КОНЕЧЕН ИЗВЕШТАЈ ЗА ИЗВРШЕНА ИТ РЕВИЗИЈА КАКО РЕВИЗИЈА НА УСПЕШНОСТ НА ТЕМА

„Систем за интегрирано планирање на ресурсите (ИПР систем)

08 2024 03 11

9 ИНДУСТРИЈА, ИНОВАЦИЈА И ИНФРАСТРУКТУРА

КОНЕЧЕН ИЗВЕШТАЈ ЗА ИЗВРШЕНА ИТ РЕВИЗИЈА КАКО РЕВИЗИЈА НА УСПЕШНОСТ НА ТЕМА

"Систем за интегрирано планирање на ресурсите (ИПР систем)

08 2024 03 11

Скопје, Јуни 2025

ИПР СИСТЕМ

СОДРЖИНА

Список на кратенки

Владата	Влада на Република Северна Македонија
Министерството	Министерство за информатичко општество и администрација[1]
МФ	Министерство за финансии
МЈА	Министерство за јавна администрација
СОЗР/Службата	Служба за општи и заеднички работи на Владата на Република Северна Македонија
ИКТ	Информациско комуникациска технологија
ИПР/ERP Ultima	Систем за интегрирано планирање на ресурсите
ИТ	Информатичка технологија
ДДВ	Данок на додадена вредност
CIS	Center for Internet Security (Центар за интернет безбедност)

[1] Член 28 точка 6 од Законот за организација и работа на органите на државната управа („Службен весник на Република Македонија" број 58/2000, 44/2002, 82/2008, 167/10 и 51/11 и „Службен весник на Република Северна Македонија" број 96/19, 110/19, 154/19 и 121/2024) - Министерството за информатичко општество и администрација продолжува да работи како Министерство за дигитална трансформација и како Министерство за јавна администрација, со надлежности утврдени со овој закон, како правни наследници на ова министерство. Министерството за дигитална трансформација го задржува единствениот даночен број на Министерството за информатичко општество и администрација, а Министерството за јавна администрација ќе добие нов даночен број најдоцна во рок од три дена од денот на конституирање на Владата.

Поимник

Симетрична енкрипција	Метод за шифрирање на податоци каде што се користи ист клуч и за енкрипција (шифрирање) и за декрипција (дешифрирање). Овој пристап е побрз и поефикасен, но бара безбедно споделување и чување на клучот, бидејќи компромитацијата на клучот значи дека енкриптираните податоци може лесно да се дешифрираат.
Асиметрична енкрипција	Користи два различни, но математички поврзани клуча – јавен и приватен. Јавниот клуч се користи за енкрипција, додека приватниот клуч служи за декрипција. Овој метод е побезбеден за размена на податоци, бидејќи приватниот клуч не треба да се споделува, но е побавен во споредба со симетричната енкрипција.
Криптиран тунел за ВПН	Метод за заштитен пренос на податоци преку јавна мрежа (како интернетот), во кој податоците се криптираат пред да бидат испратени и дешифрираат по пристигнувањето на одредениот сервер или крајна точка. Обезбедува приватност и сигурност на преносот на информации, спречувајќи неовластен пристап и посматрање на податоците додека се пренесуваат помеѓу две точки (на пример, помеѓу корисникот и серверот).
Повеќефакторска автентикација (MFA)	Multi-Factor Authentication е безбедносен процес кој бара од корисникот да ја потврди својата идентитет преку два или повеќе независни фактори, пред да му се дозволи пристап до систем или апликација.
Релациона база на податоци	Тип на база на податоци која ги складира податоците во табели (познати како релации) кои се поврзани преку заеднички атрибути или клучеви.
Енкрипција	Претворање на податоци или информации во кодирана форма
БИ извештај	Документ кој содржи анализа на податоци и информации што се користат за донесување на деловни одлуки.
IDI LOTA иницијативата	Се однесува на програма на IDI (INTOSAI Development Initiative) што има за цел да ги подобри дигиталните инфраструктури и технологиите на Врховните ревизорски институции.
Active Directory автентикација /AD	AD автентикацијата е систем базиран на Windows сервер кој ги автентицира и овластува корисниците, крајните точки и услугите на Active Directory. ИТ тимовите може да користат автентикација од AD за да го насочат управувањето со корисникот и правата додека постигнуваат централизирана контрола врз уредите и корисничките конфигурации.

ВПН (Virtual Private Network) конекција	Технологија која овозможува безбедно и приватно поврзување на два или повеќе компјутери преку јавната интернет мрежа.
Софтверски закрпи	Надградби или исправки на софтверот кои се издаваат од страна на производителот
Логови	Записи кои бележат настани, активности или трансакции кои се случуваат во систем, апликација или уред.
Криптиран/ криптирано/ криптирани	претворање на информации или податоци во нечитлива форма преку користење на криптографски алгоритам, со цел да се заштитат од неовластен пристап.
Ниво на услуги (SLA)	SLA (Service Level Agreement) или Договор за ниво на услуга е официјален договор помеѓу провајдерот на услуга и клиентот кој ги дефинира условите и обврските што се однесуваат на квалитетот, брзината и други аспекти на услугата што ќе се испорача.
Автентикација	Процес на проверка на идентитетот на корисник, систем или уред за да се утврди дали лицето или системот при најава е точно.
Декрипција	Процес на враќање на криптираните податоци во нивната оригинална, читлива форма.
Бекап	Правење резервна копија е процес на создавање копија на податоци или целокупниот систем за да се обезбеди нивно зачувување во случај на губење, оштетување или неовластен пристап.
Криптирана конекција	Вид на безбедна комуникација помеѓу два уреди (на пр., компјутер и сервер), при која податоците што се пренесуваат се шифрирани така што трети лица не можат да ги прочитаат или изменат.
Сајбер безбедност	Активности за идентификација, превенција и одговор на закани во дигиталното опкружување, со цел да се заштитат информациските системи и податоци од компромитација, манипулација или уништување.

1

Резиме

Број: 34-543/5

Дата: 19.06.2025

➘ **Поради сензитивноста на одредени информации, истите не се објавени во извештајот.**

Извршивме ИТ ревизија како ревизија на успешност на темата „Систем за интегрирано планирање на ресурсите - ИПР систем" со цел да дадеме одговор на прашањето

> **„Дали се утврдени и имплементирани мерки за ефикасна и целосна заштита на податоците во системот за интегрирано планирање со ресурсите?**

Ревизијата на успешност е извршена согласно Годишната програма за работа на Државниот завод за ревизија за 2024 година.

Со ревизија на успешност опфативме период од 01.01.2021 година до 31.01.2025 година, при што беше опфатен период пред и период по завршување на ревизијата, до денот на изготвување на овој извештај.

За да одговориме на главното ревизорско прашање, ги определивме следните специфични прашања:

- ➘ **Дали се уредени правата и обврските за заштита и пристап до податоците на институциите корисници на системот?**
- ➘ **Дали поставената конфигурација овозможува безбеден пристап до ресурсите и достапност на системот за интегрирано планирање?**
- ➘ **Дали човечките капацитети и имплементираните апликациски контроли обезбедуваат заштита и пристап до податоците на институциите корисници на системот?**

Со спроведената ревизија и применетата ревизорска методологија, прибраните ревизорски докази стекнавме разумно уверување дека:

Системот за интегрирано планирање на ресурсите (ИПР систем) го употребува Службата за општи и заеднички работи на Владата на Република Северна Македонија за ефикасно и современо извршување на сметководствено - финансиски услуги за повеќе државни институции. Иако, ИПР системот е имплементиран во 2016 година, се уште отсуствува правен акт кој ги регулира правата и обврските на Министерството како сопственик и на Службата како корисник на системот, што создава ризик од несоодветно управување со податоците. Кај ИПР системот отсуствува интегрираност на модулите во системот. Одржувањето не е континуирано и навремено обезбедено со потпишани договори. Отсуствуваат дефинирани процедури за управување со пристапи и заштита на податоците, и ажурирана документација која ја покрива конфигурацијата на системот. Не се преземени активности за редовна проверка на резервната копија (бекап) на податоците, и не постојат адекватни контроли за мониторирање на безбедноста на системот. Исто така, отсуствуваат политики и процедури за редовно тестирање на резервни копии. Работните станици користат застарен оперативен систем без безбедносни ажурирања и поддршка од производителот, што го зголемува ризикот од безбедносни напади и неовластен пристап. Конфигурацијата на ВПН пристапот, без повеќе факторска автентикација односно потврда на идентитет преку два или повеќе независни фактори и со заедничка лозинка, ја зголемува веројатноста за компромитирање на системот. Недостигот на човечки ресурси влијае на навремено и ефикасно извршување на задачите, со постојан одлив на вработени поради пензионирање и недостаток на вработени со соодветни вештини и знаења.

Ваквите состојби како и неинтегрираноста на сите модули во системот укажуваат дека утврдените и имплементираните мерки не се доволни за ефикасна и целосна заштита на податоците во ИПР системот, што го изложува системот на потенцијални безбедносни ризици и компромитирање на доверливоста на податоците.

Ревизорските активности беа насочени кон утврдени ризици во три области при што се констатирани следните состојби:

Област 1 - ИТ Управување – Правна рамка

Поради несоодветно планирање и ненавремено спроведување на постапките за одржување на системот, во период од **522 дена не бил склучен договор за регулирање на правата и обврските за негово одржување.** Ваквата состојба влијае на безбедноста, достапноста и точноста на податоците, како и до потешкотии во изготвувањето на финансиските извештаи за соодветни временски периоди.

Во периодот на одржување не се преземени активности за **редовна проверка на резервната копија (бекап) на податоците,** [redacted]

Отсуствува правен акт со кој се регулираат правата и обврските на Министерството како сопственик и Службата како корисник, што создава правна и оперативна неизвесност, зголемен ризик од несоодветно управување со податоците, квалитетот на податоците и информациите кои ги даваат финансиските извештаи, како и безбедносни пропусти.

Службата во договорите со кои ги уредува правата и обврските помеѓу давателот и корисниците на сметководствено-финансиските услуги **не ја дефинира сопственоста на податоците и нема јасна распределба на одговорностите.**

Службата нема пропишано процедури кои ги дефинираат **надлежностите и привилегиите за пристап** при

воведување на нов субјект или корисник на услугите како и при прекинување на давање на услуги.

Системот за интегрирано планирање на ресурсите е евидентиран во деловните книги на Министерството за **1.294 илјади денари помалку од неговата набавна вредност и истиот не е зголемен за износ од 18.065 илјади денари за вредноста на адаптивното одржување на системот.** Ваквата состојба влијае на точноста на финансиските извештаи и може да предизвика проблеми во планирањето на идни активности и испорака на услуги, како и на квалитетот на податоците и информациите кои го даваат финансиските извештаи.

Службата, како корисник на системот за интегрирано планирање на ресурсите која опслужува правни субјекти, **нема преземено активности за евидентирање на системот и неговите надградби во вонбилансна евиденција**.

Област 2 - ИТ Операции – Системски подесувања (конфигурација) на софтверите за пристап до ресурсите на системот за интегрирано планирање

Во Службата **недостасуваат стратешки документи кои јасно ги дефинираат насоките за развој, одржување и надградба на информациските системи, како и политики и процедури за управување со податоци** што може да доведе до неефективно управување и ранливост од безбедносни закани.

Службата **нема ажурирана системска документација** вклучувајќи ја и конфигурацијата на базите на податоци.

Пристапот до ИПР системот се реализира од повеќе локации преку ВПН конекции. **Лозинките не се временски ограничени и воопшто не се менуваат, додека администраторите користат општи кориснички имиња.**

Воспоставената конфигурацијата за снимање на настани (логови) во системот резултира со автоматско бришење на најстарите записи. **Не постои локација за чување на ревизорската трага, а системот не зачувува информации за сите настани,** што ја оневозможува контролата на пристапот и идентификацијата на неовластени активности.

[redacted] Дополнително, **на 131 база на податоци не е овозможена енкрипција** (претворање на податоци или информации во кодирана форма), што ја зголемува безбедносната ранливост и ризикот од неовластен пристап и компромитирање на податоците.

Резервните копии не се претворени во нечитлива форма, не се чуваат на надворешна локација, и не постојат формални политики и процедури за нивно редовно тестирање и обновување.

Работните станици користат застарен оперативен систем без безбедносни ажурирања и поддршка од производителот, што го зголемува ризикот од безбедносни напади и неовластен пристап. Исто така, конфигурацијата на ВПН пристапот, **без повеќе факторска автентикација** односно потврда на идентитет преку два или повеќе независни фактори и со заедничка лозинка, ја зголемува веројатноста за компромитирање на системот.

Област 3 - Апликациски контроли - Човечки капацитети и апликациски контроли на системот за ИПР

Недостигот на човечки ресурси влијае на навремено и ефикасно извршување на задачите, со **постојан одлив на вработени поради пензионирање и недостаток на вработени со соодветни вештини и знаења.**

Недостатокот на интеграција на модулите и нецелосната искористеност на постоечките функционалности на системот доведуваат до неможност за автоматизирање на процесите. Ова создава потреба за **двојно внесување на податоци**, што го зголемува ризикот од грешки и неефикасност. Дополнително, **два од модулиите што се наменети за следење на реализацијата на договорите и за буџетското работење воопшто не се користат.**

Одредени надградби на системот, како што е БИ извештајот, **не се интегрирани во ИПР системот**. БИ извештајот е наменет за вработени во институциите кои се вклучени во планирањето. За овие корисници не е извршена обука иако биле организирани обуки за вработените во Службата.

Во извештаите за надградба се евидентираат активности кои се повторуваат во подолг временски период и се однесуваат на исти задачи. И по направените надградби, **модулите сè уште не се интегрирани, не постои поврзување со платформата за Интероперабилност, а модулот за следење на реализација на договори не е инсталиран и не се користи, иако е дел од тендерската документација за набавка на ИПР системот.** Повторувањето на истите активности укажува на недостаток на ефективно планирање и координација, што доведува до неефикасност во процесот и дополнителни трошоци.

Недостаток на контролите за пристап до модулите и податоците како:

- отсуство на одобрени процедури за управување со бази на податоци и пропишана постапка за информирање на ИТ одделението за креирање и деактивирање кориснички сметки;
- активни кориснички сметки на лица кои не се вработени во Службата;
- неажуриран регистар на корисници и привилегии за пристап и отсуство на контрола за проверка на барањата за пристап и статус на пристапите;

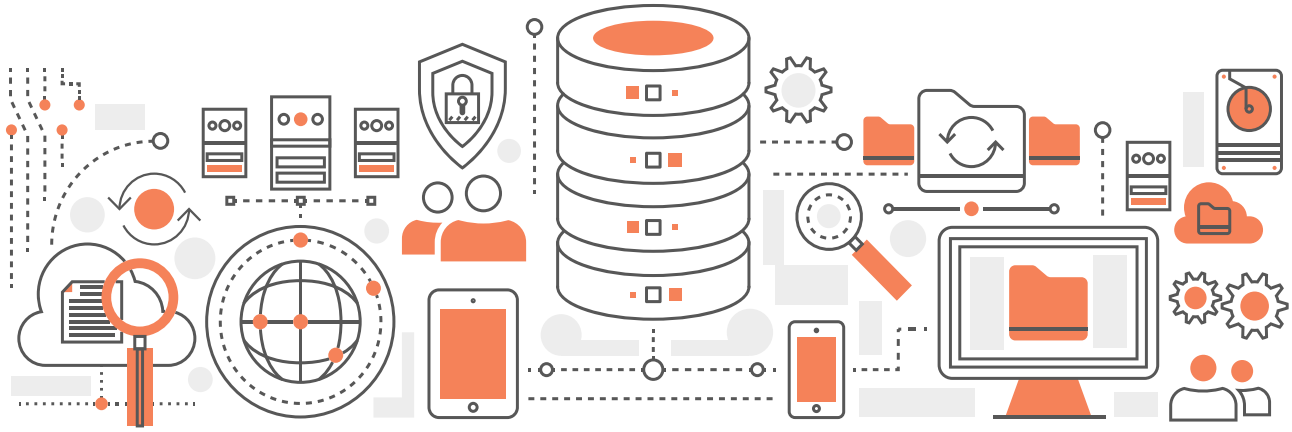
- **отсуството на политика за периодично менување на лозинки ја зголемува безбедносната ранливост на системот;**
- **отсуството на дневник на настани (логови) за пристап и промени во базата на податоци ја отежнува можноста за мониторинг и ревизија;**
- **нецелосно разграничување на должности по корисници и недостаток на ревизорска трага за настанатите промени на податоците.**

Придружната документација за извршените трансакции во системот **се чува само во хартиена форма**, без електронски копии, што го ограничува процесот на контрола и ги зголемува ризиците од губење на важни документи.

Ненавременото евидентирање на обврските во моментот на настанување, односно фактурите и нивната придружна документација се евидентираат во системот само по нивното одобрение за плаќање, што не овозможува хронолошко внесување на финансиските промени. Овој пристап го зголемува ризикот од нецелосно евидентирање на обврските и влијае на точноста на финансиските извештаи и извештаите за финансиската состојба како и на квалитетот на податоците и информациите кои ги даваат истите.

За надминување на наведените состојби дадовме препораки со цел да се преземат активности со кои ќе се создадат услови за заштита на податоците, со јасно дефинирање на правата и обврските на институциите корисници на системот, поставување на соодветни безбедносни конфигурации за пристап и интегрирање на безбедносни апликациски контроли, како и вложување во човечки капацитети кои ќе обезбедат ефикасно извршување на задачите, како и континуирана заштита на податоците и пристапот до ресурсите на системот за интегрирано планирање.

