



ДРЖАВНА
РЕВИЗОРСКА
ИНСТИТУЦИЈА

ИЗВЕШТАЈ
О РЕВИЗИЈИ СВРСИСХОДНОСТИ ПОСЛОВАЊА
Информациони систем у јавном
градском превозу у граду Новом
Саду

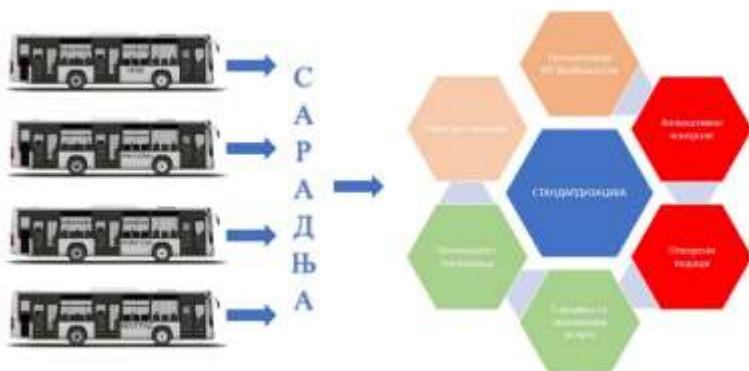


Број: 400- 488/2023-07/37
Београд, 25. децембар 2023. године



Потребно је да Јавно градско саобраћајно предузеће Нови Сад успостави сарадњу са градским управама и градским предузећима које врше услугу јавног градског превоза у Републици Србији, у циљу покретања заједничке иницијативе ка стандардизацији информационих система у јавном градском превозу, што је кључни корак ка пружању бољих и свеобухватнијих услуга грађанима и успостављању неопходне поузданости система

Информациони системи који се односе на јавни градски превоз треба да имају две основне функције: контролу наплате карата и контролу пружених услуга од стране превозника како би се плаћање вршило у складу са квалитетом и квантитетом пружених услуга, које се користе за побољшање ефикасности, као и за пружање информација путницима. У досадашњем коришћењу ових система, у Србији је утврђено да приступ системима и базама података имају и пружаоци услуга, није обезбеђен континуитет пословања у случају раскида сарадње, нису успостављени сви механизми који обезбеђују контролу наплате карата и пружених услуга када су у питању превозници, обрада података о личности није уређена на прописан начин јер базе података у овим системима могу садржати осетљиве личне податке (за месечне карте прикупљају се подаци из личне карте) и изискују примену одређених мера заштите.



Информациону безбедност треба успоставити на свеобухватан начин, што подразумева: управљање ИТ ризицима и ИТ инцидентима, успостављање адекватне организационе ИТ структуре, усвајање, ажурирање и примену одговарајућих правилника, политика и процедура у области информационе безбедности, управљање приступом системима и управљање процесом континуитета пословања, што је неопходно како би била осигурана поузданост система.

Потребно је унапредити **механизам сарадње са пружаоцима услуга** имплементирањем правила и процедура када је у питању ова област, усвајањем плана континуитета пословања у случају раскида сарадње и успостављањем процеса обраде података о личности на начин прописан законом.

Успостављен **механизам употребе апликативних контрола** омогућава контролу података када је у питању продаја карата и праћење кретања возила, и услуге грађанима у смислу информисања и интеграцију са другим информационим системима.

Препоруке

Након спроведене ревизије, Државна ревизорска институција је Јавном градском саобраћајном предузећу Нови Сад, између осталих, дала следеће препоруке:

- да уреди процес приступа систему, што подразумева усвајање процедура које уређују овај процес и контролу тог процеса, а односи се на логички приступ и рад на даљину.
- да успостави свеобухватан план континуитета пословања у ванредним околностима, што подразумева ажурирање постојећег Акта о безбедности ИКТ система, усвајање процедуре за континуитет пословања у ванредним околностима и управљање резервним копијама података, као и план континуитета пословања у случају раскида сарадње са пружаоцима услуга,
- да уреди сарадњу са пружаоцем услуга када је у питању заштита и обрада података, на начин прописан Законом о заштити података о личности,
- успостави организацију информационе безбедности која обухвата усвајање, ажурирање и имплементацију акта о информационој безбедности, процедура које се односе на ИТ безбедност, управљање инцидентима, и адекватну организациону структуру ИТ безбедности, како би биле примењене све неопходне мере безбедности и заштите података.
- да успостави управљање ИТ ризицима, што подразумева евидентирање, анализу, класификацију ИТ ризика и дефинисање стратегије за



Садржај

I Резиме откривених несврхисходности, препорука и мера предузетих у поступку ревизије	6
II Увод	11
1. Проблем	11
2. Циљ ревизије	11
3. Ревизорска питања	12
4. Обим и ограничења ревизије	14
5. Методологија у поступку рада	14
III Опис предмета ревизије	15
1. Законодавни и институционални оквир	16
2. Информациони системи BusLogic	24
IV Закључци	27
ЗАКЉУЧАК 1: Информациона безбедност није успостављена на свеобухватан начин јер нису усвојене и примењене мере заштите које обухватају управљање ИТ ризицима и ИТ инцидентима, успостављање адекватне организационе ИТ структуре, усвајање, ажурирање и примену одговарајућих правилника, политика и процедура у области информационе безбедности, управљање приступом системима и управљање процесом континуитета пословања, што је неопходно како би била осигурана поузданост система.	27
Налаз 1.1: Јавно градско саобраћајно предузеће Нови Сад није у потпуности успоставило организацију ИТ безбедности	27
Налаз 1.2: Јавно градско саобраћајно предузеће Нови Сад није успоставило процес приступа систему на задовољавајући начин.	32
Налаз 1.3: Јавно градско саобраћајно предузеће Нови Сад није успоставило план континуитета пословања у ванредним околностима	35
Налаз 1.4: Јавно градско саобраћајно предузеће Нови Сад није успоставило управљање ИТ ризицима	38
ЗАКЉУЧАК 2: Није успостављен ефективан механизам сарадње са пружаоцима услуга, зато што нису усвојена и имплементирана правила и процедуре када је у питању ова област, није обезбеђен континуитет пословања у случају раскида сарадње и није процес обраде података о личности уређен на начин прописан законом	40
Налаз 2.1: Јавно градско саобраћајно предузеће Нови Сад није у потпуности процедурама и другим актима уредило сарадњу са пружаоцем услуга	40
Налаз 2.2: Јавно градско саобраћајно предузеће Нови Сад није у потпуности уредило сарадњу са пружаоцем услуга када је у питању заштита и обрада података	41
Налаз 2.3: Јавно градско саобраћајно предузеће Нови Сад нема план континуитета пословања у случају раскида сарадње са пружаоцем услуга	44
ЗАКЉУЧАК 3: Успостављен механизам употребе апликативних контрола омогућава контролу података када је у питању продаја карата и праћење	



кретања возила, и услуге грађанима у смислу информисања и интеграцију са другим информационим системима 46

Налаз 3.1: У Јавном градском саобраћајном предузећу Нови Сад апликативне контроле које се користе за продају карата омогућавају ажурну евиденцију дневних пазара и броја продатих карата, као и извештавање 46

Налаз 3.2: У Јавном градском саобраћајном предузећу Нови Сад апликативне контроле које се користе за праћење возила омогућавају ажурну контролу кретања, као и информисање грађана путем система НСМАРТ 46

V Прилог 47

Прилог 1. Методологија у поступку рада 47



Скраћенице и термини

Табела број 1: Најчешће коришћене скраћенице у извештају

Пун назив	Скраћеница
Информационе технологије	ИТ
Информациони систем	ИС
Информационо-комуникациони систем	ИКТ систем
Јединица локалне самоуправе	ЈЛС
Јавно градско саобраћајно предузеће	ЈГСП
Општа регулатива о заштити података о личности (General Data Protection Regulation)	ГДПР
Државна ревизорска институција	ДРИ



I Резиме откритених несврсисходности, препорука и мера предузетих у поступку ревизије

Државна ревизорска институција је спровела ревизију сврсисходности пословања „Информациони систем у јавном градском превозу“.

Информациони системи у локалним самоуправама који се односе на јавни градски превоз треба да имају две основне функције: контролу наплате карата и контролу пружених услуга од стране превозника како би се плаћање вршило у складу са квалитетом и квантитетом пружених услуга.

Циљ ревизије је да се оцени ефективност и ефикасност информационих система у локалним самоуправама који се односе на јавни градски превоз, односно да се испита у којој мери су примењене мере испуниле неопходне циљеве када је у питању управљање системима, поузданост информационих система и управљање подацима корисника – грађана, као и да се испита у којој мери систем омогућава ефикасност контроле наплате и плаћања услуга превоза. Поузданост електронских података и информационих система подразумева интегритет, комплетност, тачност, конзистентност и очување података, безбедност информационог система и континуитет пословања, имајући у виду сврху за коју се ти подаци и системи користе.

У Новом Саду, услугу градског превоза пружа Јавно градско саобраћајно предузеће Нови Сад. Када је информациони систем у питању, пружалац услуге је BusLogic DOO, Пожаревац. Систем је имплементиран 2020. године и у досадашњем периоду нису спроведене ни интерна ни екстерна ревизија овог система. Систем се засад користи за евиденцију пружених услуга од стране превозника, али не и за евиденцију персонализованих картица, јер не постоје електронске персонализоване карте.

Обухваћена су четири највећа града у Србији која, са једне стране – имају највећи број становника у земљи, а са друге стране – имају процентуално највећи број грађана – корисника градског превоза, у односу на укупан број у Србији, а у овом извештају је представљен део који се односи на Јавно градско саобраћајно предузеће Нови Сад.

Након спроведене ревизије утврдили смо:

Потребно је да Јавно градско саобраћајно предузеће Нови Сад успостави сарадњу са градским управама и градским предузећима која врше услугу јавног градског превоза у Републици Србији, у циљу покретања заједничке иницијативе ка стандардизацији информационих система у јавном градском превозу, што је кључни корак ка пружању бољих и свеобухватнијих услуга грађанима и успостављању неопходне поузданости система

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

1. Информациона безбедност није успостављена на свеобухватан начин јер нису усвојене и примењене мере заштите које обухватају управљање ИТ ризицима и ИТ инцидентима, успостављање адекватне организационе ИТ структуре, усвајање, ажурирање и примену одговарајућих правилника, политика и процедура у области информационе безбедности, управљање приступом системима и управљање процесом континуитета пословања, што је неопходно како би била осигурана поузданост система.

Организација ИТ безбедности у Јавном градском саобраћајном предузећу Нови Сад, због недостатка довољно стручног знања и недостатка кадровских капацитета, није успостављена тако да обухвата примену адекватних докумената која уређују ову област,



управљање инцидентима и адекватну организациону структуру ИТ безбедности, што за последицу има већи степен рањивости информационог система (Препорука број 1).

У Јавном градском саобраћајном предузећу Нови Сад процес приступа није успостављен на задовољавајући начин, због тога што нису усвојене процедуре које уређују овај процес и није успостављена контрола тог процеса, иако је то законска обавеза, што за последицу може имати угрожену безбедност података (Препорука број 2).

Јавно градско саобраћајно предузеће Нови Сад, због недовољно финансијских средстава па самим тим и недовољно хардверских ресурса, недовољно искуства, стручног знања и обученог ИТ кадра, није усвојило ни имплементирало правила и процедуре за континуитет пословања, иако је то и законска обавеза, што за последицу може имати нефункционисање система у неодређеном временском периоду, па самим тим и отежано пружање услуга (Препорука број 3).

Јавно градско саобраћајно предузеће Нови Сад није успоставило управљање ИТ ризицима, што за последицу може имати стварање непотребно великих трошкова у случају настанка нежељеног догађаја који се могао спречити или великих нефинансијских губитака (нпр. података) због неблаговременог предузимања мера. Нарочито када се документација налази у електронском облику (Препорука број 4).

2. Није успостављен ефективан механизам сарадње са пружаоцима услуга, зато што нису усвојена и имплементирана правила и процедуре када је у питању ова област, није обезбеђен континуитет пословања у случају раскида сарадње и процес обраде података о личности није уређен на начин прописан законом

Јавно градско саобраћајно предузеће Нови Сад није у потпуности процедурама и другим актима уредило сарадњу са пружаоцем услуга, што за последицу има већи степен рањивости информационог система (Препорука број 5).

Јавно градско саобраћајно предузеће Нови Сад није у потпуности уредило сарадњу са пружаоцем услуга када је у питању заштита и обрада података, у смислу успостављања механизма којим се осигурава да је пружалац услуге усвојио услове за заштиту и безбедност података и да их спроводи, као и начина на који се прати реализација извршења уговора и на начин прописан Законом о информационој безбедности и Законом о заштити података о личности што за последицу има смањени степен поузданости система (Препорука број 6).

