ДРЖАВНА
РЕВИЗОРСКА
ИНСТИТУЦИЈА

ИЗВЕШТАЈ

О РЕВИЗИЈИ СВРСИСХОДНОСТИ ПОСЛОВАЊА

ЕФЕКТИВНОСТ ИНФОРМАЦИОНОГ СИСТЕМА МАТИЧНА ЕВИДЕНЦИЈА И ОСТВАРИВАЊЕ ПРАВА (МЕОП) У РЕПУБЛИЧКОМ ФОНДУ ЗА ЗДРАВСТВЕНО ОСИГУРАЊЕ

Број: 400-450/2023-07/22
Београд, 22. новембар 2023. године

НЕОПХОДНО ЈЕ ДА РФЗО УНАПРЕДИ ИТ УПРАВЉАЊЕ, ОБЕЗБЕДИ ВИШИ НИВО ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ И ОБЕЗБЕДИ КОНТИНУИТЕТ ПОСЛОВАЊА У СЛУЧАЈУ ПРЕКИДА САРАДЊЕ СА ПРУЖАОЦЕМ УСЛУГЕ ОДРЖАВАЊА ИС МЕОП

За спровођење обавезног здравственог осигурања, најзначајнију улогу има информациони систем МЕОП–Матична евиденција и остваривање права. Матичну евиденцију јединствено за територију Републике Србије устројава и организује РФЗО и чине је подаци о: осигураницима, члановима породице осигураника, обвезницима плаћања доприноса и коришћењу права из обавезног здравственог осигурања. Проблеми који су идентификовани у претходном периоду су: стратегијски приступ развоју информационих система, информациона безбедност, приступ подацима осигураника од стране здравствених установа и синхронизација података са здравственим установама.

РФЗО није у потпуности успоставио ефективно ИТ управљање, није израдио ИТ стратегију за период 2022–2024. године, не предузима активности у циљу препознавања свих ИТ ризика и јачања кадровских капацитета у ИТ сектору и није успоставио правила управљања подацима из матичне евиденције осигураника, којима би онемогућио приступ личним подацима осигураника и без њиховог физичког присуства.

Даље, РФЗО није у потпуности успоставио управљање информационом безбедношћу ИС МЕОП, јер не прати и не контролише додељена права приступа ИС МЕОП и, није попунио радна места у Сектору за информациону безбедност и заштиту података.

Такође, РФЗО није у потпуности успоставио ефективан механизам сарадње, односно није у потпуности уредио правилима и процедурама однос са пружаоцем услуге одржавања ИС МЕОП, као ни мере којима обезбеђује континуитет пословања у случају прекида сарадње са пружаоцем услуге одржавања ИС МЕОП. РФЗО није уредио однос са пружаоцем услуге одржавања ИС МЕОП, у делу дефинисања нивоа доступности и врсте информација, средстава којима могу приступити пружаоци услуга, начина приступа информацијама и средствима и надзора над приступом.

Препоруке

Државна ревизорска институција је субјекту ревизије (РФЗО) дала следеће препоруке:

- да у циљу успостављања организационе структуре за ИТ управљање, предузме мере за јачање кадровских капацитета кроз повећање броја и/или стручних знања запослених;
- да предузме мере на кадровском јачању Сектора за информациону безбедност и заштиту података;
- да успостави правила управљања подацима матичне евиденције осигураника којима би се, уз обавезно физичко присуство осигураника, омогућио приступ личним подацима осигураника;
- да предузме активности у циљу континуиране едукације запослених који обављају ИТ послове;
- да успостави правила и процедуре за редовну контролу и праћење приступа ИС МЕОП;
- да предузме активности у циљу успостављања континуитета пословања у делу измена/доградње информационог система МЕОП и евентуалне миграције података, у случају прекида сарадње са пружаоцем услуге.

Садржај

Скраћенице и термини 5

I Резиме откривених несврсисходности, препорука и мера предузетих у поступку ревизије 6

II Увод 11

1. Проблем 11
2. Циљ ревизије 12
3. Ревизорска питања 12
4. Обим и ограничења ревизије 13
5. Методологија у поступку рада 14

III Опис предмета ревизије 15

1) Законодавни и институционални оквир 15
   Законодавни оквир 15
   Институционални оквир 15
2) Информациони систем МЕОП 17
   Дефиниција 17
   Величина система 23
   Техничке карактеристике система 24
3) Исправа о осигурању 24

IV Закључци 26

ЗАКЉУЧАК 1: РФЗО није у потпуности успоставио ефективно ИТ управљање због недостатка кадровских капацитета, непрепознавања могућих ИТ ризика и управљања подацима из матичне евиденције осигураника. 27

Налаз 1.1: РФЗО није донео ИТ стратегију за период 2022–2024. године. 27

Налаз 1.2: ИТ управљање није успостављено на адекватан начин због непрепознавања свих ИТ ризика и недовољних кадровских капацитета. 29

Налаз 1.3: РФЗО није успоставио правила управљања подацима из матичне евиденције осигураника, којима би онемогућио приступ личним подацима осигураника и без њиховог физичког присуства. 37

ЗАКЉУЧАК 2: РФЗО није у потпуности успоставио управљање информационом безбедношћу ИС МЕОП јер није попунио радна места у Сектору за информациону безбедност и заштиту података и не прати и не контролише додељена права приступа ИС МЕОП, што може довести до неовлашћеног приступа подацима осигураника и остварeним правима у здравственој заштити. 41

Налаз 2.1: РФЗО није у потпуности успоставио логички приступ ИС МЕОП који обезбеђује поузданост информационог система (контролу права приступа). 42