Од страна на министерот на Министерството за дигитална трансформација доставени се забелешки на Нацрт извештајот на овластениот државен ревизор. Истите се разгледани и утврдено е дека седум забелешки претставуваат известување за преземени или планирани активности и една забелешка не е прифатена.



1 ВОВЕД

1 ВОВЕД

Степенот на развој на информатичката технологија овозможува електронско опфаќање, зачувување, обработка, повратување и испорака на информациите, што пак значително придонесува кон подобрување на точноста, доверливоста и навременоста на информациите. Дополнително, процесот на испорака на јавните услуги брзо се трансформира од физички во електронски, што ќе доведе до тоа владите да функционираат како дигитални платформи, овозможувајќи услуги и инфраструктура за други информациски системи базирани на информатичка технологија. Исто така, со ваквиот начин на испорака на услугите постои потреба да се осигура дека внатрешните ИТ контроли ќе ја зачуваат доверливоста, интегритетот и достапноста на податоците, кои се прифатени од субјектите во јавниот сектор.

1.1. Основ и причини за извршување на ревизијата

Согласно Годишната програма за работа на Државниот завод за ревизија за 2024 година планирана е ИТ ревизија како ревизија на успешност на тема „Систем за интегрирано планирање на ресурсите - ИПР систем".

Ревизијата е планирана како ревизија на успешност која претставува пилот ревизија во рамките на IDI LOTA иницијативата за воведување на нови ИТ технологии и алатки во ревизијата.

Темата за ревизијата е значајна од аспект на тоа да се оценат состојбите со безбедноста на информацискиот систем во Министерството за информатичко општество и администрација и Службата за општи и заеднички работи и да се даде придонес во подобрување на ефективноста на информацискиот систем во делот на водење на финансиското сметководство за субјектите со кои се потпишани договори за ваков тип на услуга, особено во делот на доверливост, достапност и комплетност на податоците во овој ИКТ систем.

Државниот завод за ревизија има потпишано Меморандум за соработка со Канцеларијата на главниот ревизор на Норвешка, во кој една од активностите е унапредување на ревизиите на успешност. Во оваа ревизија применети се ИКТ алатки за ревизија на конфигурирањето на оперативен систем и домен[2], како дел од активностите со Канцеларијата на главниот ревизор на Норвешка.

Темата на ревизија е поврзана и со остварување на **целите за одржлив развој** како една од приоритетните цели на Државниот завод за ревизија согласно Стратешкиот план за ревизија за период 2024–2027 година. Имено, **ревизијата е поврзана со Цел 9. Индустрија, иновација и инфраструктура, Подцел 9.в Значително да се зголеми пристапот до информатички и до комуникациски технологии.**

1.2. Предмет на ревизија

Предмет на ревизијата е да процениме дали преземените мерки од надлежните органи обезбедуваат ефикасна заштита на податоците во системот за ИПР, особено во делот на доверливоста, интегритетот и достапноста на податоците.

Службата за општи и заеднички работи на Владата на Република Северна Македонија дава сметководствени и книговодствени услуги за повеќе државни институции во Република Северна Македонија. Со цел поефикасно и посовремено извршување на активностите од своето работење, Министерството за информатичко општество и администрација и Министерството за транспорт и врски во 2014 година склучуваат договор[3] за групна набавка, односно јавна набавка за ИПР систем на државни институции за кои услугата ја обезбедува Службата за општи и заеднички работи на Република Македонија. Министерството за информатичко општество и администрација како реализатор на набавката (Набавка на услуга - Систем за интегрирано планирање на ресурсите на државни институции за кои услугата ја обезбедува Службата за општи и заеднички работи на Владата на Република Македонија) и склучен договор[4] во вредност од 1.743 илјади денари, има набавено Систем за Интегрирано планирање на ресурсите (ИПР систем), кој е во функција и се користи од страна на Службата за извршување на секојдневните обврски, за институциите кои се корисници на нивните услуги.

[2] MS Windows SQL сервер и доменскиот контролер MS Windows server AD
[3] Број 03-3040/1 од 16.09.2014 година
[4] Број 15/4-1300/29 од 16.07.2015 година

При набавката на системот за Интегрирано планирање на ресурсите (ИПР), предвидено е истиот да биде клиентско – серверско решение кое ќе ги содржи следните софтверски модули:

- **Буџетско работење** (планирање на буџетот (годишно, квартално и месечно планирање на приходи и расходи, проектирање на буџетот за следни 3 години), внесување и одобрување на планови како и следење на негова реализација на повеќе институции (расходи и приходи по сите типови на сметки, контрола на реализацијата на плаќања, размена на податоци со МФ), поврзан со останатите модули од интегрираниот систем),

- **Финансиско работење** (водење на финансиското и сметководствено работење на повеќе институции, со една или повеќе сметки при што треба да ги обедини од финансиски аспект сите останати модули),

- **Благајничко работење** (благајничкото работење за повеќе институции со можност за работа со повеќе благајни (денарска и девизна) при што треба да е поврзан со останатите модули од интегрираниот систем),

- **Основни средства** (евиденција на основни средства, книжења, пресметки на амортизација и ревалоризација, генерирање на налози за евидентирани приеми и пресметки за повеќе институции при што истиот да е поврзан со останатите модули од интегрираниот систем),

- **Материјално и магацинско работење** со ситен инвентар (магацинска и материјална евиденција за повеќе институции со повеќе магацини, генерирање на налози за евидентирани приеми и пресметки како и истиот да е поврзан со останатите модули од интегрираниот систем) и

- **Следење на реализација на договори** (следење на реализацијата на договорите за набавки на повеќе институции, следење на набавките на материјали, средства и услуги и потрошокот на истите при што истиот да е поврзан со останатите модули од интегрираниот систем).

Непречената и континуирана функционирање на ИПР системот зависи од неговото редовно одржување и одржување на неговите функционалности. Согласно тендерската документација за набавка на услуги за одржување, ресурсите во облакот се димензионирани за вкупно 50 институции. Според техничката спецификација, системот активно го користат 31 институција, со повеќе од 40 активни бази, а клиентскиот дел е инсталиран на околу 150 работни станици. Бројот на институции и работни станици може да се зголемува во согласност со потребите и барањата на институциите, при што договорниот орган има можност да обезбеди дополнителни ресурси во облакот. Рокот за имплементација на договорот е 4 месеци, додека гарантниот период изнесува 24 месеци. Договорот и гарантниот период завршуваат на 16.11.2017 година, а системот е во употреба од 2016 година.

Конфигурацијата на поставеното решение вклучувајќи резервна локација, поврзување и пристап до системот е прикажана на инфографик број 1:

1.3. Законска регулатива

Законската регулатива која го опфаќа предметот на ревизија претставува темел за утврдување на законските обврски и рамките за работењето на субјектите кои се предмет на ревизија.

Оваа регулатива ги вклучува следниве значајни законски акти и стандарди:

- Закон за сметководството за буџетите и буџетските корисници[5];
- Законот за јавна внатрешна финансиска контрола[6];
- Закон за системот на внатрешна финансиска контрола во јавниот сектор[7];
- Стандарди за внатрешна контрола во јавниот сектор[8];
- Закон за Владата на Република Северна Македонија[9];
- Закон за организација и работа на органите на државната управа[10];
- Закон за заштита на личните податоци[11];
- Закон за користење и располагање со стварите во државна сопственост и со стварите во општинска сопственост[12].

Подзаконски акти од областа:

- Одлука за основање на Служба за општи и заеднички работи на Владата на Република Северна Македонија;
- Уредба за условите и начинот на користење на услугите што ги врши Служба за општи и заеднички работи во Владата на Република Северна Македонија;
- Правилник за сметководството за буџетите и буџетските корисници.
- Заклучок од 131-ва седница на Владата на Република Северна Македонија одржана на 21.02.2023 година кој се однесува на Агенда за дигитална трансформација.

Стандарди со најдобри практики:

- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements[13];
- CIS Microsoft SQL Server 2016 Benchmark[14].

1.4. Институционална рамка

Ревизијата „Систем за интегрирано планирање на ресурсите - ИПР систем“ опфаќа анализирање и оценување на сигурноста, функционалноста и ефикасноста на овој систем, кој е во сопственост на Министерството, а истиот е користен од страна на Службата која дава сметководствено - финансиски услуги за повеќе државни институции во Република Северна Македонија. (Прилог 3)

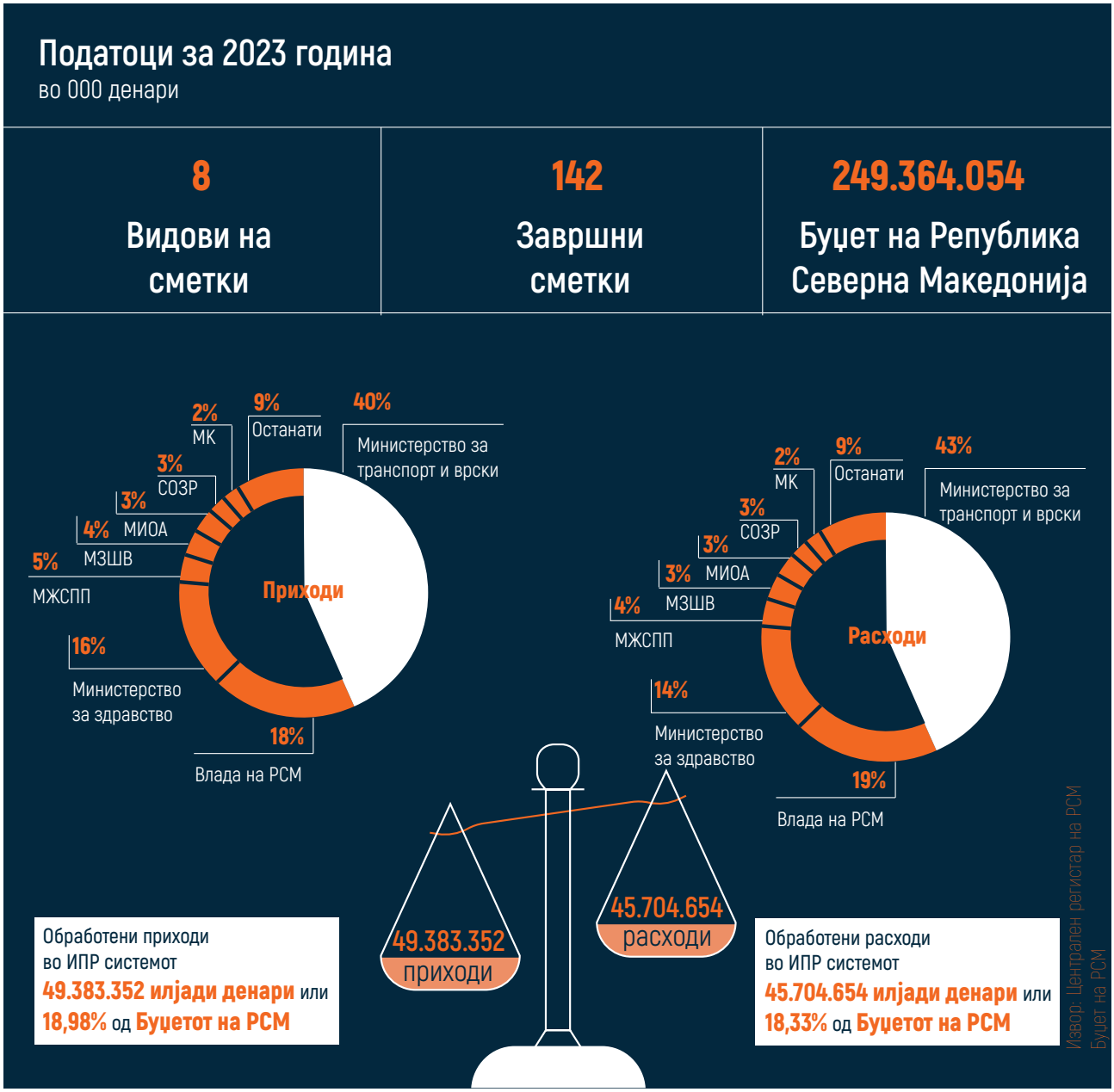
[5] Службен весник на Република Македонија бр. 61/02, 98/02, 81/05, 24/11, 145/15,170/17 и Службен Весник на Република Северна Македонија број 122/21;
[6] Службен весник на Република Македонија бр. 90/09, 12/11, 188/13, 192/15, 147/17;
[7] Службен весник на Република Северна Македонија бр. 255/24;
[8] Службен весник на Република Македонија бр. 147/10;
[9] Службен весник на Република Македонија број 59/00, -, 140/18 и Службен Весник на Република Северна Македонија број 98/19;
[10] Службен весник на Република Македонија број 58/00, - 51/11 и Службен Весник на Република Северна Македонија број 96/19, 110/19, 154/19 и 121/24;
[11] Службен весник на Република Северна Македонија бр. 42/20, 294/21;
[12] Службен весник на Република Македонија бр. 78/15, 106/15, 153/15, 190/16, 21/18, Службен весник на Република Северна Македонија бр. 101/19, 275/19, 122/21;
[13] https://www.iso.org/standard/27001
[14] https://www.cisecurity.org/cis-benchmarks

1.5. Финансирање на дејноста

Ревизијата изврши анализа на склучените договори за одржување на ИПР системот за превентивно и адаптивно одржување на системот за периодот опфатен со ревизија односно од 2021 до 2024 година. Министерството има склучено договор и два анекса на договорот во вкупна вредност од 14.400 илјади денари без вклучен ДДВ или 16.992 илјади денари со ДДВ.

Со овој систем се обработуваат податоци за 40 правни субјекти односно вкупно обработени приходи во износ од 49.383.352 илјади денари или 18,98% од Буџетот на државата и расходи во износ од 45.704.654 илјади денари или 18,33% од Буџетот на државата за 2023 година.

Детален приказ, даден на инфографик број 2.



2

ЦЕЛИ, ОПФАТ И МЕТОДОЛОГИЈА

2 ЦЕЛИ, ОПФАТ И МЕТОДОЛОГИЈА НА РЕВИЗИЈАТА

2.1. Цели на ревизијата

Целта на ИТ ревизијата како ревизија на успешност е да се даде оценка на преземените мерки од надлежните органи за обезбедување на ефикасна заштита на податоците во системот, односно да се утврди дали системот обезбедува доволно ниво на заштита, стабилност и функционалност, со фокус на унапредување на безбедносните практики и управувањето со информациите.

Системот за ИПР, кој опслужува 40 државни институции, е клучен за доверливоста, интегритетот и достапноста на финансиските податоци што ги користат овие субјекти.

Специфичните цели на ИТ ревизијата како ревизија на успешност, кои се поврзани со поединечните предметни области на ревизијата, се однесуваат на оценување **дали:**

- се уредени правата и обврските за заштита и пристап до податоците на институциите корисници на системот;
- поставената конфигурација овозможува безбеден пристап до ресурсите и достапност на системот за интегрирано планирање и
- човечките капацитети и имплементираните апликациски контроли обезбедуваат заштита и пристап до податоците на институциите корисници на системот.

Препораките кои произлегуваат од оваа ревизија, претставуваат додадена вредност во насока на подобрување на утврдените состојби во областа, ефикасна и целосна заштита на податоците во системот за интегрирано планирање со ресурсите, како и поголема стабилност и функционалност како и унапредување на безбедносните практики и управувањето со информациите на системот.

2.2. Ревизорски прашања

Ревизијата на успешност на тема „Систем за интегрирано планирање на ресурсите - ИПР систем" е активност која ја спроведовме со цел да дадеме оценка и да одговориме на главното ревизорско прашање:

„Дали се утврдени и имплементирани мерки за ефикасна и целосна заштита на податоците во системот за интегрирано планирање со ресурсите?

Специфични прашања по утврдени области се:

- Дали се уредени правата и обврските за заштита и пристап до податоците на институциите корисници на системот?
- Дали поставената конфигурација овозможува безбеден пристап до ресурсите и достапност на системот за интегрирано планирање?
- Дали човечките капацитети и имплементираните апликациски контроли обезбедуваат заштита и пристап до податоците на институциите корисници на системот?

2.3. Опфат на ревизијата

Со ИТ ревизијата како ревизија на успешност, опфативме период од 2021 до 2024 година, а одредени прашања и настани се опфатени претходно и последователно до денот на известување за ревизијата.

Согласно утврдените ризици по добиените прелиминарни информации, а врз основа на избран примерок, извршивме увид на локациите каде корисниците пристапуваат до системот, анализа на работните процеси, управувањето

со кориснички сметки и анализа на податоци од системот. Исто така, за првпат воведовме нов начин на собирање на ревизорски докази и констатирање на состојби при што со ИТ алатки е направена контрола на конфигурацијата на дата базите, апликативните контроли на ИПР системот, како и конфигурацијата на доменскиот контролер на Службата.

Со оваа ревизија покрај Министерство за информатичко општество и администрација, односно Министерство за дигитална трансформација и Службата опфатени се дополнително и 45 институции (Прилог 3) кои се поврзани со услугите кои ги обезбедува Службата, а се однесуваат на сметководствено - финансиски работи кои дополнително беа опфатени и со анкетни прашалници.

Дополнително до субјектите опфатени со ревизијата беа доставени прашалници, направени се интервјуа со одговорните лица и увид во бараната документација.

