[85] је процес обраде личних података на начин да се они више не могу приписати конкретном појединцу без коришћења додатних података. „Додатни подаци“ се, за потребе лакшег разумевања, могу сматрати неком врстом кључа (псеудоним), без кога се псеудо подаци не могу користити у изворном облику. Закон о заштити података о личности[86] прописује засебно чување посебних података, чиме се обезбеђује да се податак о личности без употребе додатних података не може приписати одређеном лицу. У процесу псеудонимизације, лични и додатни подаци замењују се псеудонимом и када подацима приступи неовлашћено лице, оно није у стању да идентификује лице до чијих је података дошло и на тај начин је спречена могућа злоупотреба.
Резултат завршеног процеса псеудонимизације јесу псеудонимизовани подаци за које се без раније поменутог „кључа“, не може одредити особа на коју се односе и као такви, усаглашени су са ЗЗПЛ правилима.

Слика број 4 Шематски приказ псеудонимизације

[85] Псеудонимизација (енг. Pseudonymization) је обрада личних података на такав начин да се лични подаци више не могу приписати одређеном субјекту података без употребе додатних информација, под условом да се такви додатни подаци чувају одвојено и подлежу техничким и организационим мерама за обезбеђивање да се лични подаци не приписују идентификованој или идентификованој физичкој особи (замена са псеудонимом).
[86] ЗЗПЛ - Закон о заштити података о личности, "Сл. гласник РС", бр. 87/2018.

Када се псеудонимизација спроведе на исправан начин, она може пружити још неке могућности у процесу обраде података, као што је нпр. профилисање корисника. Међутим, организације треба да имају у виду да се псеудонимизовани подаци и даље морају третирати пажљиво и да се са применом псеудонимизације не завршава брига о праву корисника на приватност. Чак и у случају да дође до цурења псеудонимизованих података изван организације, оне су у обавези да о томе обавесте особе, на које се подаци односе. Управо је зато важно напоменути да је псеудонимизација један, али не и једини алат, који је неопходно применити у наредном периоду како би се пословање прилагодило ЗЗЛП, уз што јачу заштиту личних података корисника.

Табела 9. Спремност базе података за псеудонимизацију

ЈКП	Табеле са личним подацима	Укупан број табела
Инфостан технологије	31	234
Информатика	40	469
Обједињена наплата	171	2.504

ЈКП Информатика – Нови Сад

ЈКП „Информатика“ Нови Сад је задужила лице за заштиту података и сада је у поступку процене утицаја обраде на безбедност података. На својој званичној презентацији **www.nsinfo.co.rs** дато је обавештење о обради података о личности у којем се наводи врста података, сврха обраде, начин чувања и одговорности у случају незаконите обраде. Наплата комуналних услуга грађанима-корисницима није могућа без личних података, имена и презимена, адресе становања и јединственог матичног броја грађанина ради идентификовања власника непокретности-обвезника плаћања комуналних услуга. Спровођење општих и посебних обавеза почела је од 21. августа 2019. године и реч је о сложеним организационим, кадровским и техничким мерама заштите (члан 42, ЗЗЛП) које требају обезбедити личне податке грађана у информационом систему предузећа за обједињену наплату. Поред захтева пројектовања „безбедног дизајна“ и „подразумеване безбедности“ предвиђена је примена псеудонимизације личних података која намеће измену модела базе података и уноси нови ризик функционисања апликације. Овај процес без значајних ресурса, људи, програмирања, тестирања апликације није могуће завршити у овако кратком року. Број табела у бази података обједињене наплате (Видети Табелу 9.) је 469, а број табела у којима се појављују лични подаци је 40, указује на потребу доброг детаљног планирања измене и унапређења модела базе података у стратешком периоду од 3 – 5 година.

Препорука: Препоручујемо ЈКП Информатика – Нови Сад да након израде Процене утицаја обраде на заштиту личних података израде план имплементације псеудонимизације личних података корисника.

ЈКП Инфостан технологије – Београд

ЈКП „Инфостан технологије“ Београд још увек није задужила лице за заштиту података иако је започела активност, и после тога треба израдити Процену утицаја обраде на безбедност података. На својој званичној презентацији **www.infostan.rs** дата је изјава у виду Политике приватности која се односи само на садржај интернет сајта, одричући се одговорности за нетачности које су заштићене ауторским правима. Недостаје обавештење о врсти података која се обрађује, сврси обраде, начину чувања и одговорности у случају незаконите обраде свих података са којима располажу. Наплата комуналних услуга грађанима-корисницима није могућа без личних података, имена и презимена, адресе становања и јединственог матичног броја грађанина ради идентификовања власника непокретности-обвезника плаћања комуналних услуга.