Налаз 2.2: РФЗО није попунио радна места у Сектору за информациону безбедност и заштиту података. 48

Налаз 2.3: РФЗО није у потпуности успоставио процес праћења и контроле приступа ИС МЕОП од стране ЗУ и запослених у РФЗО. 53

ЗАКЉУЧАК 3: РФЗО није у потпуности успоставио ефективан механизам сарадње, односно није у потпуности уредио правилима и процедурама однос са пружаоцем услуге одржавања ИС МЕОП и мере којима обезбеђује континуитет пословања у случају прекида сарадње са пружаоцем услуге одржавања ИС МЕОП. 56

Налаз 3.1: РФЗО није успоставио (уредио) однос са пружаоцем услуга одржавања ИС МЕОП у делу дефинисања нивоа доступности и врсте информација, средстава којима могу приступити пружаоци услуга, начина приступа информацијама и средствима и надзора над приступом. *56*

Налаз 3.2: РФЗО је обезбедио заштиту осетљивих података о осигураницима тако да врши псеудонимизацију података базе МЕОП. *61*

Налаз 3.3: РФЗО није предвидео мере које обезбеђују континуитет пословања у случају прекида сарадње са пружаоцем услуге одржавања ИС МЕОП...... *68*

V Прилози.....**71**

Прилог 1 – Методологија у поступку рада 71

Скраћенице и термини

У прегледу су дате скраћенице које су коришћене у извештају:

Пун назив	Скраћеница
Републички фонд за здравствено осигурање	РФЗО
Државна ревизорска институција	ДРИ
Информациони систем Матична евиденција и остваривање права (МЕОП)	ИС МЕОП
Здравствене установе	ЗУ
Конкурсна документација	КД
Матична евиденција и остваривање права	МЕОП
Централни регистар обавезног социјалног осигурања	ЦРОСО
Пореска управа	ПУ
Картица здравственог осигурања	КЗО
Информационо-комуникациони системи од посебног значаја	ИКТ системи
Јединствени матични број грађанина	ЈМБГ
Лични број осигураника	ЛБО
Потврда о поднетој пријави, промени и одјави на обавезно социјално осигурање	МА образац
Потврда о здравственом осигурању	ПЗК образац
Здравствени лист за иностраног осигураника и чланове његове породице	ИНО образац
Потврда за коришћење здравствене заштите	ПЖД образац
Обавештење о постојању трудноће, обављеном порођају, односно о мртворођеном детету, односно прекиду трудноће и у случају смрти детета до годину дана живота	ДТП образац
Регистар изабраних лекара	РИЛ

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

1. Резиме и препоруке

Државна ревизорска институција спровела је ревизију сврсисходности пословања „Ефективност информационог система Матична евиденција и остваривање права (МЕОП) у Републичком фонду за здравствено осигурање."

За спровођење обавезног здравственог осигурања најзначајнију улогу има ИС МЕОП–матична евиденција и остваривање права– Матичну евиденцију јединствено за територију Републике Србије устројава и организује РФЗО и матичну евиденцију чине подаци о: осигураницима, члановима породице осигураника, обвезницима плаћања доприноса и коришћењу права из обавезног здравственог осигурања. Проблеми који су идентификовани у претходном периоду су: стратегијски приступ развоју информационих система, информациона безбедност, приступ подацима осигураника од стране здравствених установа и синхронизација података са здравственим установама.

Циљ ревизије је да се оцени ефективност ИС МЕОП у РФЗО.
Након спроведене ревизије сврсисходности пословања утврдили смо следеће:
Неопходно је да Републички фонд за здравствено осигурање унапреди ИТ управљање, обезбеди виши ниво информационе безбедности и обезбеди континуитет пословања у случају прекида сарадње са пружаоцем услуге одржавања ИС МЕОП.

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

1. РФЗО није у потпуности успоставио ефективно ИТ управљање због недостатка кадровских капацитета, непрепознавања могућих ИТ ризика и проблема са управљањем подацима из матичне евиденције осигураника.
   - ✓ РФЗО није донео ИТ стратегију за период 2022-2024. године.
   - ✓ ИТ управљање није успостављено на адекватан начин због непрепознавања свих ИТ ризика и недовољних кадровских капацитета.
   - ✓ РФЗО није успоставио правила управљања подацима из матичне евиденције осигураника, којима би онемогућио приступ личним подацима осигураника и без њиховог физичког присуства.

2. РФЗО није у потпуности успоставио управљање информационом безбедношћу ИС МЕОП јер није попунио радна места у Сектору за информациону безбедност и заштиту података и не прати и не контролише додељена права приступа ИС МЕОП, што може довести до неовлашћеног приступа подацима осигураника и остареним правима у здравственој заштити.
   - ✓ РФЗО није у потпуности успоставио логички приступ ИС МЕОП који обезбеђује поузданост информационог система (контролу права приступа).
   - ✓ РФЗО није попунио радна места у Сектору за информациону безбедност и заштиту података.
   - ✓ РФЗО није у потпуности успоставио процес праћења и контроле приступа ИС МЕОП од стране ЗУ и запослених у РФЗО.

3. РФЗО није у потпуности успоставио ефективан механизам сарадње, односно није у потпуности уредио правилима и процедурама однос са пружаоцем услуге одржавања ИС МЕОП и мере којима обезбеђује континуитет пословања у случају прекида сарадње са пружаоцем услуге одржавања ИС МЕОП.

