ДРЖАВНА
РЕВИЗОРСКА
ИНСТИТУЦИЈА

ИЗВЕШТАЈ
О РЕВИЗИЈИ СВРСИСХОДНОСТИ ПОСЛОВАЊА

УПРАВЉАЊЕ ИНФОРМАЦИОНИМ СИСТЕМОМ ЈП „ПУТЕВИ СРБИЈЕ“

Број: 400-162/2024-07/17
Београд, 10. септембар 2024. године

ПОТРЕБНО ЈЕ УНАПРЕДИТИ ПРОЦЕС УПРАВЉАЊА КОНТИНУИТЕТОМ ПОСЛОВАЊА И УПРАВЉАЊА ИНФОРМАЦИОНОМ ИМОВИНОМ, ОБУХВАТАЈУЋИ СВЕ СИСТЕМЕ И АПЛИКАЦИЈЕ, РАДИ ОБЕЗБЕЂЕЊА ПОТРЕБНОГ НИВОА ПОУЗДАНОСТИ ИНФОРМАЦИОНОГ СИСТЕМА ЈППС

У претходним ревизијама Државна ревизорска институција је утврдила да Јавно предузеће „Путеви Србије“ није у потпуности успоставило адекватан систем ФУК и ускладило његове елементе са међународним стандардима интерне контроле који укључују концепт „COSO“ оквира, због чега постоји ризик да се циљеви и задаци пословања неће остварити на правилан, економичан, ефикасан и ефективан начин. Приходи од наплате путарине чине више од 50% укупних прихода, док најзначајнији део информационог система јавног предузећа „Путеви Србије“ чини систем наплате путарине на путевима Републике Србије.

Како систем финансијског управљања и контроле обухвата Систем наплате путарине, неопходно је било обавити уверавање у њихову ефикасност код постизања пословних циљева остварења прихода.

Слика: Управљање континуитетом пословања

Наплата накнада за коришћење јавних добара предвиђа и ослобађање одређених корисника од плаћања путарине, надлежно министарство није донело критеријуме за ослобађање плаћања, што је довело до тога да предузеће врши ослобађање примењујући сопствене критеријуме, и само у 2022. години по том основу ослободила плаћања путарине у износу од приближно 330 милиона динара.

Ценећи значај ЈППС за одвијање живота, рада и функционисање Републике Србије, као и значаја система наплате за остварење пословних циљева самог предузећа, констатовали смо следеће:

- ЈППС није успоставила ефикасан систем интерне контроле за ослобађање плаћања путарине, размена података између система за наплату путарина и финансијског информационог система се изводи мануелно и преглед записа о догађајима (логова) се не врше периодично, због чега је створен ризик да се циљеви и задаци пословања неће остварити на ефикасан и правилан начин, и може изазвати последице по пословне резултате, смањењем пословних прихода и доношењем погрешних пословних одлука;
- Услед недоношења стратешких докумената као што је: Стратегија управљања ризиком, Процена утицаја на пословање, План континуитета пословања, План опоравка од хаварије и Плана израде резервних копија, без којих није могуће одредити приоритете и пратити трошкове, створен је ризик да у случају штетних догађаја дође до неефикасног реаговања, систем буде дуготрајно недоступан, изгуби више података од планираних и тиме да угрози резултате пословања превасходно умањивањем планираних прихода, и последично непланираним расходима за опоравак система;
- ЈППС штити информациону имовину, али због недостатка стратешких докумената на нивоу предузећа, управљање ИТ имовином и информационом безбедношћу је фрагментирано, чиме је створен ризик од неовлашћеног приступа подацима и информационим ресурсима, што може довести до непланираних расхода, судских поступака и слабљења поузданости информационог система.

Препоруке

Државна ревизорска институција дала је препоруке лицима одговорним за информациони систем ЈППС, да:

- обезбеде претходно евидентирање лица/возила за ослобађање или умањење износа путарине у систем за наплату путарине;
- обезбеде размену података приликом преузимања налога из аналитике, обезбеде суштинску контролу и верификацију података за пријем у главну књигу;
- успоставе механизам који обухвата уређивање процеса периодичне анализе Дневника активности корисника и извештавају о усаглашености са уређеним рачуноводственим процесима;
- успоставе редовни процес Процене утицаја на пословање и о томе периодично извештавају управљачке органе;
- донесу План континуитета пословања, одреде лица и њихове обавезе у погледу периодичног тестирања, усклађивања и извештавања управљачких органа;
- донесу План опоравка од хаварије за ИТ систем и подсистеме, врше периодично тестирање и о томе извештавају управљачке органе;
- у сарадњи са министарством надлежним за одређивање објеката критичне инфраструктуре у сектору саобраћаја сачини Безбедносни план оператора за управљање ризиком и предвиди мере којима се обезбеђује рад у ванредним околностима;
- донесу План израде и тестирања резервних копија, уреде процедуре усклађеног функционисања свих организационих делова у циљу смањења ризика од губитка података;
- успоставе механизам динамичког управљања ризиком дефинисањем индикатора за дневно праћење стања и да редовно извештавају о стању информационе безбедности;
- имплементирају механизам управљања ИТ имовином који ће обезбедити неопходне информације у циљу смањења ризика кроз централизацију надлежности над мерама информационе заштите;
- донесу Процедуру о безбедности и заштити ИКТ система на нивоу предузећа којом би се уредио процес заштите информација, података и докумената у складу и са степеном тајности у информационом систему у циљу јачања укупне безбедности пословања.

Садржај

Скраћенице и термини **5**

I Резиме и препоруке **6**

II Увод **10**

1. **Проблем** **10**
2. **Циљ ревизије** **11**
3. **Ревизијска питања** **11**
4. **Обим и ограничења ревизије** **11**
5. **Методологија у поступку рада** **12**

III Опис предмета ревизије **13**

1. **Законодавни и институционални оквир** **13**

Закон о критичној инфраструктури **13**

Закон о накнадама за коришћење јавних добара **14**

Закон о информационој безбедности **14**

2. **Информациони систем** **15**

Сектор за управљачко информационе системе у саобраћају **15**

Сектор за наплату путарине **17**

IV Закључци **19**

ЗАКЉУЧАК 1: Имплементиране апликативне контроле не обезбеђују ефективност у довољној мери, јер се носиоци права ослобађања плаћања путарине не воде у систему за наплату, а размена података између система за наплату путарина и финансијског система се изводи мануелно и преглед записа о догађајима (логова) се не врше периодично због чега постоји ризик да се пословни циљеви неће остварити на ефикасан и правилан начин, што за последицу може имати смањење пословних прихода и доношење погрешних пословних одлука. **20**

Налаз 1.1: ЈППС евидентира носиоце права ослобађања плаћања путарине на посебне листе, а не у систем за наплату путарине, због чега постоји ризик да се у кратком времену наплате не утврде тачни идентитети имаоца права и да се право додели погрешном кориснику чиме се може довести до умањења пословних прихода. 21

Налаз 1.2: Размена података између система за наплату путарина и финансијског информационог система се изводи мануелно што за последицу може имати отежано функционисање интерних контрола и створити ризик непоузданог извештавања. 24

Налаз 1.3: Недостатак периодичних прегледа записа о догађајима (логова), ствара ризик да грешке у евидентирању не буду благовремено детектоване и исправљене и што може имати негативне последице на резултате пословања. 25

ЗАКЉУЧАК 2: Услед недоношења стратешких докумената, без којих није могуће одредити приоритете, адекватне мере заштите и пратити њихове трошкове, створен је ризик да у случају штетног догађаја дође до неефикасног реаговања, систем буде недоступан у дужем временском периоду, да се небезбедно управља тајним подацима, изгуби више података од планираних и тиме угрозе резултати пословања превасходно умањивањем планираних прихода и непланираним расходима за опоравак система **28**

Налаз 2.1: Није израђена Процена утицаја на пословање због недоношења Стратегије управљања ризиком, услед чега нису ни утврђене безбедносне категорије и приоритети заштите информационе имовине што ствара ризик од непланираних расхода и издатака за мере заштите. 31

Налаз 2.2: Није израђен План континуитета пословања због недостатка Процене утицаја на пословање, постојеће Упутство не дефинише потребан ниво доступности ИКТ система и подсистема, због чега постоји ризик да у случају штетног догађаја не дође до правилног реаговања, што може произвести нефункционисање и непланиране расходе и издатке за мере заштите. 33
Налаз 2.3: Није донет План опоравка од хаварије за ИТ систем или подсистеме због недостатка Плана континуитета пословања, и непотпуно дефинисаних ИТ ризика, што у случају штетних догађаја може довести до неефикасног реаговања и нефункционисања система у дужем временском периоду. 35
Налаз 2.4: ЈППС нема План континуитета пословања у ванредним ситуацијама због неактивности надлежног органа за одређивање објеката критичне инфраструктуре у области саобраћаја стварајући ризик небезбедног управљања тајним подацима и неадекватног реаговања у заштити лица и имовине. 36
Налаз 2.5: Иако врши израду резервних копија ЈППС нема План израде резервних копија и не тестира исправност и могућности рестаурације сервера базе података, што ствара ризик да у случају потребе систем буде недоступан, изгуби више података од планираних и тиме угрози постизање пословних циљева. 37

ЗАКЉУЧАК 3: Због недостатка стратешких докумената на нивоу предузећа, неефикасног управљања ИТ имовином и фрагментираног управљања информационом безбедношћу, због чега се увећава ризик од неовлашћеног приступа подацима и информационим ресурсима, а што може довести до злоупотребе, непланираних расхода и слабљења поузданости ИС. 39

Налаз 3.1: ЈППС није донело Стратегију управљања ризиком којом се обухватају и ИТ ризици, иако на годишњем нивоу израђује прегледе ризика, што у случају инцидената може довести до изостанка правовремене реакције и санације негативних последица у виду смањења прихода и непланираних расхода. 40
Налаз 3.2: Ефикасност управљања ИТ имовином услед недостатка података о безбедносном аспекту и децентрализацији надлежности над мерама информационе заштите је умањена, услед чега се ствара ризик од неблаговремене комуникације, успореног реаговања на малициозне нападе, могућег уништавања података и/или неовлашћеног објављивања података и информација. 42
Налаз 3.3: ЈППС није у потпуности уредило управљање заштитом информација, података и докумената у информационом систему јер није обухватила све постојеће податке, системе и апликације, одредила степен тајности и мере заштите чиме је створило ризик неовлашћеног приступа, недозвољеног објављивања података, а што за последицу може имати непланиране расходе. 44

V Захтев за доставу одазивног извештаја 46

Прилог 1 – Методологија у поступку рада 48

Апликативне контроле 48

Управљање континуитетом пословања 49

Информациона безбедност 51

Прилог 2 – Пример добре праксе ангажовања добављача у области информационе безбедности 54

Скраћенице и термини

У прегледу су дате скраћенице које су коришћене у извештају:

Пун назив	**Скраћеница**
Закон о информационој безбедности	ЗИБ
Јавно предузеће „Путеви Србије“	ЈППС
Информациони систем	ИС
Информационо-комуникациони систем	ИКТ систем
Информационе технологије	ИТ
План континуитета пословања	ПКП
План континуитета операција	ПКО
План комуникација у кризним ситуацијама	ПКК
План заштите критичне инфраструктуре	ПКИ
План одговора на сајбер инциденте	ПСИ
План опоравка од хаварије	ПОХ
План за ванредне ситуације информационог система	ПВС
План заштите лица у ванредној ситуацији	ПЗЛ

I Резиме и препоруке

Државна ревизорска институција је спровела ревизију сврсисходности пословања „Управљање информационим системом ЈП „Путеви Србије“ (ЈППС). Ревизијом је обухваћен информациони систем предузећа као његовог оператора[1], основано је Одлуком[2] и додељени су му послови управљања добрима од општег значаја.

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[3] и Методолошким правилима и смерницама за ИТ ревизију Државне ревизорске институције.[4]

Циљ ревизије је да пружи оцену да ли информациони системи у ЈППС обезбеђују ефективну подршку радним и пословним функцијама, односно омогућују аутоматизацију и интеграцију пословних процеса, обезбеђује поуздан рад у свим условима и штити информациону имовину.

Оцењујући ризике и потенцијално могуће последице, а након спроведене ревизије закључили смо:

Потребно је унапредити процес управљања континуитетом пословања и управљања информационом имовином, обухватајући све системе и апликације, ради обезбеђења потребног нивоа поузданости информационог система ЈППС.

На основу закључака, и налаза које износимо у наставку:

ЗАКЉУЧАК 1: Имплементиране апликативне контроле не обезбеђују ефективност у довољној мери, јер се носиоци права ослобађања плаћања путарине не воде у систему за наплату, а размена података између система за наплату путарина и финансијског система се изводи мануелно и преглед записа о догађајима (логова) се не врше периодично због чега постоји ризик да се пословни циљеви неће остварити на ефикасан и правилан начин, што за последицу може имати смањење пословних прихода и доношење погрешних пословних одлука.

- **Налаз 1.1:** ЈППС евидентира носиоце права ослобађања плаћања путарине на посебне листе, а не у систем за наплату путарине, због чега постоји ризик да се у кратком времену наплате не утврде тачни идентитети имаоца права и да се право додели погрешном кориснику чиме се може довести до умањења пословних прихода;

---

[1] Према Закону о информационој безбедности, “Службени гласник РС”, бр. 6 од 28. јануара 2016, 94 од 19. октобра 2017, 77 од 31. октобра 2019. године, „*оператор ИКТ система је правно лице, орган власти или организациона јединица органа власти који користи ИКТ систем у оквиру обављања своје делатности, односно послова из своје надлежности”, а чланом 6 обухваћена су посла управљања добрима од општег интереса.*

[2] Одлука о оснивању Јавног предузећа за управљање државним путевима „Путеви Србије“ („Службени гласник РС“, број 115/2005) и уписано у Регистар привредних субјеката под бројем БД 108625/2006.

[3] *Државна ревизорска институција*, (2022), Методолошка правила и смернице за ревизију сврсисходности пословања, Београд,.

[4] Државна ревизорска институција, (2019), Методолошка правила и смернице за ИТ ревизију, Београд.

- **Налаз 1.2**:Размена података између система за наплату путарина и финансијског информационог система се изводи мануелно што за последицу може имати отежано функционисање интерних контрола и створити ризик непоузданог извештавања.;
- **Налаз 1.3:** Недостатак периодичних прегледа записа о догађајима (логова), ствара ризик да грешке у евидентирању не буду благовремено детектоване и исправљене и што може имати негативне последице на резултате пословања;

ЗАКЉУЧАК 2: Услед недоношења стратешких докумената, без којих није могуће одредити приоритете, адекватне мере заштите и пратити њихове трошкове, створен је ризик да у случају штетног догађаја дође до неефикасног реаговања, систем буде недоступан у дужем временском периоду, да се небезбедно управља тајним подацима, изгуби више података од планираних и тиме угрозе резултати пословања превасходно умањивањем планираних прихода и непланираним расходима за опоравак система.

- **Налаз 2.1:** Није израђена Процена утицаја на пословање због недоношења Стратегије управљања ризиком, услед чега нису ни утврђене безбедносне категорије и приоритети заштите информационе имовине што ствара ризик од непланираних расхода и издатака за мере заштите;
- **Налаз 2.2:** Није израђен План континуитета пословања због недостатка Процене утицаја на пословање, постојеће Упутство не дефинише потребан ниво доступности ИКТ система и подсистема, због чега постоји ризик да у случају штетног догађаја не дође до правилног реаговања, што може произвести нефункционисање и непланиране расходе и издатке за мере заштите;
- **Налаз 2.3:** Није донет План опоравка од хаварије за ИТ систем или подсистеме због недостатка Плана континуитета пословања, и непотпуно дефинисаних ИТ ризика, што у случају штетних догађаја може довести до неефикасног реаговања и нефункционисања система у дужем временском периоду.
- **Налаз 2.4:** ЈППС нема План континуитета пословања у ванредним ситуацијама због неактивности надлежног органа за одређивање објеката критичне инфраструктуре у области саобраћаја стварајући ризик небезбедног управљања тајним подацима и неадекватног реаговања у заштити лица и имовине.
- **Налаз 2.5:** Иако врши израду резервних копија ЈППС нема План израде резервних копија и не тестира исправност и могућности рестаурације сервера базе података, што ствара ризик да у случају потребе систем буде недоступан, изгуби више података од планираних и тиме угрози постизање пословних циљева.

ЗАКЉУЧАК 3: Због недостатка стратешких докумената на нивоу предузећа, неефикасног управљања ИТ имовином и фрагментираног управљања информационом безбедношћу, због чега се увећава ризик од неовлашћеног приступа подацима и информационим ресурсима, а што може довести до злоупотребе, непланираних расхода и слабљења поузданости ИС.

- **Налаз 3.1:** ЈППС није донело Стратегију управљања ризиком којом се обухватају и ИТ ризици, иако на годишњем нивоу израђује прегледе ризика, што у случају инцидената може довести до изостанка правовремене реакције и санације негативних последица у виду смањења прихода и непланираних расхода;
- **Налаз 3.2:** Ефикасност управљања ИТ имовином услед недостатка података о безбедносном аспекту и децентрализацији надлежности над мерама информационе

заштите је умањена, услед чега се ствара ризик од неблаговремене комуникације, успореног реаговања на малициозне нападе, могућег уништавања података и/или неовлашћеног објављивања података и информација.;

- **Налаз 3.3:** ЈППС није у потпуности уредило управљање заштитом информација, података и докумената у информационом систему јер није обухватила све постојеће податке, системе и апликације, одредила степен тајности и мере заштите чиме је створило ризик неовлашћеног приступа, недозвољеног објављивања података, а што за последицу може имати непланиране расходе.