Спровођење општих и посебних обавеза почела је од 21. августа 2019. године и реч је о сложеним организационим, кадровским и техничким мерама заштите (члан 42, ЗЗЛП) које требају обезбедити личне податке грађана у информационом систему предузећа за обједињену наплату. Пројектовање „безбедног дизајна“ и „подразумеване безбедности“ предвиђа псеудонимизацију личних података. Процес измене базе података без значајних ресурса, људи, програмирања, тестирања апликације није могућ завршити у овако кратком року. Број табела у бази података обједињене наплате (Видети Табелу 9.) је 234, а број табела у којима се појављују лични подаци је 31, указује на потребу детаљног планирања измене и унапређења модела базе података у стратешком периоду од 3 – 5 година. Модел базе је значајан број пута допуњаван и сазрео је за ново пројектовање.

Препорука: Препоручујемо ЈКП Инфостан технологије – Београд да одреди лице за заштиту личних података и приступи изради Процену утицаја обраде на заштиту личних података, а након тога изради план план имплементације псеудонимизације личних података корисника.

ЈКПОН – Ниш

ЈКПОН – Ниш још увек није задужила лице за заштиту података иако је започела активност, и после тога треба израдити Процену утицаја обраде на безбедност података. На својој званичној презентацији **www.jkponnis.rs** дата је изјава у виду Услова коришћења која се односи само на садржај интернет сајта, одричући се одговорности за нетачности које у заштићене ауторским правима. Недостаје обавештење о врсти података која се обрађује, сврси обраде, начину чувања и одговорности у случају незаконите обраде свих података са којима располажу. Наплата комуналних услуга грађанима-корисницима није могућа без личних података, имена и презимена, адресе становања и јединственог матичног броја грађанина ради идентификовања власника непокретности-обвезника плаћања комуналних услуга.

Спровођење општих и посебних обавеза почела је од 21. августа 2019. године и реч је о сложеним организационим, кадровским и техничким мерама заштите (члан 42, ЗЗЛП) које требају обезбедити личне податке грађана у информационом систему предузећа за обједињену наплату. Поред захтева пројектовања „безбедног дизајна“ и „подразумеване безбедности“ предвиђена је примена псеудонимизације личних података која намеће измену модела базе података и уноси нови ризик функционисања апликације. Овај процес без значајних ресурса, људи, програмирања, тестирања апликације није могуће завршити у овако кратком року. Број табела у бази података обједињене наплате (Видети Табелу 9.) је 2.504, а број табела у којима се појављују лични подаци је 171, указује на потребу доброг детаљног планирања измене и унапређења модела базе података у стратешком периоду од 3 – 5 година.

Препорука: Препоручујемо ЈКПОН – Ниш да одреди лице за заштиту личних података и приступи изради Процену утицаја обраде на заштиту личних података, а након тога изради план план имплементације псеудонимизације личних података корисника.

V Захтев за доставу одазивног извештаја

Субјекти ревизије су, на основу члана 40. став 1. Закона о Државној ревизорској институцији, дужни да поднесу 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.

Субјекти ревизије су обавезни да у одазивном извештају искажу 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 је дужан 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 субјекти ревизије су у обавези да доставе 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 субјекти ревизије су у обавези да доставе акциони план у којем ће описати мере и активности које ће бити предузете ради отклањања несврсисходности или смањења ризика од појављивања несврсисходности у будућем пословању као и планирани период предузимања мера и одговорно лице;
3. За налазе, односно несврсисходности трећег приоритета, односно које је могуће отклонити у року од једне до три године субјекти ревизије су у обавези да доставе акциони план у којем ће описати мере и активности које ће бити предузете ради отклањања несврсисходности или смањења ризика од појављивања несврсисходности у будућем пословању као и планирани период предузимања мера и одговорно лице.

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

Државна ревизорска институција ће оценити веродостојност одазивног извештаја, тј. провериће истинитости навода о мерама исправљања, предузетим од стране субјекта ревизије, подносиоца одазивног извештаја. У случају потребе извршиће се и 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.

ПРИЛОЗИ

1. Прилог 1 – Методологија у поступку рада

У ревизији су коришћене технике прикупљање података и докумената у електронском облику (папирна документа ће се дигитализовати), анализа прикупљених података, анализе тренда и учешћа, интервјуи са одговорним лицима и друге технике.