- ✓ РФЗО није успоставио (уредио) однос са пружаоцем услуга одржавања ИС МЕОП у делу дефинисања нивоа доступности и врсте информација, средстава којима могу приступити пружаоци услуга, начина приступа информацијама и средствима и надзора над приступом.
- ✓ РФЗО је обезбедио заштиту осетљивих података о осигураницима тако да врши псеудонимизацију података базе МЕОП.
- ✓ РФЗО није предвидео мере које обезбеђују континуитет пословања у случају прекида сарадње са пружаоцем услуге одржавања ИС МЕОП.

Након спроведене ревизије „Ефективност информационог система Матична евиденција и остваривање права (МЕОП) у Републичком фонду за здравствено осигурање", Државна ревизорска институција даје следеће препоруке:

Републичком фонду за здравствено осигурање:

1. да донесе стратешки документ (ИТ стратегију) и акциони план, којим би се планирао развој и управљање информационим системима, рачунарским апликацијама, базама података и континуираном обуком запослених (приоритет 2[1])–Налаз 1.1.
2. да у циљу успостављања организационе структуре за ИТ управљање, предузме мере за јачање кадровских капацитета кроз повећање броја и/или стручних знања запослених (приоритет 3[2])–Налаз 1.2.
3. да успостави управљање ИТ ризицима, што подразумева евидентирање, класификацију, анализу свих ИТ ризика и дефинисање стратегије за смањивање/отклањање ризика (приоритет 2) –Налаз 1.2.
4. да успостави правила управљања подацима матичне евиденције осигураника којима би се, уз обавезно физичко присуство осигураника, омогућио приступ личним подацима осигураника (приоритет 3) –Налаз 1.3.
5. да предузме мере на кадровском јачању Сектора за информациону безбедност и заштиту података (приоритет 2) –Налаз 2.2.
6. да предузме активности у циљу континуиране едукације запослених који обављају ИТ послове (приоритет 2) –Налаз 2.2.
7. да успостави правила и процедуре за редовну контролу и праћење приступа ИС МЕОП (приоритет 2) –Налаз 2.3.
8. да успостави правила и процедуре сарадње са пружаоцем услуга развоја и одржавања ИС МЕОП, што подразумева дефинисање нивоа доступности и врсте информација, средстава којима могу приступити пружаоци услуга, начина приступа информацијама и средствима и надзора над приступом (приоритет 2) – Налаз 3.1.
9. да предузме активности у циљу успостављања континуитета пословања у делу измена/доградње информационог система МЕОП и евентуалне миграције података, у случају прекида сарадње са пружаоцем услуге (приоритет 2) –Налаз 3.3.

[1] Приоритет 2 означава несврсисходности које је могуће отклонити у року до годину дана.
[2] Приоритет 3 означава несврсисходности које је могуће отклонити у року до три године.

2. Мере предузете у току ревизије

РФЗО је у току поступка ревизије доставио Извештај о контролама управљања корисничким налозима за филијале Београд, Зрењанин и Панчево, као и матрицу привилегија администраторских и корисничких налога за ИС МЕОП након извршене анализе администраторских и корисничких налога.

Захтев за достављање одазивног извештаја

Републички фонд за здравствено осигурање је, на основу члана 40 став 1 Закона о Државној ревизорској институцији, дужан да поднесе Државној ревизорској институцији писани извештај о отклањању откривених несврсисходности(одазивни извештај) у року од 90 дана почев од наредног дана од дана уручења овог извештаја.

Одазивни извештај мора да садржи:

1) навођење ревизије, на коју се он односи;

2) кратак опис несврсисходности у пословању, које су откривене ревизијом;

3) приказивање мера исправљања.

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

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

За налазе, односно несврсисходности другог приоритета, односно које је могуће отклонити у року до годину дана и трећег приоритета, односно које је могуће отклонити у року до три године, Републички фонд за здравствено осигурање обавезан је да достави акциони план у којем ће описати мере и активности које ће бити предузете ради отклањања несврсисходности или смањења ризика од појављивања несврсисходности у будућем пословању, као и планирани период предузимања мера и одговорно лице.

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

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

Сагласно члану 57 став 1 тачка 3) Закона о Државној ревизорској институцији, ако субјект ревизије, у чијем су пословању откривене несврсисходности, не подносе у прописаном року Институцији одазивни извештај, против одговорног лица–субјекта ревизије поднеће се захтев за покретање прекршајног поступка.

Ако се оцени да одазивни извештај не указује на то да су откривене несврсисходности отклоњене на задовољавајући начин, сматра се да субјект ревизије крши обавезу доброг пословања. Ако се ради о незадовољавајућем отклањању значајне несврсисходности, сматра се да постоји тежи облик кршења обавезе доброг пословања.

У овим случајевима Државна ревизорска институције је овлашћена да предузима мере сагласно члану 40 ст 7 до 13 Закона о Државној ревизорској институцији.

Генерални државни ревизор

Др Душко Пејовић
Државна ревизорска институција
Макензијева 41
11000 Београд, Србија
22. новембар 2023. године

II Увод

Државна ревизорска институција спровела је ревизију сврсисходности пословања „Ефективност информационог система Матична евиденција и остваривање права (МЕОП) у Републичком фонду за здравствено осигурање" у периоду од априла до септембра 2023. године.[3] Ревизија сврсисходности пословања је спроведена у складу са Законом о Државној ревизорској институцији[4], Пословником Државне ревизорске институције[5] и Програмом ревизије Државне ревизорске институције за 2023. годину.

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

1. Проблем

Обавезно здравствено осигурање обезбеђује се и спроводи у РФЗО[6]. Средства за остваривање права из обавезног здравственог осигурања обезбеђују се уплатом доприноса, као и из других извора, у складу са законом[7]. За спровођење обавезног здравственог осигурања најзначајнију улогу има информациони систем МЕОП-матична евиденција и остваривање права.