У циљу побољшања управљања информационим системом ЈППС, Државна ревизорска институција препоручује одговорним лицима, да:

1. обезбеде претходно евидентирање лица/возила за ослобађање или умањење износа путарине у систем за наплату путарине. (Налаз 1.1.) – Приоритет 2[5];
2. обезбеде размену података приликом преузимања налога из аналитике, обезбеде суштинску контролу и верификацију података за пријем у главну књигу. (Налаз 1.2.) – Приоритет 2;
3. успоставе механизам који обухвата уређивање процеса периодичне анализе Дневника активности корисника и извештавају о усаглашености са уређеним рачуноводственим процесима (Налаз 1.3.) – Приоритет 2;
4. успоставе редовни процес Процене утицаја на пословање и о томе периодично извештавају управљачке органе. (Налаз 2.1.) – Приоритет 2;
5. донесу План континуитета пословања, одреде лица и њихове обавезе у погледу периодичног тестирања, усклађивања и извештавања управљачких органа. (Налаз 2.2.) – Приоритет 3[6];
6. донесу План опоравка од хаварије за ИТ систем и подсистеме, врше периодично тестирање и о томе извештавају управљачке органе. (Налаз 2.3.) – Приоритет 3;
7. у сарадњи са министарством надлежним за одређивање објеката критичне инфраструктуре у области саобраћаја, сачини Безбедносни план оператора за управљање ризиком и предвиди мере којима се обезбеђује обављање послова у ванредним околностима. (Налаз 2.4.) – Приоритет 3;
8. донесу План израде и тестирања резервних копија, уреде процедуре усклађеног функционисања свих организационих делова у циљу смањења ризика од губитка података. (Налаз 2.5.) – Приоритет 2;
9. успоставе механизам динамичког управљања ризиком дефинисањем индикатора за дневно праћење стања и да редовно извештавају о стању информационе безбедности. (Налаз 3.1.) – Приоритет 2;
10. имплементирају механизам управљања ИТ имовином који ће обезбедити неопходне информације у циљу смањења ризика кроз централизацију надлежности над мерама информационе заштите. (Налаз 3.2.) – Приоритет 2;

[5] Приоритет 2 - несврсисходности које је могуће отклонити у року до годину дана.
[6] Приоритет 3 - несврсисходности које је могуће отклонити у року до три године.

11. донесу Процедуру о безбедности и заштити ИКТ система на нивоу предузећа којом би се уредио процес заштите информација, података и докумената у складу и са степеном тајности у информационом систему у циљу јачања укупне безбедности пословања.(Налаз 3.3.) –Приоритет 2.

Генерални државни ревизор

Др Душко Пејовић
Државна ревизорска институција
Макензијева 41
11000 Београд, Србија
10. септембра 2024. године

II Увод

Државна ревизорска институција спровела је ревизију сврсисходности пословања „Управљање информационим системом ЈП „Путеви Србије“ у периоду од јануара 2024. године до јуна 2024. године[7]. Ревизија сврсисходности пословања је спроведена у складу са Законом о Државној ревизорској институцији[8], Пословником Државне ревизорске институције[9] и Програмом ревизије Државне ревизорске институције за 2024. годину у делу који се односи на сврсисходност пословања, број 06-1829/2023-02/2 од 11. децембра 2023. године.

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[10] и Методолошким правилима и смерницама за ИТ ревизију Државне ревизорске институције.[11]

1. Проблем

У претходном периоду Државна ревизорска институција је утврдила[12], да Јавно предузеће „Путеви Србије“ није у потпуности успоставило адекватан систем ФУК и ускладило његове елементе са међународним стандардима интерне контроле који укључују концепт „COSO“ оквира, због чега постоји ризик да се циљеви и задаци пословања неће остварити на правилан, економичан, ефикасан и ефективан начин. Приходи од наплате путарине чине више од 50% укупних прихода.

У 2022. години није наплаћена путарина у у износу од 329.872 хиљаде динара по основу ослобађања од плаћања путарине, а за које Предузеће, по захтеву Државне ревизорске институције, није доставило доказе односно, веродостојне и потпуне податке о регистарским ознакама возила, да је ослобађање њихових корисника од плаћања путарине у наведеном износу извршено у складу са чланом 199 ст. 1 и 2 Закона о накнадама за коришћење јавних добара[13] . Како систем финансијског управљања и контроле обухвата опште и апликативне ИТ контроле неопходно је обавити уверавање у њихову ефикасност код постизања пословних циљева остварења прихода.

---

7 Број ревизије 400-266/2023-07.

8 “Службени гласник РС”, бр. 101/05, 54/07, 36/10 и 44/18-др.закон.

9 “Службени гласник РС”, број 9/09.

10 *Државна ревизорска институција*, (2022), Методолошка правила и смернице за ревизију сврсисходности пословања, Београд,.

11 Државна ревизорска институција, (2019), Методолошка правила и смернице за ИТ ревизију, Београд.

12 Послеревизиони извештај о мерама исправљања Јавног предузећа „Путеви Србије”, Београд по ревизији сврсисходности пословања „Ефикасност успостављања интерне финансијске контроле у јавним предузећима и друштвима капитала која обављају делатност од општег интереса”, Број: 400-321/2022-06/47, Београд, од 21. марта 2023. године.

13 Извештај о ревизији финансијских извештаја Јавног предузећа „Путеви Србије” Београд за 2022. годину.

2. Циљ ревизије

Циљ ревизије је да пружи оцену да ли информациони системи у Јавном предузећу „Путеви Србије“ (ЈППС) обезбеђују ефективну подршку радним и пословним функцијама, односно омогућују аутоматизацију и интеграцију пословних процеса, обезбеђује поуздан рад у свим условима и штити информациону имовину.

Поред ИТ опреме, софтверских решења која су развијана у претходних 30 година у циљу јачања информационе безбедности, значаја критичне инфраструктуре за функционисање привреде и грађана, посебну пажњу посветили смо заштити података.

Изабраном темом помажемо јавном предузећу „Путеви Србије“ да у складу са стратешким циљем Државне ревизорске институције одговорно управља јавним средствима ради остварења највећих користи за грађане, како је дефинисано Стратешким планом за период 2024-2028. године[14].

3. Ревизијска питања

Како бисмо остварили циљ ревизије, прибавили смо одговоре на ревизијска питања:

1. У којој мери имплементиране ИТ опште контроле обезбеђују ефективност апликативних контрола ИС ЈППС?
2. У којој мери управљање континуитетом пословања обезбеђује расположивост ИС ЈППС?
3. У којој мери успостављена информациона безбедност обезбеђује поузданост ИС ЈППС?

Питања која смо формулисали се односе на три најризичније области, на основу процене ризика коју смо спровели на бази прикупљених података у фази планирања и истраживања предложене теме ревизије.

4. Обим и ограничења ревизије

Ревизијом „Управљање информационим системом ЈП „Путеви Србије“ смо обухватили три ИТ области и то процесе: област апликативних контрола у самом систему наплате путарине, обезбеђење континуитета пословања и обезбеђења информационе безбедности.

Информациони системи Јавног предузећа „Путеви Србије“ чине:

1. Информациони систем наплате путарине;
2. Пословни информациони систем (финансијска служба, архива и писарница);
3. Информациони систем везан за базе података предузећа (базе података о путевима, базе података о саобраћају, географско-информациони систем ГИС);
4. Информациони систем за надзор праћење и управљање саобраћајем (ИТС систем);
5. Информациони систем за контролу и управљање напајања електричном енергијом;
6. Као и други информациони системи попут мејл, веб, VPN сервера итд.

[14] Стратешки план Државне ревизорске институције за период 2024-2028. године https://dri.rs/storage/dokumenta/Strateski%20plan%202024-2028_SRB.pdf

У обухвату ревизије су били процеси који се одвијају употребом наведених ИТ система, размена података са фокусом на аналитичке евиденције, књижења у главној књизи која су повезана са системом наплате путарине као највећег извора финансијских средстава.

Оцењивање управљања информационим системом заснива се на *Методолошким правилима и смерницама за ревизију сврсисходности пословања*, и *Приручника за коришћење методологије за ИТ ревизију*[15], којим је дефинисан принцип ефективности који се односи на испуњавање постављених циљева и постизање планираних резултата.

Ревизијом смо обухватили период 2021-2023. година, али смо за одговоре на нека ревизијска питања обухватили и дужи временски период.

Поступци ревизије су изведени у периоду од јануара до јуна 2024. године у циљу доношења налаза, закључака и препорука заснованих на доказима који су прикупљени током ревизије.

У поступку ревизије нисмо испитивали:

- Да ли финансијски извештаји субјекта 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 органа јавне управе која су обухваћена ревизијом.

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

5. Методологија у поступку рада

Да бисмо формулисали ревизорска питања и касније одговорили на њих, анализирали смо законске и подзаконске прописе који се односе на теме и области, апликације, подршке корисника и информационе безбедности, као и податке и информације које смо добили од извора информација – произвођача апликације.

У циљу планирања ревизије сврсисходности пословања, а ради прибављања информација у вези планирања, спровођења и надзора активности организационих јединица у чијој надлежности су послови из области информационе безбедности, обавили смо интервју са представницима, прегледали достављену документацију и применили Методолошка правила и смернице за ИТ ревизију Државне ревизорске институције.

На основу прикупљених информација у фази планирања дефинисали смо потенцијални проблем, циљ ревизије, ревизорска питања, критеријуме, предмет ревизије, субјекта ревизије као и период који ће ревизија обухватити.

Током фазе спровођења ревизије, како би одговорили на ревизорска питања односно испунили циљ ревизије, анализирали смо прикупљену документацију од субјекта ревизије као и од извора информација, спроводили интервјуе и друго. (детаљније погледати у Прилогу 1.)

[15] Приручник за коришћење методологије за ИТ ревизију, 2019. година, Државна ревизорска институција.

III Опис предмета ревизије

1. Законодавни и институционални оквир

ЈП „Путеви Србије“ (ЈППС) основано је сходно Закону о јавним путевима[16] и обавља стручне послове који се односе на трајно, непрекидно и квалитетно одржавање и заштиту, експлоатацију, изградњу, реконструкцију, организацију и контролу наплате путарине, развој и управљање државним путевима првог и другог реда у Републици Србији.

Финансирање изградње и реконструкције, одржавања и заштите јавног пута обезбеђује се из накнаде за употребу државног пута – путарине, финансијских кредита, буџета Републике Србије и других извора у складу са законом.

Информационе технологије у Јавном предузећу „Путеви Србије“ обезбеђују подршку радним и пословним функцијама, односно омогућују аутоматизацију и интеграцију пословних процеса[17].

Путеви, као добра у општој употреби, су државна својина, а управљање државним путем је делатност од општег интереса.

Закон о критичној инфраструктури[18]

Овим законом уређује се национална критична инфраструктура, њена идентификација, заштита, надлежност и одговорност органа и организација у области управљања критичном инфраструктуром.

Критична инфраструктура су системи, мреже, објекти или њихови делови, чији прекид функционисања или прекид испоруке роба односно услуга може имати озбиљне последице на националну безбедност, здравље и животе људи, имовину, животну средину, безбедност грађана, економску стабилност, односно угрозити функционисање Републике Србије.

Под критичном инфраструктуром у сектору саобраћаја подразумевају се системи, мреже, објекти или њихови делови чији прекид рада проузрокује: непостојање алтернативног пута; прекид саобраћаја услед оштећења, спречавања, отежаног снабдевања основним животним намирницама или представља опасност по живот више од 50 становника насеља у брдскопланинским подручјима, више од 300 становника насеља у равничарским подручјима, више од 1.000 становника у јединицама локалних самоуправа, односно више од 5.000 становника у граду Београду, у периоду дужем од два дана[19].

Иако надлежно министарство није идентификовало и одредило критичну инфраструктуру у области саобраћаја, ЈППС је дужно да брине о сигурности и континуитету пословања и у ванредним ситуацијама.

---

[16] Закон о јавним путевима, “Службени гласник РС” бр. 101/2005, 123/2007, 101/2011, 93/2012 и 104/2013, престао да важи доношењем Закона о путевима, “Службени гласник РС” бр. 41/2018-32, 95/2018-267 (др. закон), 92/2023-340 (др. закон).

[17] Дугорочни и средњорочни план пословне стратегије и развоја 2017-2027, Јавно предузеће „Путеви Србије”, 14. децембар 2017. године , стр. 64.

[18] Закон о критичној инфраструктури, “Службени гласник РС”, бр. 87 од 13. новембра 2018.

[19] Уредба о критеријумима за идентификацију критичне инфраструктуре и начину извештавања о критичној инфраструктури Републике Србије, “Службени гласник РС”, број 69 од 24. јуна 2022.

Закон о накнадама за коришћење јавних добара[20]

Законом о накнадама за коришћење јавних добара уређене су накнаде за коришћење јавних добара, међу којима и накнада за коришћење јавних путева. Јавни пут јесте пут у смислу Закона о путевима[21], којим је уређен правни положај јавних путева.

Једна од накнада за коришћење јавних путева, која је прописана одредбама члана 186 став 1 тачка 3) Закона о накнадама за коришћење јавних добара, јесте накнада за употребу јавног пута, његовог дела или путног објекта (у даљем тексту: путарина).

Како систем финансијског управљања и контроле обухвата опште и апликативне ИТ контроле неопходно је обавити уверавање у њихову ефикасност код постизања пословних циљева остварења прихода.

Слика број 1. Наплатна рампа Врчин и ЕРЦ ЈППС

Закон о информационој безбедности[22]

У складу са Законом о информационој безбедности ИКТ системи од посебног значаја су и системи који се користе у обављању делатности од општег интереса и у обављању послова у органима власти. Истим законом прописане су мере заштите ИКТ система од посебног значаја. Оператор ИКТ система од посебног значаја одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система.

Чланом 7 овог закона дефинисано је да се мере заштите ИКТ система, између осталог, односе на: успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система; обезбеђивање да лица која користе ИКТ систем, односно управљају ИКТ системом, буду оспособљена за посао који раде и разумеју своју одговорност; заштиту од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система; идентификовање информационих добара и одређивање

[20] Закон о накнадама за коришћење јавних добара, “Службени гласник РС”, бр. 95 од 8. децембра 2018, 49 од 8. јула 2019, 92 од 27. октобра 2023.

[21] „Службени гласник РС“, бр. 41/18 и 95/18 – др. закон

[22] Закон о информационој безбедности, “Службени гласник РС”, бр. 6 од 28. јануара 2016, 94 од 19. октобра 2017, 77 од 31. октобра 2019. године.

одговорности за њихову заштиту; класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком.

2. Информациони систем

Информациони систем у Јавном предузећу „Путеви Србије“ обухвата рачунарску, комуникациону опрему и софтверске апликације који треба да омогуће запосленима да постигну радне и пословне циљеве, у складу са плановима, прописима и интерним актима, односно да омогући аутоматизоване и интегрисане пословне процесе.

У ширем смислу, као и сваки информациони систем, тако и информациони системи у ЈППС обухватају прикупљање, складиштење и обраду финансијских и рачуноводствених података који се користе за доношење одлука и извршење прописаних обавеза. Информациони системи Јавног предузећа „Путеви Србије“ чине:

1. Информациони систем наплате путарине;
2. Пословни информациони систем предузећа Hermes-MEGA (финансијска служба, архива и писарница);
3. Информациони систем везан за базе података предузећа (базе података о путевима, базе података о саобраћају, географско-информациони систем ГИС);
4. Информациони систем за надзор праћење и управљање саобраћајем (ИТС систем);
5. Информациони систем за контролу и управљање напајања електричном енергијом - Телеменаџмент;
6. Као и други информациони системи попут мејл, веб, VPN сервера итд.

Сваки од наведених ИТ система има своју специфичну инфраструктуру (специфичну архитектуру и посебне софтверске апликације). Надлежност над поменутим системима припадају различитим секторима:

1. Сектор за наплату путарине;
2. Сектор за економско финансијско и комерцијалне послове;
3. Сектор за правне кадровске и опште послове;
4. Сектор за управљачко информационе системе у саобраћају и
5. Сектор за стратегију пројектовање и развој.