Ревизорските активности кои ревизорскиот тим ги спроведе во субјектите опфатени со ревизијата беа насочени кон повеќе области и под области:

1 **ИТ Управување – Правна рамка**

Уредени права и обврски за заштита и пристап до податоците на институциите корисници на системот.

2 **ИТ Операции – Системски подесувања (конфигурација) на софтверите за пристап до ресурсите на системот за интегрирано планирање**

Конфигурацијата овозможува безбеден пристап до ресурсите и достапност на системот за интегрирано планирање.

3 **Апликациски контроли - Човечки капацитети и апликациски контроли на системот за ИПР**

Човечки капацитети за непречено користење на системот и имплементирани апликациски контроли во модулите на системот за ИПР.

2.4. Критериуми за ревизија

За оценка на ефективноста на системот за интегрирано планирање на ресурсите се искористени критериумите и показатели за оценка прикажани во Прилог бр. 1 кон ревизорскиот извештај.

2.5. Методологија на ревизијата

2.5.1. ИТ ревизијата како ревизија на успешност е извршена во согласност со стандардите на ISSAI за ревизија на успешност, Прирачникот за ревизија на успешност на Државниот завод за ревизија, Прирачникот за ИТ ревизија на ДЗР, Кодексот на етика на Државниот завод за ревизија и Упатството за ревизија на информациски системи на INTOSAI-GUID 5100 и најдобрите практики за информациска безбедност.

2.5.2. Кај оваа ревизија на успешност избравме и применивме комбиниран пристап од пристапот ориентиран кон системите, пристапот ориентиран кон проблемите и пристапот ориентиран кон резултатите. Ревизијата беше насочена кон проверка, анализа и испитување на: правата и обврските на договорните страни за заштита и пристап до податоците на институциите корисници на системот, поставеноста на системската конфигурација со цел да се обезбеди безбеден пристап до ресурсите и достапност на системот, мерките за обезбедена заштита и осигурен брз повратак во случај на катастрофа, пристап на корисниците на работните станици каде е инсталирана апликацијата до серверите. Начинот на контрола за правилно користење на системот и пристапот до ресурсите и податоците, како и имплементираните апликациски контроли во модулите на системот. Ревизијата беше насочена кон испитување, верификување и анализирање на причините за неефикасност на ИПР системот заради неможност за целосно интегрирање и преземање на податоците. Исто така, ревизијата беше насочена кон постигнатите резултати од имплементација н ИПР системот како што е замислен и дизајниран.

2.5.3. Со цел добивање на релевантни и доволни ревизорски докази кои водат кон ревизорските наоди, заклучоци и препораки, ги користевме методологијата и техниките на ревизија на успешност:

- проучување на законска и друга регулатива од областа предмет на ревизија,
- разговори со лица релевантни за темата на ревизијата,
- прашалници до релевантните субјекти,
- проверка на документација,
- анализа на податоци и информации,
- анализа на датотеки од настани/ логови од информациски системи
- физичко набљудување и увид на лице место со

фотографирање и
интернет истражување

2.5.4. Ревизијата на успешност како ИТ ревизија е извршена во периодот од 11.03.2024 до 31.03.2025 година од тим на Државниот завод за ревизија.

2.5.5. Резултатите од спроведената ревизија на успешност беа презентирани на завршен состанок со претставници на субјектите предмет на ревизија на ден 04.04.2025 година.

На ден 09.06.2025 година добиени се забелешки бр. 02-982/3 од 21.05.2025 година од г. Стефан Андоновски, министер на Министерството за дигитална трансформација, заведени во Државниот завод за ревизија под број 34-543/4. Забелешките се однесуваат на препораката број 1 за точката 3.1.2, препораката број 2 за точката 3.1.2., препораката број 3 за точката 3.1.1.1 и 3.1.1.2, препораката број 4 за точката 3.1.1.1, 3.1.1.5 и 3.1.3.2, препораката број 5 за точката 3.1.1.3, препораката број 6 за точката 3.1.1.3, препораката број 7 за точката 3.1.1.4 и препораката број 8 за точката 3.1.1. и 3.3.1.1. Забелешките се разгледани и е констатирано дека 7 (седум забелешки претставуваат известување за преземените активности и една забелешка за препораката број 2 за точката 3.1.2 не се прифаќа.

Забелешките и содржината на одговорот на забелешките се прилог на Конечниот извештај на овластениот државен ревизор.


РЕВИЗОРСКИ
НАОДИ

3 РЕВИЗОРСКИ НАОДИ

3.1. Област ИТ Управување – Правна рамка (Права и обврски за заштита и пристап до податоците на институциите корисници на системот)

3.1.1. Ниво на услуги (SLA) со економскиот оператор кој го одржува системот за ИПР и системскиот пристап

3.1.1.1 Службата врши општи работи и услуги за потребите на Претседателот на државата, Владата, министерствата и други државни органи, врз основа на склучени договори. Службата покрај другите работи и услуги дава и сметководствено - финансиски услуги. За извршување на овие услуги користи апликативен софтвер. Во 2014 година, согласно технолошкиот развој, за потребите на Службата, Министерството за информатичко општество и администрација и Министерството за транспорт и врски склучуваат договор за групна набавка[15], односно јавна набавка за ИПР систем на државни институции за кои услугата ја обезбедува Службата за општи и заеднички работи на Република Македонија. Министерството за информатичко општество и администрација како реализатор на набавката (Набавка на услуга - Систем за интегрирано планирање на ресурсите на државни институции за кои услугата ја обезбедува Службата за општи и заеднички работи на Владата на Република Македонија) и склучен договор[16] во вредност од 1.743 илјади денари, има набавено ИПР систем, кој е во функција и се користи од страна на Службата за извршување на секојдневните работи и услуги, за институциите кои се корисници на нивните услуги (Прилог број 2). По набавката на ИПР системот, истиот е инсталиран и се користи во Службата за потребите на корисниците на услугите.

Согласно потребите и Годишниот план за јавни набавки, Министерството спроведува постапка за јавна набавка со цел да обезбеди превентивно и адаптивно одржување на системот за интегрирано планирање на ресурсите. За оваа намена во текот на 2019 година по спроведена постапка за јавна набавка, склучен е договор[17] во вредност од 7.080 илјади денари со времетраење од 12 месеци и во текот на 2022 година склучен е договор[18] во вредност од 14.160 илјади денари со времетраење од 24 месеци. По истекот на договорот од 2022 година склучени се два Анекс договори[19] за одржување на системот со кој се продолжува рокот на времетраењето на договорот за вкупно 9 месеци, односно заклучно до 13.09.2024 година. Во исто време, се зголемува и вредноста на договорот за вкупно 2.832 илјади денари. Имајќи во предвид дека причините за измените на основниот договор за јавна набавка се однесуваат на продолжување на важноста и вредноста на договорот за дополнителни 9 месеци и истите не произлегуваат од случаите предвидени со Законот за јавните набавки[20], договорниот орган бил должен да спроведе нова постапка за јавна набавка за одржување на системот. Покрај наведеното, Министерството нема предвидено постапка за јавна набавка за одржување на ИПР системот со Планот за јавни набавки за 2023 година иако времетраењето на договорот бил со важност до 13.01.2024 година. Ваквата постапка за јавна набавка е планирана со втората измена на Планот за јавни набавки од октомври 2024 година како отворена постапка и истата е започната со носење на Одлука за јавна набавка во ноември 2024 година, а на 31.01.2025 година е склучен Договор за услуги за одржување на системот за интегрирано планирање на ресурсите[21]. Наведената состојба упатува на несоодветното планирање на средствата, несоодветно утврдување на приоритетите и потребите, како и ненавремено спроведување на постапките

[15] Број 03-3040/1 од 16.09.2014 година
[16] Број 1908/15 – 0307 од 16.07.2015 година
[17] Број 1414-4135/10 од 27.12.2019 година
[18] Број 19-58/6 од 13.1.2022 година
[19] Анекс бр.1, број 19-272/1 од 12.01.2024 и Анекс бр.2, број 19-189/2 од 12.07.2024
[20] член 119 од Законот за јавни набавки
[21] Договор за услуги за одржување на системот за ЕРП системот број 16-76/5 од 31.01.2025 година

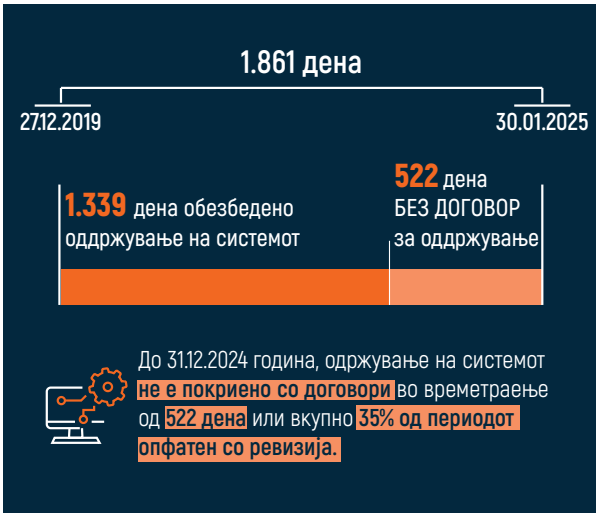
за јавни набавки за одржување на ИПР системот и влијае на рационално користење на средствата во постапките за јавни набавки и почитување на начелото на конкуренција, односно основните начела утврдени во одредбите на Законот за јавните набавки[22] при доделување на договори за јавни набавки.

3.1.1.2. Ефикасното и континуирано одржување на ИПР системот е од клучно значење за неговата функционалност, безбедност и доверливост на податоците. Обезбедувањето на редовна техничка поддршка и навремени интервенции во случај на проблеми е особено важно за непречено извршување на деловните процеси и заштита од потенцијални безбедносни закани.

Со направениот увид во документацијата поврзана со одржувањето на системот и роковите на траење на договорот, ревизијата утврди дека постојат периоди во кои не било обезбедено формално договорено одржување на системот. Заклучно до 30.01.2025 година, **одржувањето на системот не било покриено со договори во времетраење од 522 дена што претставува 35% од периодот опфатен со ревизија.**

На инфографик број 3 е прикажана анализата на времетраењето на договорот.

Склучен ДОГОВОР ЗА ОДРЖУВАЊЕ	ПОЧЕТОК НА ДОГОВОРОТ	КРАЈ НА ДОГОВОРОТ	ВРЕМЕТРАЕЊЕ НА ДОГОВОРОТ
Арх. број 1414-4135/10	27.12.2019	27.12.2020	365 дена (12 месеци)
Склучен ДОГОВОР ЗА ОДРЖУВАЊЕ	ПОЧЕТОК НА ДОГОВОРОТ	КРАЈ НА ДОГОВОРОТ	ВРЕМЕТРАЕЊЕ НА ДОГОВОРОТ
Арх. број 19-58/6	13.01.2022	13.01.2024	730 дена (24 месеци)
Склучен АНЕКС НА ДОГОВОРОТ	ПОЧЕТОК НА ДОГОВОРОТ	КРАЈ НА ДОГОВОРОТ	ВРЕМЕТРАЕЊЕ НА ДОГОВОРОТ
Арх. број 19-272/1	12.01.2024	13.06.2024	152 дена (6 месеци)
Склучен АНЕКС НА ДОГОВОРОТ	ПОЧЕТОК НА ДОГОВОРОТ	КРАЈ НА ДОГОВОРОТ	ВРЕМЕТРАЕЊЕ НА ДОГОВОРОТ
Арх. број 19-189/2	12.07.2024	13.09.2024	92 дена (3 месеци)



Во услови на отсуство на договор за одржување на системот, отсуствува и континуирано и навремено обезбедување на услуги за одржување на системот со кои се гарантира безбедноста, достапноста, интегритетот и доверливоста на податоците во ИПР системот што претставува ризик од губење или оштетување на податоците, неовластен пристап до информациите, како и неможност за навремено подготвување на финансиски извештаи, што може да влијае на целокупната точност и транспарентност на финансиското известување.

3.1.1.3. Договорот за одржување на ИПР системот, во делот IV – Обврски на носителот на набавката, ги уредува обврските на носителот да го одржува системот во согласност со условите дефинирани во тендерската документација, техничката спецификација и понудата. Обврските кои произлегуваат од договорот за одржување предвидуваат како превентивно, така и реактивно одржување, а во исто време и техничка поддршка, обезбедување на сигурност и функционалност на ИПР системот, односно следење и дијагностицирање на системската состојба, редовно одржување, инсталација на софтверски закрпи односно надградби или исправки на софтверот кои се издаваат од страна на производителот, надминување на технички дефекти, спречување на

[22] член 3 и член 5 од Законот за јавните набавки

безбедносни закани, обезбедување на заштитна копија и миграција на податоци, како и корисничка поддршка. Сите овие активности имаат за цел да ја гарантираат безбедноста, достапноста, интегритетот и доверливоста на податоците во ИПР системот.

Со анализата на договорот, тендерската документација и техничката спецификација, како и извештаите и кореспонденцијата на работната група[23] , утврдивме дека **не се преземени активности за**:

- изготвување на извештаи за спроведени активности за тестирање и следење на ИТ безбедносни закани. Оваа состојба може да доведе до зголемена изложеност на софтверското решение на безбедносни закани, што може да има негативно влијание врз неговата функционалност и безбедноста на податоците во системот;

- редовен бекап на податоците, со проверка на истите најмалку еднаш на шест месеци и доставување на извештај за направената проверка. [redacted] Недостатокот на континуирано зачувување на податоците, нивна редовна проверка и доставување на извештај за резултатите од проверката може да предизвика штета, особено ако податоците не можат да се повратат;

- дефинирање и усвојување на Процедура за пријавување на проблеми со цел исполнување на договорните обврски за техничка поддршка и одржување на софтверското решение. Иако нивоата на поддршка и дефинициите на приоритетите, кои се однесуваат на превентивни и реактивни мерки за решавање на софтверски и системски проблеми, се јасно дефинирани, утврдивме дека процедурите за пријавување на проблемите помеѓу договорниот орган и изведувачот не се дефинирани и усвоени иако предвидениот рок е 15 дена по потпишување на договорот. Во отсуство на дефинирана процедура за пријавување на проблеми претставува ризик во постапката за пријавување и решавање на проблемите, како и до потенцијални одложувања во интервенциите во случај на проблеми поврзани со функционирањето на софтверското решение, имајќи предвид дека системот го употребуваат повеќе корисници.

3.1.1.4. Со ревизијата утврдивме дека согласно Договорот за одржување на ИПР системот формирана е заедничка работна група составена од 6 члена претставници на Договорниот орган и Носителот на набавката. Покрај обезбедување на услови за непречена реализација на договорот дополнително, согласно договорените обврски, работната група треба да подготви временски план на активности во кој ќе бидат дефинирани задачите на двете договорни страни со јасни рокови за нивна реализација. До денот на ревизијата не е обезбеден ваков документ што не е во согласност на член 8 и член 9 од Договорот за одржување на ИПР системот. Наведената состојба претставува ризик од спроведување на соодветна контрола и следење на реализацијата на договорот и ризик од несоодветно приоретизирање на активностите и искористеност на часовите за адаптивно одржување на системот како и недоволна координација помеѓу договорните страни како и недостаток на транспарентност во спроведувањето на договорот.

3.1.1.5. Набавка и надградба на ИПР системот

Министерството, во 2015 година за набавка на услуга Систем за интегрирано планирање на ресурсите на државните институции за кои услугата ја обезбедува Службата има склучено договор во вредност од 1.743 илјади денари со вклучен ДДВ.

Со направениот увид во деловните книги на Министерството, утврдивме дека наведениот системот е евидентиран во вкупна вредност од 449 илјади денари односно за 1.294 илјади денари помалку од вкупната вредност на системот.

Дополнително со анализа на договорите за одржување на ИПР системот, ревизијата утврди дека во периодот од 2019-2024 година направени се надградби за адаптивно одржување. Набавната вредност на системот за интегрирано планирање на ресурсите не е зголемена за износ од 18.065 илјади денари, за вредноста на адаптивно одржување на системот, односно додавање на нови кориснички услуги со што се врши зголемување на набавната вредност на софтверската апликација и не е во согласност со законските прописи[25].

Целосен преглед на вредности за адаптивно одржување по периоди е даден на инфографик број 4:

[23] заедничка работна група составена од Договорниот орган и Носителот на набавката чија цел е обезбедување на услови за непречена реализација на договорот

[redacted]

[25] член 19 став 1 од Правилникот за сметководството за буџетите и буџетските корисници

ПРЕГЛЕД НА ВРЕДНОСТИ ЗА АДАПТИВНО ОДРЖУВАЊЕ ПО ГОДИНИ

ПЕРИОД	ЧАС	ЦЕНА	ЦЕНА СО ДДВ	ВКУПНО
Договор за одржување на ИПР системот од 2019 година				
јануари 2020	8	5.357	6.321	50.572
февруари 2020	26	5.357	6.321	164.390
март 2020	20	5.357	6.321	126.430
јуни 2020	6	5.357	6.321	37.929
август 2020	143	5.357	6.321	903.974
септември 2020	66	5.357	6.321	417.219
октомври 2020	239	5.357	6.321	1.510.838
ноември 2020	248	5.357	6.321	1.567.731
декември 2020	44	5.357	6.321	278.146
Договор за одржување на ИПР системот од 2022 година				
прв квартал 2022	280	3.100	3.658	1.024.240
втор квартал 2022	80	3.100	3.658	292.640
трет квартал 2022	113	3.100	3.658	413.354
октомври 2022	846	3.100	3.658	3.094.668
четврт квартал 2022	543	3.100	3.658	1.986.294
петти квартал 2023	600	3.100	3.658	2.194.800
осми квартал 2022	538	3.100	3.658	1.968.004
деветти квартал 2024	7	3.100	3.658	25.606
десетти квартал 2024	504	3.100	3.658	1.843.632
единаесетти квартал 2024	45	3.100	3.658	164.610

18.065.075

Нецелосното евидентирање на вредноста на набавеното средство влијае врз реалноста и објективноста на неговата вредност.