Законом о здравственом осигурању прописано је да матичну евиденцију јединствено за територију Републике Србије устројава и организује РФЗО[8]. Законом о здравственом осигурању прописано је да матичну евиденцију чине подаци о:

1) осигураницима;
2) члановима породице осигураника;
3) обвезницима плаћања доприноса;
4) коришћењу права из обавезног здравственог осигурања[9].

Према одредбама Закона о здравственој документацији и евиденцијама у области здравства, здравствена установа, приватна пракса и друго правно лице, дужни су да успоставе информациони систем, који представља свеобухватни скуп технолошке инфраструктуре (мрежних, софтверских и хардверских компонената), организације, људи и поступака за прикупљање, смештање, обраду, чување, пренос, приказивање и коришћење података и информација.[10]

У претходним годинама, уочени су проблеми у функционисању информационих система РФЗО у више области:

[3] Број ревизије: 400-450/2023-07.
[4] „Службени гласник РС", бр. 101/05, 54/07, 36/10 и 44/18-др. закон.
[5] „Службени гласник РС", број 9/09.
[6] Члан 7 Закона о здравственом осигурању.
[7] Члан 168 Закона о здравственом осигурању.
[8] члан 31 став 2 Закона о здравственом осигурању („Службени гласник РС", бр. 25/19).
[9] члан 31 став 1 Закона о здравственом осигурању („Службени гласник РС", бр. 25/19).
[10] члан 45 став 1, Закона о здравственој документацији и евиденцијама у области здравства („Службени гласник РС", бр. 123/14, 106/15, 105/17 и 25/19 - др. закон)

1) стратегијски приступ

Без усвојене стратегије развоја информационих технологија, која треба бити саставни део стратешког планирања за период од три до пет година, информационе технологије не могу у одговарајућој мери допринети остваривању и развоју пословних циљева организације, ни у системском (хардвер и софтвер) ни у кадровском (структура и знање) смислу.

2) поузданост информационих система

Проблеми који су се односили на информациону безбедност, обухватају питања:

- физичког и логичког приступа систему од стране запослених у РФЗО;
- приступа системима и базама података од стране пружаоца услуга одржавања ИС МЕОП;
- управљања лог фајловима и инцидентима (базе података садрже осетљиве податке о личности о сваком осигуранику).

3) начин пријаве осигураника и приступ картону осигураника

Здравствена исправа представља документ којим осигурано лице остварује своја права на здравствено осигурање. Процес замене папирне исправе здравственом картицом започео је 2015. године. Иако је преузето око 7 милиона електронских здравствених картица, подацима осигураника се може приступити и без њих, често и само на основу ЈМБГ, што у пракси значи чак и без присуства или чак и знања осигураника.

Такође, у ревизији сврсисходности пословања „Информациона безбедност у здравственим информационим системима“[11], утврђено је да се картону осигураника може приступити без електронске здравствене књижице, већ само употребом ЈМБГ осигураника.

4) синхронизација података са здравственим установама

ЗУ користе различите здравствене информационе системе, као што су „Heliant Health“, „NexTZU“, „ZipSoft“ и друге. То има за последицу да се подаци уносе и обрађују у појединачним информационим системима ЗУ и потом преносе у матичну евиденцију.

Базе података у информационим системима ЗУ садрже поред личних података осигураника, податке о болестима, терапијама, евиденцији лечења осигураника, издатим лековима и друго, што представља осетљиве личне податке и изискује примену одређених мера заштите.

2. Циљ ревизије

Циљ ревизије је да се оцени ефективност ИС МЕОП у РФЗО.

3. Ревизорска питања

За остварење циља ревизије формулисали смо главно питање и ревизорска питања. Имајући у виду значај који ИС МЕОП има у оквиру система обавезног социјалног осигурања, ДРИ се определила да главно питање ревизије буде:

Да ли се на адекватан начин управља ИС МЕОП Републичког фонда за здравствено осигурање?

[11] https://www.dri.rs/storage/upload/documents/revision/2021/2020-1-SV%20Informaciona%20bezbednost%20u%20zdravstvenim%20informacionim%20sistemima.pdf

Примењујући Методолошка правила и смернице за ревизију сврсисходности пословања извршили смо декомпозицију главног питања на три аспекта и три ревизорска питања. Одређивање најризичнијих аспеката главног ревизијског питања урађено је процењивањем ризика у складу са Методолошким правилама и смерницама за ИТ ревизију Државне ревизорске институције, која поставља квантитативне и квалитативне критеријуме, што је детаљније разрађено у Прилогу 1 - Методологија у поступку рада.

Да бисмо одговорили на главно питање, испитивали смо:

1. Да ли је успостављено ефективно ИТ управљање у РФЗО?
    1) Да ли је РФЗО усвојио и користи стратегију за ИТ или сличан стратешки документ као оквир за планирање циљева развоја информационог система?
    2) На који начин РФЗО предузима активности у циљу:
        - финансирања развоја и одржавања информационог система,
        - јачања и развоја кадровских капацитета,
        - управљања ИТ ризицима, кроз њихову идентификацију и спровођење плана за њихово умањење, а у складу са донетим плановима/ИТ стратегијом?
    3) На који начин се врши синхронизација података о осигураницима?
2. У којој мери успостављене мере безбедности података у ИС МЕОП обезбеђују поверљивост, заштиту и интегритет података (поузданост ИС)?
    1) Да ли РФЗО има јасна и ефикасна правила и процедуре за обезбеђивање поузданости ИС МЕОП (контроле физичког и логичког приступа и управљања лог фајловима и инцидентима)?
    2) Да ли је и на који начин у РФЗО успостављена организација ИТ безбедности и да ли су безбедносне улоге и одговорности дефинисане у вези са правилима и процедурама за безбедност информација?
    3) Да ли РФЗО прати и контролише приступ ИС МЕОП-у од стране здравствених установа и запослених у РФЗО-у?
3. У којој мери је уговорни однос са пружаоцем услуге одржавања ИС МЕОП обезбедио испуњење пословних циљева и неопходни ниво поузданости ИС?
    1) Да ли су дефинисана и да ли се примењују правила и процедуре које се односе на безбедност и заштиту података када су у питању уговори са пружаоцем услуге одржавања ИС МЕОП?
    2) Да ли постоји механизам којим се осигурава да је пружалац услуге одржавања ИС МЕОП предузео све неопходне мере за заштиту и безбедност података и да ли их спроводи?
    3) Да ли постоји механизам којим се осигурава континуитет пословања ИС МЕОП у случају отказа или непродужења уговора са пружаоцем услуге одржавања ИС МЕОП?