Сектор за управљачко информационе системе у саобраћају

Послови прикупљања, складиштења и обраде података о саобраћају, о ИТС системима и путној инфраструктури, обављају се у Сектору за управљачко информационе системе у саобраћају и обухватају следеће:

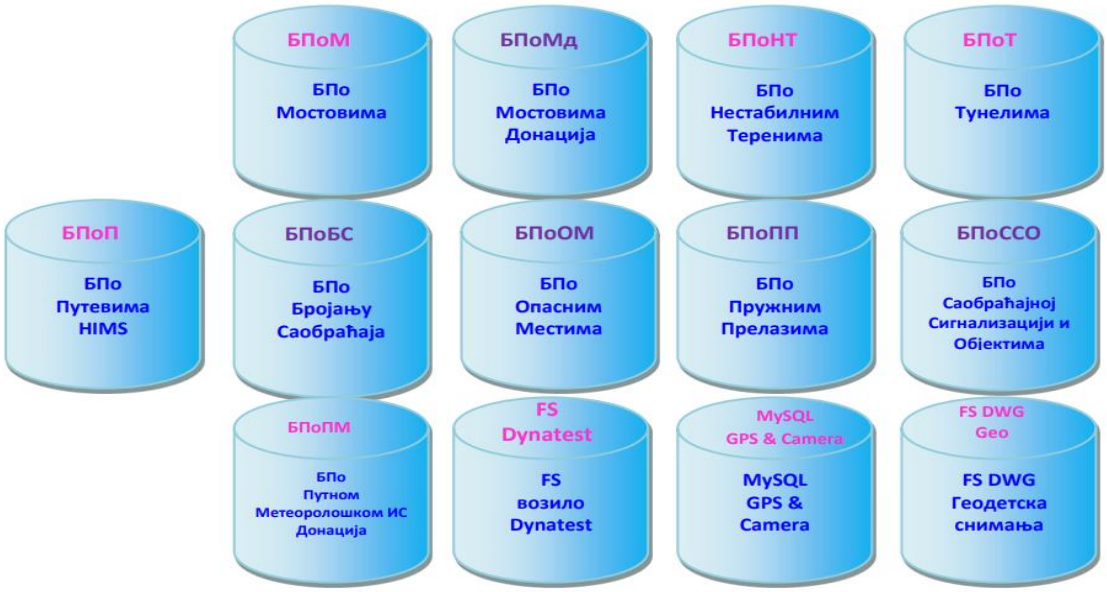
- Област интелигентних транспортних система – ИТС (развој и имплементација ИТС, надзор и управљање саобраћајем, надзор и управљање инсталираним системима у тунелима, управљање путно метеоролошким системима – ПМИС, управљање видео надзором у надлежности сектора, управљање бројачима саобраћаја – АБС и снимање саобраћаја;
- Вођење евиденција и база података, прикупљање, ажурирање, контрола, верификација и анализа података о државним путевима, означавање путева и саобраћајно техничким подацима везаним за путну мрежу, саобраћајним токовима, мостовима, објектима и нестабилним теренима, пружним прелазима, саобраћајној сигнализацији и опреми, саобраћајним незгодама итд.
- Одељење обраде података – АОП, као један од корисника Централне платформе базе података наплате путарине, врши аутоматску обраду података по захтевима и извештавање о саобраћајно-финансијским параметрима са наплате путарине, а за потребе интерних и екстерних корисника.

- Одржавање и заштите информационо комуникационе опреме у смислу хардвера и софтвера (мејл, веб, VPN сервери и сл.);
- Одржавање објеката, опреме, система, инсталација и уређаја за управљање тунелима;
- Информисање јавности о стању на путевима;
- Област безбедности и здравља на раду и заштите од пожара;
- Област интегрисаних менаџмент система и система за подршку пословању
- Област контроле квалитета,
- Као административно техничке и друге послове предузећа.

У саставу Сектора за управљачко информационе системе у саобраћају, који броји 203 запослених, налазе се следећа одељења::

1. Одељење за развој и имплементацију ИТС-а;
2. Одељење за надзор и управљање саобраћајем;
3. Одељење базе података и ГИС;
4. Одељење обраде података – АОП;
5. Одељење за одржавање управљачко информационих система;
6. Информативни центар;
7. Одељење контроле и обезбеђивања квалитета;
8. Одељење за интегрисане менаџмент системе и системе за подршку пословању предузећа;
9. Одељење за безбедност и здравље, заштиту од пожара и спасавање на раду.

У надлежности ЈП „Путеви Србије“ – Сектора за управљачко информационе системе је укупно 17 тунела – 7 тунела на К10, 6 тунела на АП „Милош Велики“ К11 и 4 тунела на Обилазници око Београда и кружном путу Кијево. Надзор и управљање саобраћајем кроз оперативне центре врши Одељење за надзор и управљање саобраћајем, развој и унапређење постојећих и имплементацију нових система, како на путним објектима тако и дуж путне мреже, обавља Одељење за развој и имплементацију ИТС-а, док је за одржавање свих ИТС-а одговорно Одељење за одржавање управљачко информационих система.



Слика број 2. Приказ постојећих база података

Базе података о путевима, путним објектима и саобраћају захтевају континуирано ажурирање, интегрисање и доступност свим корисницима, а њено адекватно коришћење захтева континуирано спровођење обука како за администраторе тако и за кориснике. Базе података су основ за успостављање ефикасног система управљања процесом одржавања путне мреже. Базе података дају индикаторе испуњавања нивоа квалитета услуге за оцену уговора о одржавању заснованих на учинку. База података о путевима, објектима и саобраћају и ГИС алати, дају могућност дефинисања нацрта инвестиционих програма и годишњих планова одржавања.

Прекатегоризацијом путне мреже, дефинисањем правног и техничког оквира, створена је могућност за успостављање системског управљања путном мрежом, у чему кључну улогу имају базе података као систем за подршку пословним процесима и одлучивању.

Развијањем базе података путева у савременом софтверском окружењу за подршку процесу одлучивања, ЈП “Путеви Србије“ су у могућности да квалитетније и ефикасније управљају основним подацима као што су:

- карактеристике путне мреже;
- саобраћајни и транспорти захтеви;
- индикатори ефикасности и ефективности различитих инвестиционих пројеката;
- израда и праћење реализације годишњег буџета;
- припрема пословних планова у области пројектовања, одржавања и изградње.

Пословни информациони систем Hermes – MEGA обухвата послове писарнице и архиве и делом финансијске службе са фокусом на завођење и дистрибуцију документације, аналитичке евиденције, књижења у главној књизи која су највише повезана са системом наплате путарине као највећим извором финансијских средстава остварених кроз реализацију пословних процеса. Наведени ИС се користи у **Сектору за правне, кадровске и опште послове**, као и **Сектору за економско финансијске и комерцијалне послове**. Техничку подршку у смислу инфраструктуре пружа Одељење за одржавање УИС Сектора за управљачко информационе системе у саобраћају.

Сектор за наплату путарине

У сектору за наплату путарине обављају се послови наплате путарине, видео надзора над процесима наплате путарине, аналитике и контроле над процесима наплате путарине, превоза и заштите новца и објеката, као и административно технички и други послови везани за делатност сектора. Број запослених 1159.

У саставу Сектора наплате путарине налазе се следећа одељења:

1. Одељење за надзор наплате путарине;
2. Одељење за оперативну наплату путарине;
3. Одељење за електронску наплату путарине;
4. Одељење за заједничке послова сектора.

Број наплатних станица до новембра 2023. године је 68. Одговорности и овлашћења за Информациони систем наплате путарине, као одржавање овог система, припадају овом сектору.

Информациони систем за контролу и управљање напајања електричном енергијом – Телеменаџмент је у надлежности **Сектора за стратегију, пројектовање и развој**.

У стратешким приоритетима ИКТ дефинисани су принципи развоја информационог система на следећим основним постулатима:

- **Скалабилност** - могућност да у следећих 5 година развоја ИКТ система као и ИКТ ресурса (технологија, кадрови) подрже развој пословања и промене пословања предузећа;
- **Поузданост** - могућност да проблеми у раду ИКТ система не утичу директно на пословање предузећа у смислу прекида рада сервиса и података;

- **Аутоматизација** – у домену усаглашавања стратешких планова, планова активности, координације рада и сарадње организационих јединица, транспарентно и документовано доношење одлука, као и доношењу стратешких и оперативних циљева;
- **Сигурност** - заштита пословања у смислу сервиса и података по CIA критеријумима и у складу са трендовима у сфери cybersecurity-а;
- **Примена стандарда** – развој ИКТ система и ресурса у складу са стандардима ISO20000, ISO27001;
- **Развој ИКТ ресу**рса и система у складу са стратегијом развоја информационог друштва у Републици Србији до 2020. године;
- **Развој ИТ односно ИКТ ресурса у складу са Листом Националних приоритета** у домену науке и технологије и Дигиталном агендом у Републици Србији.

Горе поменути постулати везани за ИКТ се инкорпорирају у сваки корак развоја било ког дела ИКТ система, радних и пословних функција из окружења рада ЈППС како би имали синхронизован развој, а све са намером испуњавања следећих циљева:

- Подршка пословним процесима ЈП „Путеви Србије“;
- Правовременост, истинитост и сигурност прикупљених и обрађених података;
- Поуздан и правовремен сервис за надлежне органе како из јавне тако и приватне сфере пословања;
- Испуњавање потреба и задовољства корисника из домена пословања ЈППС;
- Допринос општем развоју друштва одрживошћу и усклађеним развојем путне инфраструктуре из домена пословања ЈППС;
- У складу са наведеним, планирани су и предузимају се следећи кораци у развоју ИКТ система у ЈП „Путеви Србије“;
- Унапређење и развој капацитета компаније заснованог на поузданости и сигурности која обезбеђује аутоматизацију у доношењу пословних одлука;
- Перманентна интеграција ИКТ окружења, стварање услова интерактивног повезивања радних процеса и омогућавање корисницима путне инфраструктуре да приступају одређеним и потребним информацијама у реалном времену у што ширем спектру;
- Унапређење и развој капацитета из ИКТ окружења уопште увођењем и применом нових перспективних софтверско-хардверских решења модуларног типа и замена превазиђених;
- Анализа, пројектовање и имплементација различитих ИКТ подсистема као подршку за повећање безбедност расположивих или у фази увођења нових ИКТ система, у складу са Законом о информационој безбедности;
- Пројектовање и имплементација информационог система за подршку пословним процесима - ERP (Enterprise Resource Planning);
- Пројектовање и имплементација информационог система за праћење и архивирање електронских и папирних докумената – DMS (Document Management System).

IV Закључци

На основу спроведене ревизије закључили смо:

Потребно је унапредити процес управљања континуитетом пословања и управљања информационом имовином, обухватајући све системе и апликације, ради обезбеђења потребног нивоа поузданости информационог система ЈППС.

Закључак је донет на основу налаза и донетих закључака о појединачним питањима, и то:

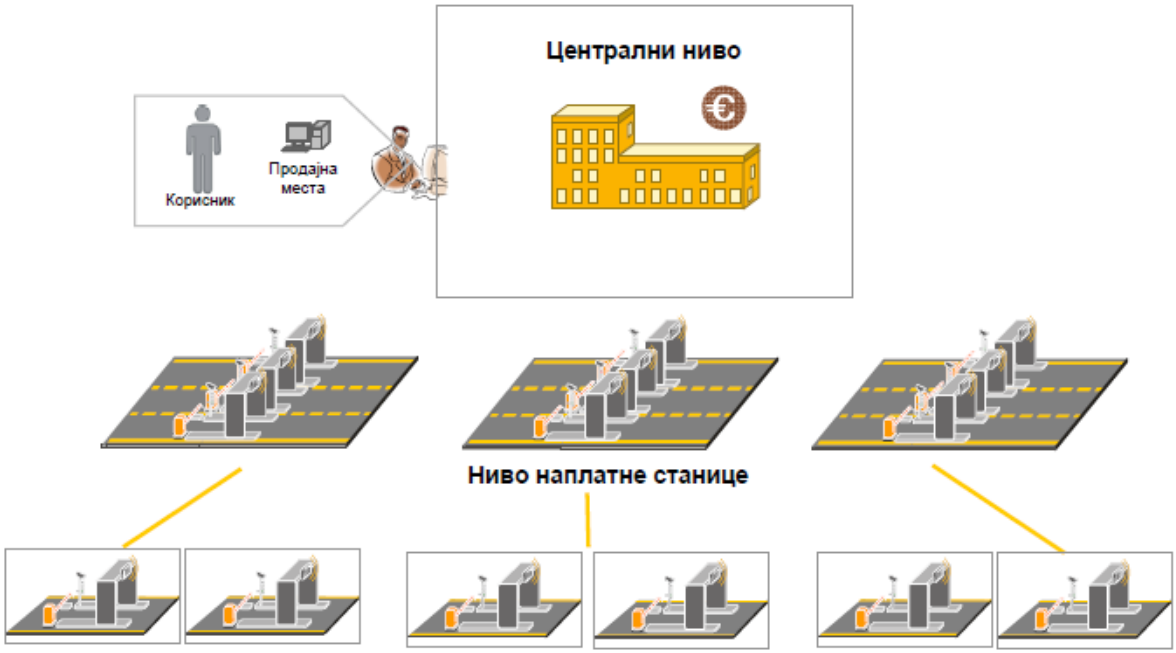
1. Имплементиране апликативне контроле не обезбеђују ефективност у довољној мери, јер се носиоци права ослобађања плаћања путарине не воде у систему за наплату, а размена података између система за наплату путарина и финансијског система се изводи мануелно и преглед записа о догађајима (логова) се не врше периодично због чега постоји ризик да се пословни циљеви неће остварити на ефикасан и правилан начин, што за последицу може имати смањење пословних прихода и доношење погрешних пословних одлука;
2. Услед недоношења стратешких докумената, без којих није могуће одредити приоритете, адекватне мере заштите и пратити њихове трошкове, створен је ризик да у случају штетног догађаја дође до неефикасног реаговања, систем буде недоступан у дужем временском периоду, да се небезбедно управља тајним подацима, изгуби више података од планираних и тиме угрозе резултати пословања превасходно умањивањем планираних прихода и непланираним расходима за опоравак система;
3. Због недостатка стратешких докумената на нивоу предузећа, неефикасног управљања ИТ имовином и фрагментираног управљања информационом безбедношћу, због чега се увећава ризик од неовлашћеног приступа подацима и информационим ресурсима, а што може довести до злоупотребе, непланираних расхода и слабљења поузданости ИС.

ЗАКЉУЧАК 1: Имплементиране апликативне контроле не обезбеђују ефективност у довољној мери, јер се носиоци права ослобађања плаћања путарине не воде у систему за наплату, а размена података између система за наплату путарина и финансијског система се изводи мануелно и преглед записа о догађајима (логова) се не врше периодично због чега постоји ризик да се пословни циљеви неће остварити на ефикасан и правилан начин, што за последицу може имати смањење пословних прихода и доношење погрешних пословних одлука.

У овом делу извештаја, наш циљ био је да одговоримо на прво ревизијско питање, односно у којој мери имплементиране ИТ опште контроле обезбеђују ефективност апликативних контрола ИС ЈППС.

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 завређују додатну пажњу. [23]

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



Слика број 3. Хијерархијска структура наплатног система

Систем за наплату путарине инсталиран на аутопутевима у Републици Србији спада у класу затворених система у којима се регистрација корисника врши на улазу на аутопут, а на излазу се врши наплата путарине у сагласности са категоријом возила и пређеним путем.

[23] Приручник за ИТ ревизију врховних ревизорских институција WGITA – IDI/INTOSAI, 2022.

Систем за наплату путарине је организован хијерархијски и састоји се од три физичка и операциона нивоа (Слика 2):нивоа наплатне траке, нивоа наплатне станице и централног нивоа.

На нивоу наплатне станице прикупљају се подаци са свих трака и обезбеђују функције надгледања, контроле и благајничке функције.

Подаци са свих наплатних станица прослеђују се на централни ниво, на Централну платформу Дата Центра наплате путарине, одакле се преузимају и обрађују подаци од стране надлежних организационих јединица за потребе пословних процеса наплате путарине. Одељење обраде података – АОП, као један од корисника Централне платформе базе података наплате путарине, врши аутоматску обраду података по захтевима и извештавање о саобраћајно-финансијским параметрима са наплате путарине, за потребе интерних и екстерних корисника. На централном нивоу се уносе и одатле се ажурирају системски параметри система за наплату путарине и прикупљају сви подаци о процесу наплате путарине са хијерархијски нижих нивоа (станица/трака).

Прикупљањем, архивирањем и обрадом ових података омогућава се добијање различитих пословних и оперативних извештаја. Ови извештаји се користе као основа за доношење тактичких и стратегијских одлука које се тичу система за наплату путарине.

Централни ниво је одговоран и за комуникацију и интеграцију како са интерним подсистемима (наплатна станица/трака), тако и са екстерним системима (нпр. Мрежа продајних места уређаја за електронску наплату путарине).

Систем је пројектован тако да може да ради и у случају када су у прекиду везе између појединих нивоа. На основу утврђених налаза чији критеријуми су одређени на основу методологије за ИТ ревизију и ревизију сврсисходности пословања, донет је закључак о стању апликативних контрола које су посматране у циљу давања одговора на потпитања:

1. Да ли је ЈППС успоставила ефективан систем интерне контроле за ослобађање плаћања путарине?
2. Да ли је ЈППС обезбедило ефикасну интерну размену података система за наплату путарине и финансијског информационог система?
3. Да ли ЈППС обезбеђује евидентирање активности корисника?

Налаз 1.1: ЈППС евидентира носиоце права ослобађања плаћања путарине на посебне листе, а не у систем за наплату путарине, због чега постоји ризик да се у кратком времену наплате не утврде тачни идентитети имаоца права и да се право додели погрешном кориснику чиме се може довести до умањења пословних прихода.

Контролне активности су политике и процедуре које обезбеђују спровођење директива руководства. Оне обезбеђују предузимање неопходних радњи за решавање ризика и остваривање циљева ентитета. Контролне активности се предузимају на свим нивоима организације, током различитих фаза пословних процеса и унутар технолошког окружења. Финансијско управљање и контрола укључује низ различитих активности као што су одобравања, овлашћења, оверавања, усклађивања, прегледи оперативне успешности (перформанси), безбедност средстава и поделу дужности. [24]

ЈППС уређује организацију рачуноводства на начин који омогућава свеобухватно евидентирање, као и спречавање и правовремено откривање погрешно евидентираних

[24] Приручник за финансијско управљање и контролу, Министарство финансија Република Србија, 2020. године.