3.1.2. Дефинирани права и обврски помеѓу Службата и Министерството

Согласно добрите практики за управување со информациски системи и принципите на јасно дефинирани договорни односи, секој информациски систем што е во употреба од различни страни треба да има формално дефинирани права и обврски со кои ќе се регулираат обемот на услугите, сопственоста, достапноста, интегритетот и безбедноста на податоците (што подразбира ракување, складирање и заштита на податоците), пристапот и овластувањата. Со цел да се обезбеди континуирано подобрување и адаптација кон новите потреби, потребно е да бидат утврдени јасни процедури за управување со промените, вклучително и процеси за барање, проценка и одобрување на модификации во рамките на системот и услугите.

Како што беше претходно истакнато, во 2014 година, за потребите на Службата, Министерството за информатичко општество и администрација и Министерството за транспорт и врски склучуваат договор за групна набавка[26], односно јавна набавка за ИПР систем на државни институции за кои услугата ја обезбедува Службата за општи и заеднички работи на Република Македонија. Притоа Службата не е договорна страна од Договорот за групна набавка и покрај тоа што системот е набавен за потребите на Службата. Министерството за информатичко општество и администрација согласно наведениот Договор за групна набавка ја реализира истата и склучува договор за набавка на ИПР систем. По набавката на ИПР системот, истиот е инсталиран и се користи од страна на Службата за извршување на секојдневните работи и услуги, за институциите кои се корисници на нивните услуги.

До денот на ревизијата, **не постои договор или акт со кои се регулираат правата и обврските на Министерството како сопственик на системот и Службата како корисник на системот.** На ревизијата не и беше презентирана Одлука со која Владата го преотстапува правото на користење на системот за интегрирано планирање на Службата како и склучен договор со кој се уредуваат правата и обврските за движните ствари кои се даваат на времено или трајно користење.

Ваквата состојба не е во согласност со Законот за користење и располагање со стварите во државна сопственост и со стварите во општинска сопственост[27] и во отсуство на јасно дефинирани договорни односи може да доведе до правна и оперативна неизвесност во користењето и одржувањето на системот, зголемен ризик од несоодветно управување со податоците и можни безбедносни пропусти кои би можеле да резултираат со загуба, неовластен пристап или нарушување на интегритетот на податоците.

3.1.3. Правно регулирање на сопственоста на податоците

3.1.3.1. Службата согласно член 2 став 3 од Одлуката за основање на Службата за општи и заеднички работи на Владата на Република Северна Македонија склучува договор за вршење на општи и заеднички работи и услуги за потребите на корисникот на работите и услугите. Согласно одредбите во договорот, Службата за потребите на корисникот на работите и услугите покрај другите услуги извршува и сметководствено-финансиски работи без надоместок.

Во рамки на финансиското управување, јасно дефинираните права и обврски помеѓу давателот на сметководствено-финансиски услуги, Службата и корисниците на овие услуги се основа за ефикасно и транспарентно функционирање. Правата и обврските помеѓу давателите и корисниците на сметководствени услуги треба да бидат уредени со формален договор или друг правен акт со кој ќе се обезбедува:

- Опсегот на услуги, односно видови на сметководствено-финансиски услуги кои се предмет на договор;
- Сопственоста на податоците, односно јасно дефинирање на сопственоста на податоците, како и правото на пристап, користење и заштита на истите;
- Заштита на податоците и безбедноста на информациите, вклучувајќи ги сите технички и организациски мерки со цел да се обезбеди заштита на доверливоста, интегритетот и достапноста на податоците;
- Права на корисниците во однос на контрола и ревизија на сметководствените податоци и финансиските извештаи, како и обврските на давателот на услуги да обезбеди точни и навремени извештаи, со почитување на сите законски и подзаконски барања;
- Обврски на давателот на услуги за ажурирање на сметководствените податоци, подготовка и потврдување на финансиски извештаи, вклучително и усогласување со актуелните законски и подзаконски акти;
- Период на чување на податоците и условите за уништување на истите по завршување на договорот или по истекување на потребниот период за чување согласно актуелните законски и подзаконски акти;

[26] Број 03-3040/1 од 16.09.2014 година
[27] член 44 став 4

Обврска за усогласеност со регулативите и решавањето на спорови.

Од направениот увид во склучените договори, **ревизијата утврди дека постојните договори не ги уредуваат горенаведените права и обврски со кои би се обезбедила јасна распределба на одговорностите помеѓу давателот и корисникот на сметководствено-финансиските услуги**. Ваквата состојба придонесува до зголемен ризик од недоволна транспарентност, дефинирање и разграничување на видот на услугата, злоупотреба на податоците особено во отсуство на прецизно регулирана сопственост на податоците како и правото на пристап до финансиските и деловните информации, одговорно управување со финансиските податоци и можни неправилности во спроведувањето на сметководствените услуги.

Со спроведената анализа на договорите помеѓу давателот на сметководствено-финансиски услуги, Службата, и корисниците, документите добиени од Службата, Техничката спецификација како дел од Тендерската документација за набавка на услуги за одржување на системот за интегрирано планирање и Кварталните извештаи од економскиот оператор кој го одржува системот утврдивме неколку недостатоци прикажани во инфографик број 5.

Права и обврски помеѓу **давателот на услуги** и **корисниците на услугите**

Отсуството на договорни односи може да доведе до нејасна распределба на одговорностите помеѓу давателот и корисниците на услугите и недоволна транспарентност во испораката на сметководствените услуги. Посебно отсуството на прецизно регулирана сопственост на податоците и правото на пристап до финансиските и деловните информации, го зголемува ризикот од злоупотреба на податоците и можни потенцијални финансиски и правни последици поради неусогласеност со законските прописи.

3.1.3.2. Обврска за евиденција на системот во Службата

Во врска со утврдената состојба во точка 3.1.1.5. од извештајот, поврзана со набавка на системот за интегрирано планирање на ресурсите и неговото евидентирање, ревизијата истакнува дека и покрај тоа што не е презентиран акт за давање на користење на системот, а имајќи предвид дека Службата е корисник на наведениот систем и опслужува 40 правни субјекти (Прилог број 2), не преземала активности за негово евидентирање во вонбилансна евиденција во вредност од 1.743 илјади денари ниту за вредноста на сите извршени надградби за адаптивно одржување на истиот во вредност од 18.065 илјади денари. Исто така, на ревизијата за периодот предмет на ревизија не и е презентирана пописна листа во која пописната комисија констатирала постоење на нематеријално средство и нејзино доставување до Министерството како сопственик на средството што е не во согласност со законската регулатива[28].

Имајќи во предвид дека на ревизијата не и е презентиран акт за користење на наведеното средство, ваквата состојба може да доведе до ризик од неправилно управување и контролни постапки при одржување и надградба на системот што упатува на потребата, Службата со надлежното Министерство и Владата да иницираат донесување на Одлука за пренесување на правото на трајно/ времено користење на наведеното средството согласно Законот за користење и располагање со стварите во државна сопственост и со стварите во општинска сопственост[29].

3.1.4. Разграничување на надлежностите и привилегиите за пристап

Согласно своите надлежности, Службата дава сметководствено-финансиски услуги за повеќе институции и за истото го користи ИПР системот[30]. Со анализа на процесот за креирање и распределба на локации[32] за институциите, како и управувањето со корисничките сметки и нивниот пристап до финансиските податоци во рамките на ИПР системот и воспоставениот начин на работа утврдивме:

- За да се реализираат финансиските сметководствени услуги, прво е неопходно да се отвори посебна база на податоци за секоја институција.
- Министерството доставува барање за отворање на локација за нов корисник до носителот на набавката за одржување на ИПР системот.
- Министерството во барањето за отворање на нов корисник ги наведува модулите од наведениот систем кои се потребни на новиот корисник. Со таа цел се формираат кориснички групи за секој модул, при што секоја група добива специфични привилегии за пристап.
- Лицето одговорно за администрација на ИПР системот од Службата креира кориснички профил и доделува улоги согласно претходно дефинираните кориснички групи.

До денот на ревизијата, не беа презентирани пишани процедури кои јасно ги дефинираат надлежностите и привилегиите за пристап при креирање и распределба на локации за институциите, управувањето со корисничките профили и нивниот пристап до финансиските податоци, како и начинот на комуникација помеѓу Службата, корисниците, Министерството и носителот на набавката.

Отсуството на вакви дефинирани процедури претставува недоследност во однос на принципите за управување со информациски системи, односно ISO 27001 (за безбедност на информациите) и ISO 9001 (за управување со квалитетот), што може да доведе до потенцијални ризици во однос на транспарентноста, контролата и безбедноста при користење на ИПР системот.

[28] Член 2 и член 8 став 2 од Законот за сметководство на буџетите и буџетските корисници и член 32 став 2 од Правилникот за сметководство за буџетите и буџетските корисници.
[29] Член 44 став 4 од Закон за користење и располагање со стварите во државна сопственост и со стварите во општинска сопственост.
[30] ERP Ultima
[31] База на податоци

3.2. Област ИТ Операции – Системски подесувања (конфигурација) на софтверите за пристап до ресурсите на ИПР системот

Во денешното дигитално деловно опкружување, информациските технологии играат клучна улога во функционирањето на институциите. ИПР системот, како интегрирано решение за управување со ресурсите, обезбедува информации кои се основа за донесување на транспарентни и навремени одлуки. За да се осигура оптимално функционирање на ИПР системот, неопходно е извршување на системски подесувања односно конфигурации на софтверите кои овозможуваат пристап до потребните ресурси.

Системските подесувања опфаќаат повеќе активности, вклучувајќи подесувања на безбедност, управување со корисничките права и конфигурација на меѓусебните поврзувања, со цел да се овозможи лесен и ефикасен пристап до информациите. Правилната конфигурација не само што ја максимизира функционалноста на ИПР системот, туку и ја зголемува безбедноста на податоците, минимизирајќи ги ризиците поврзани со неовластен пристап.

3.2.1. Безбеден пристап до ресурсите и достапност на ИПР системот - Системска конфигурација на базата на податоци споредена со најдобрите практики за безбедност

Во рамки на преземените ревизорски активности, ревизијата направи анализа на:

- конфигурациски подесувања на системот и базата на податоци
- апликативните контроли на ИПР системот инсталиран на серверите на Министерството,
- конфигурацијата на доменскиот контролер на централната локација на корисниците кои се вработени во Службата.

Со извршената ревизија утврдивме дека од периодот кога е воспоставен ИПР системот до периодот на извршување на ревизијата, не е извршена контрола на информацискатa безбедност на системот, ниту е издаден извештај за состојбата на информацискатa безбедност. Истовремено не е направена ниту проценка и анализа на ризици за безбедноста на информацискиот систем, нивно приоретизирање и преземени мерки за намалување на истите.

Имајќи ги во предвид најдобрите практики и стандарди за информациска безбедност, претходно утврдените состојби доведуваат до зголемена изложеност на системот на безбедносни закани и ризици.

Политики, системска документација и најдобри практики

3.2.1.1. Стратешки документи

Стратегиското планирање на информациските и комуникациските технологии е од суштинско значење за ефикасно управување со информациските системи. Во Службата недостасуваат стратешки документи кои јасно би ја дале насоката на развој, одржување и надградба на информациските системи како и мерки за подобрување на информацискатa безбедност. Во извештајот на Европската комисија за Република Северна Македонија за 2024 година, во Поглавје 10: Дигитална трансформација и медиуми е наведено:

> **„Што се однесува до стратегијата за дигитална трансформација, Северна Македонија допрва треба да ја усвои долгорочната стратегија за ИКТ и националната стратегија за сајбер безбедност".**

Отсуството на национална ИКТ стратегија, како и недостигот на јасно дефинирана ИКТ стратегија во Службата, може да влијае на ефикасноста и координацијата во управувањето

со имплементираниот ИПР систем. Истото влијае во одржувањето и унапредувањето на системот. Како резултат на наведеното, се зголемува ризикот од нефункционални или недоволно усогласени технолошки решенија, што може да доведе до намалена ефективност и отежнато носење на одлуки базирани на дигитални податоци.

Ревизијата истакнува дека Владата ја донесе Националната стратегија за сајбер безбедност 2025–2028 година. Дополнително, има формирано работна група за изработка на стратегија за ИКТ, и истата има изготвено Предлог СМАРТ/МК: Дигитална Македонија 2030 со која го дефинира патот за дигитална трансформација на Република Северна Македонија во согласност со нејзините карактеристики, вредности и стратешки интереси.

3.2.1.2. Политики и процедури

Политиките и процедурите за управување со информациските системи претставуваат основа за осигурување на безбедноста, интегритетот и контролата на пристапот до податоците. Тие имаат клучна улога во дефинирањето на јасни правила и одговорности, со што се минимизираат ризиците од неовластен пристап, злоупотреба на информациите и потенцијални безбедносни инциденти. Системската документација на базите на податоци е клучна за одржување на ефикасноста, безбедноста и интегритетот на податоците во информациските системи. Ова овозможува јасен преглед на структурата и процесите на управување, размена на информации, одржување и надградба на системот, како и во заштита на податоците. Воспоставувањето на соодветни политики и процедури овозможува заштита на податоците, транспарентност во нивното управување и усогласеност со релевантните законски и регулаторни барања. Во рамки на преземените ревизорски активности, ревизијата утврди дека:

- **Службата, како корисник на ИПР системот и извор на податоци во него, нема изготвено ниту одобрено политики кои го регулираат нивото на пристап до податоците и обезбедуваат информациска безбедност. Исто така, нема одобрена ИТ политика за снимање и тестирање на резервните копии како и политика за опоравување од ИТ катастрофи и континуитет во работењето што не е во согласност со меѓународниот стандард за информациска безбедност на информации, сајбер безбедност и заштита на приватноста[32].**

Отсуството на одобрени политики и процедури може да резултира со намалена отпорност на Службата кон безбедносни закани и нарушувања, загрозувајќи ја сигурноста и регуларноста на финансиските податоци и процеси и во исто време создава потенцијален ризик од неовластен или нерегулиран пристап до чувствителни информации што се обработуваат во системот, а кои се сопственост на субјектите чии финансиски податоци се водат во него, односно институциите корисници на системот (Прилог број 2).

- **Службата нема ажурирана системска документација која ја опфаќа конфигурацијата на базите на податоци, како и анализата на потенцијалните слабости и закани што произлегуваат од постојната системска верзија и конфигурација. Исто така не постојат формално пропишани процедури за управување со базите на податоци, ниту е дефиниран временскиот период и начинот на зачувување на резервните копии на податоците. Не е утврдено нивото на заштита, вклучувајќи енкрипција на податоците односно претворање на податоци или информации во кодирана форма, снимање и анализа на логовите (настани) за пристап. Ваквите состојби не се во согласност со меѓународниот стандард за информациска безбедност на информации, сајбер безбедност и заштита на приватност[33].**

Отсуството на оперативни процедури за управување со капацитетите за обработка на информации и базите на податоци претставува ризик за несоодветно документирање на задачите кои се извршуваат во системот и нивната следливост, што може да доведе до неконзистентност во начинот на нивно спроведување во зависност од тоа кој ги извршува.