4. Обим и ограничења ревизије

Ревизијом смо обухватили три ИТ области у РФЗО за период од 1. јануара 2020. године до 31. децембра 2022. године.

Предмет испитивања је било:

1) ИТ управљање - подразумева ИТ операције у организацији како би се обезбедило да организација задовољава потребе пословања у садашњости и да укључује

планове за будуће потребе и развој. Основна улога ИТ управљања је да обезбеди: да ИТ систем одговара пословним потребама; да планира будуће промене на систему; да обезбеди неопходан ниво интерних контрола; да има одговарајућу организациону структуру и прецизно дефинисане описе послова запослених на ИТ пословима; и да примењује неопходне политике и процедуре који се односе на ИТ систем;[12]

2) Информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;[13]
3) Сарадња са пружаоцем услуге подразумева сарадњу са добављачем услуга развоја и одржавања информационих система. Главна питања су ИТ безбедност, заштита и поверљивост података, резервне копије података и ризик од непродужења/отказа уговора од стране пружаоца услуге.

У поступку ревизије нисмо испитивали:

- Да ли финансијски извештаји РФЗО истинито и објективно приказују њихово финансијско стање, резултате пословања и новчане токове, у складу са прихваћеним рачуноводственим начелима и стандардима;
- Финансијске трансакције и одлуке РФЗО у вези са примањима и приходима и расходима и издацима, ради утврђивања да ли су односне трансакције извршене у складу са законом, другим прописима и за планиране сврхе.

5. Методологија у поступку рада

Да бисмо остварили циљ ревизије и одговорили на ревизорска питања, анализирали смо законску и подзаконску регулативу, користили стручну литературу (WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions[14]), као и све податке добијене од РФЗО. Анализирали смо податке и информације за период од 2020. до 2022. године.

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

Приручником[15] је предвиђена оцена сложености информационог система и могућност избора области за испитивање (ревизију) и то: ИТ управљање; развој и набавка; ИТ операције; Сарадња са пружаоцима услуга; Планови континуитета пословања и опоравка од хаварије; Информациона безбедност и Апликативне контроле.

Проценили смо ревизијски ризик и одабрали области за ревизију: ИТ управљање, Информациона безбедност и Сарадња са пружаоцима услуга.

[12] WGITA – IDI Приручник за ИТ ревизију врховних ревизорских институција (енг. WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions).
[13] Члан 7 став 3 Закона о информационој безбедности.
[14] INTOSAI Радна група за ИТ ревизију.
[15] WGITA – IDI Приручник за ИТ ревизију врховних ревизорских институција (енг. WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions).

III Опис предмета ревизије

ИС МЕОП представља информациони систем за евиденцију осигураника РФЗО и евиденције остварених права у систему здравственог осигурања (обрачун и контролу боловања, рад лекарских комисија РФЗО, обрачун путних трошкова...).

1) Законодавни и институционални оквир

Законодавни оквир

Законом о здравственом осигурању уређују се права из обавезног здравственог осигурања и услови за њихово остваривање, финансирање обавезног здравственог осигурања, уговарање здравствене заштите, организација обавезног здравственог осигурања и друга питања од значаја за систем обавезног здравственог осигурања (члан 2).[16]

Обавезно здравствено осигурање је осигурање којим се осигураним лицима и другим лицима обезбеђује право на здравствену заштиту и право на новчане накнаде (члан 3 Закона о здравственом осигурању).

Право на здравствену заштиту обезбеђује се за случај настанка болести и повреде ван рада, као и у случају повреде на раду или професионалне болести (члан 51 Закона о здравственом осигурању).

Право на здравствену заштиту обухвата:

1) мере превенције и раног откривања болести;
2) прегледе и лечење у вези са планирањем породице, у току трудноће, порођаја и до 12 месеци након порођаја;
3) прегледе и лечење у случају болести и повреде;
4) прегледе и лечење болести уста и зуба;
5) медицинску рехабилитацију у случају болести и повреде;
6) лекове;
7) медицинска средства (члан 52 став 1 Закона о здравственом осигурању).

Право на новчане накнаде обухвата:

1) право на накнаду зараде, односно накнаду плате за време привремене спречености за рад осигураника;
2) право на накнаду трошкова превоза у вези са коришћењем здравствене заштите[17].

За спровођење обавезног здравственог осигурања најзначајнију улогу има ИС МЕОП - Матична евиденција и остваривање права. Матичну евиденцију јединствено за територију Републике Србије устројава и организује РФЗО.