пословних промена и уређује интерне рачуноводствене контролне поступке.[25] Редни број треба да у току календарске године буде једнозначан и да се аутоматски додељује.[26] Дозвола за бесплатан пролаз аутопутевима Србије поседује регистарски број возила, власника дозволе, број личне карте/заводни број[27], регистарска ознака и релација[28], регистарски број возила, месец, од/до, заводни број, категорија возила.[29]

Одељење за ИМС и СППП (Одељење за интегрисане менаџмент системе и системе пословне подршке) је у оквиру ИМС донело Процедуру за наплату путарине ПР 750.05 у којој је уредила ослобађање од плаћања за возила и лица у складу са Законом о накнадама.

Ослобађање учесника у саобраћају од плаћања путарине врши се на основу Закона о јавним путевима, тј. издате Пропуснице за бесплатан пролазак аутопутевима - ФМ 750.517 и Дозволе за бесплатан пролазак аутопутевима Србије – ФМ 750.518. Пропуснице издаје овлашћени радник по овлашћењу генералног директора, а Дозволе Одељење за комерцијалне послове, а све у складу са Законом о јавним путевима. Ослобађање у резервном режиму се евидентира у обрасцу „Евиденција возила ослобођених плаћања путарине“ – ФМ 750.519. Пролазак возила са „Претплатном картом“ - ФМ 750.593, у аутоматском режиму рада евидентира се у рачунару а у резервном режиму рада се евидентира преко „Дневног извештаја о корисницима претплатних карата у РРР“- ФМ 750.580.[30]

На основу прикупљених података о проласцима возила кроз наплатне станице који су ослобођени наплате путарине за 2022. годину, утврђен је значајан број возила која немају евидентиране регистарске ознаке у евиденцији.[31] Евиденција возила ослобођених плаћања или умањених износа путарине води се у посебној евиденцији ван система за наплату путарине и инкасанти морају након обављене категоризације возила наплатити или ослободити од наплате у кратком временском року. Право ослобађања или умањења се додељује непосредним увидом у видна обележја на возилу или увидом у Пропусницу, Дозволу или Претплатну карту, где у кратком временском року није у могућности да изврши проверу, основа, деонице, времена, категорије итд.

Како се евиденција возила и лица која остварују право на бесплатну путарину не води на јединствен начин, евиденција је нејасна, некомплетна и чију веродостојност не можемо потврдити. Тако постоји ризик од нетачних исказа и погрешна приказивања финансијских позиција, што може довести до погрешних пословних одлука. Систем интерне контроле не може обезбедити уверавање руководства да ће се циљеви и задаци пословања остварити на ефикасан и правилан начин, тако може изазвати последице по пословне резултате, смањењем пословних прихода и довести до доношења погрешних пословних одлука.

Препорука: Препоручујемо одговорним лицима да обезбеде претходно евидентирање лица/возила за ослобађање или умањење износа путарине у систем за наплату путарине.

[25] Закон о рачуноводству, члан 8, "Службени гласник РС", број 73, 2019-11, број 44/2021-4 (др. закон).
[26] Национални рачуноводствени софтверски стандард 33.58/РСС 33, ревидиран 2008, Београд, Савеза рачуновођа и ревизора Србије, од 12.02.2008. године.
[27] ФМ.750.518 – Дозвола за бесплатан пролаз аутопутевима Србије, по процедури ПР.750.05.
[28] ФМ.750.517 – Пропусница за бесплатан пролазак аутопутевима, по процедури ПР.750.05.
[29] ФМ.750.593 – Претплатна/Месечна карта, по процедури ПР.750.05.
[30] ПР.750.05 – Наплата путарине, бр. 953-12566 од 4.08.2011. године, допуна 7.03.2012. године.
[31] Извештај о ревизији финансијских извештаја Јавног предузећа „Путеви Србије“, Београд за 2022. годину, Број: 400-795/2023-06/15, Београд, 22. децембар 2023. године

Слика број 4. Мапа наплатних станица на територији Републике Србије

Налаз 1.2: Размена података између система за наплату путарина и финансијског информационог система се изводи мануелно што за последицу може имати отежано функционисање интерних контрола и створити ризик непоузданог извештавања.

Рачуноводствени софтвер мора да аутоматизује помоћне књиге, сагласно Закону о рачуноводству и рачуноводственом стандарду. [32]

Налози добијени из аутоматизованих помоћних аналитика (материјалног и робног пословања, основних средстава, ситног инвентара, благајни и других) не смеју се аутоматски прихватати у главну књигу. Њиховом укључивању у главну књигу мора да претходи одређена контрола (програмска, визуелна и суштинска од стране надлежног контисте) и тек по добијању верификације - електронског потписа, аутоматски формиран налог се може прихватити у процес књижења.[33]

Завршетак рада инкасанта подразумева одјављивање и преузимање електронског извештаја „Финансијско раздужење“ – ФМ 750.514. Остварени пазар се избројан, сортиран и спакован (засебно динарска средства плаћања од девизних), „Слип платне картице“- ФМ 750.574 и „Слип допуне ТАГ-а“- ФМ 750.573) предаје у касу уз спецификацију истог у обрасцима „Дневни извештај о уплати пазара“ – ФМ 750.532 и „Дневни извештај о уплати девизног пазара“ – ФМ 750.533 евиденције у образац Предаја готовине - новца – ФМ 750.534 и Предаја врећа-кутија, извештаја-коверти ФМ 750.553. По завршетку рада на дистрибуцији картица инкасант/сменовођа дужан је да попуни „Евиденцију магнетних картица из бокса дистрибутера“- ФМ 750.575, који се заједно са картицама доставља Одељењу аутоматске обраде података.

Формиране извештаје (ФМ 750.509, ФМ 750.510, ФМ 750.514, ФМ 750.515, ФМ 750.516 и ФМ 750.519) инкасанти предају пословођи на наплатној станици по завршетку рада у кабини, који је дужан да исте проследи Сектору за управљачко информационе системе у саобраћају, Одељењу обраде података са наплате путарине (АОП-у) записнички кроз образац „Евиденција о примопредаји документације служби контроле АОП“ – ФМ 750.535. Пословођа наплатне станице је дужан да електронски извештај „Дневни збирни извештај о догађањима на наплатној станици“ – ФМ 750.536 проследи Одсеку аналитике.[34]

Како је систем наплате путарине развијан независно од пословног информационог система, са више добављача од којих ИМП има 78% наплатних рампи, а Орион Телеком 22%, и да је реч о независно развијеним технолошким решењима који раде у одвојеним рачунарским мрежама, потребно је прво објединити све податке. Потом у складу са рачуноводственим политикама и процесима, податке и документацију за формирање налога преузимати у пословни информациони систем предузећа Hermes-MEGA без ручног уноса, него у облику електронског документа. Након преузимања, формирања и књижења налога, податке и извештаје у систему наплате путарине треба заштити механизмом непорецивости. Тако обезбеђени извештаји на основу којих су вршена књижења се не могу накнадно мењати.

Тек тада ће систем интерне контроле обезбедити уверавање руководства да ће се циљеви и задаци пословања остварити на ефикасан и правилан начин, у противном, може изазвати негативне последице по пословне резултате, смањењем пословних прихода и последично, довести до доношења погрешних пословних одлука.

---

[32] Национални рачуноводствени софтверски стандард 33.56/РСС 33, ревидиран 2008, Београд, Савеза рачуновођа и ревизора Србије, од 12.02.2008. године.

[33] Национални рачуноводствени софтверски стандард 32.64/РСС 33, ревидиран 2008, Београд, Савеза рачуновођа и ревизора Србије, од 12.02.2008. године.

[34] ПР.750.05 – Наплата путарине, бр. 953-12566 од 4.08.2011. године, допуна 7.03.2012. године.

Препорука: Препоручујемо одговорним лицима да обезбеде размену података приликом преузимања налога из аналитике, обезбеде суштинску контролу и верификацију података за пријем у главну књигу.

Налаз 1.3: Недостатак периодичних прегледа записа о догађајима (логова), ствара ризик да грешке у евидентирању не буду благовремено детектоване и исправљене и што може имати негативне последице на резултате пословања.

Према Правилнику[35] „Ревизорски траг[36] (у даљем тексту Журнал) је запис који обезбеђује хронолошко документовање и праћење пословних промена у оквиру пословних процеса, активности или операција од почетка до краја.“ Руководилац корисника јавних средстава одговоран је и за документовање свих пословних промена и послова и обезбеђење ревизорског трага унутар корисника јавних средстава.

Журнал поред праћења тока пословног процеса у Пословном информационом систему Hermes – MEGA, омогућава утврђивање индивидуалне одговорности за сваку радњу корисника, обезбеђујући податке за накнадну реконструкцију догађаја, снимајући трагове свих активности корисника омогућава и детекцију упада од стране неовлашћених лица и на крају омогућава идентификовање проблема који су довели до таквих појава.[37]

Журнал треба да садржи довољно информација да се утврди који су се догађаји десили и ко (или шта) их је узроковао. Дефинисање обима и садржаја ревизорског трага треба пажљиво да се уради како би се уравнотежиле безбедносне потребе са могућим перформансама, приватношћу или другим трошковима. Иако структура није прописана, запис догађаја треба да садржи: врсту догађаја, датум и време настанка догађаја, кориснички налог и најмање још програм, модул или команду која је покренула догађај.

Детаљније о садржају журнала (RFC 5424, The Syslog Protocol, Март 2009) може се видети https://datatracker.ietf.org/doc/html/rfc5424.

Сигурност је мера којом се утврђује да ли рачуноводствени софтвер обезбеђује прихватљив ниво ризика од погрешака у књиговодственим евиденцијама, прегледима и финансијском извештавању у одређеним условима употребе и за одређену организацију.[38]

Рачуноводствени софтвер мора да обезбеди меморисање системских порука у посебну базу података (LOG) (меморисани секвенционални дневник порука) које су последица нерегуларних ситуација (прекиди, грешке и сл.) Формирана LOG база података мора у потпуности да задовољи дефинисане захтеве из Међународних стандарда ревизије.[39]

Приступ апликацији се обавља дефинисаним креденцијалима корисничког имена и лозинке. Пожељно је спровести вођење дневника извршених – обављених трансакција (енг. log)

---

[35] Правилник о заједничким критеријумима и стандардима за успостављање, функционисање и извештавање о систему финансијског управљања и контроле у јавном сектору, "Службени гласник РС", број 89 од 18. децембра 2019.

[36] Појам **ревизорски траг** није адекватан јер га не „оставља“/генерише ревизор, него рачунарска апликација, а сврха таквих хронолошких записа је накнадно утврђивање тока процеса и учешћа корисника у реализацији пословног процеса употребом информационог система и/или рачунарске апликације. Поред интерне контроле, интерне ревизије корисник тих записа (ревизорског трага) је у крајњој инстанци и екстерни ревизор. Уместо појма ревизорски траг користимо **Дневник активности/Журнал**.

[37] NIST SP 800-14 – Принципи и праксе за безбедност ИТ система, септембар 1996, Повучен 2018.

[38] Национални рачуноводствени софтверски стандард 33.25/РСС 33, ревидиран 2008, Београд, Савеза рачуновођа и ревизора Србије, од 12.02.2008. године.

[39] Национални рачуноводствени софтверски стандард 33.49/РСС 33, ревидиран 2008, Београд, Савеза рачуновођа и ревизора Србије, од 12.02.2008. године.

за сваки кориснички рачунар или корисника, за контролне сврхе и статистичке анализе приступа подацима.[40]

ThreadID	ns1:Channel	ns1:Computer	ns1:Security	ns1:Data	Name2
96	Security	jpps-ad.jpps.local		S-1-5-21-3433641461-923192373-1833595427-1315	TargetUserSid
96	Security	jpps-ad.jpps.local		JPPS-ADMIN$	TargetUserName
96	Security	jpps-ad.jpps.local		JPPS	TargetDomainName
96	Security	jpps-ad.jpps.local		0x4a3e23e	TargetLogonId
96	Security	jpps-ad.jpps.local		3	LogonType
96	Security	jpps-ad.jpps.local		S-1-0-0	SubjectUserSid
96	Security	jpps-ad.jpps.local		-	SubjectUserName
96	Security	jpps-ad.jpps.local		-	SubjectDomainName
96	Security	jpps-ad.jpps.local		0x0	SubjectLogonId
96	Security	jpps-ad.jpps.local		S-1-5-21-3433641461-923192373-1833595427-1122	TargetUserSid
96	Security	jpps-ad.jpps.local		admin	TargetUserName
96	Security	jpps-ad.jpps.local		JPPS	TargetDomainName
96	Security	jpps-ad.jpps.local		0x4a3e31a	TargetLogonId
96	Security	jpps-ad.jpps.local		3	LogonType
96	Security	jpps-ad.jpps.local		Kerberos	LogonProcessName
96	Security	jpps-ad.jpps.local		Kerberos	AuthenticationPackageName
96	Security	jpps-ad.jpps.local			WorkstationName
96	Security	jpps-ad.jpps.local		{fc0c1b60-08d5-4b93-8350-83d625642169}	LogonGuid
96	Security	jpps-ad.jpps.local		-	TransmittedServices
96	Security	jpps-ad.jpps.local		-	LmPackageName
96	Security	jpps-ad.jpps.local		0	KeyLength

Слика број 5. Дневник догађаја који се повезују са активностима корисника у рачуноводственој апликацији

Журнал свој садржај заснива на Дневницима догађаја (LOG) аутоматски генерисаним записима које генеришу: оперативни системи, базе података, апликације и мрежни уређаји. Зато је необично важно управљање и архивирање тих записа тј. Дневника догађаја и Журнала активности.

Журнали су витално средство који се користе у ревизији како би утврдили одговорност за поступке. Без употребе ревизорских трагова за потврду финансијских информација, не би било разлога да се верује у легитимност финансијских извештаја.

ЈППС је у Акту о безбедности информационо-комуникационог система од посебног значаја, одредила садржај записа које системи морају бележити о активностима корисника, али није успоставила процес периодичног прегледа и извештавања.

Сектор за УИСС не врши периодичне анализе дневника активности корисника и не сачињава периодичне извештаје. У инцидентним случајевима утврђивања разлога за недоследности у евиденцијама прегледава дневник непосредно у апликацији без извожења или друге врсте архивирања.

Необичне и критичне трансакције је могуће погрешно извршити и неуочену грешку пропагирати кроз систем обраде и извештавање. На пример могуће је: евидентирати податке са погрешним датумом, са датумом који претходи стварној пословној промени, да се унесе промена са некомплетним подацима, да се обавезе према добављачима не могу утврдити у целокупном износу и да ИОС образац не буде тачан, итд.

ИКТ систем ЈППС формира записе о догађајима (логови) где се евидентирају активности корисника, грешке, као и други догађаји у вези са информационом безбедношћу.[41]

[40] Национални рачуноводствени софтверски стандард 33.26/РСС 33, ревидиран 2008, Београд, Савеза рачуновођа и ревизора Србије, од 12.02.2008. године.

[41] Акт о безбедности информационо-комуникационог система од посебног значаја ЈППС, 2.17, 31.5.2017, допуна бр. 953-4322 од 18.02.2021. године.

ЈППС је у Акту о безбедности информационо-комуникационог система од посебног значаја, одредила садржај записа које системи морају бележити о активностима корисника, али није успоставила процес периодичног прегледа.

Необављање ових контролних активности може омогућити злоупотребе у дужем временском периоду од периода извештавања чиме се ствара ризик да се корекције не могу исправити пре стварања финансијских последица.

Препорука: Препоручујемо одговорним лицима да успоставе механизам који обухвата уређивање процеса периодичне анализе Дневника активности корисника и извештавају о усаглашености са уређеним рачуноводственим процесима

ЗАКЉУЧАК 2: Услед недоношења стратешких докумената, без којих није могуће одредити приоритете, адекватне мере заштите и пратити њихове трошкове, створен је ризик да у случају штетног догађаја дође до неефикасног реаговања, систем буде недоступан у дужем временском периоду, да се небезбедно управља тајним подацима, изгуби више података од планираних и тиме угрозе резултати пословања превасходно умањивањем планираних прихода и непланираним расходима за опоравак система

Управљање континуитетом пословања је процес којим пословна организација (у овом случају ЈППС) се припрема за будуће инциденте који би могли да угрозе основну мисију организације и њену дугорочну одрживост. Такви инциденти укључују догађаје као што су пожари нестанци струје, рачунарске мреже, земљотреси, или догађаји попут пандемијских болести. Компоненте процеса су:

- **Подршка управљачких органа** — Руководство мора показати подршку одговарајућој припреми, одржавању и примени Плана континуитета пословања (BCP) одређивањем адекватних ресурса, људи и буџетских средстава.
- **Управљање ризиком** — Потенцијални ризици као што су кварови, пожари, поплаве, итд. морају бити идентификовани, а вероватноћа и потенцијални утицај на пословање морају бити утврђени. Ово се мора урадити на нивоу физичке локације и организационе јединице, како би се осигурало да се ризици свих догађаја разумеју и да се са њима на одговарајући начин управља.
- **Процена утицаја на пословање** — Има сврху идентификације оних пословних процеса који су саставни део одржавања пословне способности у случају катастрофе или хаварије и за одређивање колико брзо ови интегрални процеси треба да се опораве након катастрофе или хаварије.
- **Стратегија опоравка и континуитета пословања** — Ова стратегија се бави стварним корацима, људима и ресурсима потребним за опоравак критичног пословног процеса.
- **Свест запослених и обука** — Образовање и свест запослених у познавању програма, планова и поступака континуитета пословања су веома важни за извршење.
- **Вежбе** — Запослени би требали редовно да учествују и провежбавају у спровођењу програма и планова.
- **Ажурирање** — Способности и документација се морају редовно ажурирати, како би се осигурало да остану ефикасни и усклађени са пословним приоритетима.[42]

Овде желимо да одговоримо на друго ревизијско питање, односно у којој мери управљање континуитетом пословања обезбеђује расположивост ИС ЈППС.