Јавно градско саобраћајно предузеће Нови Сад нема план континуитета пословања у случају раскида сарадње са пружаоцем услуга што за последицу може имати отежану продају карата, контролу персонализованих карата и онемогућено информисање грађана у дужем временском периоду. (Препорука број 7).

3. Успостављен механизам употребе апликативних контрола омогућава контролу података када је у питању продаја карата и праћење кретања возила, и услуге грађанима у смислу информисања и интеграцију са другим информационим системима.



У Јавном градском саобраћајном предузећу Нови Сад апликативне контроле које се користе за продају карата омогућавају ажурну евиденцију дневних пазара и броја продатих карата, као и извештавање

У Јавном градском саобраћајном предузећу Нови Сад апликативне контроле које се користе за праћење возила омогућавају ажурну контролу кретања, као и информисање грађана путем система HSMART

Након спроведене ревизије „Информациони систем у јавном градском превозу у граду Новом Саду“, Државна ревизорска институција даје следеће препоруке:

Јавном градском саобраћајном предузећу Нови Сад да:

1. успостави организацију информационе безбедности која обухвата усвајање, ажурирање и имплементацију аката која уређују ову област – акта (правилника) о информационој безбедности, процедура које се односе на ИТ безбедност, управљање инцидентима, и адекватну организациону структуру ИТ безбедности, како би биле примењене све неопходне мере безбедности и заштите података. (приоритет 2¹);
2. уреди процес приступа систему, што подразумева усвајање процедура које уређују овај процес и контролу тог процеса, а односи се на логички приступ, рад на даљину и физичку заштиту система. (приоритет 2);
3. успостави свеобухватан план континуитета пословања у ванредним околностима, што подразумева ажурирање постојећег Правилника о безбедности ИКТ система, усвајање процедуре за континуитет пословања у ванредним околностима и управљање резервним копијама података. (приоритет 2);
4. успостави управљање ИТ ризицима, што подразумева евидентирање, анализу, класификацију ИТ ризика и дефинисање стратегије за смањивање/отклањање ризика. (приоритет 2);
5. усвоји/ажурира и имплементира правила и процедуре за безбедност података када је у питању сарадња са пружаоцима услуга што подразумева обавезну примену мера заштите података, и успостављање механизма за праћење примене тих мера. (приоритет 2);
6. уреди сарадњу са пружаоцем услуга када је у питању заштита и обрада података, на начин прописан Законом о информационој безбедности и Законом о заштити података о личности. (приоритет 2);
7. успостави план континуитета пословања у случају раскида сарадње са пружаоцима услуга. (приоритет 2);

¹ ПРИОРИТЕТ 2 – Несврсисходности које је могуће отклонити у року до годину дана



Захтев за достављање одазивног извештаја

Јавно градско саобраћајно предузеће Нови Сад је, на основу члана 40 став 1 Закона о Државној ревизорској институцији, дужно да поднесе Државној ревизорској институцији писани извештај о отклањању откривених несврсисходности (одазивни извештај) у року од 90 дана почев од наредног дана од дана уручења овог извештаја.

Одазивни извештај мора да садржи:

- 1) навођење ревизије, на коју се он односи;
- 2) кратак опис несврсисходности у пословању, које су откривене ревизијом;
- 3) приказивање мера исправљања.

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

Субјект ревизије је у обавези да у одазивном извештају искаже мере исправљања по основу откривених несврсисходности односно свих закључака и налаза датих у Извештају о ревизији сврсисходности пословања, као и да поступи по датим препорукама, осим у случају оних несврсисходности које су отклоњене у току обављања ревизије и које су садржане у поглављу Мере предузете у поступку ревизије. За мере исправљања, дужан је да уз одазивни извештај достави доказе према следећем:

1. За налазе, односно неправилности/несврсисходности првог приоритета, односно које је могуће отклонити у року од 90 дана субјект ревизије је у обавези да достави доказе о отклањању неправилности/несврсисходности односно предузимању мера исправљања;
2. За налазе, односно неправилности/несврсисходности другог приоритета, односно које је могуће отклонити у року до годину дана, и трећег приоритета, односно које је могуће отклонити у року до три године, субјект ревизије обавезан је да достави акциони план у којем ће описати мере и активности које ће бити предузете ради отклањања неправилности/несврсисходности или смањења ризика од појављивања неправилности/несврсисходности у будућем пословању као и планирани период предузимања мера и одговорно лице.

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

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

Сагласно члану 57 став 1 тачка 3) Закона о Државној ревизорској институцији, ако субјект 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 на то 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 институција је овлашћена да предузима мере сагласно члану 40 ст. 7 до 13 Закона о Државној ревизорској институцији.

Генерални државни ревизор

Др Душко Пејовић
Државна ревизорска институција
Макензијева 41
11000 Београд, Србија
25. децембар 2023. године



II Увод

Државна ревизорска институција спровела је ревизију сврсисходности на тему „Информациони систем у јавном градском превозу у граду Новом Саду“. Ревизија је спроведена у складу са Законом о Државној ревизорској институцији², Пословником Државне ревизорске институције³ и Програмом ревизије Државне ревизорске институције за 2023. годину. Поступци ревизије су спроведени у периоду од јуна до новембра 2023. године.

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

1. Проблем

Информациони системи у локалним самоуправама који се односе на јавни градски саобраћај треба да имају две основне функционалности: контролу наплате карата и контролу пружених услуга од стране превозника како би се плаћање вршило у складу са квалитетом и квантитетом пружених услуга.

Базе података у овим системима садрже осетљиве личне податке (за месечне карте прикупљају се подаци из личне карте) и изискују примену одређених мера заштите. Управљање овим системима треба да обухвати све оне мере прописане у циљу успостављања адекватног нивоа информационе безбедности, што је дефинисано Законом о информационој безбедности, Законом о заштити података о личности итд. У досадашњем коришћењу, али и у раније спроведеним ревизијама утврђено је да приступ системима и базама података имају и пружаоци услуга, није обезбеђен континуитет пословања у случају раскида сарадње, нису успостављене све апликативне контроле које обезбеђују контролу наплате карата и пружених услуга када су у питању превозници.

2. Циљ ревизије

Циљ успостављања информационих система у градском превозу је побољшање ефикасности, кроз бољу наплату и анализу података, пружање информација путницима, итд. Потребно је да се оцени ефективност и ефикасност информационих система који се користе за функционисање јавног градског превоза путника.

Изабрана тема је повезана са Циљем 1 из Стратешког плана ДРИ за период 2019-2023, да ће ДРИ одговорити на тренутне и хитне изазове у раду корисника јавних средстава, односно потциљем 1.3: Опште јавне услуге.: ДРИ ће својим радом допринети унапређењу пружања услуга од стране јавног градског превоза. Осим тога, може се наћи веза и са циљем 2 Утврдити проблеме и предложити решења за међусекторске проблеме на свим нивоима, ради унапређивања одговорности и транспарентности, односно у оквиру тога Потциљ 2.5: Унапредити јавно управљање и коришћење информационих технологија (ИТ)⁴.

ИТ системи су од кључног значаја за пословање у оквиру јавног сектора и активности постају све скупље, сложеније и као и степен осетљивости података које оне садрже. Осим тога, иницијативе е-управе у Србији имају за циљ унапређење коришћења ИТ и интернета широм јавне управе да би се обезбедиле информације грађанима и

² „Службени гласник РС“, бр. 101/05, 54/07, 36/10 и 44/18-др.закон

³ „Службени гласник РС“, број 9/2009

⁴ Стратешки план Државне ревизорске институције за период 2019-2023.

http://www.dri.rs/upload/documents/Opsti_dokumenti/DRI%20Strateski%20plan%202018-2023.pdf



привредним друштвима. ДРИ је кроз своје ревизије ранијих година утврдила да неки субјекти ревизије нису предузели неопходне мере у области безбедности ИТ система - укључујући и право на приступ подацима и поверљивост података. Нису спровели неопходне процене ризика, нити су усвојили стратегије које регулишу развој ИТ технологија. Ово неадекватно планирање ИТ развоја довело је до кашњења у реализацији пројеката укључујући и нови интегрисани пословни ИТ систем и резултирало је у додатним трошковима.

Циљ ДРИ је и да се помогне да се унапреди способност ИТ система да сви јавни програми постану ефикаснији, а да се при томе штите кључно пословање и осетљиве информације.

3. Ревизорска питања

Како бисмо остварили циљ ревизије, усмерили се на давање одговора на следећа ревизијска питања:

1. У којој мери успостављене мере информационе безбедности обезбеђују поузданост информационих система који се користе у градском превозу?

- ⚡ Да ли постоје имплементирана правила и процедуре за информациону безбедност?
- ⚡ Да ли је и на који начин успостављена организација ИТ безбедности?
- ⚡ На који начин су успостављене мере физичке заштите и контроле логичког приступа системима?
- ⚡ На који начин се управља континуитетом пословања у ванредним околностима?
- ⚡ На који начин се спроводи управљање ИТ ризицима?
- ⚡ На који начин се у системима управља инцидентима?

2. У којој мери је успостављен механизам сарадње са пружаоцима услуга испунио све неопходне циљеве, укључујући и поузданост података?

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

3. У којој мери је успостављене апликативне контроле обезбеђују контролу наплате карата и контролу пружених услуга од стране ангажованих превозника?

- ⚡ Да ли постоје правила и процедуре које се односе на употребу апликације за наплату и апликације за контролу пружених услуга од стране превозника?
- ⚡ Да ли постоји механизам којим се осигурава валидација улазних података, детекција и корекција грешака?
- ⚡ На који начин се прати тачност података који се односе на наплату карата?
- ⚡ На који начин се прати извршење пружених услуга од стране превозника?
- ⚡ Да ли информациони систем генерише све потребне извештаје - када је у питању временски интервал и свеобухватност?

Како је циљ ревизије да се оцени ефективност информационих система формулисали смо три питања која се односе на три најризичније области, по нашој оцени



и процени ризика коју смо спровели на бази доступних тј. прикупљених података у досадашњем периоду рада на предстудији.

Прво питање се односи на информациону безбедност, укључујући и континуитет пословања и у склопу тога управљање резервним копијама. Ризици у овој области се односе на усвајање и имплементацију планова и процедура које уређују ова питања, а што је и законска обавеза свих оператера ИКТ система од посебног значаја, успостављање одговарајуће организационе ИТ структуре, примену неопходних мера заштите система, како физичке заштите, тако и контроле логичког приступа и редовну контролу примене тих мера, успостављање континуитета пословања у ширем смислу, што подразумева и одговарајући план опоравка од катастрофе (како се то дефинише у ИТ пракси, ИТ приручнику, итд.), тј. на континуитет пословања у ванредним околностима (како се то дефинише у Закону о информационој безбедности, тј. Уредби о ближем уређењу мера заштите ИКТ система од посебног значаја), и управљање резервним копијама, а што сада није случај. Безбедност података, а у овом случају се ради о осетљивим подацима које третира и Закон о заштити података, и други закони, је важно питање ове ревизије, због чега се и анализирају сва остала питања. Управљање ИТ ризицима је такође потребно уредити на одговарајући начин, а што обавезно треба да обухвати идентификацију свих ИТ ризика, њихову оцену, и доношење плана/стратегије за умањење или уклањање тих ризика, а то је такође и законска обавеза. И као последње питање у овој области, што је исто законска обавеза, јесте управљање и пријављивање ИТ инцидената.

Друго питање се односи на успостављање ефективног механизма сарадње са пружаоцима услуга. Као и у случају претходна два питања, најпре се анализирају правила и процедуре које се односе на сарадњу са пружаоцима услуга, а посебно када је у питању ИТ безбедност, тј. заштита података. Такође, потребно је анализирати механизам за контролу спровођења уговора, и опет, нарочито у погледу поверљивости. У том смислу потребно је анализирати обавезе субјекта и судова у вези Закона о заштити података о личности.

Треће питање се односи на успостављање ефективних апликативних контрола. Апликативне контроле обухватају унос података (настанак и унос података); обраду трансакције; излазне податке (дистрибуција резултата) и безбедност (евидентирање, комуникација, чување). Циљ контроле улазних података је да се осигура да је извор података валидан, тачан и потпун и да ће апликација одбацити неважеће податке. Циљ мера контрола обраде је да се осигура интегритет података, њихова ваљаност и поузданост и да се сачувају од погрешних обрада кроз циклус обраде трансакција – од времена пријема података, па уноса у систем до времена када се податак шаље у базу података, даљу комуникацију или подсистеме за излазне податке. Оне такође осигуравају да се ваљани унети подаци обрађују само једном и да детекција погрешних трансакција не ремети обраду ваљаних трансакција. Циљеви контроле излазних података представљају мере уграђене у апликацију како би се осигурало да су излазни подаци трансакције комплетни, тачни и тачно дистрибуирани. Такође настоје да се подаци који су обрађени у апликацији заштите од недозвољених модификација или дистрибуције.