Институционални оквир

Републички фонд за здравствено осигурање

Обавезно здравствено осигурање обезбеђује и спроводи у РФЗО, док добровољно здравствено осигурање могу да организују и спроводе правна лица која обављају делатност осигурања, као и РФЗО, у складу са Законом о здравственом осигурању и законом којим се уређује осигурање (члан 7 Закона о здравственом осигурању).

[16] „Службени гласник РС“, бр. 25/19.
[17] члан 71 Закона о здравственом осигурању.

Према одредбама члана 228 Закона о здравственом осигурању, обезбеђивање и спровођење обавезног здравственог осигурања обавља РФЗО, са седиштем у Београду. РФЗО врши јавна овлашћења у обезбеђивању и спровођењу обавезног здравственог осигурања, као и у решавању о правима из обавезног здравственог осигурања, у складу са тим законом.

Према одредбама члана 229 Закона о здравственом осигурању, РФЗО је правно лице са статусом организације за обавезно социјално осигурање у којем се обезбеђују средства за обавезно здравствено осигурање и остварују права из обавезног здравственог осигурања, у складу са законом. Права, обавезе и одговорност РФЗО утврђене су законом и статутом РФЗО.

Сходно Правилнику о организацији и систематизацији послова у РФЗО[18], организационе јединице РФЗО су:

1) Дирекција РФЗО;
2) Покрајински фонд;
3) филијале РФЗО.

Средства за остваривање права из обавезног здравственог осигурања обезбеђују се уплатом доприноса, као и из других извора, у складу са законом (члан 9 став 1 Закона о здравственом осигурању).

Средства РФЗО могу се користити само за намене одређене законом и то за:

1) остваривање права осигураних лица из обавезног здравственог осигурања;
2) унапређивање система здравственог осигурања;
3) остваривање права осигураних лица из добровољног здравственог осигурања које организује и спроводи РФЗО;
4) трошкове спровођења здравственог осигурања;
5) друге расходе, у складу са законом (члан 254 Закона о здравственом осигурању).

Матична евиденција

Према одредбама члана 31 став 1 Закона о здравственом осигурању, матичну евиденцију чине подаци о:

1) осигураницима;
2) члановима породице осигураника;
3) обвезницима плаћања доприноса;
4) коришћењу права из обавезног здравственог осигурања.

Сагласно члану 31 став 2 Закона о здравственом осигурању, матичну евиденцију јединствено за територију Републике Србије устројава и организује РФЗО.

Према одредбама члана 32 Закона о здравственом осигурању, у матичну евиденцију подаци се уносе преузимањем из ЦРОСО, преузимањем из службених евиденција, односно из других доказа достављених путем средстава за електронску обраду података или достављених непосредно филијали РФЗО.

Према одредбама члана 33 став 1 Закона о здравственом осигурању, подаци о коришћењу права из обавезног здравственог осигурања воде се одвојено од других података и тим подацима рукује за то овлашћено лице РФЗО, у складу са законом, док је ставом 2 истог закона прописано да се обрада података који чине матичну евиденцију,

[18] 12 бр. 110-5/20 од 31.01.2020. године.

њихово архивирање и мере заштите врши у складу са законом којим се уређује заштита података о личности.

Табела број 1. Преглед броја осигураника по филијалама РФЗО[19] закључно са 31.12.2022

Назив филијале	Број осигураника по филијалама
1	*2*
Филијала Суботица	164.849
Филијала Зрењанин	161.258
Филијала Кикинда	119.978
Филијала Панчево	261.881
Филијала Сомбор	164.974
Филијала Нови Сад	601.324
Филијала Сремска Митровица	277.073
Филијала Шабац	263.194
Филијала Ваљево	145.321
Филијала Смедерево	173.955
Филијала Пожаревац	147.751
Филијала Крагујевац	270.648
Филијала Јагодина	182.247
Филијала Бор	106.194
Филијала Зајечар	87.206
Филијала Ужице	257.168
Филијала Чачак	189.098
Филијала Краљево	149.824
Филијала Крушевац	199.524
Филијала Ниш	351.775
Филијала Прокупље	76.778
Филијала Пирот	76.907
Филијала Лесковац	186.726
Филијала Врање	196.167
Филијала Приштина	39.655
Филијала Косовска Митровица	45.114
Филијала Гњилане	19.846
Филијала Београд	1.664.517
Филијала Нови Пазар	133.737
Укупно	6.714.689

2) Информациони систем МЕОП

Дефиниција

ИС МЕОП представља информациони систем за евиденцију осигураника РФЗО и евиденције остварених права у систему здравственог осигурања (обрачун и контролу боловања, рад лекарских комисија РФЗО, обрачун путних трошкова...).

ИС МЕОП инсталиран је у 29 филијала и око 150 испостава РФЗО и има око 1.500 активних корисника. Кроз апликацију је евидентирано преко 8.000.000 осигураника који остварују или су остваривали своја права из обавезног здравственог осигурања. На месечном нивоу, у просеку се изврши око 500.000 пријава/промена/одјава осигураника, 800.000 овера здравствених исправа, обрачуна и евидентира 30.000 боловања и унесе око

[19] подаци достављени од РФЗО.

120.000 одлука лекарских комисија. У оквиру осталих остваривања права, изда се или евидентира око 150.000 докумената и налаза месечно[20].

ИС МЕОП се састоји из следећих подсистема[21]:

1. МЕ - Матична евиденција осигураника,
2. ЗИ - Здравствене исправе,
3. ОП - остваривање права,
4. Електронска размена података са интерним системима РФЗО,
5. Електронска размена података са спољним институцијама.