- **Начинот на пристап до податоците и нивното архивирање во Службата е без пропишани политики за управување со податоците во делот на временскиот рок за чување, нивната сопственост како и начинот на примопредавање на податоците на сопствениците од страна на Службата. Исто така не е дефиниран начинот на постапување за приклучување на нови субјекти, корисници на услугите кои ги дава Службата, односно начинот на отворање на нови бази, нивно затворање во случај на прекин на услугите и начинот на отстапување на податоците од системот.**

Ваквите состојби не се во согласност со меѓународниот стандард за информациска безбедност на информации, сајбер безбедност и заштита на приватноста ISO/IEC 27001: 2022[34]. Отсуството на пропишани политики за управување со податоците, вклучително и нивниот временски рок за чување, сопственоста и начинот на примопредавање, може да доведе до несигурност и неконзистентност во управувањето со

[32] ISO/IEC 27001: 2022 во делот Анекс А 5.1 Политика за безбедност на информациите
[33] ISO/IEC 27001: 2022 во делот Анекс А 5.37, Документирани оперативни процедури, Анекс А 8.9 Управување со конфигурација, Анекс А 8.32 Управување со промени
[34] во делот Анекс А 8.32 Управување со промени

чувствителните информации. Недефинираните процедури за приклучување и исклучување на субјектите од системот создаваат ризик од неовластено задржување, губење или злоупотреба на податоците, што може да има сериозни правни и безбедносни последици

3.2.1.3. Кориснички пристапи до базите на податоци

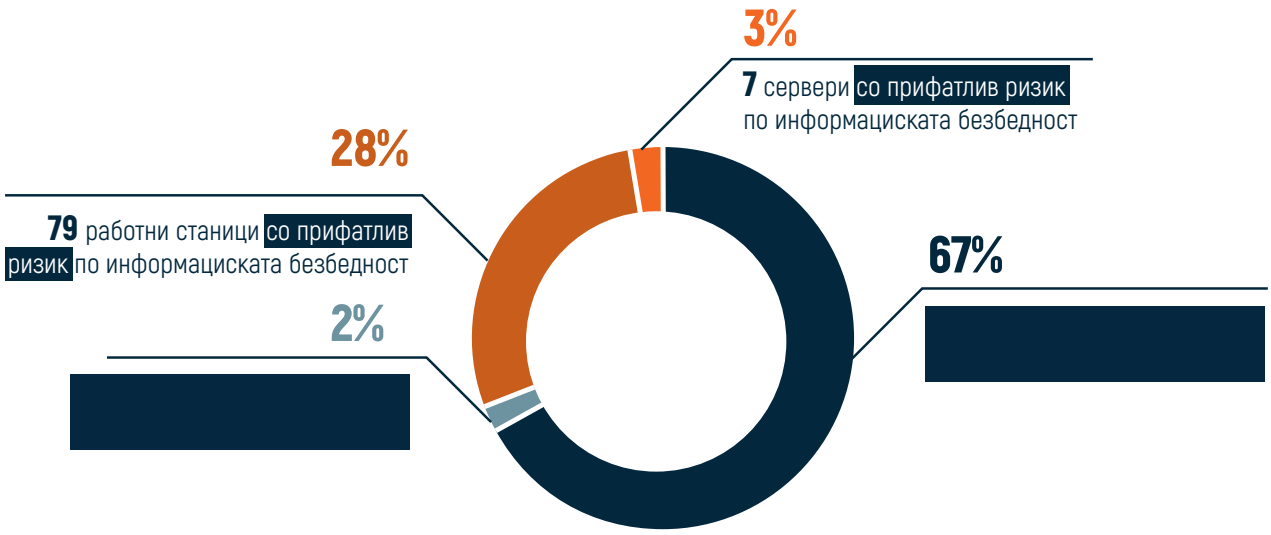
Ефикасното управување со корисничките права на пристапи до базите на податоци е од суштинско значење за обезбедување на интегритетот, доверливоста и достапноста на информациите. Воспоставувањето на јасни политики за автентикација, управување со привилегии и контрола на пристапите претставува клучен елемент во заштитата на податоците од неовластен пристап, злоупотреба или компромитација.

Ревизијата утврди дека пристапот на корисниците до ИПР системот не е реализиран преку серверски доменски контролер со Active Directory автентикација, туку преку ВПН мрежа и директно најавување на базата со корисничко име и лозинка. Корисничките лозинки не се временски ограничени и не се менуваат со текот на времето, а во исто време должината на корисничките лозинки е помала од препорачаните безбедносни стандарди што претставува значителен безбедносен ризик, односно го зголемува ризикот од компромитација преку напади со погодување или автоматизирани алатки за пробивање на лозинки.

Со извршената ревизија на начинот на администраторскиот пристап до серверите, утврдивме дека за креирање на корисничка сметка за администратор се користат општи кориснички имиња и со недефиниран временски период за важност на лозинката, а некои немаат дефинирано временски период на истекување на пристапот.

Во отсуство на дефиниран систем за управување со кориснички сметки, кориснички групи и проверка на автентичноста на корисничките сметки по вработен не може да се утврди точниот идентитет на лицата кои имаат пристап до системот при што постои ризик од неовластен пристап до системот и податоците особено доколку некој вработен го напуштил работното место, а лозинките остануваат непроменети. Во Службата вработени се 2 лица кои имаат администраторски пристап, додека администраторскиот пристап до системските ресурси на ИТ системот на Службата [redacted] Со ревизијата утврдивме дека за сите бази на податоци вкупно 131 дата база, се пристапува од една администраторска сметка која е дефинирана со општо корисничко име и со пристап до сите податоци во системот.

Со увид во конфигурацијата на доменскиот контролер на централната локација од кој пристапуваат корисниците на ИПР системот констатиравме состојби за дефинирани корисници во доменскиот контролер, број на корисници со активен пристап до системот на Службата, број на корисници со оневозможен пристап, ниту еден корисник за кој е истечен пристапот, број на корисници за кои лозинката не истекува односно нема потреба од задолжително периодично менување, минимална должина на лозинката како и исклучен праг на заклучување на сметка по неколку погрешни обиди. Во делот на проверка на серверите и работните станици при Службата утврдивме дека 46% од серверите и 70% од работните станици се со ризик по информациска безбедност. Овие состојби се прикажани на инфорграфик број 6.



Ваквите состојби не се во согласност со добрите практики за управување со пристапи и безбедносните стандарди[35] кои уредуваат секој корисник кој има администраторски привилегии да има уникатена корисничка сметка со уникатно корисничко име и лозинка или друг облик на автентикација кои се доделени на секој корисник поединечно за најава, што може да доведе до потенцијални безбедносни инциденти и неовластено управување со системот.

3.2.1.4. Информациска безбедност на сервисите

Од исклучителна важност по информациската безбедност е сите непотребни сервиси кои се нудат од страна на дата база серверот да бидат исклучени доколку не се употребуваат, вклучувајќи ги и портите за комуникација на тие сервиси.

Иако базата не испраќа автоматски е-пораки, утврдивме дека активна е опцијата за праќање на електронски пораки од базата на податоци со што се зголемуваат можностите за напад на дата база серверот [redacted] Ако стандардниот администраторски корисник остане активен, се зголемува веројатноста напаѓачот да се насочи кон оваа позната корисничка сметка, која често се користи со највисоки администраторски привилегии, што дополнително го зголемува ризикот од напад кон овој корисник.

3.2.1.5. Записи за ревизија и дневник на настани

Системските софтвери даваат можност за конфигурирање

[35] ISO/IEC 27001:2022

на снимање на настани (логови), што е клучно за подоцнежна анализа, идентификација на грешки и следење на активностите во системот. Ревизијата утврди дека конфигурацијата за снимање на настани на серверот на базата на податоци е поставена на автоматско бришење на најстарите записи по достигнување на максималниот број на датотеки. Ова претставува ризик од губење на важни историски податоци за настани што се случиле во системот.

За базите на податоци не е конфигурирана локација за чување на ревизорската трага, што значи дека не постои формален запис за активностите во системот. Исто така, системот не е поставен да зачувува информации за сите настани, вклучително и успешните и неуспешните најави на корисници, што оневозможува следење и контрола на пристапот.

Недостатокот на евидентирање на грешки и најави во системот претставува безбедносен ризик, и може да доведе до неоткривање на неовластени пристапи, преземање или менување на податоци без дозвола. Имајќи предвид дека податоците за настаните на серверот не се чуваат во определен период, не постои можност да се утврди дали имало неавторизирано преземање на податоци, што дополнително ја загрозува безбедноста и интегритетот на информациите во системот.

3.2.1.6. Верзии, ажурирања и безбедносни надградби (patches) на дата базата

Ревизијата утврди дека на [redacted] производителот на базата на податоци со безбедносни подобрувања, кои не се инсталирани. Ова значително ги зголемува безбедносните слабости во системот, што може да доведе до неовластен пристап или компромитирање на податоците.

На серверот има вкупно 131 база на податоци, но на ниту една од нив не е овозможена симетрична или асиметрична енкрипција на податоците. Ова значи дека во случај на неовластено преземање или копирање на податоците, истите би биле читливи без потреба од декрипција, вклучително и податоците зачувани во резервните копии.

Ваквите состојби не се во согласност со меѓународниот стандард за информациска безбедност на информации, сајбер безбедност и заштита на приватноста ISO/IEC 27001:2022 како и со заклучокот на Владата од 131-та седница[36] во делот Агенда за дигитална трансформација точка 5.

Неажурирањето на базата на податоци со најновите безбедносни надградби значително го зголемува ризикот од безбедносни закани, што може да резултира со неовластен пристап, загрозување на интегритетот на податоците или нивна злоупотреба, од причини што лесно се читливи, дури и ако се преземени или копирани од резервните копии. Ваквите пропусти ја изложуваат институцијата на потенцијални безбедносни инциденти, загуба на доверливи информации и усогласеност со регулаторните барања.

3.2.2. Заштита и правење на резервна копија на податоците и поврат во случај на катастрофа

Обезбедувањето редовен и безбеден бекап, чувањето на надворешна локација со јасно дефинирани процедури за поврат на податоци е значајно за заштита на податоците и континуитет во работењето, особено во случај на хардверски дефект, безбедносни напади или катастрофи како и загуба или неовластен пристап. Ревизијата утврди:

- Со Договорот за одржување на ИПР системот се предвидува техничка поддршка и редовно извршување на резервни копии на податоците од страна на договорниот орган, со задолжителна проверка на нивната исправност најмалку еднаш на 6 месеци и изготвување на извештај за извршената проверка. Анализата на конфигурацијата за автоматско креирање резервни копии на серверот за базата на податоци покажа дека бројот на зачувани резервни копии е поставен на минимум, односно 6 предефинирани резервни копии, што значително го намалува капацитетот за враќање на податоците во случај на системска грешка или загуба на информации. Со извршената ревизија и направениот увид во доставените извештаи за одржување на ИПР системот, утврдивме дека не е евидентирана активност за периодична проверка на исправноста на резервните копии, освен еден допис[37] со потврда за успешно направен локален бекап на серверот. Резервните копии на податоците не се криптирани / заштитени, и истите би биле читливи во случај на неовластено преземање што претставува висок безбедносен ризик.

- Во службата не постојат одобрени политики и процедури за дефинирање на процесот на заштита и зачувување на резервни копии на податоците, како и механизам за редовна проверка и изготвување на извештаи за успешноста за направениот бекап и можноста за враќање на податоците.

- Ревизијата утврди дека не е презентиран доказ за постоење на пропишана и заштитена надворешна локација за чување на резервни копии на податоците, серверските и апликативните конфигурации. Иако Министерството достави

[36] Заклучок на Влада со архивски бр. 40-2051/2 од 21.02.2023 година
[37] Допис бр. 104-2193/1 од 26.06.2020 година

извештај од 11.01.2025 година за извршен бекап и тестирање на резервните копии од страна на компанијата одговорна за хостирање на инфраструктурата со користење на облак, за периодот пред овој датум не се доставени уредни и веродостојни документи за потврда на континуирано архивирање и заштита на податоците.

- Одговорноста за правење резервна копија на ИПР системот, согласно техничката спецификација од јавната набавка, е на компанијата која го одржува системот и истата се прави на локален сервер на дневна и месечна основа.

- Институциите кои користат сметководствено-финансиски услуги во ИПР системот немаат надворешна електронска копија од направените трансакции за тековната и претходните години. Ова создава висок ризик од неповратна загуба на клучни финансиски информации и може сериозно да го наруши континуитетот на работењето.

Ваквите состојби не се во согласност со меѓународниот стандард за информациска безбедност на информации, сајбер безбедност и заштита на приватноста[38] како и со заклучокот на Владата од 131-та седница[39] каде се задолжуваат институциите со воведување на минимални стандарди за информациска безбедност.

Состојбите со некриптираните резервни копии, неодложување на заштитната копија на надворешна локација како и нејзина периодична проверка го зголемува ризикот од неповратна загуба на податоци.

3.2.3. Пристап до серверите од работните станици каде е инсталирана апликацијата

Обезбедувањето на контролиран и безбеден пристап до серверите од работните станици е значајно за заштита на интегритетот и безбедноста на системот.

Работните станици користат оперативен систем од постара верзија и за кој производителот веќе не обезбедува поддршка, безбедносни ажурирања или софтверски закрпи (надградби или поправки на софтверски системи). Пристапот на работните станици до серверите е преку ВПН и создава криптиран тунел, а конфигурацијата на пристапот е со заедничка лозинка за секоја локација и не е променета од нејзиното воспоставување. Овој далечински пристап на ВПН серверот се овозможува со користење на единствени кориснички имиња и лозинки, без примена на повеќе факторска автентикација.

Вака воспоставената конфигурација на работните станици и пристап од надворешна локација до серверот не е во согласност со најдобрите практи на CIS[40] и критериумите за безбедност согласно ИСО 27001:2022 стандардот[41].

Оваа состојба претставува висок безбедносен ризик, бидејќи не е можна прецизна идентификација на корисниците што пристапуваат до системот како и од која работна станица се воспоставува ВПН конекцијата. Воспоставениот начин без задолжително периодично менување на лозинките, кои се исти од нивното воспоставување, како и пристап без повеќе факторска автентикација, носи ризик од неовластен пристап до системот.

Дополнителен ризик е оперативниот систем на работните станици кој е од постара генерација на оперативни системи, подложен на многу безбедносни слабости и за него од страна на производителот не се прават безбедносни надградби. Исто така на работните станици не е инсталиран антивирус и истите се конфигурирани во доменски контролер на институциите каде физички е локацијата од која вработените на Службата ги даваат услугите што дополнително ги оневозможува вработените во ИТ одделението на Службата да имаат можност да интервенираат на истите.

Недостатокот на закрпи за безбедносни пропусти и инсталација на безбедносен софтвер го зголемува ризикот од далечинско извршување на злонамерен код, безбедносни напади, подложност на малициозен софтвер и неовластен пристап.

[38] ISO/IEC 27001: 2022 во делот А8.13-Резервна копија на информации
[39] Заклучок на Влада со архивски број 40-2051/2 од 21.02.2023 година во делот Агенда за дигитална трансформација точка 5
[40] https://www.cisecurity.org/cis-benchmarks
[41] ISO/IEC 27001: 2022 во делот А 8.19-Инсталација на софтвер на оперативни системи

3.3. Област Апликациски контроли - Човечки капацитети и апликациски контроли на системот за ИПР

3.3.1. Човечките капацитети на Службата за општи и заеднички работи за давање услуги на тековните корисници на ИПР системот како и проширување со нови корисници и услуги

Службата за општи и заеднички работи склучува договори со повеќе органи на државната управа за вршење на општите и заедничките работи и услуги што се потребни за нивното функционирање. Со овие договори се утврдуваат правата и обврските меѓу договорните страни во врска со исполнувањето на услугите и работите кои се предмет на договорот. Службата, без надоместок а во висина на планираните средства во буџетот, извршува различни општи и заеднички работи и услуги за потребите на органите на државната управа, вклучувајќи и сметководствено – финансиски работи. Договорите за вршење општи и заеднички работи и услуги се склучуваат за временски период од една фискална година.

Со извршената ревизија во договорите за вршење општи и заеднички работи ревизијата утврди дека не е направено разграничување на надлежностите и видовите на услуги што ги извршуваат вработените во Секторот за финансиско-сметководствено работење на Службата и вработените во секторите за финансиско работење на институциите. Општата формулација "сметководствено-финансиски работи" што ја содржат наведените договори како и отсуството на дефинирани конкретни работни обврски и задачи на вработените во актите за распоредување на работните места не даваат јасна слика за услугите што се опфаќаат односно активностите што се извршуваат за институциите корисници на услугите.

Ревизијата со увид во ИПР системот кој е во функција утврди дека **сите модули не се користат, нема целосна интегрираност на модулите и нема можност за пристап, внесување и преземање на податоците од страна на вработените во институциите корисници на услугите.** Исто така **дел од институции користат и други апликации што предизвикува двојно внесување на исти податоци во различни апликации и дополнителни трошоци на институциите за користење на дополнителни софтверски апликации.**

Исто така ревизијата утврди дека сметководствено - финансиските работи се обезбедуваат за сите сметки на институциите, што доведува до **значително зголемување на обемот на работа на вработените од Секторот за финансиско - сметководствено работење на Службата**, особено во поголемите институции и министерства. Точноста на завршните сметки и на финансиските извештаи како и нивната усогласеност со законските одредби се врши од страна на лица - одговорни сметководители од Секторот за финансиско-сметководствено работење во Службата односно лица овластени од страна на одговорните лица на институциите за која се подготвуваат завршините сметки.

Во актот за систематизација на работните места во Службата, во Секторот за финансиско - сметководствено работење се систематизирани работни места за кои во работни задачи и обврски е предвидено извршување на исти активности и за органите на државната управа. Со увид во истата, ревизијата утврди дека **за пет работни места не се утврдени работни задачи и обврски поврзани со органите на државната управа, иако Службата извршува сметководствени работи во повеќе области.**

Со извршената ревизија на бројот на систематизирани и пополнети работни места, ревизијата утврди дека за периодот 2021-2024 година бројот на систематизирани работни места изнесува 94 додека за истиот период бројот на пополнети и испразнети работни места е прикажан на инфографик број 7.

Наведената состојба упатува на констатацијата дека:

- **бројот на пополнети систематизирани работни места не е на потребното ниво, што влијае врз навремено и ефективно остварување на надлежностите;**
- **постојан одлив на вработени кои извршуваат сметководствено-финансиски работи. Одливот на вработени се должи на: престанок на работен однос поради стекнување на услов за старосна пензија, по барање на вработените, дефицит на стручни кадри во областа, лимитирани плати во јавната администрација.**

Поради недостиг на човечки ресурси, на крајот од 2023 година, **Службата упатува допис до четири органи на државната управа**, со кој ги информира дека **не е во можност да обезбеди сметководствени услуги во 2024 година.** Состојбата на недоволни човечки ресурси е потврдена и од страна на вработените во Секторот за финансиско-сметководствено работење во дадените одговори на анкетните прашалници доставени од страна на ревизијата.

Недоволната кадровска екипираност на Секторот за финансиско-сметководствено работење во Службата влијае на непречено и навремено извршување на обврските и задачите предвидени за органите на државната управа со кои Службата има склучено договор, одржување на континуитетот и квалитетот на работниот процес како и на информациите и податоците што ги даваат финансиските извештаи. Исто така недостатокот на човечки ресурси ја ограничува Службата да ги извршува сметководствено-финансиските работи за постојаните корисници, како и да ги проширува услугите кон нови корисници.