Посебно морамо имати у виду да министарство надлежно за одређивање објеката критичне инфраструктуре у области саобраћаја није одредило који објекти припадају критичној инфраструктури из чега произилазе обавезе у погледу доношења безбедносни планова[43]. Министарство надлежно за одређивање објеката критичне инфраструктуре у сектору

[42] GTAG10 – Упутство за управљање континуитетом пословања, Институт интерних ревизора, 2008.
[43] Закон о критичној инфраструктури, “Службени гласник РС”, бр. 87 од 13. новембра 2018.

саобраћаја није плановима обухватило објекте критичне инфраструктуре којим управља ЈППС, што би морало директно да утиче на циљеве управљања континуитетом пословања ЈППС.

Методолошким правилима и смерницама за ИТ ревизију Државне ревизорске институције[44] и Приручником[45], ефикасно управљање континуитетом пословања има неколико заједничких фаза за све информационе системе:

- Полису/Политику, План и организација континуитета пословања;
- Успостављање тима за управљање континуитетом пословања;
- Процена утицаја на пословање и процена ризика;
- Превентивне и контроле окружења;
- Планску документацију;
- План тестирања/провере и обуку;
- Имплементацију безбедности; и
- Резервне копије и опоравак од хаварије за услуге добављача.

Ове фазе представљају кључне елементе у свеобухватној способности планирања континуитета пословања.

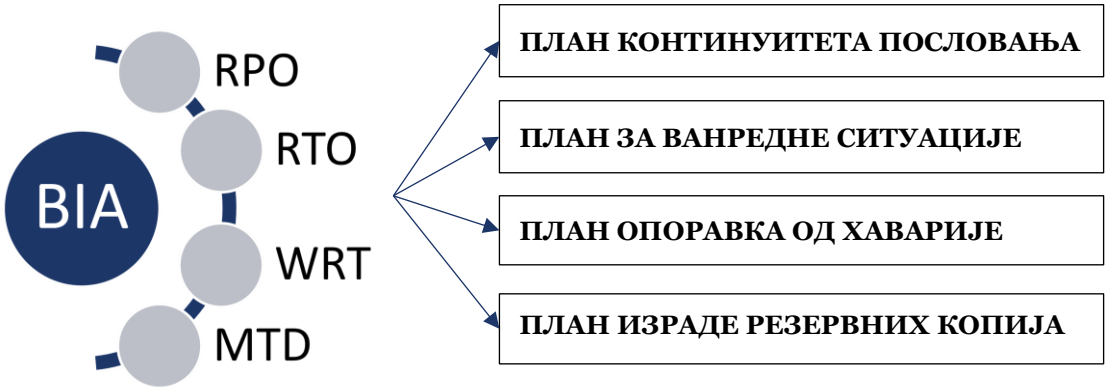
Слика број 6. Управљање континуитетом пословања

Како је у процесу планирања ревизије утврђено постојање одређених докумената који уређују ова питања, као и недостатке у тим документима која стварају ризик по пословање, поставили смо следећа питања:

1. Да ли се врши процена утицаја на пословање у ЈППС?
2. Да ли ЈППС има План континуитета пословања?
3. Да ли ЈППС има План опоравка од хаварије?
4. Да ли ЈППС има тим и План реаговања у ванредним ситуацијама?
5. Да ли ЈППС има План израде резервних копија и редовно врши верификацију исправности копија података?

[44] Методолошка правилима и смернице за ИТ ревизију Државне ревизорске институције, 2019.
[45] Приручник за ИТ ревизију врховних ревизорских институција WGITA – IDI/INTOSAI, 2022.

Поред Стратегије управљања ризиком која ће одредити ризике да би одредили многе параметре управљања континуитетом пословања, неопходно је проценити и утицаје тих ризика на процесе, ресурсе, људе, пословање итд.



Слика број 7. Планска документа неопходна за управљање континуитетом пословања

Табела 1. Врсте Планова

План	**Сврха**	**Обим**	**Веза са Планом**
План континуитета пословања (**ПКП**)	Даје процедуре за очување пословних операција и опоравак од значајног поремећаја.	Обухвата пословне процесе на нижем или проширеном нивоу из ПКО за критичне процесе.	Фокусиран на пословни процес и може се активирати у координацији са ПКО за критичне процесе.
План континуитета операција (**ПКО**)	Даје процедуре и смернице за очување критичних процеса организације на алтернативној локацији до 30 дана.	Обухвата критичне процесе у објекту и/или информационе системе који подржавају критичне процесе.	Фокусиран на критичне процесе и може се активирати са једним или више ПКП, ПВС и ПОХ, према потреби.
План комуникација у кризним ситуацијама (**ПКК**)	Даје процедуре за интерну и екстерну комуникацију, обезбедити критичне информације о статусу и контроли гласине.	Бави се комуникацијом са особљем и јавношћу и није фокусиран на информациони систем.	План заснован на инцидентима активира се са ПКО или ПКП, али се може користити самостално током јавног догађања.
План заштите критичне инфраструктуре (**ПКИ**)	Даје политике и процедуре за заштиту делова националне критичне инфраструктуре, у складу са Националним Планом.	Обухвата делове критичне инфраструктуре које подржава или њима управља организација.	План управљања ризиком који подржава ПКО за организације са критичном инфраструктуром и кључним ресурсима.
План одговора на сајбер инциденте (**ПСИ**)	Даје процедуре за ублажавање и отклањање сајбер напада, као што су вируси, црви или тројанци.	Подразумева ублажавање и изолацију погођених система, чишћење и минимизоване губитке информација.	Фокусиран на ИС који може активирати ПВС или ПОХ, у зависности од обима.
План опоравка од хаварије (**ПОХ**)	Даје процедуре за премештање операција информационих система на алтернативну локацију.	Активира се након великих поремећаја система са дугорочним ефектима.	Фокусиран на ИС који активира један или више ПВС за опоравак појединачних система.
План за ванредне ситуације информационог система (**ПВС**)	Даје процедуре и одређује способности за опоравак информационог система.	Обухвата опоравак једног информационог система на тренутној или, ако је прикладно, алтернативној локацији.	Фокусиран на ИС који се може активирати независно од других планова или као део већег напора за опоравак координисаног са ПОХ, ПКО и/или ПКП.
План заштите лица у ванредној ситуацији (**ПЗЛ**)	Даје координиране процедуре за минимизирање губитка живота или повреда и заштиту имовине од штете као одговор на физичку угроженост.	Фокусира се на особље и имовину за конкретан објекат, није заснован на пословном процесу или информационом систему.	План заснован на инцидентима који се покреће одмах након догађаја, пре ПКО или ПОХ активације.

Слика број 8. Приказ међувеза имплементираних планова и фокус области

Обим ЈППС и његов значај за живот и рад у Републици Србији, посебно имајући у виду распрострањеност организационих делова и свих ресурса на целокупној територији, намеће потребу за ангажовањем свих организационих делова у израду неопходних планских докумената и увежбавање могућих сценарија за умањење ризика.

Налаз 2.1: Није израђена Процена утицаја на пословање због недоношења Стратегије управљања ризиком, услед чега нису ни утврђене безбедносне категорије и приоритети заштите информационе имовине што ствара ризик од непланираних расхода и издатака за мере заштите.

Анализа утицаја на пословање ће помоћи да се препозна и направи списак кључних/критичних система, пословних процеса и механизама, узимајући у обзир утицај штетних догађаја, дозвољену дужину застоја и услове за опоравак.

Процес израде Стратегије управљања ризицима је у току и још увек није доживео коначну форму. Прегледе ризика којима су обухваћени и информациони системи (у форми регистра) израђују Сектори, односно власници процеса заједно са Сектором за УИСС на годишњем нивоу.

Процена утицаја на пословање (Business Impact Analysis - BIA) је кључни корак у управљању континуитетом пословања и обухвата неколико активности. Ове активности укључују:

- **Идентификација критичних пословних функција:** Први корак је идентификација основних пословних функција које су кључне за опстанак ЈППС. Ове функције су обично

оне које генеришу приход, одржавају односе са купцима, и осигуравају усклађеност са законским и регулаторним захтевима.

- **Идентификација ресурса**: Ово обухвата идентификацију свих ресурса потребних за подршку критичним пословним функцијама. Ови ресурси могу укључивати људске ресурсе, информационе технологије, опрему, добављаче и инфраструктуру.
- **Оцену утицаја прекида**: Ово укључује процену утицаја прекида пословања на ЈППС. Ова анализа обухвата финансијске губитке, репутациону штету, правне и регулаторне последице, и друге кључне утицаје на пословање.
- **Одређивање временских оквира**: Дефинисање временских оквира који су неопходни за наставак процеса планирања и израду свих неопходних докумената, као што је:
  - **RPO** (Recovery Point Objective): Циљна тачка опоравка — Одређује максималну количину података коју организација може изгубити (мерено временом) пре инцидента;
  - **RTO** (Recovery Time Objective): Циљно време опоравка — Одређује максимално време које може протећи од тренутка када дође до инцидента до тренутка када се информациони систем поново функционалан;
  - **WRT** (Work Recovery Time): Време опоравка рада — Представља време потребно за потпуни опоравак пословних активности након техничког опоравка. Ово време је веће од RTO и обухвата опоравак свих система и целокупног процеса;
  - **MTD** (Maximum Tolerable Downtime): Максимално толерисан испад — Ово време је веће од WRT и представља укупно време које организација може толерисати да њени кључни процеси буду прекинути.
- **Документовање налаза**: Сви налази се документују како би се направила основа за развој стратегија и планова опоравка. Ово укључује приоритизацију пословних функција и процеса, као и потребних ресурса за опоравак.
- **Извештавање и препоруке**: Налази и препоруке се представљају вишем менаџменту како би се обезбедила подршка за даље активности у континуитету пословања и опоравку од инцидената.
- **Ревизија и ажурирање**: Процена утицаја на пословање је динамичан процес који се треба редовно ревидирати и ажурирати како би се осигурало да остане релевантан у односу на промене у пословном окружењу и оперативним условима.

Пример из праксе

Подаци из система показују да је просечна цена 670 дин, и да 25 возила излазе са аутопута у минути, што износи 16.750,00 дин Ево како би изгледала примена овог концепта:

1. **RPO**: ЈППС одлучује да је максимално прихватљив губитак података 5 минута. То значи да морају да праве резервне копије података сваких 5 минута, потенцијални губитак 83.750,00 дин
2. **RTO**: ЈППС одређује да морају вратити своје системе у радно стање у року од 15 мин након инцидента, да би се избегли већи губици и незадовољство возача, а то је 251.250,00 дин.
3. **WRT**: Након што су системи враћени у радно стање, потребно је додатних 30 минута за обављање свих активности опоравка, као што су провера интегритета података, обнова свих услуга и тестирање функционалности.
4. **MTD**: ЈППС је одредила да укупно време у којем њихови кључни пословни процеси могу бити прекинути не сме прећи 45 минута. То значи да је MTD = RTO (15 мин) + WRT (30 мин).

У случају инцидента, ако ЈППС успе да опорави своје системе и заврши све активности опоравка у оквиру MTD-а, могу се минимизирати негативне последице и одржати континуитет пословања. Одређивањем ових параметара директно одређујемо трошкове имплементирања техничког решења. Што су краћа времена то су виши трошкови имплементације, и обрнуто.

Утврђене безбедносне категорије информационе имовине ЈППС се заснивају на њиховом потенцијалном утицају на пословање, у случају неочекиваних догађаја који угрожавају информације и/или информационе системе који су потребни да ЈППС оствари пословне циљеве, заштити своју имовину, испуни своје прописане обавезе, настави редовно пословање и заштити запослене.[46]

Ове активности омогућавају ЈППС да разуме своје слабости и да развије ефективну стратегије за умањење ризика и обезбеди континуитет пословања у случају прекида.

Услед не одређивања критичности по пословне процесе, њихов утицај на укупно пословање може доћи до већих расхода и издатака за примену заштитних мера него што је корист или утицај на пословни резултат.

Препорука: Препоручујемо одговорним лицима да успоставе редовни процес Процене утицаја на пословање и о томе периодично извештавају управљачке органе.

Налаз 2.2: Није израђен План континуитета пословања због недостатка Процене утицаја на пословање, постојеће Упутство не дефинише потребан ниво доступности ИКТ система и подсистема, због чега постоји ризик да у случају штетног догађаја не дође до правилног реаговања, што може произвести нефункционисање и непланиране расходе и издатке за мере заштите.

ЈППС је донело *Упутство за обезбеђење континуитета пословања и опоравак од нежељеног догађаја ИКТ система* којим су уређена следећа питања: предмет и подручје примене упутства, лица која су овлашћена за реаговање, критеријуми покретања активности по Упутству, одржавање Упутства, активности на обезбеђењу континуитета, идентификација, процена штете, интервентни процеси, активности након догађаја, комуникација и одлучивање, враћање у редовно стање, време ажурирања и дистрибуцију Упутства.

Упутство није обухватило захтеве за доступност ИКТ система, који неопходни ниво расположивости, који подсистеми, којим редоследом и којим поступцима се врши обнављање или успостављање редовног пословања.

Ако узмемо у обзир да, Оператор ИКТ система треба да верификује успостављене и имплементиране контроле континуитета пословања у редовним условима рада, како би оне биле важеће и ефективне током ванредне ситуације.

Оператор ИКТ система треба да идентификује захтеве за доступност ИКТ система. Редундантне компоненте треба размотрити онда када се доступност не може гарантовати коришћењем постојећих архитектура система.[47]

План континуитета пословања (Business Continuity Plan, BCP) је стратешки документ који дефинише како ЈППС одржава критичне функције и минимизира прекиде у случају непредвиђених догађаја као што су природне катастрофе, технолошки проблеми или људске грешке. Развој оваквог плана захтева свеобухватан приступ и укључује различите факторе и кораке. Ево кључних докумената и сврха употребе на основу којих се доноси План континуитета пословања:

1. Одређивање приоритета на основу Анализе утицаја на пословање описана у налазу 2.1:
   - Идентификација критичних пословних функција и процеса;
   - Процена утицаја прекида на те функције, укључујући финансијске и оперативне последице;

[46] NIST FIPS PUB 199 – Стандард за безбедносну категоризацију федералних информација и информационих система, фебруар 2004, https://csrc.nist.gov/files/pubs/fips/199/final/docs/fips-pub-199-final.pdf

[47] Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, „Службени гласник РС“, број 94 од 24. новембра 2016. године.

- Одређивање временских параметара описаних у налазу 2.1;

2. Процена ризика и претњи из Стратегије управљања ризиком:
   - Идентификација потенцијалних ризика и претњи које могу утицати на пословање (нпр. рансомвер напади, малвер напади, технолошки кварови, природне катастрофе, итд.);
   - Процена вероватноће и могућих последица тих ризика;
   - Развој стратегија за ублажавање идентификованих ризика;
3. Развој стратегија опоравка:
   - Одређивање метода и ресурса потребних за опоравак критичних функција;
   - Разматрање алтернатива као што су резервне локације, спољни добављачи и ИТ резервне копије;
   - Дефинисање процедура за комуникацију и координацију током кризе;
4. Дефинисање улога и одговорности:
   - Именовање тима за континуитет пословања и одређивање њихових задатака;
   - Јасно дефинисање улога и одговорности у случају активације плана;
5. Развој планова за реаговање на инциденте:
   - Детаљни планови за конкретне сценарије, укључујући процедура за евакуацију, сајбер нападе, итд;
   - Стварање протокола за брзо и ефикасно реаговање;
6. Тренинг и едукација:
   - Редовна обука запослених о процедурама и протоколима дефинисаним у плану;
   - Спровођење симулација и вежби како би се тестирала ефикасност плана и спремност особља;
7. Одржавање и ажурирање Плана:
   - Периодичне ревизије и ажурирања плана како би се ускладио са променама у пословању, технологији и окружењу;
   - Континуирано праћење и анализа нових ризика и претњи;
8. Комуникациони план:
   - Развијање стратегија за унутрашњу и спољашњу комуникацију током кризе; и
   - Дефинисање метода за комуникацију са запосленима, клијентима, добављачима и медијима.

Иако је ЈППС у доброј мери елиминисала ризике оперативним поступцима описаним у Упутству, поред допуне неопходно је да донесу документ на нивоу целокупног предузећа и да обухвате све системе.

Услед недостатка Процене утицаја на пословање као предуслова и недостатак свести о значају плана континуитета пословања и реаговања на штетне догађаје у складу са приоритетима по пословање ЈППС. Недостатком планских активности у случајевима реализације ризика у виду прекида дела пословних процеса може доћи до непланираних трошкова на санацији последице уместо превентивног деловања.

Препорука: Препоручује се одговорним лицима да донесу План континуитета пословања, одреде лица и њихове обавезе у погледу периодичног тестирања, усклађивања и извештавања управљачких органа.

Налаз 2.3: Није донет План опоравка од хаварије за ИТ систем или подсистеме због недостатка Плана континуитета пословања, и непотпуно дефинисаних ИТ ризика, што у случају штетних догађаја може довести до неефикасног реаговања и нефункционисања система у дужем временском периоду.

Како Оператор ИКТ система врши израду резервних копија које треба да обухвате све системске информације, апликације и податке који су неопходни за опоравак целокупног система у случају наступања последица изазваних ванредним околностима[48] потребно је израдити План опоравка од хаварије[49] који ће омогућити ЈППС да на једном месту дефинише све техничке кораке за успешан опоравак информационог подсистема или система у целини.