Да би се извршила провера постојања и функционисања општих и апликативних контрола и квалитета ИТ система, а у складу с наведеном методологијом управљања ризицима, руководство субјекта ревизије треба да успостави континуиране контролне активности: контролу управљања заштитом ИТ система, контролу логичког и физичког приступа програмима и апликацијама, контролу управљања конфигурацијама и изменама програма и контролу поделе дужности и одговорности корисника. Правилно дефинисаним (програмираним) контролним поступцима у оквиру апликација, база података и оперативних система могуће је остварити ефективно раздвајање дужности и одговорности запослених у свакодневним пословним активностима. У овом случају, контролне активности представљају комбинацију мануелних и аутоматских (програмских) контролних поступака, с тим да врста контролних поступака зависи од природе, сложености и квалитета ИТ система.

Слика број 5 Ревизорско разумевање ИТ окружења и идентификовање општих контрола ИТ[87]

Примена Приручника за ИТ ревизију IDI/INTOCAI[88] обухвата следеће области:

- ИТ управљање,
- Развој и набавка,
- ИТ операције,
- Апликативне контроле,
  - Контроле улаза података у систем,
  - Контроле обраде података,

[87] Међународне стандарде врховних ревизорских институција, ISSAI 1315, издаје INTOSAI, Међународна организација врховних ревизорских институција. **www.issai.org**

[88] Приручник усвојен на XXI Конгресу INTOSAI одржаном у Пекингу, Кина, октобар 2013. године

- Контроле излаза података из система,
- Безбедносне контроле,
- Контроле за обезбеђење интегритета, аутентичности и непорецивости.

• Екстернализација услуга,
• План континуитета пословања (БЦП) и План опоравка од хаварије (ДРП),
• Информациона безбедност.

Методологија подразумева процену ризика по областима и подобластима и детаљно је обрађена у Приручнику.

Очекивани резултати ревизије

Приликом оцењивања ИТ управљања применићемо скалу од 1 до 5 са следећим ознакама:

1) Оцена 1 - потпуно незадовољавајуће,
2) Оцена 2 - делимично незадовољавајуће,
3) Оцена 3 - делимично задовољавајуће,
4) Оцена 4 - задовољавајуће и
5) Оцена 5 - потпуно задовољавајуће.

Да бисмо одговорили на ревизорска питања, анализирали смо законску и подзаконску регулативу, стручну литературу, као и документацију и информације добијене од субјеката ревизије (ЈКП „Информатика“ Нови Сад, ЈКП „Инфостан технологије“ Београд и ЈКП „Обједињена наплата Ниш“). Анализирали смо податке и информације за период од 2018. до 2019. године. Такође смо за поједине анализе користили и податке из 2020. године.
У вези са управљањем информационим системима у јавним предузећима за обједињену наплату анализиране су области континуитета пословања и плана опоравка у случају хаварије, управљања безбедношћу информационих система јавних предузећа за обједињену наплату и примене општих и апликативних контрола улаза, обрачуна и излаза података у информационим системима јавних предузећа за обједињену наплату. У циљу потврђивања информација из документације и прикупљања података који нису доступни у документима, обавили смо интервјуе, послали анкете и упитнике ЈКП за обједињену наплату - субјектима ревизије.

Анкета за јединице локалне самоуправе

У циљу планирања ревизије и упознавањем са темом, идентификацијом потенцијалних проблема и ради прикупљање релевантних података, ревизорски тим је послао анкету на е-мејл адресе свих јединица локалне самоуправе са следећим питањем:

- Да ли се наплата комуналних производа и услуга у вашој општини/граду врши преко обједињене наплате?

Састанци са представницима ЈКП за обједињену наплату

У циљу планирања ревизије и упознавањем са темом, идентификацијом потенцијалних проблема и ради прикупљање релевантних података, ревизорски тим је обавио разговор са одговорним и надлежним лицима из области информационих технологија у одређеним ЈКП за обједињену наплату и на састанку поставили унапред припремљена питања из следећих области:

- ИТ управљања;
- Развоја и набавке ИТ;

- ИТ операције;
- Уговори са добављачима ИТ услуга;
- Планови континуитета пословања и опоравка од хаварије;
- Информациона безбедност;
- Апликативне контроле.

Због ограниченог времена трајања састанака и опширности питања иста смо послали и на е-мејл адресе и уз питања затражили и одговарајућу документацију која се односи на постављена питања.