3.3.1.1. Ефикасност на системот за Интегрирано планирање на ресурсите

При набавката на ИПР системот, предвидено е стандардизирање на сметководствените услуги и унифициран начин на водење на работните процеси за институциите корисници на услугите. Имено, ваквата набавка предвидува воведување на централизирана релациона база на податоци со единствен сметковен план за сите институции, како и шифрарник за коминтенти. Во исто време, предвидува евидентирање на корисниците на услугите кои ги дава Службата да се водат во една база, при што секој корисник ќе има пристап само до сопствените податоци. При имплементација на набавката, се продолжило со користење на стариот начин на работа, каде што за секоја институција се водат посебни бази на податоци, со различни шифрарници за коминтенти и сметковен план.

Во однос на употребата на ИПР системот, ревизијата го утврди следното:

Модул за материјално и магацинско работење со ситен инвентар

Модулот за материјално и магацинско работење со ситен инвентар е имплементиран и се користи само од страна на две институции исклучиво за потребите на СОЗР и Управа за хидрометеоролошки работи.

Модул за основни средства

Модулот за основни средства се користи од страна на 22 институции (Прилог 4). Дел од останатите институции користат дополнителни системи за кои се одвојуваат дополнителни финансиски средства. Пристапот на вработени од институциите како и членови на пописните комисии не е воспоставен со што би се овозможило поефикасно извршување на работите.

Модул за благајничко работење

Модулот за благајничко работење се користи во 15 институции (Прилог 4). Кај една институција утврдивме дека услугите за благајничко работење се прават рачно иако модулот е имплементиран и истиот не се користи.

Модул за буџетско работење

Во минималните барања за модулот буџетско работење од техничката спецификација за набавка на системот меѓу другото барано е и реализација на плаќања и размена на податоци со МФ, која не е имплементиран и не се користи.

Од овој модул имплементиран е само делот за модул Трезор и БИ извештајот кој дава три годишни прегледи наназад но само за 8 институции и за фиксен период. Меѓутоа овие делови не се интегрирани со останатите модули на ИПР системот. Ревизијата сака да истакне дека во новиот договор за одржување на ИПР системот не е вклучен овој модул.

Модул за следење на реализација на договорите

Модулот за следење на реализација на договорите не е имплементиран и не се користи. За истиот нема доставено упатства за користење кои се обврска на носителот на набавката согласно тендерската документација.

Модул за финансиско и сметководствено работење

Модулот за финансиско и сметководствено работење се користи во 40 институции (Прилог 4).

Интегрираност на модулите

Ревизијата утврди дека иако било предвидено поврзување на модулите во системот истото не функционира односно не постои интегрираност помеѓу модулите што доведува до неможност за автоматизирање на процесите во работата и потребата од двојни внесови на исти податоци во различни модули.

По имплементација на системот, истиот се одржува и надградува. Надградбите се однесуваат за секоја институција поодделно, со што значително се отежнува и дополнително се усложнува одржувањето на системот. Овој начин на работа го отежнува и самото документирање на надградбите, креирање на ажурна организациона шема на чувањето на податоците во дата базите и нивната поврзаност, пристапот и контролата на пристапот до истите. Промените во апликацијата треба автоматски да бидат применливи за сите институции, но тоа не е обезбедено со постојната поставеност на системот.

Активностите кои се преземени при надградбите на системот се наведени во квартални/месечни извештаи. Ваквите извештаи редовно се доставуваат од страна на носителот на набавката до работната група на министерството задолжена за следење на договорот. Ваквиот начин е утврден со Договорите за одржување на ИПР системот.

Со направениот увид во извештаите утврдивме дека постојат активности кои се повторуваат во подолг временски период (од јануари 2022 до октомври 2024 година), а се однесуваат за исти задачи и тоа:

- **бизнис анализа за интегрирање на модулот Трезор кон ИПР системот;**
- **дневна синхронизација со бизнис регистарот во Централен регистар на Република Северна Македонија преку платформата за Интероперабилност;**
- **бизнис анализа за модулот за следење на реализација на договори.**

И покрај направените надградби утврдивме дека модулот за Трезор (ликвидатура) – плаќања од трезор, **се уште не е интегриран и не се отстранети недостатоците кои се констатирани од корисниците.** Нема поврзување преку платформата за Интероперабилност со Централен регистар на Република Северна Македонија за синхронизација во единствен шифрарник на коминтенти.

Модулот за следење на реализација на договори по јавни набавки **не е инсталиран и не се користи** иако е составен дел на тендерската документација при набавката на ИПР системот. Ревизијата сака да истакне дека во новиот договор за одржување на ИПР системот не е вклучен овој модул.

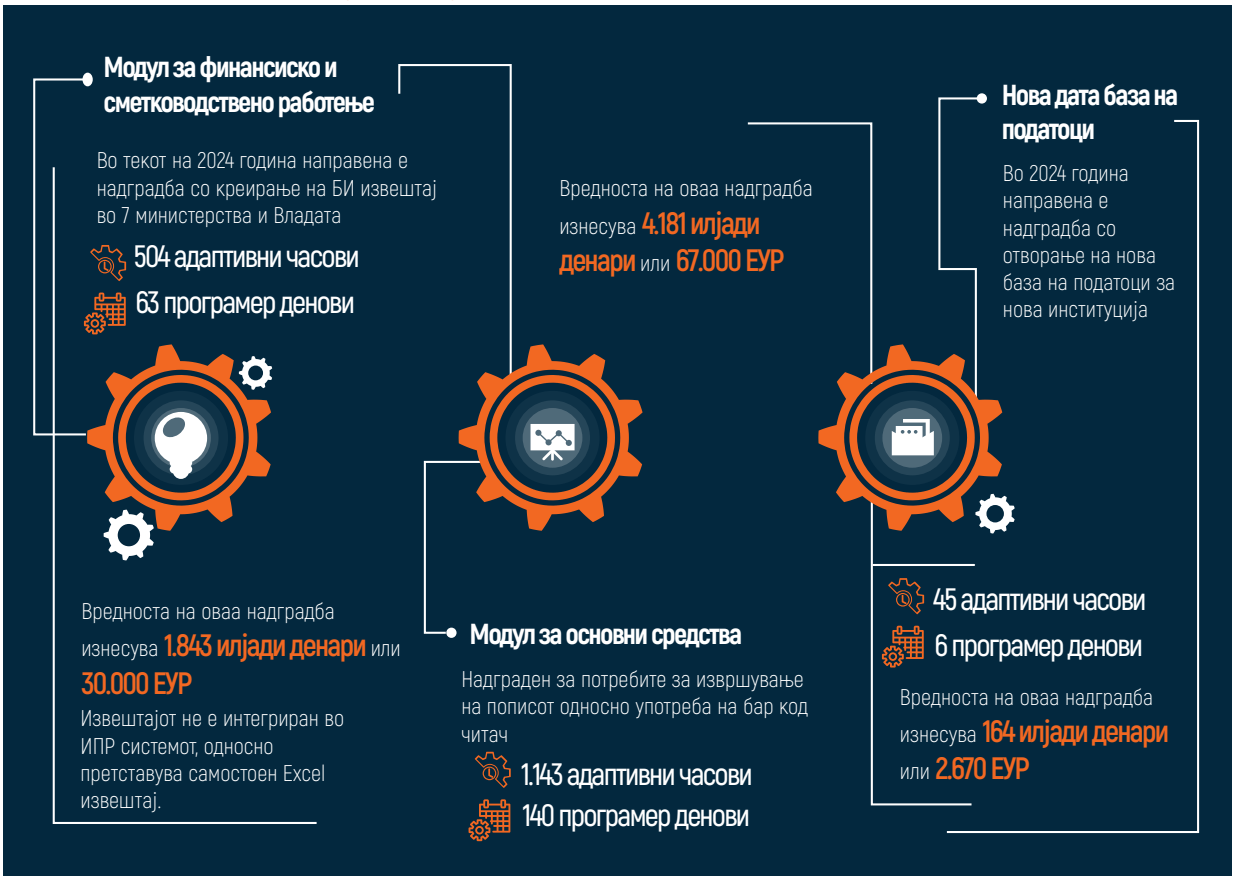
Во извештаите евидентно е **отсуството на координација помеѓу Министерството и Службата** со цел заеднички активности во подобрувањето на самиот ИПР систем и негова зголемена ефикасност при надградбите.

Ваквите состојби каде имаме активности кои се повторуваат укажуваат на недостаток на ефективно планирање и координација, што доведува до неефикасност во процесот на имплементација и усогласување на модулите во системот. Повторувањето на истите активности во текот на подолг период резултира со трошоци кои можеле да се избегнат и забавување на напредокот на проектот.

Во однос на надградбите на ИПР системот, ревизијата го утврди следното:

- Во текот на 2024 година е направена надградба на модулот за финансиско сметководство со креирање на БИ извештај за 7 министерства и Владата. За оваа надградба се исплатени вкупно 1.843 илјади денари. Извештајот не е интегриран во ИПР системот, односно претставува самостоен Excel извештај. БИ извештајот е наменет да биде консолидиран извештај за анализа на финансиското работење на институцијата со цел подобро планирање на потребните средства од буџет и анализа на направените трошоци во дадениот период. На овој начин се добива поголема контрола на следење на трошоците на институција. По имплементацијата на БИ извештајот, организирана е обука за 12 вработени лица во Службата кои вршат сметководствени услуги за осум институции, а не лица вработени во институциите кои имаат потреба од вакви анализи. По обуката нема доставено упатство за користење ниту известување до институциите дека можат да побараат ваков тип на извештај. Ревизијата утврди дека ваквиот начин на надградба без анализа за потребата за БИ извештај како и не опфаќањето на сите институции кои го користат системот е целосно неефикасен односно обемот на надградба е за 7 пати поголем бидејќи е изведен поодделно за секоја институција чии податоци се децентрализирани во поодделни бази. Притоа периодот за кој извештајот дава податоци е ограничен на 2021-2023 година и корисниците не можат самите да го променат овој период и да користат податоци после овој период туку за промена може да биде потребно дополнително адаптивно надградување.
- Модулот за основни средства е надграден за потребите за извршување на пописот на средствата и нивните извори односно употреба на бар код читач при што се потрошени средства во вкупна вредност од 4.181 илјади денари. При дефинирање на бараните спецификации за надградба земени се во предвид постојните бар код читачи во Службата што може да ја отежни употребата кај други институции кои не поседуваат ваков тип на читач. Службата поседува и печатар за инвентарни броеви но целата постапка и сите работни процеси при ставање во употреба на средства како и на обележување и попишување на постојаните средства, се прави само за потребите на службата и истата не е соодветно уредена за да се воспостави и кај другите институции.
- За овозможување услови за давање услуги на нова институција потребно е отворање на нова база на податоци. За таа цел во 2024 година направена е надградба и искористени се средства во вкупен износ од 164 илјади денари поради постојната инфраструктура во системот и постојниот начин на работа.

Претходните состојби се прикажани на инфографик број 7.



- **Во минималните барања за модулот буџетско работење од техничката спецификација за набавка на системот меѓу другото барано е и реализација на плаќања и размена на податоци со МФ, кој не е имплементиран и не се користи. Услугите кои Службата ги дава на институциите за ликвидатура (поднесување на плаќање на електронски вирмани кон трезорот на Министерството за финансии на одобрени трансакции за исплата) како и пресметка и исплата на плати, за што Службата користи посебни системи од други производители, за кои се плаќа дополнително годишно одржување. Направените надградби за плаќање на електронски вирмани се имплементирани и се користат во една институција, односно во Министерството. Овие надградби не се поврзани со модулот за финансиско работење со цел автоматско пополнување на ставки кои се одобруваат за плаќање.**

Како причини за ваквата состојба се немање соодветни извештаи за следење на фактурите, неповрзаност со шифрарници за комитенти, односно автоматско преземање на податоци, потешкотии при внесување на податоци во системот, немање можност за повторување на веќе внесени податоци што го отежнува начинот на работа, како и непреземање на податоците во модулот за финансиско работење по извршено трезорско плаќање односно истите мора повторно да се внесуваат во ИПР системот.

Утврдените состојби кои се однесуваат на недостигот на имплементација на клучни модули, како што се следење на реализацијата на договорите и буџетско работење, како и направените надградби за системот без соодветно планирање и недоволен број на обуки може да доведат до потешкотии во финансиското управување на институциите. Исто така, неповрзаноста помеѓу модулите како и користењето на други системи го спречува автоматизирањето на процесите, што резултира со зголемени трошоци и забавување на работата. Повторувањето на истите активности во долг период, како и нецелосната имплементација на клучните функционалности, резултира со неефикасност и го намалуваат ефектот од инвестициите при што го отежнуваат користењето на системот од страна на институциите.

3.3.2. Контрола за користење на ИПР системот и пристап до модулите и податоците

Пристапот до ИПР системот е организиран како пристап од работните станици до сервер, а потоа како пристап до модулите и податоците во системот.

Пристапот на работните станици до серверот каде е инсталирана дата базата на ИПР системот е преку ВПН криптирана конекција. Работните станици користат оперативен систем кој е повеќе од 15 години стар и за кој производителот веќе не обезбедува поддршка, безбедносни ажурирања или софтверски закрпи. Пристапот преку ВПН е со создавање заштитен тунел, а конфигурацијата на пристапот е поставена со заедничка лозинка за секоја локација и не е променета од нејзиното воспоставување. Овој далечински пристап на ВПН серверот се овозможува со користење на единствени кориснички имиња и лозинки, без примена на повеќе факторска автентикација. Подетално е објаснето во точка 3.2.3.

По воспоставување на ВПН конекција односно работна станица - сервер, се овозможува пристап до модулите и податоците во системот со употреба на кориснички сметки, кои се состојат од корисничко име и лозинка.

Управувањето со кориснички сметки е организирано така што за секоја институција за која се даваат услуги, се креира посебна дата база на податоци каде ќе се чуваат податоците за таа институција. Барање за отворање на база на податоци за соодветна институција доставува Министерството до носителот на набавката кој го одржува ИПР системот.

По отворање на база се креираат кориснички групи со кои се поврзуваат корисничките сметки за добивање на привилегии на пристап до модулите. При креирањето на корисничките групи се дефинираат привилегиите за пристап до соодветен модул. Потоа, лицето со задолжение за администрирање на системот во Службата, може да креира кориснички сметка, односно корисничко име и лозинка. Корисничкото име и лозинката се генерираат за најава во системот на вработените во Службата кои даваат услуги за соодветната институција односно корисникот на услугата. Пристапот до модулите во системот се овозможува преку припадноста на корисничка сметка во кориснички групи каде претходно се дефинирани соодветни привилегии за пристап.

Со ревизијата утврдивме:

- **отсуство на одобрени процедури за управување со бази на податоци, што укажува на недостаток на пропишана комуникација и распределба на задолженијата во процесот на отворање и одржување на базите на податоци за институциите, со што се обезбедува стандардизирање на постапката за различни институции;**
- **недостаток на ажуриран регистар на корисници со привилегии за пристап до соодветен сет на податоци како и извештај за направена контрола за пристапот до податоците и привилегиите дадени од страна на корисниците;**
- **отсуство на процедури за распределба на задолженија и задачи, од кои може да се утврди кој вработен конкретно за кои институции треба да обезбедува услуги и на кој модул да пристапува. Задолженијата по институции и модули се доделуваат усно, без соодветни акти или формални документи за распределба на должностите, што не е во согласност со Стандардот 13 за внатрешна контрола во јавниот**

сектор - Поделба на должностите, со кој е пропишано дека поделбата на должностите и одговорностите претставува еден од начините преку кои се намалува ризикот од грешки, измами, непочитување на регулативата, како и ризикот од неоткривање на овие неправилности;

- отсуство на пропишана постапка за информирање на ИТ одделението од страна на лица вработени во секторот за човечки ресурси, со цел креирање, активирање и деактивирање корисничка сметка во системот. Отсуството на ваков акт значи дека не постои јасен и стандарден процес кој ќе овозможи навремено и точно информирање за креирање, активирање и деактивирање корисничка сметка во системот што влијае на безбедноста и интегритетот на податоците, како и на функционалноста на системот;

- отсуство на контрола со која би се потврдило дали сите дозволени пристапи се согласно добиени документирани барања, односно поднесени барања за пристап, барања за деактивирање на кориснички сметки и барања за забрана за пристап на лица кои заминале од Службата или се прераспределени на други работни места во соодветни институции. Ова укажува на тоа дека не се евидентираат сите барања за пристап и не се следи статусот на пристапите, што го зголемува ризикот од неовластен пристап и можни безбедносни инциденти. Во институцијата не се назначени лица за редовна контрола на пристапите до ИПР системот, ниту се спроведува таков увид;

- отсуство на Политика за периодично менување на лозинките што е клучно за одржување на безбедноста на пристапот до системот и за спречување на неовластен пристап. При најава во системот вработените се најавуваат со првично доделената лозинка за пристап која не е смената. Лозинките не се менуваат редовно, а постојат случаи на споделување кориснички сметки меѓу вработените, што го зголемува ризикот од неовластен пристап, особено во зголемен обем на работа;

- во базата на кориснички сметки за пристап на ИПР системот постојат активни кориснички сметки на лица кои повеќе не се вработени во Службата. Дел од овие сметки се користат од страна на постојните вработени во Службата за најава и работа со ИПР системот;

- кориснички сметки кои имаат привилегии за пристап до повеќе модули во системот, притоа пристапот не е ограничен само до податоците кои се потребни за нивна работа. Ова може да доведе до потенцијални конфликти на интереси и злоупотреби. Секоја корисничка сметка треба да биде строго дефинирана и да припаѓа само на една корисничка група, во согласност со принципот на поделба на должности и

- пристап до податоци од системот од страна на институции кои не се задолжени да даваат сметководствено финансиски услуги. Односно во системот постојат кориснички сметки и дадени се привилегии за пристап до финансиските податоци на институции за кои немаат обврска да даваат сметководствено - финансиски услуги.