4. Обим и ограничења ревизије

Ревизијом смо обухватили активности Дирекције за јавни превоз града Ниша, Јавно комунално предузеће Шумадија – Крагујевац, Градску управу Града Београда, Секретаријат за јавни превоз и Јавно градско саобраћајно предузеће Нови Сад у периоду од 2020-2022. године.

Детаљније испитивање смо извршили код субјеката ревизије који су приказани на следећој илустрацији:



Илустрација 1. Преглед субјеката ревизије

Поступке ревизије: прикупљање доказа, доношење налаза и закључака, писање извештаја, спровели смо од јуна до новембра 2023. године.

Ограничење ове ревизије је био ризик да подаци субјеката ревизије као и других извора информисања који су прикупљени у поступку ревизије, нису потпуни, упоредиви и тачни.

5. Методологија у поступку рада

Да бисмо одговорили на ревизорска питања, анализирали смо законску и подзаконску регулативу, користили стручну литературу (WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions⁵), као и све податке добијене од субјеката. Анализирали смо податке и информације за период од 2020. до 2022. године.

У вези са информационим системима Kentkart Southeast Europe и BusLogic, анализиране су области информациона безбедност, успостављање ефективног механизма сарадње са пружаоцима услуга и апликативне контроле.

У циљу потврђивања информација из документације и прикупљања података који нису доступни у документима, обавили смо интервјуе и послали анкете и упитнике корисницима информационог система здравствених установа.

Детаљнији опис коришћене методологије дат је у Прилогу 1

⁵ INTOSAI Радна група за ИТ ревизију



III Опис предмета ревизије

Предмет испитивања би биле области:

1) Информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица⁶;

2) Успостављање ефективног механизма сарадње са пружаоцима услуга како би се осигурало да се услуге пружају према очекивањима субјекта. Субјект ревизије треба да има процесе у циљу обезбеђивања периодичног праћења статуса пројекта, квалитета услуге и тестирања производа пре увођења у оперативно окружење. Осим тога, као део процеса праћења извршења обавеза пружаоца услуга, субјект ревизије може да врши и ревизију интерног процеса осигурања квалитета пружених услуга, како би се обезбедило да кадар пружаоца услуга прати уговорно одобрену политику и планове за све своје послове.⁷

3) Апликативне контроле обухватају унос података (настанак и унос података); обраду трансакције; излазне податке (дистрибуција резултата) и безбедност (евидентирање, комуникација, чување). Циљ контроле улазних података је да се осигура да је извор података валидан, тачан и потпун и да ће апликација одбацити неважеће податке. Циљ мера контрола обраде је да се осигура интегритет података, њихова ваљаност и поузданост и да се сачувају од погрешних обрада кроз циклус обраде трансакција – од времена пријема података, па уноса у систем до времена када се податак шаље у базу података, даљу комуникацију или подсистеме за излазне податке. Оне такође осигуравају да се ваљани унети подаци обрађују само једном и да детекција погрешних трансакција не ремети обраду ваљаних трансакција. Циљеви контроле излазних података представљају мере уграђене у апликацију како би се осигурало да су излазни подаци трансакције комплетни, тачни и тачно дистрибуирани. Такође настоје да се подаци који су обрађени у апликацији заштите од недозвољених модификација или дистрибуције.

У поступку ревизије није било испитивање да ли: (1) финансијски извештаји субјектата ревизије објективно и истинито приказују њихово финансијско стање, резултате пословања и новчане токове, у складу са прихваћеним рачуноводственим начелима и стандардима; (2) су финансијске трансакције и одлуке у вези са примањима, приходима, расходима и издацима извршене у складу са законом и другим прописима и за планиране сврхе.

Када су у питању информациони системи, предмет ревизије била би два наведена система

Ревизијом је обухваћен период од 2020. до 2022. године.

⁶ Члан 7. став 3. Закона о информационој безбедности

⁷ WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions



1. Законодавни и институционални оквир

↓ Законодавни оквир

Градски и приградски превоз путника, регулисан је у више закона и у наставку дајемо преглед најважнијих одредби према надлежностима.

Устав Републике Србије

Уставом, као највишим правним актом у држави дата је надлежност јединицама локалне самоуправе да, преко својих органа, у складу са законом уређују и обезбеђују обављање и развој комуналних делатности⁸.

Закон о локалној самоуправи

Законом је експлицитно дата општини надлежност⁹ да, преко својих органа, у складу са Уставом и законом, уређује и обезбеђује обављање комуналних делатности. У том циљу, у складу са законом, јединица локалне самоуправе за остваривање својих права и дужности и за задовољавање потреба локалног становништва може основати предузећа, установе и друге организације које врше јавну службу, али и уговором, у складу са начелима конкуренције и јавности, поверити правном или физичком лицу обављање својих послова.

Закон о превозу путника у друмском саобраћају

Овим законом уређују се услови и начин обављања јавног превоза путника и превоза лица за сопствене потребе у друмском саобраћају у домаћем и међународном превозу, пружања станичних услуга на аутобуским станицама и инспекцијски надзор¹⁰.

Организацију и начин обављања јавног градског превоза путника, који се обавља на територији ЈЛС, сходно наведеном Закону, уређује и обезбеђује, јединица локалне самоуправе¹¹.

Такође, јединица локалне самоуправе уређује начин регистрације и овере реда вожње у градском и приградском превозу, тачније, регистрацију и оверу реда вожње за градски и приградски превоз врши општинска, односно градска управа, односно управа надлежна за послове саобраћаја¹².

Закон о комуналним делатностима

Градски и приградски превоз путника, као једна од најзначајнијих комуналних делатности дефинисана је Законом о комуналним делатностима. Комуналним делатностима, сматрају се делатности пружања комуналних услуга од значаја за остварење животних потреба физичких и правних лица код којих је јединица локалне самоуправе дужна да створи услове за обезбеђење одговарајућег квалитета, обима, доступности и континуитета, као и надзор над њиховим вршењем¹³.

У том смислу, ЈЛС уређује услове обављања комуналних делатности, права и обавезе корисника комуналних услуга, обим и квалитет комуналних услуга и начин вршења надзора над обављањем комуналних делатности обезбеђујући нарочито¹⁴:

⁸„Службени гласник РС“, бр. 98/2006, члан: 189 и 190. став 1. тачка 1

⁹„Службени гласник РС“, бр. 129/07, 83/14 – др. закон, 101/16 – др. закон и 47/18, члан 20. став 1. тачка 2.

¹⁰„Службени гласник РС“, бр. 68/15, 41/18, 44/18 – др. закон, 83/18 и 31/19, члан 1.

¹¹„Службени гласник РС“, бр. 68/15, 41/18, 44/18 – др. закон, 83/18 и 31/19, члан 57.

¹²„Службени гласник РС“, бр. 68/15, 41/18, 44/18 – др. закон, 83/18 и 31/19, члан 64. и 65

¹³„Службени гласник РС“, бр. 88/11, 104/16 и 95/18, члан 2. став 1

¹⁴„Службени гласник РС“, бр. 88/11, 104/16 и 95/18, члан 4. став 3



1) одговарајући обухват, обим и квалитет комуналних услуга, који подразумева нарочито: здравствену и хигијенску исправност према прописаним стандардима и нормативима, тачност у погледу рокова испоруке, сигурност и заштиту корисника у добијању услуга, поузданост, приступачност и трајност у пружању услуга;

2) развој и унапређивање квалитета и асортимана комуналних услуга, као и унапређивање организације рада, ефикасности и других услова пружања услуга;

3) сагласност са начелима одрживог развоја, која су дефинисана посебним законом који уређује одређену комуналну делатност;

4) ефикасно коришћење ресурса и смањење трошкова обављања комуналних делатности успостављањем сарадње две или више јединица локалне самоуправе и другим активностима када за то постоји могућност;

5) конкуренцију у обављању делатности.

Законом о информациој безбедности¹⁵

У складу са Законом о информациој 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 предузима мере заштите ИКТ система.

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

Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја¹⁶

Уредба уређује мере заштите информационо-комуникационих система од посебног значаја. Чланом 2. ове уредбе уређено је успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система од посебног значаја.

Уредбом о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја¹⁷

Начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја, ближе се уређује садржај акта о безбедности информационо-комуникационих система од посебног значаја.

¹⁵„Службени гласник РС“, бр. 6/16, 94/17 и 77/19

¹⁶„Службени гласник РС“, број 94/16

¹⁷„Службени гласник РС“, број 94/2016



Закон о заштити података о личности¹⁸

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

Члан 16. закона уређује пристанак малолетног лица у вези са коришћењем услуга информационог друштва, те је дефинисано да малолетно лице које је навршило 15 година може самостално да даје пристанак за обраду података о својој личности у коришћењу услуга информационог друштва. Ако се ради о малолетном лицу које није навршило 15 година, за обраду података пристанак мора дати родитељ који врши родитељско право, односно други законски заступник малолетног лица. Руковалац мора предузети разумне мере у циљу утврђивања да ли је пристанак дао родитељ који врши родитељско право, односно други законски заступник малолетног лица, узимајући у обзир доступне технологије.

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

1) примени одговарајуће техничке, организационе и кадровске мере, као што је псеудонимизација, које имају за циљ обезбеђивање делотворне примене начела заштите података о личности, као што је смањење броја података;

2) обезбеди примену неопходних механизма заштите у току обраде, како би се испунили услови за обраду прописани овим законом и заштитила права и слободе лица на која се подаци односе (став 1).

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

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

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

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

Обрада од стране обрађивача мора бити уређена уговором или другим правно обавезујућим актом, који је закључен, односно усвојен у писменом облику, што обухвата и електронски облик, који обавезује обрађивача према руковоацу и који уређује предмет

¹⁸„Службени гласник РС“, број 87/2018



и трајање обраде, природу и сврху обраде, врсту података о личности и врсту лица о којима се подаци обрађују, као и права и обавезе руковоаца (став 3).

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

- 1) обрађује податке о личности само на основу писмених упутстава руковоаца, укључујући и упутство у односу на преношење података о личности у друге државе или међународне организације, осим ако је обрађивач законом обавезан да обрађује податке. У том случају, обрађивач је дужан да обавести руковоаца о тој законској обавези пре започињања обраде, осим ако закон забрањује достављање тих информација због потребе заштите важног јавног интереса;
- 2) обезбеди да се физичко лице које је овлашћено да обрађује податке о личности обавезало на чување поверљивости података или да то лице подлеже законској обавези чувања поверљивости података;
- 3) предузме све потребне мере у складу са чланом 50. овог закона;
- 4) поштује услове за поверавање обраде другом обрађивачу из ст. 2. и 7. овог члана;
- 5) узимајући у обзир природу обраде, помаже руковоацу применом одговарајућих техничких, организационих и кадровских мера, колико је то могуће, у испуњавању обавеза руковоаца у односу на захтеве за остваривање права лица на које се подаци односе из Главе III овог закона;
- 6) помаже руковоацу у испуњавању обавеза из члана 50. и чл. 52. до 55. овог закона, узимајући у обзир природу обраде и информације које су му доступне;
- 7) после окончања уговорених радњи обраде, а на основу одлуке руковоаца, избрише или врати руковоацу све податке о личности и избрише све копије ових података, осим ако је законом прописана обавеза чувања података;
- 8) учини доступним руковоацу све информације које су неопходне за предочавање испуњености обавеза обрађивача прописаних овим чланом, као и информације које омогућавају и доприносе контроли рада обрађивача, коју спроводи руковалац или друго лице које он за то овласти.

У случају из става 4. тачка 8) овог члана, обрађивач је дужан да без одлагања упозори руковоаца ако сматра да писмено упутство које је од њега добио није у складу са овим законом или другим законом којим се уређује заштита података о личности.

Члан 50. овог закона уређује безбедност обраде тако да у складу са нивоом технолошких достигнућа и трошковима њихове примене, природом, обимом, околностима и сврхом обраде, као и вероватноћом наступања ризика и нивоом ризика за права и слободе физичких лица, руковалац и обрађивач спроводе одговарајуће техничке, организационе и кадровске мере, како би достигли одговарајући ниво безбедности у односу на ризик (став 1).

У складу са ставом 2, према потреби, мере из става 1. овог члана нарочито обухватају:

- 1) псеудонимизацију и криптозаштиту података о личности; 2) способност обезбеђивања трајне поверљивости, интегритета, расположивости и отпорности система и услуга обраде; 3) обезбеђивање успостављања поновне расположивости и приступа подацима о личности у случају физичких или техничких инцидената у најкраћем року и 4) поступак редовног тестирања, оцењивања и процењивања делотворности техничких, организационих и кадровских мера безбедности обраде.