На основу добре праксе План опоравка од хаварије треба да садржи:

Циљеви и обухват Плана:
- Циљеви плана укључују брзо и ефикасно враћање ИТ система и минимизирање времена недоступности.
- Опсег плана дефинише који системи и процеси су обухваћени планом опоравка.

Контакт информације за хитне случајеве:
- Листа кључних контаката укључује ИТ тим, управу, добављаче и друге релевантне особе.
- Укључује и информације за контакт са спољним партнерима и сервис провајдерима.

Опис критичних ИТ ресурса:
- Детаљан попис критичних система и апликација.
- Процена важности сваког система за пословање и последице њиховог губитка.

Процедуре за хитне случајеве:
- Прецизни кораци који се морају предузети одмах након хаварије.
- Укључује процедуре за безбедно гашење система како би се спречили додатни губици података.

Резервне копије и стратегије опоравка података:
- Политике за прављење резервних копија података (фреквенција, типови резервних копија).
- Детаљи о локацијама где се чувају резервне копије и процедуре за враћање података.

Резервне локације и опрема:
- Планови за премештање на алтернативну локацију ако примарна локација постане недоступна.
- Информације о резервним серверима и мрежној опреми.

Планови опоравка за специфичне системе:
- Корак-по-корак упутства за опоравак сваког критичног система.
- Враћање сервера, база података, апликација и мрежних услуга.

Комуникациони план:
- Планови за информисање запослених, клијената и партнера о стању опоравка.
- Канали комуникације и одговорне особе за комуникацију.

Тестирање и обука:
- Редовно тестирање плана опоравка кроз симулације и провере.

---

[48] Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, "Службени гласник РС", број 94 од 24. новембра 2016. године

[49] Иако у стручној литератури се назива Disaster Recovery Plan – DRP, по своме садржају овај План обухвата све неопходне кораке за опоравак након техничког проблема тј. хаварије и адекватније је употребљавати реч хаварије него катастрофе која подразумева природне катастрофе.

- Обука особља о њиховим улогама и дужностима у случају хаварије.

Одржавање и ажурирање плана:

- Процедуре за редовно ажурирање плана како би одражавао промене у пословању и технологији.
- Периодичне ревизије и ажурирања на основу резултата тестова и промене околности.

Ови елементи су кључни за ефикасно управљање опоравком од хаварије и осигурање континуитета ИТ услуга након инцидената[50].

Садржај Плана се заснива на повезивању утицаја, и потенцијалне претње у облику ризика који може довести до хаварије и које мере тј. кораке треба да предузме тим за опоравак како би систем у што краћем року, уз што мање трошкове довели у исправно стање.

Избор сценарија је веома важан, у контексту ангажовања добављача, употребе клауд услуга, резервних делова, резервних дискова, доступности резервних копија, итд. Хипотетички, ако нам је рансомвер напад закључао сервер базе података, у плану ће писати, ко када и како ће оправити систем, нпр. где се налазе резервни дискови, извршити замену са „криптованим“ дисковима (последица рансомвер напада), инсталирати оперативни систем, ажурирати, инсталирати сервер базе података, рестаурирати резервну копију, подесити све параметре система да би рачунарска апликација и корисници могли да му приступе, обавести власнике процеса, кључне/најважније кориснике система, утврде ажурност копије (да ли не достају неки подаци), обавесте кориснике о поновном уносу (ако не постоји други начин), и коначно обавесте сви корисници да могу несметано наставити са радом.

Како и у овом хипотетичком случају можемо видети да је реч о низу активности више лица и заинтересованих страна, поред плана неопходно је периодично тестирати исправност Плана и увежбавати активности пре него што се и догоди стварна хаварија или инцидент.

Као могућа последица недостатка периодичне провере Плана, план може постати неизводљив у планираном периоду и може довести до делимичног или трајног губитка података и апликација са не могућношћу опоравка целокупног система и обнављања пословања који се заснива на датом информационом систему.

Препорука: Препоручујемо одговорним лицима да донесу План опоравка од хаварије за ИТ систем и подсистеме, врше периодично тестирање и о томе извештавају управљачке органе.

Налаз 2.4: ЈППС нема План континуитета пословања у ванредним ситуацијама због неактивности надлежног органа за одређивање објеката критичне инфраструктуре у области саобраћаја стварајући ризик небезбедног управљања тајним подацима и неадекватног реаговања у заштити лица и имовине.

У циљу смањења ризика по пословање ЈППС како је предвиђено Законом о информационој безбедности, Оператор ИКТ система (ЈППС) 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.

Тако, Оператор ИКТ система треба да успостави, документује, имплементира и одржава процесе, процедуре и контроле да би осигурао захтевани ниво континуитета пословања током ванредне ситуације.

[50] NIST SP800-34 Рев.1 – Водич за планирање опоравка федералних информационих система у ванредним ситуацијама , мај 2010, https://www.nist.gov/privacy-framework/nist-sp-800-34

Оператор ИКТ система треба да верификује успостављене и имплементиране контроле континуитета пословања у редовним условима рада, како би оне биле важеће и ефективне током ванредне ситуације.

Оператор ИКТ система треба да идентификује захтеве за доступност ИКТ система. Редундантне компоненте треба размотрити онда када се доступност не може гарантовати коришћењем постојећих архитектура система.[51]

План за ванредне ситуације информационог система (ПВС) успоставља процедуре за процену услова када је неопходан опоравак система након прекида. ПВС пружа кључне информације потребне за опоравак система, укључујући улоге и одговорности, информације о инвентару, процедуре анализе стања, детаљне процедуре опоравка и тестирање система.

ПВС се разликује од ПОХ првенствено по томе што су процедуре плана за ванредне ситуације информационог система развијене за опоравак система без обзира да ли се ради о примарној или резервној локацији. ПВС се може активирати на тренутној локацији система или на резервној локацији. Насупрот томе, ПОХ се првенствено односи на специфичну локацију и посебно је развијена процедура за премештање операција једног или више информационих система са угрожене локације на привремену или резервну локацију. Када ПОХ успешно пренесе информациони систем на резервну локацију, сваки погођени систем би тада користио свој одговарајући ПВС за обнављање, опоравак и тестирање рада.

Настанак ванредних услова и селидба на резервну локацију могу бити координирани са активностима надлежног министарства или покренути по плану, у којем јасно морају бити предвиђени ресурси и лица која ће бити ангажована на пословима селидбе.

Резервна локација мора да испуњава одређене критеријуме у складу са оцењеним нивоом критичне инфраструктуре.

ЈППС није донело План континуитета пословања у ванредним ситуацијама, тако да ни реаговање у циљу ублажавања последица техничких хаварија и природних катастрофа на објекте критичне инфраструктуре није дефинисано као ни увежбано.

Главни узрок недоношења Плана континуитета пословања у ванредним ситуацијама је да још увек није завршен поступак утврђивања критичне инфраструктуре у области саобраћаја. Министарство грађевинарства, саобраћаја и инфраструктуре задужено је за идентификацију и одређивање критичне инфраструктуре у сектору саобраћаја

Због непланирања потребних ресурса и недовољне увежбаности ЈППС за случајеве ванредне ситуације, може доћи до угрожавања услова рада, здравља и живота грађана у делу или целој територији Републике Србије, све у складу са процењеним критеријумима из Уредбе.

Препорука: Препоручујемо одговорним лицима да у сарадњи са министарством надлежним за одређивање објеката критичне инфраструктуре у области саобраћаја, сачини Безбедносни план оператора за управљање ризиком и предвиди мере којима се обезбеђује обављање послова у ванредним околностима.

Налаз 2.5: Иако врши израду резервних копија ЈППС нема План израде резервних копија и не тестира исправност и могућности рестаурације сервера базе података, што ствара ризик да у случају потребе систем буде недоступан, изгуби више података од планираних и тиме угрози постизање пословних циљева.

Како је дефинисано Уредбом, Оператор ИКТ система дефинише време чувања и заштите резервних копија, обим и учесталост резервних копија, безбедно место чувања резервних копија, обезбеђује физичку заштиту резервних копија и заштиту од спољашњих утицаја,

[51] Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, „Службени гласник РС“, број 94 од 24. новембра 2016. године.

проверава носаче података како би се осигурало њихово исправно функционисање и поузданост у складу са планом израде резервних копија.

Оператор ИКТ система врши израду резервних копија које треба да обухвате све системске информације, апликације и податке који су неопходни за опоравак целокупног система у случају наступања последица изазваних ванредним околностима. [52]

ЈППС је послове израде резервних копија уредио Процедуром[53] у складу је са Уредбом[54] и Актом[55] којом је заштита од губитака података раздвојена по секторима. Сектор за финансије и комерцијалне послове врши израду резервних копија свакодневно, Сектор наплате путарине и Одељење обраде података-АОП приликом додавања нових података и базе података једном недељно.

Општи принципи поступања спровођења заштите од губитака података су уређени процедуром и у складу са својим пословним процесима свака организациона јединица својом процедуром дефинише начин заштите од губитка података, а које још увек нису израдили. Оригинални подаци су сачувани на хард дисковима на серверима и персоналним рачунарима.

За заштиту и безбедност података на мрежним серверима задужено је Одељење за одржавање УИС односно Одсек за развој и одржавање рачунарске опреме и мрежа, док за индивидуалне податке на персоналним рачунарима одговарају корисници, чувајући исте на одговарајућим расположивим медијима - резервне копије. Одговорно лице у организационим целинама и/или администратор врши одлагање свих докумената и складиштење у архиву.

Ка што је наведено у налазу 1.1. недостатак *Процене утицаја на пословање* имало је за последицу да нису утврђени неопходни параметри да би могли израдити План израде резервних копија којим ће се периодично контролисати и исправност резервних копија.

Исправност резервних копија података до сада ни једном није тестирана, тако да није познато да ли омогућавају успешну рестаурацију снимљеног стања. 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. Субјект ревизије треба да обезбеди да су резервне копије података ажурне и адекватно заштићене, а поступци опоравка тестирани и успешни.

Обавеза израде и чувања је неформално делегирана Секретаријату за опште послове и активности се не синхронизују. Може доћи до делимичног или трајног губитка података и апликација са не могућношћу опоравка целокупног система, обнављања пословања у ванредним ситуацијама.

Препорука: Препоручујемо одговорним лицима да донесу План израде и тестирања резервних копија, уреде процедуре усклађеног функционисања свих организационих делова у циљу смањења ризика од губитка података.

[52] Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, "Службени гласник РС", број 94 од 24. новембра 2016. године

[53] ПР.422.03 – Коришћење и заштита података на рачунарима, бр. 953-20627 од 8.12.2011. године, допуна 12.09.2022. године.

[54] Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, "Службени гласник РС", број 94 од 24. новембра 2016. године

[55] Акт о безбедности информационо-комуникационог система од посебног значаја ЈППС, 31.5.2017, допуна бр. 953-4322 од 18.02.2021. године

ЗАКЉУЧАК 3: Због недостатка стратешких докумената на нивоу предузећа, неефикасног управљања ИТ имовином и фрагментираног управљања информационом безбедношћу, због чега се увећава ризик од неовлашћеног приступа подацима и информационим ресурсима, а што може довести до злоупотребе, непланираних расхода и слабљења поузданости ИС.

Један од циљева био је да одговоримо на треће ревизијско питање, односно у којој мери успостављена информациона безбедност обезбеђује поузданост ИС ЈППС.

Методолошким правилима и смерницама за ИТ ревизију Државне ревизорске институције[56], под информационом безбедношћу подразумевају се процеси управљања ризиком, политика информационе безбедности, класификација података, организација безбедности, управљање комуникацијама, управљање имовином, безбедност запослених, физичка безбедност, контрола приступа систему, одржавање, обучавање о питањима безбедности, управљање инцидентима и управљање континуитетом пословања. Та питања су ређена Законом о информационој безбедности[57] и посебно питање је, да ли постојећи систем интерне контроле даје довољан ниво уверавања руководству да су сви процеси обезбеђују извршење прописа у овој области.

Према одредбама члана 8 став 1 Закона о информационој безбедности, оператор ИКТ система дужан је да донесе акт о безбедности ИКТ система, док је ставом 2 истог члана прописано да се тим актом одређују 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.

ЈППС је од 2011. године започео организационо прилагођавање и припрему за увођење интегрисаног менаџмент система ИМС, имплементацијом СРПС ISO 9001:2008 и иницијално се сертификовао 26. априла 2012. године. Транзиција на ISO 9001:2015 се десила у јуну 2018. године. Још у оквиру почетних активности донео је процедуру ПР 423.03 Коришћење и заштита података на рачунарима од 8.12.2011. године, бр. 953-20627.

Постојећа процедура је ажурирана и допуњена у септембру 2023. године и својим садржајем уређује многа питања, што је био добар предуслов пре самог доношења Закона о информационој безбедности. Тако је ЈППС и донело Акт о безбедности информационо-комуникационог система од посебног значаја, 2017. године и ажурирало га исте године и 2021. године. Овим актом су, у складу са Законом о информационој безбедности, ближе уређене 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. Мере заштите ИКТ система које су ближе уређене наведеним актом служе превенцији од настанка инцидената, минимизацији штете које могу да настану и њихова примена је обавезна за све запослене.

На основу анализе Акта и прибављених доказа о поступању по дефинисаним процедурама и интервјуа са запосленим лицима која су одговорна за поступање, оцењујући најзначајније ризике из области информационе безбедности донели смо закључак оцењујући одговоре на следећа питањима:

1. Да ли ЈППС има ефективан и добро документован механизам процене ИТ ризика?

[56] Методолошка правилима и смернице за ИТ ревизију Државне ревизорске институције

[57] Закон о информационој безбедности, “Службени гласник РС”, бр. 6 од 28. јануара 2016, 94 од 19. октобра 2017, 77 од 31. октобра 2019. године.

2. Да ли се ефикасно управља ИТ имовином?
3. Да ли је ЈППС ефикасно управља заштитом информација, података и докумената у информационом систему?

Налаз 3.1: ЈППС није донело Стратегију управљања ризиком којом се обухватају и ИТ ризици, иако на годишњем нивоу израђује прегледе ризика, што у случају инцидената може довести до изостанка правовремене реакције и санације негативних последица у виду смањења прихода и непланираних расхода.

Ризик представља вероватноћу да ће се десити одређени догађај који би могао имати негативан утицај на остваривање циљева корисника јавних средстава. Ризик се мери кроз његове последице и вероватноћу дешавања[58]. Процес управљања ризицима треба посматрати као један од кључних делова сваког система финансијског управљања и контроле[59]. ЈППС још увек израђује стратегију управљања ризиком која ће обухватити све информационе ресурсе који се употребљавају. Сектор за управљачки информациони систем врши процену ИТ ризика на стратегијском нивоу, и ризици обухватају све расположиве ресурсе у начелу.

У ревидираном периоду 2021-2023. године, ЈППС је набавило услугу Одржавање и унапређење софтвера и продужења корисничких лиценци за антивирус програме, где добављач услуге периодично - месечно врши скенирање слабости мејл сервера и корисничких рачунара и о томе сачињава аутоматизован извештај.

У истом периоду извршило је Набавку услуга у области развоја, унапређења и заштите ИТ система. Добављач услуге периодично - месечно врши скенирање слабости свих сервера и корисничких рачунара и о томе сачињава аутоматизован извештај.

Иако Стратегија још увек није завршена, једном годишње се врши процена ризика, што је ретко, ако умемо у обзир да се ризици у ревидираном периоду од три године, готово нису мењали. Како се једном годишње израђује *Преглед ризика* који обухвата ризике на општем нивоу посматрања и не обухвата мере за њихово умањење или избегавање. Мере за умањење постоје, али нису довољно детаљне.

Предложена форма *Регистра ризика* има за циљ документовање процењених ризика и садржи: циљ пословног процеса, опис ризика, његов утицај, вероватноћу појављивања, рангирање, одговор на ризик, лице које спроводи одговор на ризик, рок за извршење и датум следеће провере.

Значај управљања ризицима треба да обезбеди да ЈППС буде оспособљен да управља ИТ ризицима на исправан, етички, економичан, ефективан и ефикасан начин који је у потпуности усаглашен за законима и другим прописима, чува средства од губитака, злоупотребе, штете на документован начин.

Процена ИТ ризика је процес идентификовања и анализе релевантних ризика повезаних са остваривањем пословних циљева употребом ИТ, ови ризици могу бити интерни (нпр. људска грешка, превара, пад ИТ система/програма), и екстерни (нпр. измене прописа, природне катастрофе, хаварије, хакерски напади итд.). ЈППС треба да успостави јасну процедуру за процену ризика која укључује улоге и одговорности руководилаца и да периодично извештава.[60]

[58] Правилник о заједничким критеријумима и стандардима за успостављање, функционисање и извештавање о систему финансијског управљања и контроле у јавном сектору, “Службени гласник РС”, број 89/2019.
[59] Смернице за управљање ризицима, Министарство финансија Републике Србије, 2020.
[60] Приручник за финансијско управљање и контролу, Министарство финансија Република Србија, 2020. године.

Да би спровели потребне радње за ублажавањем ризика, што подразумева предузимање мера заштите неопходно је идентификовати сва информациона добра[61] и одредити одговорност за њихову заштиту. То значи да треба обухватити опрему, оперативне системе, софтвер и запослене који раде на тим пословима и приступају систему.

Адекватност одабраних мера зависи пре свега од тога колико планирани пословни циљеви ЈППС зависе од доступности ИКТ система, тј. његове доступности корисницима и другим заинтересованим странама. Доступност ИКТ система је однос времена рада и застоја, тако да финансијска вредност уложена у одабрану меру заштите треба да буде адекватна губитку који настаје за време застоја.