Наведените состојби не се во согласност со стандардот ИСО 27001, кој бара строго ограничен пристап до податоци и редовно ажурирање на корисничките профили, како и со Законот за јавна внатрешна финансиска контрола, кој пропишува јасна комуникација и дефинирани правила за управување со финансискиот систем систем и со Стандардот 13 за внатрешна контрола во јавниот сектор - Поделба на должностите, со кој е пропишано дека поделбата на должностите и одговорностите претставува еден од начините преку кои се намалува ризикот од грешки, измами, непочитување на регулативата, како и ризикот од неоткривање на овие неправилности.

Овие состојби влијаат на безбедноста на податоците и може да доведат до безбедносни инциденти, неовластен пристап до податоците во системот и неможност да се утврди кој извршил одредена активност, како и отсуство на целосна контрола врз корисниците кои пристапуваат до истиот.

3.3.3. Контроли на модулот за финансиско работење и останатите модули

Апликативни контроли во ИПР системот

Со анализа на примената на апликативните контроли во различни модули, модулите за финансиско сметководство, ликвидатура, основни средства, водење на благајна во ИПР системот, како и БИ извештајот, направено е директно тестирање и интервјуа со корисниците на системот. Ревизијата утврди недоследности во примената на апликативните контроли кои имаат клучна улога во обезбедувањето на точноста и безбедноста на податоците во системот, и тоа:

- заклучување на податоците од претходните години и неможност за нивно менување не е обезбедено. Оваа контрола претставува добра пракса која гарантира точност и интегритет на историските податоци, и го намалува ризикот од неовластени измени;

- недостатоци во поставените контроли во конфигурациите на дата базата, односно не се чува дневник на настани/ логови на пристап и промени, што ја отежнува можноста за мониторинг и ревизија, како и следење на автентичноста на пристапите до ресурсите;

- недостаток на контрола на автентикација на пристапот до ресурсите односно идентитетот на корисникот со што системот е изложен на

потенцијални безбедносни закани и може да доведе до компромитирање на доверливоста на податоците;

- отсуство на целосно разграничување на должности по корисници, сметки, неспроведување на ревизорска трага за запишани и променети податоци, како и недостаток на соодветна контрола или изготвен извештај за направена контрола не дава можност за следење на активностите на поединечни корисници, како и на внесените и изменетите податоци;

- не е поставена соодветна контрола при внесувањето на шифра на конто и инвентарен број, бидејќи апликацијата дозволува внесување на алфанумерички карактери, а не само на бројки. Дозволувањето на внес на алфанумерички карактери може да доведе до погрешно внесување на податоци во полето за конто и инвентарен број (обележување на средствата). Ова може да влијае на точноста на финансиските и инвентарните записи и да предизвика финансиски импликации за субјектите.;

- нема контрола на кодната страна дали се внесува кириличен или латиничен алфа карактер што може да доведе до неконзистентност во податоците, го намалува интегритетот на внесените информации и може да влијае на квалитетот на извештаите.;

- во модулот за основни средства нема можност да се прави задолжување на вработените со основните средства бидејќи системот нема опција за суб-аналитика. Поради тоа, отсуствуваат детални информации за употребата и распределбата на основните средства, што ја намалува точноста на евиденцијата за основни средства и го отежнува управувањето со имотот на институциите.;

- недостатокот на пропишан начин за пристап на вработените во институциите кои ги користат услугите на Службата и отсуството на можност за увид во внесените податоци и извештаи ја ограничува транспарентноста и ја намалува можноста на раководството да ги следи податоците за донесување навремени и правилни одлуки.

Наведените состојби не се во согласност со Законот за сметководството на буџетите и буџетските корисници, Правилникот за сметководството на буџетите и буџетските корисници, и Законот за јавна внатрешна финансиска контрола и влијаат на интегритетот, точноста и безбедноста на податоците во системот и ја намалуваат доверливоста на системот и ја зголемуваат можноста за неовластени промени и манипулации со податоците што може да доведе до погрешни финансиски извештаи.

3.3.4. Внесување на придружна документација и увид во истата

Во секој сметководствен систем, управувањето со придружната документација претставува клучен аспект за обезбедување на точност, транспарентност и отчетност во процесот на сметководствено книжење. **Сепак, моменталната поставеност на ИПР системот не овозможува внесување и увид во документацијата која претставува основ за сметководствено евидентирање како и основ за извршените трансакции.**

Целокупната придружна документација кај сите институции на кои службата им дава услуги, се одлага и се чува во хартиена форма. Истите се чуваат во класери кои се поделени по сметки и налози редоследно согласно времето кога се евидентираат.

Вработените во службата не поседуваат скенери за да можат да прават електронска копија на добиената придружна документација, ниту пак истата ја добиваат во електронска форма од страна на институциите.

Со приемот на фактурите и нивната придружна документација не се врши нивно евидентирање како обврски во моментот на настанување. По нивно одобрување за плаќање истите се евидентираат во системот како обврски и се врши плаќање. Пропратната документација на фактурите се чува во хартиена форма. На крајот на годината се отстапува од овој начин на работа, каде обврските настанати по основ на примени фактури се евидентираат во системот на соодветна сметка.

Вака воспоставениот начин не овозможува хронолошко внесување на финансиските промени и трансакции. Истовремено, недостатокот на електронска копија од придружната документација го ограничува процесот на дополнителна контрола на евидентирање и создава ризик од губење на важни документи во случај на непогода (кражба, поплава, пожар, земјотрес). Наведеното не е во согласност со Законот за сметководството на буџетите и буџетските корисници, Правилникот за сметководството за буџетите и буџетските корисници и Законот за јавна внатрешна финансиска контрола. Постои ризик сите примени фактури да не бидат евидентирани, како и ризик од недостаток на целокупната документација која претставува основ за сметководственото евидентирање што влијае на точноста и веродостојноста на податоците во финансиските извештаи и точен увид за финансиската состојба.

4

ЗАКЛУЧОК

4 ЗАКЛУЧОК

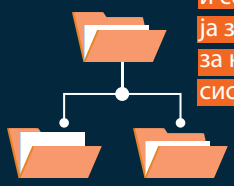
Системот за интегрирано планирање на ресурсите (ИПР систем) го употребува Службата за општи и заеднички работи на Владата на Република Северна Македонија за ефикасно и современо извршување на сметководствено - финансиски услуги за повеќе државни институции.

Исто така, отсуствуваат политики и процедури за редовно тестирање на резервни копии.

Работните станици користат застарен оперативен систем без безбедносни ажурирања и поддршка од производителот, што го зголемува ризикот од безбедносни напади и неовластен пристап.

Иако, ИПР системот е имплементиран во 2016 година, се уште отсуствува правен акт кој ги регулира правата и обврските на Министерството како сопственик и на Службата како корисник на системот, што создава ризик од несоодветно управување со податоците.

Конфигурацијата на ВПН пристапот, без повеќе факторска автентикација односно потврда на идентитет преку два или повеќе независни фактори и со заедничка лозинка, ја зголемува веројатноста за компромитирање на системот.



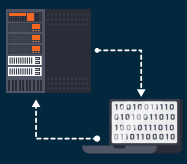
Кај ИПР системот отсуствува интегрираност на модулите во системот.

Одржувањето не е континуирано и навремено обезбедено со потпишани договори.

Недостигот на човечки ресурси влијае на навремено и ефикасно извршување на задачите, со постојан одлив на вработени поради пензионирање и недостаток на вработени со соодветни вештини и знаења.

Отсуствуваат дефинирани процедури за управување со пристапи и заштита на податоците, и ажурирана документација која ја покрива конфигурацијата на системот.

Ваквите состојби како и неинтегрираноста на сите модули во системот укажуваат дека утврдените и имплементираните мерки не се доволни за ефикасна и целосна заштита на податоците во ИПР системот, што го изложува системот на потенцијални безбедносни ризици и компромитирање на доверливоста на податоците.



Не се преземени активности за редовна проверка на резервната копија (бекап) на податоците, и не постојат адекватни контроли за мониторирање на безбедноста на системот.

4

5 ПРЕПОРАКИ

5 ПРЕПОРАКИ

Од ревизијата произлегоа препораки за надлежните институции во насока на надминување и подобрување на утврдените состојби.

Одговорните лица во Министерството и Службата да преземат активности за:

1. Уредување на правата и обврските за ИПР системот со кои ќе се регулираат обемот на услугите, сопственоста, достапноста, интегритетот и безбедноста на податоците (што подразбира ракување, складирање и заштита на податоците), пристапот и овластувањата со договор или друг акт. **(3.1.2.)**

2. Предлагање на Владата за донесување на акт со која го преотстапува правото на користење на системот за интегрирано планирање на Службата. **(3.1.2.)**

3. Подобрување на процесот на планирање на средствата, утврдување на приоритетите и потребите, како и навремено спроведување на постапките за јавни набавки за одржување на ИПР системот. **(3.1.1.1, 3.1.1.2.)**

4. Точно евидентирање на вредноста на системот вклучително и сите негови адаптивни надградби. **(3.1.1.1., 3.1.1.5, 3.1.3.2.)**

5. Воспоставување на механизам за заштита и управување со ИТ безбедноста, кој ќе вклучува:

   - редовно тестирање и следење на безбедносните закани, како и редовно изготвување и доставување на извештаи за преземените активности, идентификуваните закани и мерките за нивно ублажување.
   - редовно проверка на податоците со дефинирана динамика на проверка најмалку еднаш на шест месеци. **(3.1.1.3.)**

6. Дефинирање и усвојување на Процедура за пријавување на проблеми. **(3.1.1.3.)**

7. Подготвување на временски план на активности од работната група во кој ќе бидат дефинирани задачите на двете договорни страни со јасни рокови за нивна реализација.**(3.1.1.4.)**

8. Интегрирање на сите модули за размена на податоците и стандардизирање на сметководствените услуги и унифициран начин на водење на работните процеси за институциите корисници на услугите. **(3.3.1., 3.3.1.1.)**

Одговорните лица во Службата да преземат активности за:

9. Вклучување во Договорите со институциите корисници на услугите јасна распределба на одговорностите помеѓу давателот и корисниците на услугите со прецизно регулирана сопственост и постапувањето со податоците. **(3.1.3.1.)**

10. Изработка, одобрување и имплементирање сеопфатни политики и процедури за:

    - управување со ресурсите, базите на податоци и корисничките сметки, документирано барање за креирање, активирање и деактивирање на корисничка сметка, распределба на задолженија, периодично менување на лозинки, внатрешно информирање за настанатите промени во човечките ресурси како и процедури за начинот на одобрување и забрана на пристап до ресурсите на ИПР системот, начинот на негово следење и контрола;
    - дефинирање на роковите за чување на податоците, нивната сопственост, како и начинот на примопредавање на податоците;
    - за правење на резервна копија, тестирање на истата, планови за опоравување од ИТ катастрофи и обезбедување на континуитет

во работењето

- имплементација на контролни механизми за управување со промените на информациските системи и обработката на податоците и
- разграничување на должности по корисници, сметки и нивна имплементација. **(3.2.1.1., 3.2.1.2., 3.1.4., 3.3.2, 3.3.3.)**

11. Изработка и донесување на стратешки документ за употреба на ИКТ. **(3.2.1.1.)**

12. Анализа за проценка на ризици како и безбедносна проверка на системот, со цел да се идентификуваат најризичните и најкритичните точки за нарушување на информацискатa безбедност. **(3.2.1.1, 3.2.1.2.)**

13. Воспоставување на редовна контрола на креираните кориснички сметки и привилегиите за пристап до податоците во системот. **(3.3.2)**

14. Воспоставување дневник на настани односно логови на пристап и промени, како и негово чување. **(3.3.3.)**

15. Континуирано заклучување на податоците од претходните години по доставување на финансиските извештаи. **(3.3.3.)**

16. Редовно доставување на податоците од ИПР системот и направените трансакции за секоја институција корисник на услугите. **(3.2.2.)**

17. Редовна надградба на дата базата со сигурносните надградби издадени од производителот. **(3.2.1.6.)**

18. Правење редовен бекап на податоците од ИПР системот и заштита на резервната копија, обезбедување на заштитена надворешна локација за чување на резервните копии и редовно тестирање. **(3.2.2.)**

19. Замена на оперативни системи на работните станици со поддржани верзии кои редовно добиваат безбедносни закрпи и ажурирања од производителот. **(3.2.3.)**

20. Конфигурација на ВПН пристапот согласно барањата на стандардите за ИТ безбедност и имплементација на повеќефакторска автентикација за сите корисници кои имаат пристап до серверите. **(3.2.3)**

21. Обезбедување на потребните човечки ресурси за извршување на услугите. **(3.3.1.)**

22. Дополнување на актот за систематизација за сите работни места кои немаат дефинирани активности поврзани со органите на државната управа. **(3.3.1.)**

23. Дефинирање на конкретни услуги односно активности во рамките на финансиско-сметководствените услуги во договорите за вршење општи и заеднички работи и утврдување на конкретни работни обврски и задачи во актите за распоредување на работните места на вработените. **(3.3.1., 3.3.1.1.)**

24. Дефинирање јасен и стандардизиран начин за пристап на вработените во институциите кои ги користат услугите на системот, како за внесување на податоци така и за добивање на извештаи во реално време. **(3.3.1.1., 3.3.3)**

25. Подготовка на точна листа со услуги кои Службата ги овозможува на институциите на кои им се дава услугата. **(3.3.1.1.)**

26. Воспоставување механизам за задолжителна промена на лозинка во системот и комплексност на истата. **(3.2.1.6, 3.3.2.)**

27. Поставување на контрола на внес само на нумерички знаци за шифрите на конто и инвентарен број како и користење единствена кодна страна за внесување на податоци. **(3.3.3.)**

28. Воведување на електронска копија на целата придружна документација на институциите на кои им се даваат услуги, а кои се користат како влез во сметководствените налози и истата да биде внесена во системот. **(3.3.4.)**

29. Чување на придружна документација за евиденција на побарувањата и обврските во електронска форма и на институциите кои се корисници на услугите да им се овозможи брз увид во придружна документација. **(3.3.4)**

30. Воспоставување начин на хронолошко внесување на финансиските промени на обврските при нивното настанување. **(3.3.4.)**

ПРИЛОЗИ

Прилог 1 Критериуми и показатели за оценка на ефективноста

КРИТЕРИУМИ И ИНДИКАТОРИ ЗА ОЦЕНКА

Главно прашање[42]:

> Дали се утврдени и имплементирани мерки за ефикасна и целосна заштита на податоците во системот за интегрирано планирање со ресурсите?

Област 1: ИТ Управување – Правна рамка

Специфично прашање[43]	Потпрашање[44]	Критериуми за оценка	Индикатори
1	2	3	4
Специфично прашање: Дали се уредени правата и обврските за заштита и пристап до податоците на институциите корисници на системот?	**1.1.1.** Дали се уредени правата и обврските за нивото на услуги (SLA) со економските оператори кои ги одржуваат системите за ИПР и системскиот пристап? **1.1.2.** Дали помеѓу СОЗР и МИОА се дефинирани сите неопходни права и обврски? **1.1.3.** Дали е правно регулирана сопственоста на податоците? **1.1.4.** Дали се утврдени и разграничени надлежностите и привелигиите за пристап?	• Закон за јавна внатрешна финансиска контрола Точка 11. Контроли, член 16; • Дефинираните права и обврски во договорите помеѓу засегнатите страни. • Пишани политики и процедури за користење на ИПР системот; • Пишани барања и одобрувања пристап на корисниците до ресурси.	Потпишани договори помеѓу засегнатите страни. Извештаи/документи за имплементација, одобрени политики и процедури за користење на ИПР системот, барање и одобрување пристап на корисниците до ресурси.

[42] Основна/главна цел (прашање прво ниво)
[43] Специфично прашање (прашање второ ниво)
[44] Потпрашање (прашање трето ниво). Според проценка на ревизорот може да се определуваат/развиваат и други потпрашања (други нивоа)

Област 2: ИТ Операции – Системски подесувања (конфигурација) на софтверите за пристап до ресурсите на системот за интегрирано планирање

Специфично прашање[43]	Потпрашање[44]	Критериуми за оценка	Индикатори
1	2	3	4
Специфично прашање: Дали поставената конфигурација овозможува безбеден пристап до ресурсите и достапност на системот за интегрирано планирање?	2.1.1. Дали системската конфигурација на базата на податоци е во согласност со најдобрите практики за безбедност?	• Ревизорска програма за SQL сервер (изработена со колеги од ОАГН) и ISO 27001 најдобри практики.	Усогласеност со најдобрите практики за ревизија на конфигурација на SQL сервер.
	2.1.2. Дали е дизајнирана и се применува заштита и резервна копија на податоците и осигурен брз поврат во случај на катастрофа?	• Политики и процедури за заштита и резервна копија на податоците и поврат во случај на катастрофа.	Извештаи и резултати од тестирање на исправноста на резервната копија. Дефинирани насоки за поврат во случај на катастрофа извештаи од направени тестирање. Увид на последно направен back up.
	2.1.3. Дали истата се чува на безбедна и заштитена локација со брз пристап за поврат на податоците?		
	2.1.4. Дали работните станици каде е инсталирана апликацијата обезбедуваат безбеден пристап до серверите?	• Поставеност на пристапот и безбедноста на оперативните системи на работните станици.	Воспоставен безбеден ВПН пристап и безбедни оперативни системи на работните станици.