Захтев за доставу документације од субјеката ревизије

Субјектима ревизије су путем мејла послата питања и захтев за доставу документације. Захтев за доставу документације и питања су послата на адресе контакт особа у ЈКП „Информатика“ Нови Сад, ЈКП „Инфостан технологије“ Београд, ЈКП „Обједињена наплата“ Ниш. Захтев за доставу документације је следеће садржине:

РБ	Захтевани подаци и документација
1	Уредбе, правилнике, процедуре и упутства која примењујете у свом раду а везани су за управљање информационим системом обједињене наплате
2	Укупан број корисника и број корисника по ЈКП даваоцу услуге којима се издају рачун обједињене наплате на 31.12.2019. и закључно са прошлим месецом
3	Број и називи давалаца комуналних и других услуга чије услуге се наплаћују преко обједињене наплате (на 31.12.2019. и на 18.6.2020.)
4	Скениране уговоре (протоколе) са свим даваоцима комуналних и других услуга чије услуге се наплаћују преко обједињене наплате
5	Стратегија процена ризика на нивоу целог предузећа (ЈКП)
6	Стратегија процене ИТ ризика и ризика која утичу на ИТ ресурсе
7	Политика пословног континуитета
8	План за резервне копије -хардвер, податке, софтвер, апликације, бекап логови
9	Политика за случај ванредне ситуације
10	План опоравка од хаварије
11	Информација да су запослени упознати са политикама (горе наведеним)
12	Записници, белешке са састанка радне групе тела које је донело политике (процедуре)
13	Организациона структура ЈКП -целе организације-
14	Организациона структура ИТ сектора, одељења, службе (систематизовано-попуњено) - распоред и број запослених - додати привремене и повремене послове
15	Улоге и одговорности за спровођење Бекап - безбедност резервне локације - извештај о активности и провери резервне копије
16	Стратегија развоја ИТ у ЈКП- Постоји, усвојена, за који период, извештаји
17	Политика везана за ИТ безбедност- Усвојена, достављена запосленима на које се односи, упознати запослени -
18	Формалне и неформална задужења везана за ИТ безбедност (група или појединац, његове надлежности, обавезе, одговорности, извештавање)
19	Политика управљања инцидентима- Регистар ризика, извештаји о управљању инцидентима, инцидентни догађаји у протекле 3 године
20	Документовани или усмени одговори о начину решавања инцидентних догађаја
21	CLA уговори (уговори са добављачима који пружају услуге везане за ИТ – хардвер и софтвер) који су повезани са ИТ системом и да ли су потписани изјава о поверљивости података
22	Листа корисника ИС (информациони систем) обједињене наплате са привилегијама

23	Да ли постоје корисничка упутства за употребу ИС?
24	Који су начини, системи заштите откривања и спречавања недозвољеног приступа ИТ инфраструктури?
25	Пословни захтеви и улоге корисника ИС обједињене наплате? Како је уређена валидација података?
26	Структура ИС и веза са осталим апликацијама, софтверима (рачуноводство, ЈКП даваоци услуга)
27	Документација о имплементацији апликације ИС за обједињену наплату?
28	Мапа пословних процеса и њихова поставка у ИС за обједињену наплату?
29	Како се осигурава интегритет и потпуност свих трансакција које се обављају у информационом систему?
30	Методи преноса и размене података са даваоцима услуга? Дневно, недељно, месечно, начини усаглашавања података, име презиме и функција одговорних запослених
31	Врсте извештаја из ИС обједињене наплате?

Обављени су састанци са субјектима ревизије, примљена су документа од субјеката ревизије путем електронске поште и интранет портала ДРИ, прикупљена су документа из јавно доступних извора.

У поступку ревизије затражени су подаци и информације од извора информација, од по три јавно комунална предузећа која пружају комуналне услуге на територији града Београда, Новог Сада и Ниша, и то:

1. Број корисника (по врсти: физичка и правна лица) комуналних услуга са стањем на 31.12.2018. и 31.12.2019. године којима директно наплаћујете комуналне услуге, а не преко система обједињене наплате.
2. Изводе из прописа (закон, уредба, правилници) на основу којих вршите директну наплату комуналних услуга за физичка и правна лица.

На овај начин, до саме израде извештаја, прикупљене су све четири категорије ревизијских доказа:

Нематеријални докази (интервјуи, упитници и анкете) од субјеката ревизије ЈКП „Информатика“ Нови Сад, ЈКП „Инфостан технологије“ Београд, ЈКП „Обједињена наплата“ Ниш.

Документарни докази као писани документи – документација прикупљена од субјеката ревизије ЈКП „Информатика“ Нови Сад, ЈКП „Инфостан технологије“ Београд, ЈКП „Обједињена наплата“ Ниш, евиденције, статистички подаци, и други извештаји.

Физички докази – прикупљени обиласком субјеката ревизије ЈКП „Информатика“ Нови Сад, ЈКП „Инфостан технологије“ Београд, ЈКП „Обједињена наплата“ Ниш.

Аналитички докази – анализе рађења на бази добијених одговора на анкете и упитнике, анализе информационих система и база података ЈКП за обједињену наплату – субјеката ревизије.

Извршена је квантитативна и квалитативна анализа и након тога се приступило изради извештаја.