Матична евиденција осигураника

Основни подсистем је матична евиденција осигураника, односно евидентирање полисе осигурања и свих измена над полисом. Да би се нека полиса евидентирала или изменила потребно је да се спроведе низ формалних и логичких контрола укључујући и успешно слање на ЦРОСО. Такође, иницијатор настанка или измене полисе може да буде и нека друга институција о чему РФЗО добија податке од ЦРОСО. Подаци који се евидентирају су дефинисани МА обрасцем. Осим података са МА обрасца, додатно се евидентирају и подаци од интереса за РФЗО као што су приоритет полисе, емаил, напомена итд.

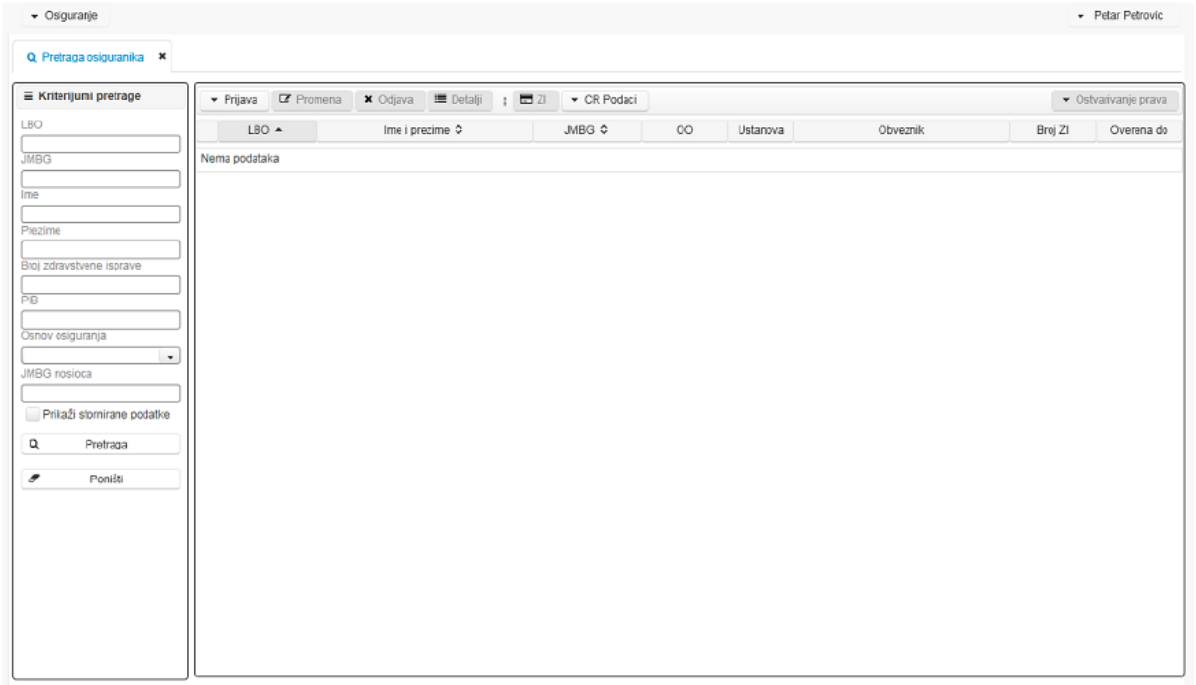
Подаци о обвезницима се воде кроз део апликације за рад са обвезницима. Обвезници правна лица се преузимају са ЦРОСО, док се физичка лица уносе кроз цМЕОП. У рад са обвезницима, имплементирана је контрола „Провера уплате доприноса“ која омогућава проверу задужења обвезника на основу података ПУ и/или ЦРОСО[22].

[20] Подаци преузети из документа „Опис и спецификација предмета, услови испоруке или извршења“ Партија 1 – Матична евиденција и остваривање права (цМЕОП), јавна набавка број 404-1-208/22-116, покренута у 2022. години под називом „Услуга одржавања дела софтверских система РФЗО“, страна 10 од 16.

[21] подаци преузети из документа „Опис и спецификација предмета, услови испоруке или извршења“, Партија 1 – Матична евиденција и остваривање права (цМЕОП), јавна набавка број 404-1-208/22-116, покренута у 2022. години под називом „Услуга одржавања дела софтверских система РФЗО“, страна 8 од 16.

[22] подаци преузети из документа „Опис и спецификација предмета, услови испоруке или извршења“, Партија 1 – Матична евиденција и остваривање права (цМЕОП), јавна набавка број 404-1-208/22-116, покренута у 2022. години под називом „Услуга одржавања дела софтверских система РФЗО“, страна 8 од 16.

Слика број 1: Основни изглед прозора ИС МЕОП за претрагу осигураника



ЗИ – здравствене исправе

Битан део ИС МЕОП је вођење евиденције о здравственим исправама и њиховим оверама. Ово подразумева рад са КЗО (подношење захтева, уручивање, овере, синхронизацију са ЦАМС[23]) као и издавање више типова ПЗК образаца.