Слика број 9. Сценарио ИТ ризика

Табела 2. Прорачун времена трајања застоја на основу доступности ИКТ система

Доступност %	Застоји годишње	Застоји по кварталу	Застоји месечно	Застоји недељно	Застој у току 24 сата
90% („једна деветка“)	**36,53 дана**	**9,13 дана**	**73,05 сати**	**16.80 сати**	**2.40 сати**
95% („једна и по деветка“)	18,26 дана	4,56 дана	36,53 сати	8.40 сати	1.20 сати
97%	10,96 дана	2,74 дана	21,92 сати	5,04 сати	43,20 min
98%	7,31 дана	43,86 сати	14.61 сати	3.36 сати	28.80 min
99% („две деветке“)	**3,65 дана**	**21,9 сати**	**7.31 сати**	**1,68 сати**	**14.40 min**
99,5% ("две и по деветке")	1,83 дана	10.98 сати	3,65 сати	50,40 min	7.20 min
99,8%	17.53 сати	4,38 сати	87,66 min	20,16 min	2,88 min
99,9% („три деветке“)	**8,77 сати**	**2,19 сати**	**43,83 min**	**10.08 min**	**1,44 min**

[61] Информациона добра обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, записе о коришћењу хардверских компоненти, података из датотека и база података и спровођењу процедура ако се исти воде, унутрашње опште акте, процедуре и слично, по Закону о информационој безбедности.

Доступност %	Застоји годишње	Застоји по кварталу	Застоји месечно	Застоји недељно	Застој у току 24 сата
99,95% ("три и по деветке")	4,38 сати	65,7 min	21,92 min	5,04 min	43,20 s
99,99% ("четири деветке")	**52.60 min**	**13.15 min**	**4,38 min**	**1,01 min**	**8,64 s**
99.995% ("четири и по деветке")	26.30 min	6,57 min	2,19 min	30.24 s	4,32 s
99.999% ("пет деветки")	**5,26 min**	**1.31 min**	**26,30 s**	**6,05 s**	**864,00** ms
99.9999% ("шест деветки")	**31,56 s**	**7.89 s**	**2,63 s**	**604,80 ms**	**86.40 ms**
99.99999% ("седам деветки")	**3,16 s**	**0,79 s**	**262,98 ms**	**60,48 ms**	**8,64 ms**
99.999999% ("осам деветки")	**315,58 ms**	**78,89 ms**	**26,30 ms**	**6,05 ms**	**864,00 µs**
99.9999999% ("девет деветки")	**31,56 ms**	**7,89 ms**	**2,63 ms**	**604,80 µs**	**86.40 µs**

Одабране мере заштите су повезане са ризичним догађајем који може настати, као и са њима повезаним негативним финансијским последицама по пословање. Зато је неопходно да Регистар ризика обухвати и ИТ ризике, обзиром да се пословање не може ни замислити без употребе информационог система.

У оквиру налаза 2.1 дат је пример из праксе, где се види да у случају штетног догађаја, ЈППС треба да за систем и сваки подсистем одреди ниво доступности из табеле 2. Тај ниво доступности треба да обезбеде све имплементиране превентивне контроле, како опрема, комуникациона инфраструктура, увежбаност запослених, итд.

Главна последица непрепознавања ИТ ризика је неспремност на инциденте, непостојање превентивних мера које могу умањити или спречити негативне последице по функционисање информационог система, умањењем прихода и стварање непланираних расхода.

Препорука: Препоручујемо одговорним лицима да успоставе механизам динамичког управљања ризиком дефинисањем индикатора за дневно праћење стања и да редовно извештавају о стању информационе безбедности.

Налаз 3.2: Ефикасност управљања ИТ имовином услед недостатка података о безбедносном аспекту и децентрализацији надлежности над мерама информационе заштите је умањена, услед чега се ствара ризик од неблаговремене комуникације, успореног реаговања на малициозне нападе, могућег уништавања података и/или неовлашћеног објављивања података и информација.

Идентификовање информационих добара и одређивање одговорности за њихову заштиту уређено је Актом[62], у ставу 2.5. где су одређене опште смернице на нивоу полисе (политике). Одређено је шта обухватају информациона добра: рачунарска опрема (која обухвата рачунаре, сервере, свичеве, мобилне уређаје и носаче података); софтвер; базе података; техничка и пројектна документација; општа документација и ИМС документација. Рачуноводствена евиденција се заснива на улазним документима која не садрже неопходне елементе за правилно разврставање опреме, употребу те евиденције за ИТ послове, и за обезбеђивање информационе имовине неопходно је водити евиденцију са безбедносног становишта. Мрежна опрема као што су свичеви, рутери, мрежне баријере (енг. Firewall), медија конвертери, приступне тачке за бежични приступ (енг. Wireless AP), итд.

ЈППС не може штитити ИТ имовину за коју нема података о мерама заштите, рачуноводствена евиденција не располаже подацима о технолошком решењу и које рањивости она поседује. Управљање ИТ имовином игра критично важну улогу у безбедносном надзору, реаговању на инциденте, резервним копијама података, опоравку делова или целог система.

[62] Акт о безбедности информационо-комуникационог система од посебног значаја ЈППС, 31.5.2017, допуна бр. 953-4322 од 18.02.2021. године

ЈППС треба да зна који подаци где се налазе на којој опреми, на којој локацији, ко јој има право приступа, и колико је важан ИТ систем, рачунар, сервер за остваривање пословних резултата.

Мрежна опрема информационог система ЈППС путем које се приступа свим подсистемима иако се физички налази на локацијама предузећа, не представља логичку целину и не управља се централизовано. Опрема која је застарела, 5% рачунара са оперативним системом Windows 7, нема подршку произвођача и ствара ризик да буде основни вектор за малициозне нападе на ИТ имовину.

Одељење за одржавање управљачко информационих система води евиденцију са припадајућим елементима: рбр, спрат, канцеларија, име, презиме, сектор, инвентарски број, тип и модел, као рачуноводствену аналитику и нису обухваћени елементи неопходни за процену и праћење ризика. Поред рачунарске опреме, рачунарског софтвера, мрежне опреме, аудио комуникационе опреме, видео надзора, алармних система, база података, корисничких налога, администраторских налога, добављача услуга одржавања или других права приступа одређеном систему, тј. опреми треба да буде основ те евиденције за потребе информационе сигурности, пружања подршке корисницима, омогућавања приступа добављачима и физичког обезбеђивања у крајњем случају.

Управљање ИТ имовином обухвата праћење, управљање и оптимизовање ИТ имовине, укључује хардвер, софтвер, мрежну опрему, и друге компоненте информационих технологија. Ове активности обухватају следеће:

- **Прописе**: уређење интерним актима за управљање ИТ имовином, укључујући радне процедуре, процедуре заштите, и друге интерне акте;
- **Обуке**: Запослени морају имати потребно знање и свест о политикама и процедурама везаним уз ИТ имовину и како се правилно користе;
- **Инвентар**: праћење ИТ имовине, укључујући рачунарску опрему, мобилне уређаје, штампаче, сервере, мрежну опрему, лиценцирани софтвер и друге ИТ компоненте, ко их користи, стање исправности, одржавање, чување, итд.;
- **Лиценце и апликације**: праћење софтверских лиценци, управљање њиховим обновама и обезбеђивање да се користе у складу с условима лиценцирања;
- **Одржавање и надоградња**: управљање одржавањем ИТ имовине како би се осигурала поузданост и сигурност. Ово укључује надоградње хардвера и софтвера када је то потребно;
- **Безбедност**: ИТ имовина мора да буде заштићена од претњи, укључујући антивирусну заштиту, мрежне баријере, ажурирање конфигурација, заштита ИТ ресурса од оштећивања, крађе, злоупотребе, заштита личних података и безбедност података и софтвера;
- **Праћење перформанси**: праћење перформанси ИТ система како би се обезбедило да раде ефикасно и да испуњавају тражене захтеве;
- **Планирање капацитета**: предвиђање будућих потреба за ИТ ресурсима на основу анализе трендова потрошње и планирање набавки нових ресурса када је то потребно;
- **Оптимизација трошкова**: Оптимизација трошкова, укључујући праћење трошкова лиценци, потрошње енергије, одржавање и други оперативни трошкови.

Оператор ИКТ система је дужан да идентификује и класификује информациона добра, односно средства и имовину, путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИКТ систему, изврши попис информационих добара, односно

средстава и имовине, и успостави, одржава и редовно ажурира њихову евиденцију.[63]

Оператор ИКТ система је дужан да класификацију врши према степену осетљивости и критичности, узимајући у обзир могуће последице нарушавања поверљивости, интегритета и расположивости добара, да доследно примењује ту класификацију, као и да, у складу с тим, обезбеди адекватан ниво заштите ових добара. За свако информационо добро, односно средство и имовину, потребно је одредити задужено лице за њихову заштиту.[64]

Приступ ИТ имовини (серверима, апликацијама, базама података итд.) од стране неауторизованих рачунара и корисника може довести до губитка података, неефикасне информационе заштите и застоја у раду, са последицом по приходе и стварањем непланираних расхода.

Препорука: Препоручујемо одговорним лицима да имплементирају механизам управљања ИТ имовином који ће обезбедити неопходне информације у циљу смањења ризика кроз централизацију надлежности над мерама информационе заштите.

Налаз 3.3: ЈППС није у потпуности уредило управљање заштитом информација, података и докумената у информационом систему јер није обухватила све постојеће податке, системе и апликације, одредила степен тајности и мере заштите чиме је створило ризик неовлашћеног приступа, недозвољеног објављивања података, а што за последицу може имати непланиране расходе.

Ограничење приступа подацима и средствима за обраду података подразумева дефинисање прецизних правила приступа тако што се дефинише ко има право чему да приступи и која су ограничења приступа подацима и средствима за обраду података, а водећи рачуна о специфичностима података и опреме и одговорностима и радним задужењима лица која приступају подацима и опреми.[65]

Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа уређено је Процедуром[66] у складу је са Уредбом[67] и Актом[68]. Поступак коришћења електронске поште, коришћење интернета, коришћења информационих ресурса.[69]

ЈППС је донела Акт о информационој безбедности, којег је ажурирала, и којим је уредила питања одобравање овлашћеног приступа давањем смерница која су прописана Уредбом. Делегирањем задатак евиденције о додељеним и одузетим налозима на надлежне администраторе система је уредила Процедуром. Процедуром је уређено питање заштите приступа рачунару, дефинисан приступ пословним апликацијама, базама података и ДИМС[70]. Дефинисани су и услови дефинисања лозинки, процедура поседује дефинисане обрасце као што су: ФМ.422.31 - Картица рачунара; ФМ.422.32 - Захтев за инсталацију софтвера; ФМ.422.33 - Регистар софтвера у коришћењу; ФМ.422.34 - Захтев за овлашћење или одузимање овлашћења;

[63] Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, “Службени гласник РС”, број 94 од 24. новембра 2016. године

[64] Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, "Службени гласник РС", број 94 од 24. новембра 2016. године

[65] Акт о информационој безбедности, став 2.4, 2.8, 2.9, 2.10, 31.5.2017, допуна бр. 953-4322 од 18.02.2021. године

[66] ПР.422.03 – Коришћење и заштита података на рачунарима, бр. 953-20627 од 8.12.2011. године, допуна 12.09.2022. године.

[67] Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, "Службени гласник РС", број 94 од 24. новембра 2016. године

[68] Акт о информационој безбедности, 31.5.2017, допуна бр. 953-4322 од 18.02.2021. године

[69] Коришћење и заштита података на рачунарима 30.11.2011, допуна бр. 953-20627 од 12.09.2023. године.

[70] ДИМС – документи интегрисаном менаџмент система.

ФМ.422.35 - Захтев за промену конфигурације; ФМ.630.11 - Основни идентификациони картон опреме/објекта; и ФМ.422.36 - Регистар рачунара и корисника апликација по организационим целинама – секторима.

ЈППС је у Акту под ставом 2.5. дефинисано је да Одсек за безбедност и заштиту ИКТ система успоставља евиденцију у складу са Процедуром.

Сврха Процедуре о безбедности и заштити ИКТ система је да обезбеди структуриран и доследан приступ заштити информационо-телекомуникационих ресурса ЈППС. Конкретно, сврха процедуре је:

1. **Заштита интегритета података:** Осигурање да подаци остану непромењени и тачни, без неовлашћених измена;
2. **Очување поверљивости:** Спречавање неовлашћеног приступа осетљивим и поверљивим информацијама;
3. **Обезбеђивање доступности**: Осигурање да су подаци и системи доступни овлашћеним корисницима када су им потребни;
4. **Управљање ризицима**: Идентификација, процена и управљање потенцијалним ризицима који могу угрозити информационе системе и податке;
5. **Усклађеност са прописима и стандардима**: Осигурање да ЈППС испуњава све релевантне законе, прописе и стандарде у вези са безбедношћу информација;
6. **Подизање свести и обука**: Обезбеђивање да су сви запослени свесни значаја безбедности информација и да имају потребна знања за заштиту информација и система;
7. **Припрема за инциденте**: Развијање и имплементација планова и процедура за брзи одговор на безбедносне инциденте и опоравак од њих; и
8. **Одржавање континуитета пословања:** Осигурање да критичне функције организације могу да се наставе и у случају озбиљних поремећаја или катастрофа.

Ова процедура помаже ЈППС да умањи ризике, заштити своје ресурсе и одржи висок ниво безбедности информација, што је од суштинске важности за очување поверења корисника и пословних партнера. ЈППС је у Акту под ставом 2.6. описала шему класификације података у општем смислу наводећи три до четири нивоа поверљивости. Наводећи да класификација докумената мора бити усклађена са Процедуром о приступу посебно осетљивим подацима и информацијама у ИКТ систему. Које још нису дефинисане, попуњене за сву опрему, софтвер и кориснике, чиме се ЈППС излаже различитим ризицима који могу негативно утицати на њено пословање и заштиту информационе имовине.

Остварење ризика по ЈППС због некомплетног документовања активности може довести до проблема који могу утицати на различите аспекте пословања и то: немогућности функционисања система интерне контроле, смањења ефикасности и продуктивности, дуплирањем послова, грешкама и пропустима, кашњењу у остваривању циљева, повећању трошкова, губитком прихода, незадовољством корисника услуга, тужбама, казнама и другим правним последицама итд.

Неовлашћени приступ подацима, информацијама и документима, погрешно манипулисање, може имати за последицу недозвољено обелодањивање података и непланиране расходе судских поступака.

Препорука: Препоручујемо одговорним лицима да донесу Процедуру о безбедности и заштити ИКТ система на нивоу предузећа којом би се уредио процес заштите информација, података и докумената у складу и са степеном тајности у информационом систему у циљу јачања укупне безбедности пословања.

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 следеће, 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;

1. 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;
2. 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

Прилог 1 – Методологија у поступку рада

Да бисмо одговорили на ревизорска питања, анализирали смо законску и подзаконску регулативу, стручну литературу, као и све податке добијене од субјекта и извора информација, корисника система. Анализирали смо податке и информације за период од 2021. до 2023. године. Такође смо за поједине анализе користили и податке како из претходног периода тако и податке о функционисању система интерне контроле током спровођења ревизије у 2024. години.

Обављени су састанци са субјектом ревизије, примљена су документа путем портала за документацију, електронском поштом и из јавно доступних извора.

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

- Нематеријални докази (интервјуи, упитници и анкете) од субјекта ревизије и извора информација;
- Документарни докази као писани документи – документација прикупљена од субјекта ревизије, евиденције, статистички подаци, и други извештаји;
- Физички докази – прикупљени обиласком, рачунског центра, корисника система;
- Аналитички докази – анализе рађења на бази добијених одговора на упитник, анализе достављених података главне књиге, друге анализе и обрачуни.

Извршена је квантитативна и квалитативна анализа и након тога се приступило изради извештаја. Применом методолошких правила[71] имајући у виду технолошко решење, више од 10 година употребе система, узимајући у обзир материјалност и ревизијско узорковање за сврхе детаљног испитивања како би донели разумне ревизијске закључке, фокус нам је био на следећим областима: апликативне контроле, план континуитета пословања и опоравка од хаварије, и информационе безбедности.

Апликативне контроле

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 завређују додатну пажњу. [72]

Слика број 10. Систем апликативних контрола

Примењујући методологију из Приручника за ИТ ревизију IDI/INTOSAI обавили смо тестирање апликативних контрола улаза података у систем, обраде података, излаза података из система и безбедност података.

[71] Државна ревизорска институција, (2019), Методолошка правила и смернице за ИТ ревизију, Београд.
[72] WGITA – IDI/INTOSAI, (2022), Приручник за ИТ ревизију врховних ревизорских институција, IFPP (issai.org).

Информациони систем обухвата: улаз —за улазне податке и документе; обрада — која обрађује унете податке примењујући математичка и логичка правила; излаз — где се појављују резултати обраде у виду екранског приказа, штампаног извештаја, итд. Посебан аспект је заштита — података, информација и/или целокупног система. Информациони системи су повезани на интернет када су изложени ризицима од губитка података, крађе, неовлашћене промене, као и других видова злоупотребе.

Апликативне контроле су јединствене за сваку ИТ апликацију. Када се пословни процеси аутоматизују у ИТ апликацији, уграђена пословна правила у виду апликативних контрола треба да обезбеде комплетност, тачност, валидност, поверљивост и доступност трансакција и података у току обраде.