Приликом процењивања одговарајућег нивоа безбедности из става 1. овог члана посебно се узимају у обзир ризици обраде, а нарочито ризици од случајног или незаконитог уништења, губитка, измене, неовлашћеног откривања или приступа подацима о личности који су пренесени, похрањени или обрађивани на други начин (став 3).

Руководалац и обрађивач дужни су да предузму мере у циљу обезбеђивања система у којем свако физичко лице које је овлашћено за приступ подацима о личности од стране руковоаца или обрађивача, обрађује ове податке само по налогу руковоаца или ако је на то обавезано законом (став 5).

Члан 56. став 2. тачка 1) прописује да су руководалац и обрађивач дужни да одреде лице за заштиту података о личности, ако се обрада врши од стране органа власти. Тачка 2) прописује да су руководалац и обрађивач дужни да одреде лице за заштиту података о личности ако се основне активности руковоаца или обрађивача састоје у радњама обраде које по својој природи, обиму, односно сврхама захтевају редован и систематски надзор великог броја лица на које се подаци односе.

Законом о електронском документу и електронској идентификацији¹⁹

Чланом 7. је прописано је да се електронском документу не може оспорити пуноважност, доказна снага, као ни писана форма само зато што је у електронском облику. Такође, у истом закону, у члану 15. је прописано да се електронско општење и електронско достављање између органа јавне власти и странака врши у складу са законом којим се уређује општи управни поступак, законом којим се уређује електронска управа и другим прописима, као и путем услуге квалификоване електронске доставе.

Закон о електронској управи²⁰

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

¹⁹ „Службени гласник РС“, број 94/17 и 52/2021

²⁰ „Службени гласник РС“, број 27/2018



Институционални оквир



Јавно градско саобраћајно предузеће „Нови Сад“ организовано је Одлуком Скупштине Града Новог Сада 21. 12. 1989. године и послује као јавно предузеће. Град Нови Сад је власник 100% удела у основном капиталу јавног предузећа. Јавни превоз на ширем гравитационом подручју Града Новог Сада организован је на три основна режима

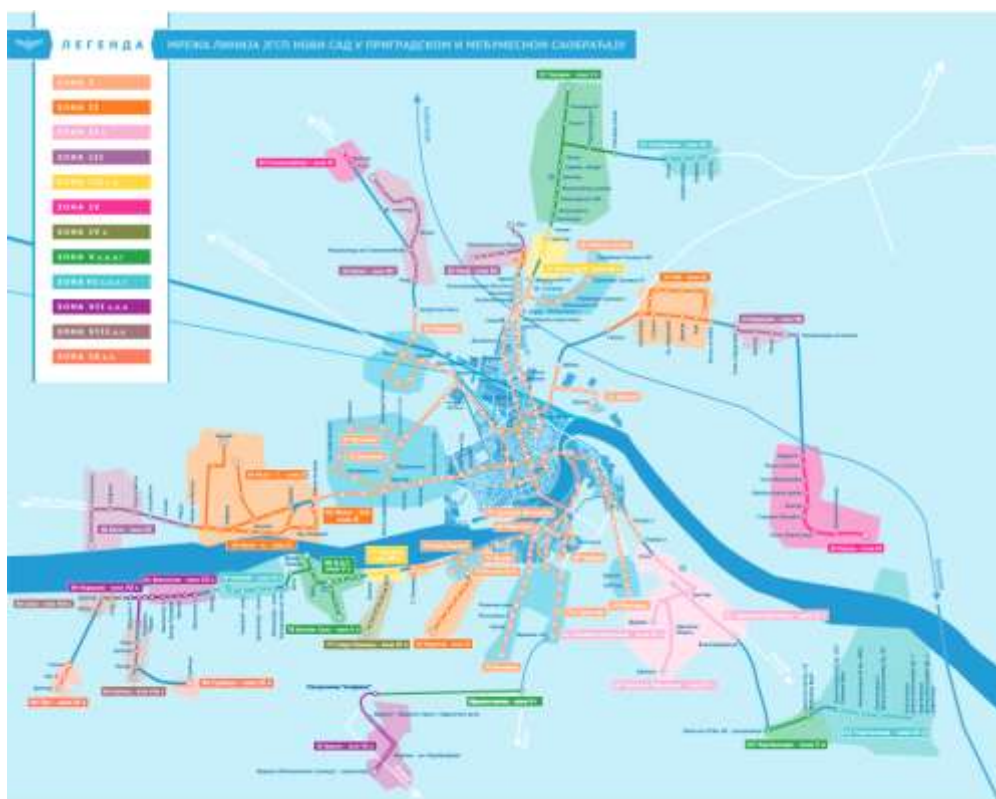
саобраћаја: градски, приградски и међумесни.

Предузеће је низом дугорочних опредељења усредсређено на свакодневно побољшање квалитета услуге:

- Обнављањем возног парка модерним, еколошки прихватљивим аутобусима;
- Увођењем модерних техничко-технолошких достигнућа у обележавању правца кретања аутобуса, продаји и наплати превоза и осталих услуга;
- Осавремењавањем комуникације са корисницима услуга;
- Перманентном обуком кадрова;
- Повезивањем са предузећима исте или сличне делатности, ради стицања увида у најсавременија техничка и друга достигнућа у јавном превозу путника.

Мониторинг рада возила јавног превоза и систем наплате карата и у Новоме Саду

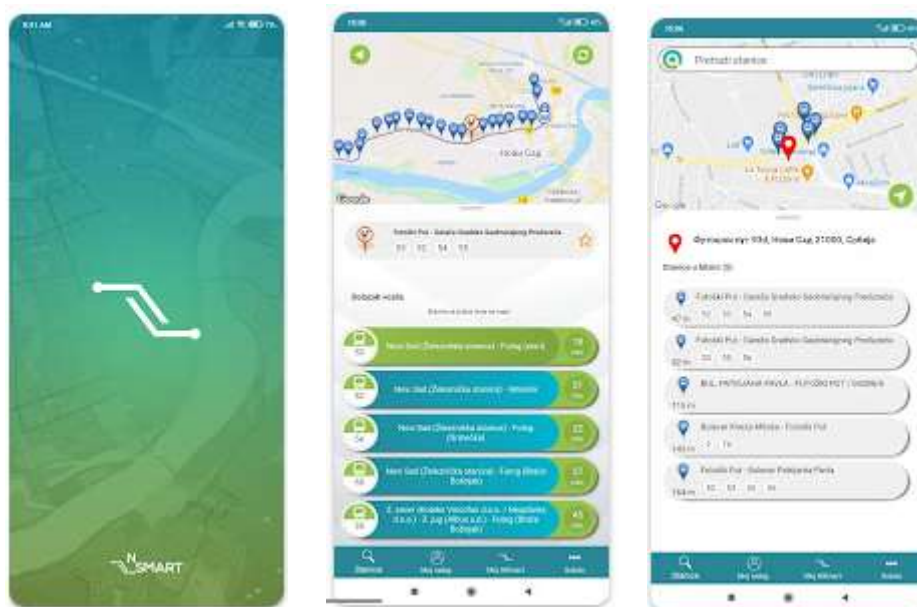
- Систем јавног превоза чини:
 - 94 градских линија, 51 приградских линија и 28 међумесне линије



Илустрација 2. Мапа градских линија



- Мониторинг рада возила јавног превоза
 - Програм Buslogic
 - Опрема (трекери, сервери...)
 - Људски ресурси (возно особље, диспечери ЈГСП Нови Сад)
- Приказ рада система
 - Формирање стајалишта
 - Формирање сваке појединачне линије јавног превоза припадајућим стајалиштима
 - Формирање типског распореда рада – колског реда вожње од стране превозника
 - Организација рада возача на дневном нивоу
- Мониторинг рада система
 - Аутоматска обрада података у систему на бази задатих параметара
 - Обрада података од стране диспечера
- NSMART апликација
 - Најава долазака возила у реалном времену
 - Уплата средстава за NSMART картицу



Илустрација 3. NSmart апликација

- Карте у систему јавног превоза

Персонализована НСмарт картица могу бити:

- Месечне карте издају се грађанима, Ученицима/ студентима, Запосленим лицима, Пензионерима до 65 године и Носиоцима права на новчану и социјалну помоћ.
- Годишње карте издају се Ученицима/ студентима, деца од 6 до 10 година и Повлашћеним лицима

Персонализована НСмарт картица издаје се на име корисника, садржи личне податке и фотографију ради визуелне контроле и није преносива на другог корисника.



Персонализована картица може се израдити само на продајним местима ЈГСП Нови Сад. Цена израде персонализоване картице је 375 динара.

Неперсонализоване карте могу бити:

- Карте за једну возњу купљене код возача купују се у аутобусу код возача и могу се користити само једном током трајања започете возње.
- Дневне карте се продају у сваком аутобусу. Цена дневне карте за све линије у градском саобраћају износи 278,00 динара.



- Појединачне карте – Дневна карта продаја у возилу од стране возача

- Појединачне карте – Карте за једну возњу купљене код возача



- Персонализована НСмарт пластична картица

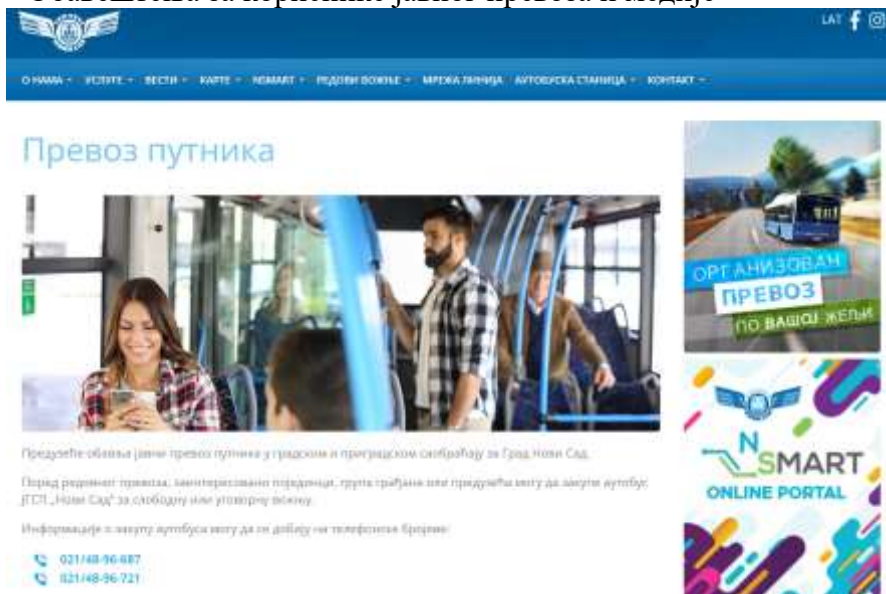


Илустрација 4. Карте у систему јавног превоза Нови Сад



➤ Сајт ЈГСП Нови Сад

- Обавештења за кориснике јавног превоза и медије



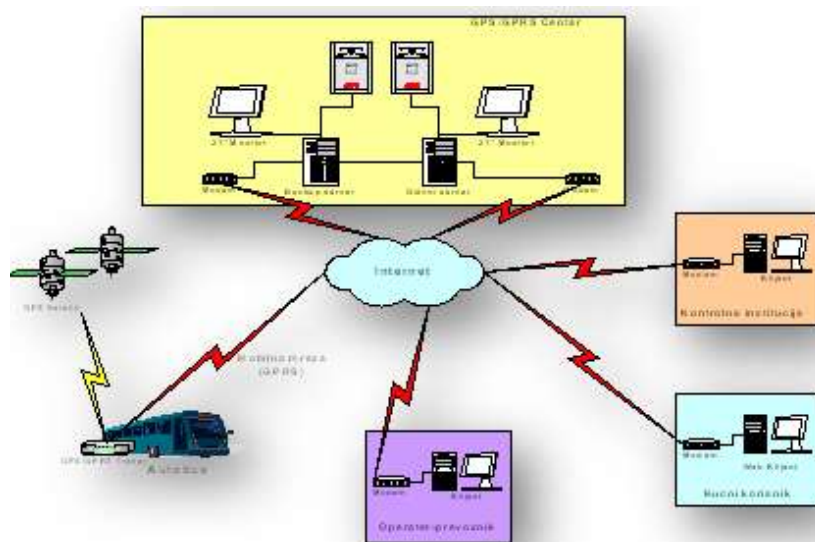
Илустрација 5. Сајт Јавно градско саобраћајно предузеће „Нови Сад“

➤ Најава стајалишта

- Информациони систем намењен путницима у реалном времену

2. Информациони системи BusLogic

Програм Buslogic је информациони систем који користи Јавно градско саобраћајно предузеће Нови Сад. Програм се састоји од Buslogic – Мониторинг рада возила јавног превоза и Buslogic – Електронске наплате карата.