Област 3: Апликациски контроли - Човечки капацитети и апликациски контроли на системот за ИПР

Специфично прашање[43]	Потпрашање[44]	Критериуми за оценка	Индикатори
1	2	3	4
Специфично прашање: Дали човечките капацитети и имплементираните апликациски контроли обезбедуваат заштита и пристап до податоците на институциите корисници на системот?	3.1.1. Дали човечките капацитети на СОЗР се доволни за да ги опслужат тековните корисници на ИПР системот и дали се доволни за проширување со нови корисници или нови услуги?	• Внатрешна организација и систематизација на СОЗР; • Решенија за работно распоредување и извршување на работните задачи; • Анализа на работни места и работни задачи.	Систематизирани работни позиции со задачи поврзани со ИТ за администрација и ИТ заштита. Решенијата за распределба на работно место со задачи поврзани со ИТ за администрација и ИТ заштита. Број на лица ангажирани со задачи поврзани со ИТ за администрација и ИТ заштита
	3.1.2. Како се врши контрола за користење на ИПР системот и пристапот до модулите и податоците?	• Логовите за пристап на корисниците до модулите и податоците.	Број на извршени контроли на логовите за пристап на корисниците до модулите и податоците.извештаи од направени тестирање.
	3.1.3. Дали се воспоставени контроли на модулот за финансиско работење?	• Техничка спецификација на модулот за финансиско работење и увид во модулот.	Резултати од анализа на техничката спецификација и тестирање на модулот за финансиско работење.
	3.1.4. Дали во системот е овозможено внесување на документација што претставува основа за сметководствено книжење и увид во истата?	• Правилник за сметководството за буџетите и буџетските корисници, член 11 и 12.	Резултати од тестирања по случаен избор, овозможено е тестирање и постои документација која е основа за пропуштање на системот на документација која е сметководствено книжење.системи на работните станици.

Прилог 2 Корисници на ИПР систем

р.бр	Корисници на системот
1	Агенција за остварување на правата на заедниците
2	Агенција за примена на јазикот што го зборуваат најмалку 20% од граѓаните на Република Северна Македонија
3	Агенција за храна и ветеринарство
4	Биро за застапување на Република Северна Македонија пред Европскиот суд за човекови права
5	Биро за Метрологија
6	Биро за регионален развој
7	Биро за судски вештачења
8	Влада на Република Северна Македонија
9	Државен завод за индустриска сопственост
10	Државен пазарен инспекторат
11	Државна комисија за жалби по јавни набавки
12	Државна комисија за спречување на корупција
13	Државна фитосанитарна лабораторија
14	Инспекторат за употреба на јазиците
15	Инспекциски Совет Скопје
16	Комитет за истрага на воздухопловни несреќи
17	Македонска Академска Истражувачка Мрежа МАРНЕТ
18	Министерство за Економија
19	Министерство за животна средина
20	Министерство за здравство
21	Министерство за земјоделство, шумарство и водостопанство
22	Министерство за информатичко општество и администрација
23	Министерство за култура
24	Министерство за локална самоуправа
25	Министерство за политички систем и односи меѓу заедниците
26	Министерство за правда
27	Министерство за транспорт и врски
28	Секретаријат за европски прашања
29	Секретаријат за законодавство
30	Служба за општи и заеднички работи на Влада на Република Северна Македонија

31	Служба за просторен и информативен систем
32	Управа за водење на матични книги
33	Управа за водостопанство
34	Управа за животна средина
35	Управа за заштита на растенијата (фитосанитарна управа)
36	Управа за извршување на санкции
37	Управа за наменско производство
38	Управа за семе и семенски материјал
39	Управа за сигурност во железничкиот систем
40	Управа за хидрометеоролошки работи

Прилог 3 Институции опфатени со ревизијата заедно со органите на министерствата и Службата

р.бр	Институции опфатени со ревизија
1	Агенција за остварување на правата на заедниците
2	Агенција за примена на јазикот што го зборуваат најмалку 20% од граѓаните на Република Северна Македонија
3	Агенција за храна и ветеринарство
4	Биро за застапување на Република Северна Македонија пред Европскиот суд за човекови права
5	Биро за Метрологија
6	Биро за регионален развој
7	Биро за судски вештачења
8	Влада на Република Северна Македонија
9	Геолошки завод на Република Северна Македонија
10	Државен завод за индустриска сопственост
11	Државен инспекторат за локална самоуправа
12	Државен пазарен инспекторат
13	Државна комисија за жалби по јавни набавки
14	Државна комисија за одлучување во втор степен во областа на инспекцискиот надзор и прекршочна постапка на РСМ
15	Државна комисија за спречување на корупција
16	Државна фитосанитарна лабораторија
17	Инспекторат за употреба на јазиците
18	Инспекциски Совет Скопје
19	Кабинетот на Претседателот на РСМ
20	Комисија за заштита од дискриминација
21	Комитет за истрага на воздухопловни несреќи
22	Македонска Академска Истражувачка Мрежа МАРНЕТ
23	Министерство за Економија
24	Министерство за животна средина и просторно планирање
25	Министерство за здравство
26	Министерство за земјоделство, шумарство и водостопанство
27	Министерство за информатичко општество и администрација
28	Министерство за култура

29	Министерство за локална самоуправа
30	Министерство за политички систем и односи меѓу заедниците
31	Министерство за правда
32	Министерство за транспорт и врски
33	Секретаријат за европски прашања
34	Секретаријат за законодавство
35	Служба за просторен и информативен систем
36	Служба за општи и заеднички работи на Влада на Република Северна Македонија
37	Управа за афирмирање и унапредување на културата на припадниците на заедниците
38	Управа за водење на матични книги
39	Управа за водостопанство
40	Управа за животна средина
41	Управа за заштита на растенијата (фитосанитарна управа)
42	Управа за извршување на санкции
43	Управа за наменско производство
44	Управа за развој и унапредување на образованието на јазиците на припадниците на заедниците
45	Управа за семе и семенски материјал
46	Управа за сигурност во железничкиот систем
47	Управа за хидрометеоролошки работи

Прилог 4 Листа на модули кои се користат во ИПР системот со вид на услуги за институција

р.бр	Корисници на системот	Финансиско работење	Благајничко работење	Основни средства
1	Агенција за остварување на правата на заедниците	✓		
2	Агенција за примена на јазикот што го зборуваат најмалку 20% од граѓаните на Република Северна Македонија	✓		
3	Агенција за храна и ветеринарство	✓		
4	Биро за застапување на РСМ пред Европскиот суд за човекови права	✓		
5	Биро за Метрологија	✓	✓	✓
6	Биро за регионален развој	✓		
7	Биро за судски вештачења	✓		
8	Влада на Република Северна Македонија	✓	✓	✓
9	Државен завод за индустриска сопственост	✓		
10	Државен пазарен инспекторат	✓		
11	Државна комисија за жалби по јавни набавки	✓	✓	✓
12	Државна комисија за спречување на корупција	✓	✓	✓
13	Државна фитосанитарна лабораторија	✓		
14	Инспекторат за употреба на јазиците	✓		
15	Инспекциски Совет Скопје	✓		✓
16	Комитет за истрага на воздухопловни несреќи	✓		
17	Македонска Академска Истражувачка Мрежа МАРНЕТ	✓	✓	
18	Министерство за Економија	✓	✓	✓
19	Министерство за животна средина и просторно планирање	✓	✓	✓
20	Министерство за здравство	✓	✓	✓
21	Министерство за земјоделство, шумарство и водостопанство	✓		✓
22	Министерство за информатичко општество и администрација	✓	✓	
23	Министерство за култура	✓	✓	
24	Министерство за Локална Самоуправа	✓	✓	
25	Министерство за политички систем и односи меѓу заедниците	✓	✓	✓
26	Министерство за правда	✓		✓
27	Министерство за транспорт и врски	✓		✓
28	Секретаријат за европски прашања/Министерство за европски прашања	✓	✓	✓
29	Секретаријат за законодавство	✓		

30	Служба за општи и заеднички работи на Влада на Република Северна Македонија	✓	✓	✓
31	Служба за просторен и информативен систем	✓		
32	Министерство за правда - Управа за водење на матични книги	✓		✓
33	Управа за водостопанство	✓		
34	Управа за животна средина	✓		
35	Управа за заштита на растенијата (фитосанитарна управа)	✓		
36	Управа за извршување на санкции	✓		✓
37	Управа за наменско производство	✓		
38	Управа за семе и семенски материјал	✓		
39	Управа за сигурност во железничкиот систем	✓		
40	Управа за хидрометеоролошки работи	✓	✓	✓

Прилог 5 Забелешки по нацрт извештај

Република Северна Македонија

Министерство за дигитална трансформација

Архивски број: 02-982/3
Датум: 29.05.25

Предмет: Одговор по препораки од извршена ревизија на ЕРП системот

Почитувани,

Согласно доставениот нацрт извештај со арх.бр.02-982/2 од 12.05.2025год. Овластениот државен ревизор за извршена ИТ ревизија на Системот за интегрирано планирање на ресурсите (ЕРП), во насока на надминување и подобрување на утврдените состојби на системот, сакам да Ве информиран дека Министерството за дигитална трансформација веќе презема некои активности според дадените Препораки од нацрт извештајот.
Имено, по Препораките од нацрт извештајот за:

- *Препорака бр1.Уредување и обврските за ИПР системот со кои ќе се регулираат обемот на услугите, сопственоста, достапноста, интегритетот и безбедноста на податоците (што подразбира ракување, складирање и заштита на податоците), пристапот и овластувањата со договор или друг акт (3.1.2)*

Министерството за дигитална трансформација во рок од два месеци ќе изготви Договор за уредување и регулирање на обемот на услугите, сопственоста, достапноста, интегритетот и безбедноста на податоците.

- *Препорака бр.2 Предлагање на Владата за донесување на акт со кој се отстапува правото на користење на системот за интегрирано планирање во Службата (3.1.2)*

Министерството за дигитална трансформација се произнесува дека не го отстапува правото на користење на ЕРП системот, од причина што планирано е употребата на системот да се проширува и во други институции.

- *Препорака бр.3 Подобрување на процесот на планирање на средства, утврдување на приоритетните и потребите, како и навремено спроведување на постапките за јавни набавки за одржување на ИПР (3.1.1.1, 3.1.1.2)*

Министерство
за дигитална трансформација на
Република Северна Македонија
Ул. „Филип Втори Македонски" бр.11, Скопје
Република Северна Македонија
+389 2 320 0999
www.mdt.gov.mk

Министерството за дигитална трансформација има склучено договор со арх. бр.16-76/5 од 31.05.2025год и Допис за дефинирање на обврски со арх.број 16-76/10 меѓу МДТ и Службата за општи и заеднички работи.

- *Препорака бр.4.Точно евидентирање на вредноста на системот вклучително и сите негови адаптивни надградби (3.1.1.1, 3.1.1.5, 3.1.3.2)*

Министерството за дигитална трансформација во наредниот период ќе изврши точно евидентирање на вредноста на системот вклучително и сите негови адаптивни надградби

- *Препорака бр.5 Воспоставување на механизам за заштита и управување со ИТ безбедност, кој ќе вклучува:*
  - *Редовно тестирање и следење на безбедносните закани, како и редовно изготвување и доставување на извештаи за преземени активности, идентификуваните закани и мерките за нивно ублажување,*
  - *Редовна проверка на податоците со дефинирана динамика на проверка најмалку еднаш на шест месеци (3.1.1.3)*

Министерството за дигитална трансформација подготвува квартален извештај во кој се вградени и бараните извештаи од оваа препорака.

- *Препорака бр.6 Дефинирање и усвојување на Процедура за пријавување на проблеми (3.1.1.3)*

Министерството за дигитална трансформација во тек е на изготвување на Процедура за пријавување на проблеми, во кој се состојат бараните процедури од оваа препорака

- *Препорака бр.7 Подготвување на временски план на активности од работната група во кој ќе бидат дефинирани задачите на двете договорени страни со јасни рокови за нивна реализација (3.1.1.4)*

Министерството за дигитална трансформација има подготвено Работен план на активности, во кој јасно се дефинирани работните задачи и временските рокови предвидени за нивно извршување, при што овој план тековно се ажурира со активности согласно имплементацијата на ЕРП системот.

- *Препорака бр.8. Интегрирање на сите модули за размена на податоците и стандардизирање на сметководствените услуги и унифициран начин на водење на работните процеси за институциите корисници на услугите(3.3.1.3, 3.3.1.1)*

Фирмата изведувач Дуна ДОО ќе пристапи кон изведување на оваа препорака да започне од јуни 2025 со модулот интеграција на Трезорско работење во Ултима ЕРП во институцијата МДТ, а потоа етапно институција по институција. Интеграцијата на системот по модули и институции ќе се спроведува етапно, со цел да се обезбеди стабилност, функционалност, и контрола врз процесот на имплементација. Планот опфаќа фази на подготовка,програмирање, интеграција, тестирање, имплементација и обука.

Со оглед на тоа дека дека Министерството за дигитална трансформација веќе презема активности согласно дадените препораки, Ве замолуваме истите да бидат земени во превид при креирање на конечниот извештај за спроведената ревизија на ЕРП системот.

Со почит,

Министер
Стефан Андоновски

Подготвил: Александра Ставрева Стојаноска
Конторолирал: Оливера Јакшиќ Транталовска
Согласен: Гордана Клинчарова

Министерство
за дигитална трансформација на
Република Северна Македонија

Ул. „Филип Втори Македонски" бр.11, Скопје
Република Северна Македонија

+389 2 320 0999
www.mdt.gov.mk

Прилог 6 Одговор на Забелешки по нацрт извештај

Добиени се забелешки бр. 02-982/3 од 21.05.2025 година на Нацрт извештајот за извршена ИТ ревизија како ревизија на успешност на тема „ Систем за интегрирано планирање на ресурсите - ИПР систем“, од страна на одговорното лице на Министерството за дигитална трансформација, г-дин Стефан Андоновски, министер, а заведени во Државниот завод за ревизија под број 34-543/4 од 09.06.2025 година.

Забелешките се разгледани од страна на Овластениот државен ревизор и констатирано е следното:

- Забелешките на препораката број 1 за точката 3.1.2. за уредување на правата и обврските за ИПР системот со кои ќе се регулираат обемот на услугите, сопственоста, достапноста, интегритетот и безбедноста на податоците (што подразбира ракување, складирање и заштита на податоците), пристапот и овластувањата со договор или друг акт претставуваат известување за планирани активности за донесување на Договор за уредување и регулирање на обемот на услуги, сопственоста, достапноста, интегритетот и безбедноста на податоците.

- Забелешката на препораката број 2 за точката 3.1.2. за не отстапување на правото на користење на ЕРП системот поради проширување и во други институции не се прифаќа од причини што препораката се однесува за донесување на акт со која го преотстапува правото на користење на системот за интегрирано планирање на Службата.

- Забелешките на препораката број 3 за точката 3.1.1.1 и 3.1.1.2 за подобрување на процесот на планирање на средствата, утврдување на приоритетите и потребите, како и навремено спроведување на постапките за јавни набавки за одржување на ИПР системот претставуваат известување за преземени активности за склучување договор на Министерството за дигитална трансформација и Службата за за општи и заеднички работи.

- Забелешките на препораката број 4 за точката 3.1.1.1, 3.1.1.5 и 3.1.3.2 за евидентирање на вредноста на системот претставуваат известување за планирани активности за точно евидентирање на вредноста на системот вклучително и сите негови адаптивни надградби.

- Забелешките на препораката број 5 за точката 3.1.1.3 за воспоставување на механизам за заштита и управување со ИТ безбедност претставуваат известување за планирани активности за изготвување на квартални извештаи преземени активности, идентификувани закани и мерки за нивно ублажување.

- Забелешките на препораката број 6 за точката 3.1.1.3 за дефинирање и усвојување на Процедура за пријавување на проблеми претставуваат известување за планирани активности за изготвување на Процедура за пријавување на проблеми.

- Забелешките на препораката број 7 за точката 3.1.1.4 за подготвување на временски план на активности од работната група во кој ќе бидат дефинирани задачите на двете договорни страни со јасни рокови за нивна реализација подобрување на процесот на планирање на средствата, утврдување на приоритетите и потребите, како и навремено спроведување на постапките за јавни набавки за одржување на ИПР системот претставуваат известување за преземени активности за подготвување на Работен план на активности со дефинирани работни задачи и временски рокови предвидени за нивно извршување и редовно ажурирање.

- Забелешките на препораката број 8 за точката 3.1.1. и 3.3.1.1 за интегрирање на сите модули за размена на податоците и стандардизирање на сметководствените услуги и унифициран начин на водење на работните процеси за институциите корисници на услугите претставуваат известување за планирани активности за јуни 2025 година за интеграција на модулите во Министерството за дигитална трансформација, а потоа етапно во другите институции, со цел да се обезбеди стабилност, функционалност и контрола на процесот.