- **Контрола комплетности** треба да пруже разумно уверавање да су све трансакције које су се десиле унете у систем, прихваћене за обраду, обрађене једном и само једном од стране система и правилно укључене у излаз;
- **Контроле тачности** треба да пруже, између осталог, разумно уверавање да су трансакције правилно евидентиране, са тачним износом/подацима и благовремено.
- **Контроле валидности** треба да пруже разумно уверавање да су све евидентиране трансакције стварно настале, да се односе на организацију и да су прописно одобрене у складу са овлашћењем руководства; и да су искази и извештаји засновани само на валидним подацима;
- **Контроле поверљивости** треба да пруже разумно уверавање да су подаци и извештаји апликације и други резултати заштићени од неовлашћених приступ.
- **Контроле доступности** треба да пруже разумно уверавање да су апликација, подаци, извештаји и друге пословне информације лако доступне корисницима када су потребна.

Слика број 11. Апликативне контроле према системској функционалности

Контрола улаза	▪ Унос података/провере поља (нпр. валидација унетих бројева, датума …); ▪ Управљање изворним документима (нпр. процедуре припреме и чувања); ▪ Механизми за руковање грешкама (поруке о грешци, обустављене датотеке, игнорисани подаци); ▪ Давање овлашћења за унос података (нпр. подела дужности);
Контроле обраде	▪ Мапирање пословних правила; ▪ Провере интегритета и комплетности, извештај о неравнотежи; ▪ Аутоматизовани прорачуни; ▪ Улазна усаглашавања;
Контрола излаза	▪ Потврђивање комплетности и тачности, усаглашавање; ▪ Преглед и праћење резултата; ▪ Преглед и праћење извештаја о изузетцима генерисаним у апликацији; ▪ Процедуре обележавања, руковања, задржавања и дистрибуције излаза;
Контроле заштите података	▪ Механизми надзора (ревизијски трагови, преглед евиденције, употреба јединствених идентификатора); ▪ Логичка контрола приступа функционалностима и подацима апликације; ▪ Заштита сачуваних података.

Методом узорковања на основу достављених база података одабрали смо наплатне станице са највећим прометом возила, детектована необична извештавања и репрезентативне примерке како би се уверили да се управља и контролише на адекватан начин.

Управљање континуитетом пословања

Ревизорски тим је предузео низ активности да би се уверио у ефикасност Плана континуитета пословања (ПКП). Прегледао је достављену документацију повезану са ПКП, што

је ажурирано Упутство за континуитет пословања и Процедуре које уређују питања из области континуитета пословања. Интервјуисали смо руководиоце и особље одговорним за ПКП, особље одговорно за безбедност и управљање ризицима. Нисмо тестирали функционисање у симулираним ситуацијама, и нисмо верификовали да ли су сви запослени упознати са својим улогама у оквиру ПКП. Ове активности су помогле ревизорском тиму да процени ефикасност Плана континуитета пословања и да предложи побољшања која ће обезбедити да ЈППС може брзо и ефикасно да реагује на неочекиване и штетне догађаје. Доступност и исправан рад ИТ система је од кључног значаја за способност пословних организација да испуне своје пословне обавезе у складу са законом. Ови системи играју важну улогу у тако разноврсним активностима као што су процена и наплата пореза и царинских прихода; исплата државних пензија и социјалних давања; и у обради националних статистика (нпр. рођени, умрли, криминал и болести). У ствари, многе активности се не могу ефикасно спровести — ако уопште — без подршке информационих система. Да би ограничиле прекиде и застоје ових система, организације треба да развију стратегију планирања континуитета и повезане процедуре.

Иако се сви ови догађаји не могу избећи, планирање континуитета често може ограничити утицај ових неочекиваних догађаја. Губитак струје, пожар и злонамерна оштећења могу имати катастрофалне ефекте на информационе системе. Организацији може бити потребно много недеља да настави са ефикасним пословањем ако нема изводљив план континуитета. Поред тога, многе ИТ операције се често поверавају спољним добављачима услуга. Ако су операције код спољног пружаоца услуга поремећене због хаварије, то такође може имати негативан ефекат на организацију.

Да би спречиле могуће прекиде услуга због познатих ризика, организације треба да спроводе различите активности управљања континуитетом пословања како би помогле у спречавању поремећаја услуга, укључујући **планирање континуитета пословања, планирање опоравка од хаварије** и **планирање непредвиђених ситуација информационог система**, између осталог. Термини планирање континуитета пословања и планирање опоравка од хаварије понекад се користе као синоними, али су у ствари два различита, али комплементарна термина. Оба су важна за ИТ ревизора, јер заједно обезбеђују да организација може да ради са одређеним капацитетом након природног или вештачког поремећаја. Планирање непредвиђених ситуација информационог система је слично планирању опоравка од хаварије, али се фокусира на опоравак система без обзира на локацију система. Услови су додатно објашњени у наставку:

Планирање континуитета пословања је процес који организација користи за планирање и тестирање опоравка својих пословних процеса након прекида. Такође описује како ће организација наставити да функционише у неповољним условима који могу настати (на пример, природне или друге хаварије, или чак у одсуству кључног особља). Крајњи циљ планирања континуитета пословања је да организација створи најотпорнију могућу организацију. Ово укључује континуиране функције критичне за мисију у сваком тренутку током било које врсте хаварије или поремећаја.

Планирање опоравка од хаварије је процес планирања и тестирања за опоравак ИТ инфраструктуре након природне или друге хаварије. Комплементарно је планирању континуитета пословања. Планирање континуитета пословања примењује се на организационе пословне функције, док се планирање опоравка од хаварије примењује на ИТ инфраструктуру која подржава пословне функције.

Планирање непредвиђених ситуација информационог система је процес планирања и тестирања за опоравак појединачних информационих система. Ово је такође додатак планирању континуитета пословања и бави се опоравком једног система. Планирање

непредвиђених ситуација информационог система је замишљено да буде водич за опоравак система и може се активирати за тај систем без обзира на локацију.

Информациона безбедност

Информациона безбедност (Information security) 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[73].

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[74].

Према одредбама члана 7 Закона о информационој безбедности оператор ИКТ система од посебног значаја одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система. Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидента, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима[75]. Мере заштите ИКТ система су у Закону о информационој безбедности подељене на 28 мера заштите[76]. 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.

Губитак напајања, хаварија, ватра и злонамерна оштећења могу имати катастрофалне последице на рачунарским системима. Може потрајати неколико недеља да организација настави са ефективним пословним операцијама ако немају успешан план континуитета пословања. Појмови План за континуитет пословања и план опоравка од хаварије се понекад користе као синоним, али су заправо два различита али комплементарна појма.

Слаба безбедност информација може довести до делимичне или потпуне штете на имовини, као и до:

- Кршења прописа;
- Плаћања казни, одштета, непланираних трошкова поправке или рестаурације података;
- Смањење ефективности и/или ефикасности целе услуге и незадовољства јавности;
- Губитка или крађе нематеријалне имовине, рачунарских ресурса и опреме;
- Неовлашћен приступ и откривање, модификацију или уништавање осетљивих информација, које могу бити личне, или класификоване информације;
- Хаковање и криптовање података са уцењивањем плаћања откупнине;
- Прекид основних функционалности које подржавају критичну инфраструктуру, националну одбрану или хитне службе;

[73] Члан 2 став 1 тачка 3 Закона о информационој безбедности.
[74] WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions.
[75] Члан 7 став 2 Закона о информационој безбедности.
[76] Члан 7 став 3 Закона о информационој безбедности.

- Подривање рада организације, нарушавање угледа и поверења јавности у локалну или државну управу;
- Коришћење рачунарских ресурса у неовлашћене сврхе или за покретање напада на друге системе; и
- Оштећење мрежа и опреме.

Ова штета може бити узрокована:
- Неовлашћени упади у ИКТ систем;
- неовлашћене приступи систему путем удаљеног приступа (ВПН, итд.);
- објављивање информација — откривање осетљивих информација неовлашћеним странама. Један пример како се то може догодити је познат као друштвени инжењеринг, што је техника манипулације коришћена од стране нападача који се ослања на основни људски инстинкт поверења;
- инсајдер претње — од стране запослених који имају овлашћени приступ једним информацијама, и покушавају добити приступ њима не дозвољеним информацијама, ради приступа, обелодањивања или наношења друге штете; и
- системске рањивости — употреба застарелих оперативних система и софтвера који поседују грешке које се могу злоупотребити од стране нападача.

Како је тешко аутоматизовати ефикасну заштиту информационе имовине, и сви вектори напада иду преко запослених, што их чини најслабијом кариком у систему безбедности неопходно је перманентно предузимати активности на јачању безбедносне културе запослених.
Кључни елементи безбедносне организационе културе су:
- **Стварање свести о информационој безбедности.** Ово се састоји од општих активности подизања свести о безбедности информација и циљаних едукативних сесија за запослене. Ове сесије су добре прилике за почетак увођења одговорности у области безбедности информација. Служба људских ресурса може бити одговорна за почетну обуку о подизању свести за нове запослене. Обука треба да се настави током запослења па све до престанка рада да би се увек унапредила свест о безбедности.
- **Посвећеност руководства.** Посвећеност руководства је важна компонента у формирању организационе културе информационе безбедности. Посвећеност од стране руководства се не огледа само у изради формалне документације, усвајању интерних аката о безбедности информација и безбедносним политикама, него и активним укључивањем у спровођењу мера безбедности. Ако руководство не подржава истински програм информационе безбедности, то може обесхрабрити запослене да осећају обавезу или одговорност према програму. Због тога је од кључне важности да руководство прихвати одговорност за безбедност информација и у потпуности подржи програм за јачање информационе безбедности.
- **Јачање координације и размене информација свих тимова**. Како информациона безбедност укључује многе аспекте организације рада она захтева и координацију напора свих учесника у пословним процесима. Јачање хоризонталне комуникације између организационих делова и добављача услуге, подразумева размену информација и координацију активности, посебно важним у случају појаве безбедносних инцидената.

Треба имати у виду да свака пословна организација која управља критичном инфраструктуром има обавезу примене и Закона о информационој безбедности, а то подразумева да: упише ИКТ систем од посебног значаја којим управља у евиденцију оператора ИКТ система од посебног значаја; предузме мере заштите ИКТ система од посебног значаја; донесе акт о безбедности ИКТ система; врши проверу усклађености примењених мера заштите ИКТ система са актом о

безбедности ИКТ система и то најмање једном годишње; уреди однос са трећим лицима на начин који обезбеђује предузимање мера заштите тог ИКТ система у складу са законом, уколико поверава активности у вези са ИКТ системом од посебног значаја трећим лицима; доставља обавештења о инцидентима који значајно угрожавају информациону безбедност ИКТ система; и достави тачне статистичке податке о инцидентима у ИКТ систему.

Уредбом о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја[77] дефинисане су групе инцидената које су оператори ИКТ система од посебног значаја дужни да пријављују надлежном CERT-у, као што се може видети у следећој табели.

Табела 3. Листа група и врста безбедносних инцидената

Група инцидената	Врста инцидента
Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. „malware”)	Вирус
	Црв(енгл. „worm”)
	Рансомвер(енгл. „ransomware”)
	Тројанац
	Шпијунски софтвер(енгл. „spyware”)
	Руткит(енгл. „rootkit”)
Неовлашћено прикупљање података	Скенирање портова
	Пресретање података између рачунара и сервера(енгл. „sniffing”)
	Социјални инжењеринг(лажно представљање и други облици)
	Компромитовање или цурење података(енгл. „data breaches”)
Превара	Фишинг(енгл. „phishing”)
	Неовлашћено коришћење ресурса(енгл. „cryptojacking” и други облици)
Покушаји упада у ИКТ систем	Покушај искоришћавања рањивости система
	Покушај откривања креденцијала(енгл. „brute force attack”, „dictionary attack” и сл.)
Упад у ИКТ систем	Откривање или неовлашћено коришћење привилегованих налога(енгл. „privileged account compromise”)
	Откривање или неовлашћено коришћење непривилегованих налога(енгл. „unprivileged account compromise”)
	Неовлашћени приступ апликацији
	Мрежа заражених уређаја(енгл. „botnet”)
Недоступност или ограничена доступност ИКТ система	Напад са циљем онемогућавања или ометања функционисања ИКТ система(енгл. „denial-of-service attack” – DoS)
	Дистрибуирани напад са циљем онемогућавања или ометања функционисања ИКТ система(енгл. „distributed denial-of-service attack” – DDoS)
	Саботажа
	Прекид у функционисању система или дела система(енгл. „outage”)
Угрожавање безбедности података	Неовлашћен приступ подацима
	Неовлашћена измена или брисање података
	Криптографски напад
Оперативни инциденти	Отказивање хардверских компоненти
	Проблеми у раду са софтверским компонентама
Инциденти физичко-техничке безбедности	Крађа хардверских компоненти
	Пожар
	Поплава
Остали инциденти	Инциденти који не спадају у горе наведене категорије

Извор: Уредба о поступку обавештавања о инцидентима у ИКТ системима од посебног значаја

[77] Уредба о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја ("Службени гласник РС", број 11 од 7. фебруара 2020);

Прилог 2 – Пример добре праксе ангажовања добављача у области информационе безбедности

Контекст

Јавно предузеће „Путеви Србије“ (даље ЈППС) обавља делатност управљања државним путевима, као делатност од општег интереса, која обухвата: коришћење државног пута (организовање и контрола наплате накнаде за употребу државног пута, вршење јавних овлашћења и сл.), заштита државног пута; вршење инвеститорске функције на изградњи и реконструкцији државног пута; организовање и обављање стручних послова на изградњи, реконструкцији, одржавању и заштити државног пута; уступање радова на одржавању државног пута; организовање стручног надзора над изградњом, реконструкцијом, одржавањем и заштитом државног пута; планирање изградње, реконструкције, одржавање и заштита државног пута; означавање државног пута и вођење евиденције о државним путевима и о саобраћајно - техничким подацима за те путеве, као и управљање саобраћајем и организовање и обављање бројања возила на државном путу.

За те послове употребљавају се:

1. Информациони систем наплате путарине;
2. Пословни информациони систем предузећа Hermes-MEGA (финансијска служба, архива и писарница);
3. Информациони систем везан за базе података предузећа (базе података о путевима, базе података о саобраћају, географско-информациони систем ГИС);
4. Информациони систем за надзор праћење и управљање саобраћајем (ИТС систем);
5. Информациони систем за контролу и управљање напајања електричном енергијом - Телеменаџмент;
6. Као и други информациони системи попут мејл, веб, VPN сервера итд.

ЈППС је суочено са растућим бројем сајбер претњи и потребом за бољом заштитом својих информационих система. Одлучено је да се ангажују два специјализована добављача услуга у области информационе безбедности: један за антивирусну заштиту корисничких рачунара и мејл сервера, и други за мониторинг и надзор над укупном информационом заштитом информационе имовине.

Дефинисање проблема

- Учестале сајбер претње, укључујући малвер и фишинг нападе, угрожавале су безбедност корисничких рачунара и мејл сервера.
- Недостатак централизованог мониторинга и надзора отежавао је брзу детекцију и реаговање на инциденте.

Слика број 12. Информациона безбедност предузећа

Решење

Ангажовање два специјализована добављача услуга:

1. Добављач антивирусне заштите:
   - Изабран је добављач „А“ због њихове стручности у пружању напредне антивирусне заштите.
   - Спровођење антивирусне заштите за све корисничке рачунаре и мејл сервере, редовна ажурирања и скенирања.
2. Добављач мониторинга и надзора:
   - Изабран добављач „Б“ за централизовани мониторинг и надзор над укупном информационом заштитом.
   - Увођење система за детекцију и превенцију упада (IDS/IPS), праћење активности у реалном времену и реаговање на инциденте.

Имплементација

- Детаљна анализа потреба компаније и дефинисање захтева за оба добављача.
- Спровођење тендера и избор добављача на основу њихових референци и техничких могућности.
- Координисана имплементација антивирусне заштите и мониторинг система.
- Обука запослених и успостављање канала за брзу комуникацију са добављачима.

Резултати

1. Побољшана антивирусна заштита:
   - Смањен број заражених уређаја за 80%.
   - Повећана свест корисника о безбедности захваљујући редовним ажурирањима и скенирањима.
2. Побољшан мониторинг и надзор:

- Бржа детекција и реаговање на претње (смањено време реакције са неколико сати на неколико минута).
- Побољшана видљивост над мрежним активностима и смањен број успешних напада.
- Редовна извештавања и анализа података о безбедносним инцидентима.

Закључак

Ангажовање два специјализована добављача услуга омогућило је ЈППС да значајно побољша своју информациону безбедност. Ова стратегија је показала да комбиновање специјализованих решења може довести до свеобухватније и ефикасније заштите информационих система.

Кључне тачке добре праксе

- Јасна дефиниција потреба: Пре ангажовања добављача, компанија је прецизно дефинисала своје потребе и захтеве.
- Пажљив избор добављача: Избор је базиран на техничким могућностима и референцама добављача.
- Координисана имплементација: Имплементација је извршена у координацији са оба добављача, уз континуирану комуникацију.
- Континуирана обука и подршка: Запослени су редовно обучавани, а подршка је обезбеђена 24/7.
- Мониторинг и анализа резултата: Редовно праћење резултата и прилагођавање стратегија на основу анализе података.

Овај пример добре праксе илуструје како компанија може ефикасно користити специјализоване услуге за побољшање своје информационе безбедности. Ангажовање два добављача услуга за антивирусну заштиту и централизовани мониторинг омогућило је да значајно смањи број безбедносних инцидената и побољша укупну безбедност својих информационих система.