Илустрација 6 Мониторинг рада возила јавног превоза Нови Сад

надзире и обезбеђује већу сигурност и комфор за своје путнике, а исто тако може да одпратити реализацију возила.

Обједињавањем дигиталних сервиса наплате карата и сателитског праћења положаја возила, као и праћења основних података попут брзине кретања, температуре, броја обртаја мотора и нивоа горива у резервоару. На основу ових података могуће је вршити комплетано праћење возила, чиме ЈГСП Нови Сад добија пуну контролу над линијама превоза које



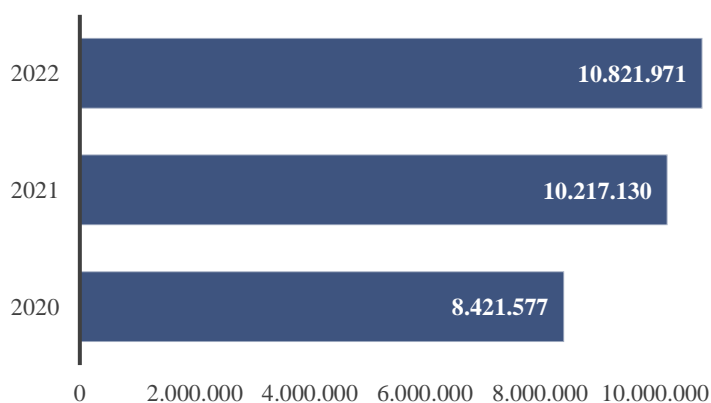
Електронска продаја и наплата карата се врши путем система за продају карата. Продаја карата је омогућена у аутобусу, ван аутобуса, шалтерска продаја аутобуских карата, онлине резервација и продаја карата преко веб сајта превозника, у наредном периоду биће омогућен и електронски новчаник.



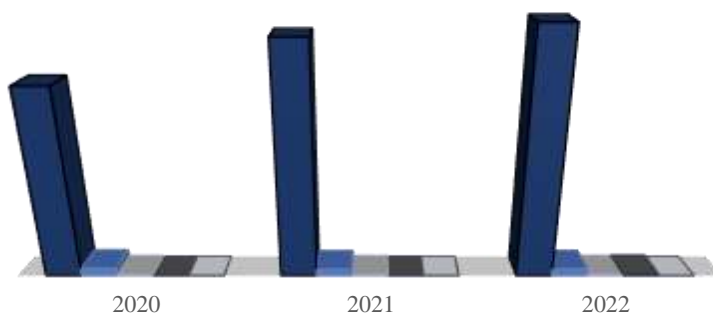
Илустрација 7. Програм Buslogic

Програм Buslogic садржи следеће компоненте:

- Администраторски модул
- Извештајни модул:
 - продаја карата
 - статистике
 - приходи
- Диспечерски модул:
 - реализација
 - праћење возила (мапа),
 - извештаји о реализацији возила
- Благајнички модул
 - Раздуживање карте
 - Увоз продаја превозника
- Електронске карте
 - Електронски новчаник



Графикон број 1. Број продатих карата у периоду од 2020. до 2022. године



	2020	2021	2022
■ Неперсонализоване карте	8.050.816	9.883.983	10.420.200
■ Персонализоване карте	328.171	291.814	299.707
■ Годишње карте	40.429	38.936	45.354
■ Дневне карте	684	472	55.600
□ Недељне карте	1.477	1.925	1.110

Графикон број 2. Број продатих карата по врстама карата у периоду од 2020. до 2022. године



IV Закључци

У овом поглављу износимо закључке до којих смо дошли спроводећи ревизију сврсисходности на тему „Информациони системи у јавном градском превозу“, код субјекта ревизије:

Јавно градско саобраћајно предузеће Нови Сад, Футошки пут 46, Нови Сад

Донети закључци представљају одговоре на постављена ревизијска питања, дефинисана у делу извештаја II Увод – 2. Циљ ревизије. Закључци су донети на основу утврђених налаза – сваки закључак је изведен на основу припадајућих налаза.

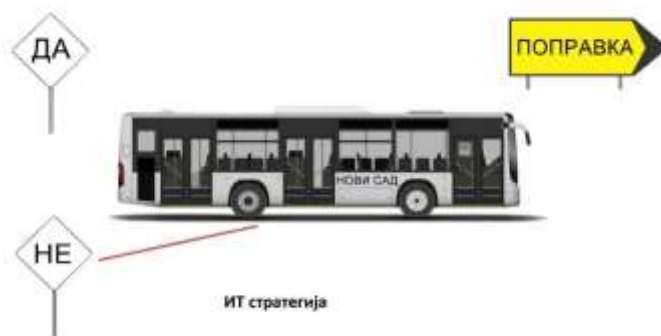
ЗАКЉУЧАК 1: Информациона безбедност није успостављена на свеобухватан начин јер нису усвојене и примењене мере заштите које обухватају управљање ИТ ризицима и ИТ инцидентима, успостављање адекватне организационе ИТ структуре, усвајање, ажурирање и примену одговарајућих правилника, политика и процедура у области информационе безбедности, управљање приступом системима и управљање процесом континуитета пословања, што је неопходно како би била осигурана поузданост система.

Наш закључак заснивамо на следећим налазима:

Налаз 1.1: Јавно градско саобраћајно предузеће Нови Сад није у потпуности успоставило организацију ИТ безбедности

Организација ИТ безбедности у Јавном градском саобраћајном предузећу Нови Сад, због недостатка довољно стручног знања и недостатка кадровских капацитета, није успостављена тако да обухвата примену адекватних докумената која уређују ову област, управљање инцидентима и адекватну организациону структуру ИТ безбедности, што за последицу има већи степен рањивости информационог система.

ЈГСП Нови Сад нема усвојен стратешки документ којим се планира употреба и развој ИТ капацитета.



Илустрација 8. ИТ Стратегија



ЈГСП Нови Сад је донела Акт о безбедности информационо-комуникационог система, 01.07.2019. године. Наведени документ је документ који се односи на све информационе системе у предузећу, дакле не искључиво на информациони систем у јавном градском превозу. Између осталог, не садржи одредбе које се односе на поверавање послова, тј. однос са пружаоцима услуга, у конкретном случају то је фирма BusLogic Пожаревац. Законом о информационој безбедности је у члану 8, став 3, прописано да Акт о безбедности мора бити усклађен са променама у окружењу и у самом ИКТ систему. Са друге стране, Уредба о ближем садржају Акта о информационој безбедности ИКТ система од посебног значаја прописује обавезу усклађивања акта о информационој безбедности са мерама заштите из члана 7. Закона о информационој безбедности и Уредбом о ближем решењу мера заштите ИКТ система од посебног значаја.



Илустрација 9. Акт о безбедности ИКТ система

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



Илустрација 10. Процедуре у вези информационе безбедности

ЈГСП Нови Сад није документовало да је другим актима послове информационе безбедности уредило на начин дефинисан наведеном уредбом, и на начин који омогућава јасну поделу дужности и одговорности, али и контролу свих тих послова.

ЈГСП Нови Сад је Правилником о систематизацији радних дефинисала седам радних места које се односе на ИТ послове.



Од предвиђених седам места, попуњено је шест - није попуњено радно место Сарадник информационих технологија. Што се тиче информационе безбедности, код двоје запослених у опису послова је наведена безбедност и заштита на раду, док послове администрирања обавља двоје запослених.



Илустрација 11. Организациона ИТ структура

ЈГСП Нови Сад није утврдила процедуре нити дефинисала одговорна лица задужена за превенцију и реаговање, план поступања у случају опасности од настанка безбедносних инцидената или настанка безбедносних инцидената, обавезу вођења евиденције о предузетим активностима, обавезу извештавања и размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама.



Илустрација 12. Управљање ИТ инцидентима

Препорука 1: Препоручујемо Јавном градском саобраћајном предузећу Нови Сад да успостави организацију информационе безбедности која обухвата усвајање, ажурирање и имплементацију аката која уређују ову област – акта (правилника) о информационој безбедности, процедура које се односе на ИТ безбедност, управљање инцидентима, и адекватну организациону структуру ИТ безбедности, како би биле примењене све неопходне мере безбедности и заштите података.

ИТ стратегија представља међусобно усклађивање између ИТ технологије и пословних стратешких циљева. Стратешки циљеви ИТ треба да размотре тренутне и будуће потребе пословања, тренутни ИТ капацитет за пружање услуга и захтеве за



ресурсима. Стратегија треба да размотри постојећу ИТ инфраструктуру и архитектуру, инвестиције, модел испоруке, ресурсе, укључујући кадар, и постави стратегију која их интегрише у заједнички приступ за подршку пословним циљевима.²¹

ИТ стратегија обично обухвата планирање, имплементацију, одржавање и управљање ИТ системима. ИТ стратегија обично садржи анализу тренутног стања (процена тренутних ИТ ресурса, инфраструктуре, процеса и капацитета), дефинисање визије у погледу примене ИТ технологија, идентификовање потреба организације и утврђивање како ИТ може најбоље подржати те потребе, одређивање кључних пројеката како би се остварили циљеви ИТ стратегије, затим планирање потребних финансијских, људских и техничких ресурса за спровођење стратегије, примену заштитних мера у циљу заштите информационих система и праћење напретка у остваривању циљева ИТ стратегије те редовно извештавање о резултатима.

ИТ стратегија треба да буде усвојена јер помаже у усклађивању ИТ технолошких решења са пословним циљевима. ИТ послове из области информационе безбедности је неопходно детаљно уредити одговарајућим процедурама у смислу праћења активности, ревизије и надзора у оквиру управљања информационом безбедношћу, зато што се на тај начин са једне стране пружа могућност за контролу квалитета рада на тим пословима, а са друге стране омогућава да у случајевима кадровских промена, новозапослена лица могу веома брзо и лако наставити са свим пословима, што би у случају да процедура нема било скоро немогуће, или немогуће у неком краћем временском периоду. Како би биле функционалне, неопходно је да процедуре буду довољно детаљне и свеобухватне, да поред описа свих процеса садрже и податке ко ради на којој активности (не у смислу имена него у смислу одређеног радног места), као и податке о изменама итд. У оквиру организационе структуре утврђују се послови и одговорности запослених за заштиту информационих добара, односно средстава и имовине за надзор над пословним процесима од значаја за информациону безбедност, за управљање инцидентима у области информационе безбедности, као и за послове предвиђене процедурама у области информационе безбедности.

Законом о информационој безбедности, у складу са чланом 6а тачка 3 и тачка 4, прописано је да је обавеза оператора ИКТ система од посебног значаја да донесе акт о безбедности ИКТ система, и да врши проверу усклађености примењених мера заштите ИКТ система са актом о безбедности ИКТ система и то најмање једном годишње;

Законом о информационој безбедности, члан 8., дефинисано је да Акт из става 1. овог члана мора да буде усклађен с променама у окружењу и у самом ИКТ систему.²²

ИТ послове је неопходно детаљно уредити одговарајућим процедурама, зато што се на тај начин са једне стране пружа могућност за контролу квалитета рада на тим пословима, а са друге стране омогућава да у случајевима кадровских промена, ново запослена лица могу веома брзо и лако наставити са свим пословима, што би у случају да процедура нема било скоро немогуће, или немогуће у неком краћем временском периоду. Како би биле функционалне, неопходно је да процедуре буду довољно детаљне и свеобухватне, да поред описа свих процеса садрже и податке ко ради на којој активности (не у смислу имена него у смислу одређеног радног места), као и податке о изменама итд.

Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја прописано је да оператор ИКТ система од посебног значаја, између осталог, успоставља организациону структуру, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом

²¹ IT Audit Handbook

²² Закон о информационој безбедности



безбедношћу у оквиру оператора ИКТ система од посебног значаја, обезбеђивање да лица која користе ИКТ систем, односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност; заштиту од ризика који настају при променама послова или престанка радног ангажовања лица запослених; идентификовање информационих добара и одређивање одговорности за њихову заштиту итд.

Законом о информационој безбедности, у члану 7. тачка 1. прописано је да се мере заштите ИКТ система се односе на успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система.

Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, у члану 2. прописано је: оператор ИКТ система од посебног значаја (у даљем тексту: оператор ИКТ система) је дужан да, у оквиру организационе структуре, у складу са природом, обимом и сложеносту пословања утврди послове и одговорности запослених, у циљу управљања информационом безбедношћу.

Оператор ИКТ система утврђује, у оквиру организационе структуре, послове и одговорности запослених за заштиту информационих добара, односно средстава и имовине за надзор над пословним процесима од значаја за информациону безбедност, за управљање ризицима у области информационе безбедности, као и за послове предвиђене процедурама у области информационе безбедности.

Подела одговорности запослених треба да се изврши тако да се онемогући неовлашћена или ненамерна измена, оштећење или злоупотреба средстава, односно информационих добара оператора ИКТ система, као и да се онемогући приступ, измена или коришћење средстава без овлашћења и без евиденције о томе.

Раздвајање одговорности (енг. separation of duties, СоД) је кључни концепт у информационим технологијама и управљању сигурношћу који има за циљ спречавање злоупотреба и минимизирање ризика унутар организације. Овај концепт подразумева да се одређене функције и одговорности раздвајају између различитих особа или улога како би се осигурало да ниједан појединац или ентитет нема превише контроле над критичним процесима или ресурсима. Раздвајање одговорности помаже у спречавању ситуација у којима би појединац могао да злоупотреби своје овлашћење или да направи грешку која би могла проузроковати озбиљне проблеме. Кључни принципи раздвајања одговорности у ИТ систему између осталих обухватају принцип двоструког одобрења (енг. dual authorization) - за критичне трансакције или промене, захтева се одобрење од две различите особе, затим принцип најмањег привилегија (енг. principle of least privilege) - особе или системи добијају само оне привилегије и овлашћења који су им потребни да обављају свој посао и ништа више, затим веома важан принцип раздвајања администратора и ИТ ревизора или особе која врши надзор - особе које су одговорне за администрацију система и ресурса не би требале бити исте особе које врше ревизију и надзор над тим истим системима. Чест је случај и неусклађености са принципом раздвајања између развоја и имплементације – наиме особе или тимови који развијају софтвер или апликације не би требали имати директну контролу над њиховим имплементирањем у продукцијском окружењу. Раздвајање одговорности захтева пажљиво планирање и правилну организацију, али може значајно допринети јачању сигурности и смањењу ризика у ИТ системима.

Оператор ИКТ система успоставља процедуре ради праћења активности, ревизије и надзора у оквиру управљања информационом безбедношћу. Приликом утврђивања одговорности запослених потребно је предвидети и одговорност за обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима.



Оператор ИКТ система утврђује процедуре комуникације са другим институцијама у случају инцидента у циљу благовремене пријаве, односно решавања насталог безбедносног инцидента.

Чланом 11. Закона о информационој безбедности прописана је обавеза оператора ИКТ система да обавештавају Надлежни орган о инцидентима који могу имати значајан утицај на нарушавање информационе безбедности.

Поступак достављања података о инцидентима у информационо-комуникационим системима од посебног значаја (у даљем тексту: ИКТ системи од посебног значаја) који могу да имају значајан утицај на нарушавање информационе безбедности, листа, врсте и значај инцидента и поступак обавештавања о инцидентима у ИКТ системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности прописан је Уредбом о поступку достављања података, листи, врстама и значају инцидента и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја.

Чланом 28. Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја прописано је да је оператор ИКТ система у обавези да утврди процедуре којима се дефинишу одговорна лица задужена за превенцију и реаговање, план поступања у случају опасности од настанка безбедносних инцидента или настанка безбедносних инцидента, обавезу вођења евиденције о предузетим активностима, обавезу извештавања и размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама.

Циљ управљања инцидентима је успостављање механизма да се најпре инциденти евидентирају, а затим и да се правовремено реагује. Како се инцидент може десити било где у систему, запослени који уочи настали проблем треба обавестити надлежно лице, које ће предузети даље кораке, или дати инструкције. Уколико се не врши евидентирање инцидента, и не спроводе мере како се такав инцидент не би поновио, то може као последицу имати понављање инцидента, које није морало да се деси, самим тим и настанак додатне штете у систему (оштећење, нестанак рачунарске опреме, штете настале активирањем малициозног кода, неовлашћен приступ систему, покушаји упада у систем итд.).

Налаз 1.2: Јавно градско саобраћајно предузеће Нови Сад није успоставило процес приступа систему на задовољавајући начин.

У Јавном градском саобраћајном предузећу Нови Сад није успостављен процес приступа на задовољавајући начин, због тога што нису усвојене процедуре које уређују овај процес и није успостављена контрола тог процеса, иако је то законска обавеза, што за последицу може имати угрожену безбедност података.

У складу са чланом 18. Акта о безбедности ИКТ система ЈГСП Нови Сад корисничке налоге додељује шеф Одељења, односно шеф ИТ одељења или овлашћено лице на основу захтеба руководиоца запосленог.

Чланом 7. је дефинисано између осталог да је за контролу и надзор над обављањем послова корисника, у циљу заштите и безбедности ИКТ система надлежан шеф Одељења информационих технологија

Чланом 9. је дефинисано да је лице овлашћено од стране директора дужно да контролише приступ ресурсима ИКТ система предузећа и проверава да ли има приступа са непознатих уређаја. Није међутим успостављена процедура о чувању и контроли



активности корисника и администратора (лог фајлови). Лог фајлови се не чувају у ЈГСП Нови Сад.

Чланом 10. је дефинисано да шеф Одељења информационих технологија води евиденцију приватних уређаја са којих ће бити омогућен приступ ИКТ систему. Ови уређаји морају бити подешени од стране шефа Одељења информационих технологија односно овлашћеног лица и могу се користити само за обављање послова у надлежности корисника и то у периоду када није могуће користити уређај у валсништву предузећа. У пракси, не врши се евиденција нити контрола уређаја са којих се приступа систему.

Чланом 19. је дефинисано да се у циљу физичке сигурности информатичких ресурса морају обезбедити следећи услови: да сервери морају бити смештени у посебној просторији, тј. сервер соби, да приступ соби, поред лица која су задужена за одржавање ИКТ система, могу имати и друга лица, уз претходно одобрење директора предузећа, односно овлашћеног лица, такође, дефинисано је и да приступ медијима са поверљивим подацима морају бити заштићени од науторизованог приступа и прегледа. Чланом 20. је дефинисано ко и у ком случају има права уласка у сервер собу. Међутим, сервер рачунари се како је то наведено у техничкој спецификацији налазе у Телекому, као једном од пружаоца услуга, а у складу са Уговорима о јавној набавци²³.

Како су навела одговорна лица у ЈГСП Нови Сад, администраторски налог има и фирма BusLogic Пожаревац.

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



Илустрација 13. Логички и физички приступ систему

Препорука 2: Препоручујемо Јавном градском саобраћајном предузећу Нови Сад да уреди процес приступа систему, што подразумева усвајање процедура које уређују овај процес и контролу тог процеса, а односи се на логички приступ, рад на даљину и физичку заштиту система.

Мере заштите ИКТ система се између осталог односе на одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа, такође и на безбедан приступ када је у питању рад на даљину.

Чланом 10. Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја, прописано је одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа и то:

²³ Уговор број 1351 од 14.02.2020. године и Уговор број 8844 од 02.11.2020. године



Оператор ИКТ система је у обавези да предвиди процедуру за одобравање и укидање овлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа, тако што предвиђа услове за одобравање и укидање овлашћеног приступа, проверу адекватности одобреног нивоа приступа и доделу јединствене идентификационе ознаке лицу којем се одобрава приступ (став 1);

Оператор ИКТ система води евиденцију о додељеним и одузетим ознакама, утврђује услове за коришћење заједничке идентификационе ознаке у случајевима када је то неопходно, дефинише начин и услове онемогућавања и уклањања јединствених идентификационих ознака, као и услове за доделу и коришћење администраторских права (став 2);

Лицима којима се одобрава овлашћени приступ омогућује се приступ на основу података за аутентификацију (лозинке, криптографски кључеви, подаци складиштени на токенима и сл.) (став 3);

Додела и коришћење администраторских права приступа треба да буде ограничена и контролисана (став 4);

Оператор ИКТ система дужан је да обезбеди механизам за укидање права приступа у случајевима промене радног места, престанка радног односа и, по потреби, у другим случајевима (став 5).

Чланом 18. прописано је чување података о догађајима који могу бити од значаја за безбедност ИКТ система тако да оператор ИКТ система треба да обезбеди да се у ИКТ систему формирају записи о догађајима (логови) у вези активности корисника, грешкама и догађајима у вези са информационом безбедношћу, а који се морају чувати и редовно проверавати. Средства за записивање и записи треба да буду заштићени од неовлашћеног приступа и промене. У оквиру ИКТ система записују се активности администратора и корисника и редовно преиспитују у циљу заштите. У циљу обезбеђивања поузданости записа, времена у свим подсистемима ИКТ система морају бити синхронизована међусобно, као и са референтним тачним временом.

Чланом 3. Уредбе о ближејем уређењу мера заштите ИКТ система од посебног значаја, прописано је постизање безбедности рада на даљину и употребе мобилних уређаја.

Оператор ИКТ система који у свом систему дозвољава рад на даљину и употребу мобилних уређаја дужан је да успостави и одржава безбедност рада на даљину и употребе мобилних уређаја, узимајући у обзир ризике који могу постојати услед неадекватног коришћења мобилних уређаја. (став 1.)

Оператор ИКТ система је дужан да дефинише услове и ограничења за рад на даљину тако да се не угрози безбедност ИКТ система, при чему оператор ИКТ система узима у обзир физичку безбедност места и окружења са кога се обавља рад на даљину, услове за безбедност комуникације између ИКТ система оператора и места са којег се ради на даљину, превенцију или свођење на неопходни минимум обраде и чувања информација на личном уређају лица које ради на даљину, превенцију од неовлашћеног приступа, услове за коришћење локалне мреже и бежичних мрежних сервиса, захтеве за заштиту од злонамерних софтвера и друге мере које су потребне за безбедност рада на даљину. (став 2.)

Приликом коришћења мобилних уређаја мора да се обезбеди заштита података од интереса за оператора ИКТ система и смање ризици коришћења мобилних уређаја у незаштићеним окружењима (јавним местима, мрежама са непознатом или недовољном заштитом и слично), при чему оператор ИКТ система узима у обзир следеће:

- 1) евиденцију мобилних уређаја;



- 2) мере физичке заштите мобилних уређаја (од уништења, оштећења, губитка или неовлашћеног приступа уређајима и подацима од интереса за оператора ИКТ система);
- 3) ограничења за инсталацију и ажурирање софтвера;
- 4) инсталацију адекватних софтвера за мобилне уређаје и њихово редовно ажурирање;
- 5) ограничење коришћења услуга информационог друштва које би угрозиле информациону безбедност ИКТ система;
- 6) контроле приступа мобилном уређају и подацима на њему;
- 7) криптографске технике;
- 8) заштиту од вируса и других злонамерних софтвера;
- 9) даљинско управљање мобилним уређајем у случају инцидента, од стране овлашћеног лица оператора ИКТ система, путем којег је могуће да се изврши неповратно брисање података и онемогућавање даљег коришћења уређаја;
- 10) успостављање и одржавање резервне копије (backup) података;
- 11) омогућавање безбедног коришћења интернет сервиса и апликација. (став 3.)

Ако оператор ИКТ система дозвољава у свом систему коришћење приватних мобилних уређаја дужан је да обезбеди услове из става 3. овог члана и предузме мере ради раздавајања приватног од пословног коришћења ових уређаја. (став 4.)

Чланом 27. Уредбе прописано је да у циљу одржавања уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга, оператор ИКТ система успоставља механизме надзора над пружањем услуга, именује лице које је задужено за праћење реализације пружања услуга и контролу испуњености нивоа информационе безбедности, применом одговарајућих процедура и успоставом надзора.

Налаз 1.3: Јавно градско саобраћајно предузеће Нови Сад није успоставило план континуитета пословања у ванредним околностима

Јавно градско саобраћајно предузеће Нови Сад, због недовољно финансијских средстава па самим тим и недовољно хардверских ресурса, недовољно искуства и стручног знања и обученог ИТ кадра, није усвојила ни имплементирана правила и процедуре за континуитет пословања, иако је то и законска обавеза, а што може за последицу имати нефункционисање система у неодређеном временском периоду, па самим тим и отежано пружање услуга

ЈГСП Нови Сад није успоставило план/процедуру континуитета пословања у ванредним околностима.



Илустрација 14. Континуитет пословања у ванредним околностима

Препорука 3: Јавном градском саобраћајном предузећу Нови Сад препоручујемо да успостави свеобухватан план континуитета пословања у ванредним околностима, што подразумева ажурирање постојећег Правилника о безбедности ИКТ система, усвајање процедуре за континуитет пословања у ванредним околностима и управљање резервним копијама података.

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

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

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



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

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

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

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

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

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

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

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

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

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

План опоравка од катастрофе, када су ови ризици у питању, садржи мере које су усмерене на опремање и употребу секундарне (резервне) локације у оваквим случајевима. Та локација се успоставља на удаљености која треба да обезбеди њено функционисање у случају неких од наведених догађаја (наравно, у зависности од природе послова, њиховог обима и важности, величине система итд). На резервној локацији се поставља неопходна опрема за функционисање система: електрично напајање, мрежна инфраструктура, секундарни сервери – апликативни и за складиштење података итд.

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

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

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



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

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

Налаз 1.4: Јавно градско саобраћајно предузеће Нови Сад није успоставило управљање ИТ ризицима

Јавно градско саобраћајно предузеће Нови Сад није успоставило управљање ИТ ризицима, што за последицу може имати стварање непотребно великих трошкова у случају настанка нежељеног догађаја, а који се могао спречити, или великих нефинансијских губитака (података на пример) због неблаговременог предузимања мера. Нарочито када се документација налази у електронском облику.

ЈГСП Нови Сад није успоставило управљање ИТ ризицима. У Правилнику о систематизацији радних места нису дефинисани послови који се односе на управљање ризицима.



Илустрација 15. Управљање ИТ ризицима

Препорука 4: Јавно градско саобраћајно предузеће Нови Сад препоручујемо да успостави управљање ИТ ризицима, што подразумева евидентирање, анализу, класификацију ИТ ризика и дефинисање стратегије за смањивање/отклањање ризика.



Основно што треба знати: немогуће је успоставити ефикасан систем без успостављеног процеса управљања ризиком.

Разлози зашто је то тако су управо последице које могу настати или које су већ настале у информационим системима, а које стварају губитке, финансијске или нефинансијске природе (података на пример), који се добром проценом ризика могу избећи.

Другим речима, уколико се жели поуздан, али истовремено и ефикасан систем, без процене ризика то се не може постићи. На пример, могуће је све елементе система дуплирати, и тако постићи скоро 100% поуздан систем. Али због цене дуплирања, такав систем се не може сматрати ефикасним, јер се можда исти циљ (поузданост) може постићи и са мање улагања.

Када су у питању ИТ ризици, у пракси се примењује тзв. 3Д приступ (претња, рањивост, последица) или 2Д приступ (вероватноћа, утицај). Сама класификација ризика се најчешће врши према утицају, а кораци који обично следе обухватају анализу ризика (вероватноћа појављивања сваког ризика понаособ и процена утицаја), дефинисање стратегије за смањивање/отклањање ризика, а крајњи циљ је да се дође до поузданог информационог система код кога су ризици добро процењени тако да функционише у потпуности, а са најмањим утрошком ресурса.

У Уредби о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, у члану 2. прописано је да оператор ИКТ система утврђује, у оквиру организационе структуре, послове и одговорности запослених за заштиту информационих добара, односно средстава и имовине за надзор над пословним процесима од значаја за информациону безбедност, за управљање ризицима у области информационе безбедности.



ЗАКЉУЧАК 2: Није успостављен ефективан механизам сарадње са пружаоцима услуга, зато што нису усвојена и имплементирана правила и процедуре када је у питању ова област, није обезбеђен континуитет пословања у случају раскида сарадње и није процес обраде података о личности уређен на начин прописан законом

Наш закључак заснивамо на следећим налазима:

Налаз 2.1: Јавно градско саобраћајно предузеће Нови Сад није у потпуности процедурама и другим актима уредило сарадњу са пружаоцем услуга

Јавно градско саобраћајно предузеће Нови Сад није у потпуности процедурама и другим актима уредило сарадњу са пружаоцем услуга, што за последицу има већи степен рањивости информационог система.

Нису усвојене процедуре које уређују сарадњу са пружаоцем услуга. Акт о безбедности ИКТ система у ЈГСП Нови Сад, у члану 27. дефинише да пружаоци услуга могу приступити само оним подацима који се налазе у базама података које су део софтвера који су они израдили, односно за које постоји уговором дефинисан приступ. Дефинисано је да су шеф службе развоја и шеф одељења одговорни за контролу приступа и надзор над извршењем уговорних обавеза. ЈГСП Нови Сад није документовало да се овај надзор обавља, и на који начин.



Илустрација 16. Процедуре за сарадњу са пружаоцима услуга

Препорука 5: Препоручујемо Јавном градском саобраћајном предузећу Нови Сад да усвоји/ажурира и имплементира правила и процедуре за безбедност података када је у питању сарадња са пружаоцима услуга што подразумева обавезну примену мера заштите података, и успостављање механизма за праћење примене тих мера.

ИТ послове из области информационе безбедности када је у питању сарадња са пружаоцима услуга је неопходно детаљно уредити у смислу примене правила и процедуре које се односе на безбедност података, праћења активности, ревизије и надзора у оквиру управљања информационом безбедношћу. На тај начин се са једне



стране пружа могућност за контролу квалитета рада на тим пословима, а са друге стране омогућава да у случајевима кадровских промена, ново запослена лица могу веома брзо и лако наставити са свим пословима, што би у случају да процедура нема било скоро немогуће, или немогуће у неком краћем временском периоду. Како би биле функционалне, неопходно је да процедуре буду довољно детаљне и свеобухватне, да поред описа свих процеса садрже и податке ко ради на којој активности (не у смислу имена него у смислу одређеног радног места), као и податке о изменама итд.

Уредбом о ближем уређењу мера заштите ИКТ система од посебног значаја предвиђена је заштита средстава оператора ИКТ система која су доступна пружаоцима услуга тако да оператор ИКТ система у својим процедурама предвиђа ниво доступности и врсту информација и средства којима могу да приступе пружаоци услуга, начине приступа информацијама и средствима и надзор над приступом. Оператор ИКТ система треба да идентификује и успостави процедуре безбедности информација које се конкретно баве приступом информацијама пружаоца услуга унутар организације. Обавезе пружаоца услуга у вези са информацијама и средствима која су доступна пружаоцима услуга оператора ИКТ система регулишу се споразумом између оператора ИКТ система и пружаоца услуга, чијим одредбама се обезбеђује адекватан ниво заштите информација и средстава, у складу са прописима и техничким стандардима. Оператор ИКТ система дужан је да обезбеди да пружалац услуга обавља поверене активности у складу са актом о безбедности ИКТ система, односно другим актима којима се уређује безбедност његовог информационог система. (Члан 26.).

Налаз 2.2: Јавно градско саобраћајно предузеће Нови Сад није у потпуности уредило сарадњу са пружаоцем услуга када је у питању заштита и обрада података

Јавно градско саобраћајно предузеће Нови Сад није у потпуности уредило сарадњу са пружаоцем услуга када је у питању заштита и обрада података, у смислу успостављања механизма којим се осигурава да је пружалац услуге усвојио услове за заштиту и безбедност података и да ли их спроводи, начина на који се прати реализација извршења уговора и на начин прописан Законом о информационој безбедности и Законом о заштити података о личности што за последицу има смањени степен поузданости система.

Није успостављен механизам када је у питању сарадња са пружаоцем услуга и контрола да ли је пружаоц услуге усвојио услове за заштиту података, и да ли их спроводи. Такође, није документован начин на који се прати извршење уговора у делу смислу безбедности података. Увидом у уређаје који се на продајним местима користе за допуну електронских месечних карата утврђено је да је на њима могуће видети личне податке грађана, и да их сваки пут када се допуњује карта ови подаци виде, и да их могу видети продавци. Обзиром да се ови подаци „повлаче-читају“ из базе, увид у ове податке може остварити, без ограничења, и пружаоц услуге. Овакво решење није у складу са Законом о заштити података о личности. ЈГСП Нови Сад је у смислу Закона о заштити података о личности, руковаоц подацима. Пружаоц услуге, фирма BusLogic, Пожаревац у овом случају је обрађивач података. Уговором није уређен однос у смислу примене одредаба Закона о заштити података. Правилником о систематизацији није одређено лице које је задужено за сарадњу са пружаоцима услуга.



Илустрација 17. Могу се видети поверљиви подаци грађана



Илустрација 18. Механизам сарадње са пружаоцем услуга

Препорука 6: Препоручујемо Јавном градском саобраћајном предузећу Нови Сад да уреди сарадњу са пружаоцем услуга када је у питању заштита и обрада података, на начин прописан Законом о информационој безбедности и Законом о заштити података о личности.

Механизам сарадње са пружаоцима ИТ услуга може да обухвати скуп политика, процедура, упутстава, докумената, али и активности које су усмерене на идентификацију циљева и послова за чије остварење, тј. обављање се користе информациони системи, израду специфичних захтева у смислу потреба за хадврским, софтверским и људским ресурсима, али и примене стандарда, начине на које се ангажују пружаоци услуга, стандардизацију уговора који се потписују са пружаоцима услуга, а који подразумевају и делове који се односе на информациону безбедност, начин на који се прате пружене услуге, осигурава законитост у раду, обезбеђује континуирана сарадња и комуникација, евидентирање будућих потреба, припрему и имплементацију нових захтева, одређивање лица која су задужена за сарадњу са пружаоцима услуга итд. ИТ послове из области



информационе безбедности када је у питању сарадња са пружаоцима услуга је неопходно детаљно уредити у смислу примене правила и процедура које се односе на безбедност података, праћења активности, ревизије и надзора у оквиру управљања информационом безбедношћу. Када су у питању информациони системи у јавном градском превозу, градске управе или градска предузећа су руковојци подацима, док су у случају ангажовања пружаоца услуга, они обрађивачи. Законом о заштити података о личности, прописане су обавезе и однос руковојца и обрађивача, нарочито када су у питању безбедносне мере. Ако се обрада врши у име руковојца, руковојца може да одреди као обрађивача само оно лице или орган власти који у потпуности гарантује примену одговарајућих техничких, организационих и кадровских мера, на начин који обезбеђује да се обрада врши у складу са одредбама овог закона и да се обезбеђује заштита права лица на које се подаци односе (став 1). Анализом мера заштите, може се закључити да ли су све неопходне мере прописане и примењене. Законом о информационој безбедности уређују се мере заштите ИКТ система од посебног значаја.

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

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

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

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

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



Налаз 2.3: Јавно градско саобраћајно предузеће Нови Сад нема план континуитета пословања у случају раскида сарадње са пружаоцем услуга

Јавно градско саобраћајно предузеће Нови Сад нема план континуитета пословања у случају раскида сарадње са пружаоцем услуга што за последицу може имати отежану продају карата, контролу персонализованих карата и онемогућено информисање грађана у дужем временском периоду.

Не постоји план континуитета пословања у случају раскида сарадње са пружаоцем услуга. У постојећим уговорима са пружаоцем услуга је предвиђена обавеза пружаоца услуга у случају раскида сарадње или не продужења уговора. Да се Испоручилац обавезује да по истеку важења уговора Наручиоцу безусловно испоручи изворни код и све податке са Cloud сервера. Наручилац на тај начин постаје власник изворног кода. Међутим, имајући у виду да ЈГСП Нови Сад не располаже одговарајућом хардверском инфраструктуром, нити је на било који други начин обезбедио неопходну кадровску инфраструктуру у систему који је тренутно у употреби, у случају раскида сарадње било би у дужем временском периоду онемогућено праћење возила па самим тим и онемогућено информисање грађана о кретању возила. Такође, била би отежана продаја карата, контрола персонализованих карата итд. Уговором није предвиђена миграција података, што за последицу може имати отежани или онемогућен наставак коришћења података у новом систему.



Илустрација 19. Континуитет пословања у случају раскида сарадње са пружаоцем услуга

Препорука 7: Препоручујемо Јавно градско саобраћајно предузеће Нови Сад да успостави план континуитета пословања у случају раскида сарадње са пружаоцима услуга.

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

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



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

Међутим, план континуитета пословања се може посматрати као „дводелни“ план – план континуитета пословања у случају ванредних околности у периоду када постоји сарадња са пружаоцем услуга, где је чест случај да се мере и активности дефинишу уговорима и/или техничким спецификацијама и да их у тим ситуацијама спроводи пружаоц услуге, и као план континуитета пословања у случају раскида сарадње са пружаоцима услуга, дакле када више нема сарадње са пружаоцем услуга.

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

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

– Оператор ИКТ система треба да предвиди мере којима се обезбеђује обављање послова у ванредним околностима, а које подразумевају одржавање информационе безбедности на задовољавајућем нивоу, дефинисање одговорности, планова, поступака у случају ванредних догађаја и процедура за опоравак ИКТ система, у оквиру редовних процедура за одржавање информационе безбедности или доношењем посебних процедура.

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

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

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

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

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

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



ЗАКЉУЧАК 3: Успостављен механизам употребе апликативних контрола омогућава контролу података када је у питању продаја карата и праћење кретања возила, и услуге грађанима у смислу информисања и интеграцију са другим информационим системима

Наш закључак заснивамо на следећим налазима:

Налаз 3.1: У Јавном градском саобраћајном предузећу Нови Сад апликативне контроле које се користе за продају карата омогућавају ажурну евиденцију дневних пазара и броја продатих карата, као и извештавање

ЈГСП Нови Сад продају карата врши у својим објектима, или код возача, саму продају обављају запослени на тим пословима у предузећу, а апликативни софтвер се користи ради евиденције пазара, и прегледа броја карата по врстама.

Налаз 3.2: У Јавном градском саобраћајном предузећу Нови Сад апликативне контроле које се користе за праћење возила омогућавају ажурну контролу кретања, као и информисање грађана путем система НСМАРТ

ЈГСП Нови Сад услугу превоза реализује својим возилима, возачи су запослени у предузећу, а апликативне контроле се користе за праћење кретања возила ради бољег управљања и информисања грађана

Када је у питању употреба отворених података, како је наведено на Порталу отворених података²⁴: „Отворени подаци су подаци у машински читљивом и отвореном облику доступни за поновну употребу. Подаци морају бити у облику који је погодан за рачунарску обраду, односно облику који омогућава лак приступ и манипулацију подацима помоћу рачунарских програма (машински читљиви). Подаци морају бити у облику који је погодан за рачунарску обраду, односно облику који омогућава лак приступ и манипулацију подацима помоћу рачунарских програма (машински читљиви). Подаци морају бити доступни у форматима записа чија је употреба могућа без плаћања накнаде или других ограничења, као и за чију обраду је доступан најмање један алат слободног софтвера (отворени облик).“ Отворени подаци могу укључивати информације о тренутној локацији аутобуса (или других возила, као на пример у Београду тролејбуса, трамваја итд.), локацијама стајалишта, ценама карата, тренутних застоја, кашњења, привременој промени траса, информације о томе која су возила прилагођена инвалидима итд. Овако структуране податке могу користити и физичка и правна лица, за израду апликација, што може бити корисно нарочито код лица која не користе званичну апликацију градских предузећа или градских управа.

У граду Новом Саду, могуће је на овај начин добити податке о локацијама станица и реду вожње путем система НСМАРТ. Није омогућено информисање путем стандардних апликација на мобилним уређајима, као што је то Google Maps или слична.

²⁴ <https://data.gov.rs/sr/>

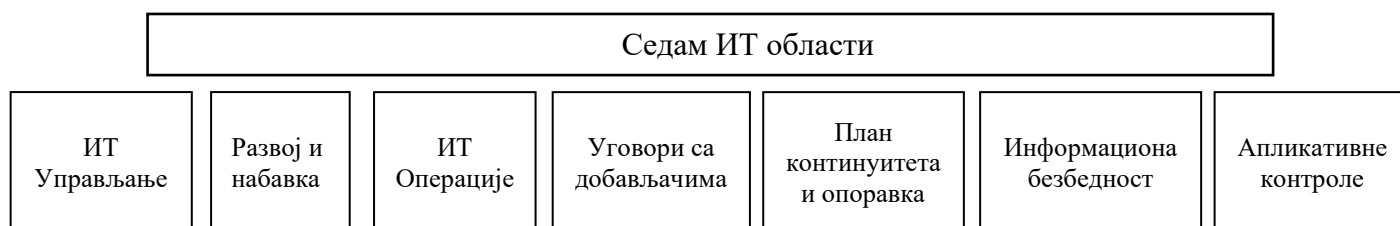


V Прилог

Прилог 1. Методологија у поступку рада

У току предревизије послали смо упитник²⁵ Дирекцији за јавни превоз града Ниша, Јавном комуналном предузећу Шумадија – Крагујевац, Градској управу Града Београда, Секретаријат за јавни превоз и Јавном градском саобраћајном предузећу Нови Сад.

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



Илустрација 20. ИТ области

На основу прикупљених података ревизорски тим је одradio процену ризика. Одабране су следеће три области Успостављање ефективног механизма сарадње са пружаоцима услуга и Апликативна контрола и Информациона безбедност података у највећој мери одређују ризик када је у питању безбедност података путника и корисника ИС у јавном градском превозу у Републици Србији, и пружају простор да се ово питање уреди на модернији и свеобухватнији начин. Не постоји идеално решење, али је циљ ове ревизије да се дође до бољег решења у овој области него што је то сада.

У циљу одговора на ревизорска питања, а имајући у виду законодавни и институционални оквир у периоду 2020 – 2022. године, за субјекте ревизије изабрани су²⁶:

- Дирекцији за јавни превоз града Ниша,
- Јавном комуналном предузећу Шумадија – Крагујевац,
- Градској управу Града Београда, Секретаријат за јавни превоз и
- Јавном градском саобраћајном предузећу Нови Сад

Да бисмо одговорили на ревизорска питања, анализирали смо законодавни и институционални оквир, као и:

За прво ревизијско питање:

- Анализа Акта о безбедности ИКТ система;
- Преглед докумената за процену да су правила и процедуре у складу са Законом о информационој безбедности и Уредбом о ближејем уређењу мера заштите;
- Анализа Правилника о унутрашњем уређењу и систематизацији радних места, посебно у делу који се односи на информациону безбедност;

²⁵ 23-109-0003 упитник

²⁶ 23-109-0004 упитник



- Утврђивање да ли је одговорност за ИТ безбедност формално и јасно наведена;
- Преглед извештаја о спроведеним обукама који се односе на информациону безбедност;
- Анализа шта су примарне контроле физичке безбедности организације субјекта ревизије. Провера да ли одговарају најновијој анализи ризика ако постоји;
- Прегледање локацијских и физичких мера предострожности у смислу кључних елемената ИТ инфраструктуре. Провера какве су контроле за заштиту животне средине успостављене (апарат за гашење пожара, аларм, системи за напајање, итд.);
- Утврђивање да ли су спроведене препоруке релевантних служби;
- Анализа извештаја о инцидентима ради процене шта је предузето;
- Одабир узорка корисничких и системских налога да би се утврдило постојање јасно дефинисане улоге и/или привилегије мапирање према функцијама посла као и овлашћење власника података и руководства (тј. потписане/ писане сагласности);
- Провера процедура у циљу утврђивања колико често се прегледају различити приступи и привилегије које запослени или корисници имају у организацији;
- Интервјуи са узорком корисника и провера упутства да би се утврдило како су корисници упознати са својим одговорностима за заштиту осетљивих информација или имовине, када им се одобри приступ;
- Анализа других привилегија осим лозинке, нпр. како се проверава да ли корисник заиста има довољан приступ и привилегије за тражени ресурс?;
- Анализа документације и процена пројекта, имплементације, приступа и прегледање основе за ревизијски траг. Провера структуре основе за ревизијски траг и других докумената да би се потврдило да је основа за ревизијски траг ефективно пројектована. Испитивање ко може онемогућити или избрисати основе за ревизијски траг;
- Анализа спискова корисника ради оцене ажурности;
- Провера процедуралних мера које је установа предузела да би се ускладила са захтевима поверљивости;
- Провера да ли уговорни услови и обавезе дефинишу безбедносна ограничења и обавезе које контролишу како ће извођачи користити имовину организације и приступати информационим системима и услугама;
- Провера да ли су извођачи извршили повреде безбедности информација. Провера активности руководства у погледу таквих кршења;
- Прегледање матрица улога за утврђивање одговорности за администрирање конфигурације и опсега контроле конфигурације у операцијама;
- Преглед докумената да би се проценило да правила и процедуре узимају у обзир захтеве за континуитет пословања кроз дефинисање организационих циљева за непредвиђене ситуације;
- Преглед или интервјуисање запослених да би се утврдило колико често се правила и процедуре за континуитет пословања ажурирају уколико се промене услови;



- Преглед докумената да би се проценило да план за прављење резервних копија садржи све кључне хардвере, податке, апликативне софтвере;
- Преглед докумената да би се проценило да су израђене детаљне процедуре за прављење резервних копија;
- Преглед докумената да би се проценило да се план за прављење резервних копија адекватно спроводи;
- Анализа евидентирања да би се проценило да је прављење резервних копија почело у утврђеним временским оквирима и да су резервне копије задржане за назначен временски период;
- Провера да је доступна права верзија резервне копије;
- Преглед докумената да би се проценила адекватност локације резервне копије и начина транспорта датотека, итд., резервне копије на локацију резервне копије;
- Провера да је безбедност, како логична тако и физичка, адекватна за локацију резервне копије;
- Провера да се резервне копије датотека могу користити за опоравак;
- Преглед докумената да би се проценило да су израђене детаље процедуре за опоравак и да садрже параметре за поновно постављање система, инсталационе закрпе, успостављајући поставку конфигурације, доступност системске документације и оперативних процедура, реинсталацију апликативних и системских софтвера, доступност најновијих резервних копија, тестирање система;
- Преглед докумената да би се проценило да је ИТ кадар обучен на пољу процедура за прављење резервних копија и опоравак;
- Преглед докумената да би се проценило да ли су све релевантне ставке обухваћене тестирањем;
- Преглед докумената да би се проценило да ли се реализују тестирања у одређеним временским интервалима, и благовремено;
- Преглед докумената да би се проценило да су препоруке након тестирања адекватно праћене и да су план за континуитет пословања и план за опоравак након катастрофе адекватно ажурирани;
- Провера да ли организација контролише да ли су подаци, апликативни софтвер и хардвер били подвргнути променама током поступка прављења резервне копије или током опоравка након катастрофе;
- Провера да ли се организација постарала да је континуитет пословања садржан у споразуму о пружању услуге;
- Анализа стратегије за управљање ризицима;

За друго ревизијско питање:

- Анализирати како је уређен приступ пружаоца услуге информационим системима и серверима, као и другим потребним ресурсима и да ли се то евидентира и где?
- Проверити да ли се прати извршење обавеза пружаоца услуге када су у питању нивои услуга дефинисани уговором?
- Провера извештаја о безбедносним инцидентима и докумената за праћење како би се утврдило које активности субјект предузима када пружаоц услуге крши безбедносна правила и процедуре.



- Провера процедура које је субјекат предузео а које се односе на питања поверљивости.
- Провера да ли уговорни услови и обавезе дефинишу безбедносна ограничења и обавезе које контролишу како ће пружаоц услуге користити имовину организације и приступати информационим системима и услугама.
- Провера да ли су пружаоци услуга извршили повреде безбедности информација. Провера активности руководства у погледу таквих кршења.
- Анализа шта су примарне контроле физичке безбедности система. Провера да ли одговарају најновијој анализи ризика.
- Прегледање локацијских и физичких мера предострожности у смислу кључних елемената ИТ инфраструктуре. Провера какве су контроле за заштиту животне средине успостављене (апарат за гашење пожара, аларм, системи за напајање, итд.)
- Провера процедура у циљу утврђивања колико често се прегледају различити приступи и привилегије које запослени код пружаоца услуга имају
- Провера да ли постоје документоване процедуре за обележавање осетљивих излазних информација апликација и, где је то потребно, слање осетљивих излазних информација на посебне уређаје са контролом приступа.
- Добијање документације и процена пројекта, имплементације, приступа и прегледање.
- Проверити да ли је, уз нулте или минималне трошкове, могуће из постојећег система добити додатне услуге, превасходно у области услуга ка грађанима?
- Да ли постоје капацитети да се услуге које сада обезбеђује пружаоц услуга реализују унутар субјеката?
- Да ли је однос између субјеката и пружаоца услуга у складу са Законом о заштити података о личности?

За треће ревизијско питање:

- Анализа Матрице приступа са улогама и привилегијама како би се утврдило да ли су корисници добили улоге и права у складу са пословима и одговорностима које имају;
- Анализа Log фајлова како би се утврдило да ли су само овлашћена лица приступала систему, и у које сврхе, као и у ком временском тренутку;
- Да ли се систему приступало у "необично" време, ко је и зашто приступао;
- Анализа Извештаја о тестирању апликација: када се тестирала апликација, како, итд.
- Тестирање евидентирања уплате у реалном времену;
- Документација која се односи на ИТ правила и процедуре, које се односе на употребу апликације, процес развоја, техничким захтевима приликом набавке итд.;
- Организациона ИТ структура и опис послова;
- Извештаји о спроведеним обукама - да ли су обављене обуке, када, шта су обухватиле итд.;



- Обављање Интервјуа са одговорним лицима и једним бројем корисника система како би се проверило да ли су упознати са свим доступним функционалностима, да ли су имали предлоге за измене и допуне програма итд;
- Документација субјекта ревизије - анализа шта садржи и у ком обиму, колико је детаљна;
- Уговори са пружаоцима услуга и техничка спецификација;
- Извештаји са продајних места - структура извештаја, динамика достављања, провера тачности и свеобухватности;
- Извештаји који садрже финансијске податке везане за финансирање превоза - провера тачности, свеобухватности.