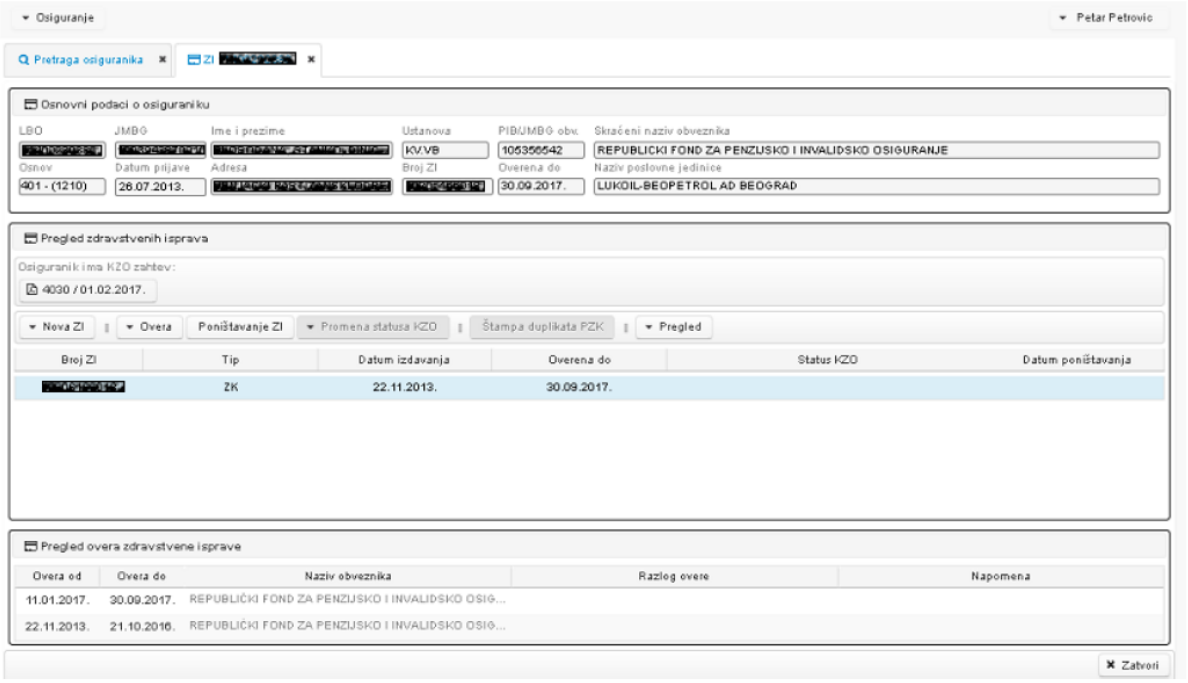
Модул за рад са КЗО омогућава креирање и слање захтева за КЗО, уручивање, овере, промене статуса, синхронизацију података са ЦАМС-ом.

Модул за аутоматску оверу КЗО врши свакодневно оверавање картица осигураника у складу са пословним правилима РФЗО као и подацима о плаћеним доприносима из система ПУ и/или ЦРОСО.

Модул за администрацију КЗО је десктоп апликација коју користе шалтерски радници за читање података са картице, упис на картицу података са ЦАМС-а као и рад са корисничким кључевима и сертификатима на картици.

[23] Card management system – софтвер за управљање здравственим књижицама.

Слика број 2: Основни изглед прозора ИС МЕОП за преглед здравствене исправе осигураника24



Остваривање права

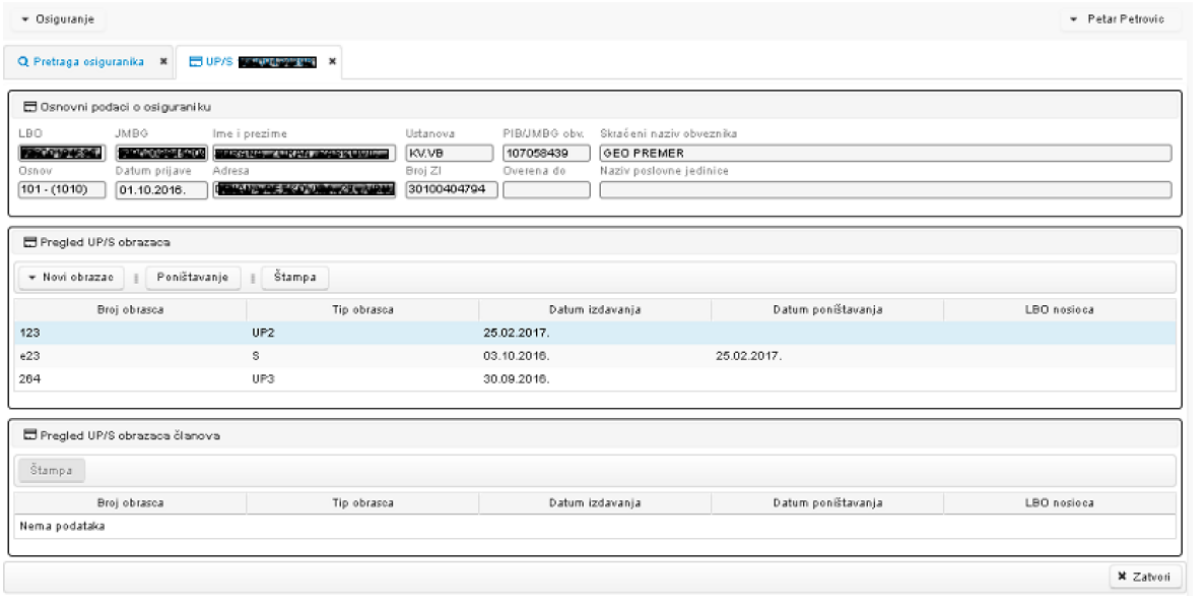
Остваривање права обухвата права који проистичу из осигурања. Обухвата:

- оверу медицинско техничких помагала,
- евиденцију и обрачун боловања, вођење спискова боловања као и евидентирање налаза инвалидских комисија,
- евиденцију лечења осигураника у здравственим установама,
- евиденцију путних трошкова,
- издавање и евиденцију ИНО образаца,
- подршку раду лекарских комисија и креирање налаза лекарских комисија,
- издавање и евиденцију УП/С[25] образаца,
- издавање и евиденцију ПЖД образаца,
- издавање и евиденцију ДТП образаца.

[24] лични подаци осигураника су засенчени.

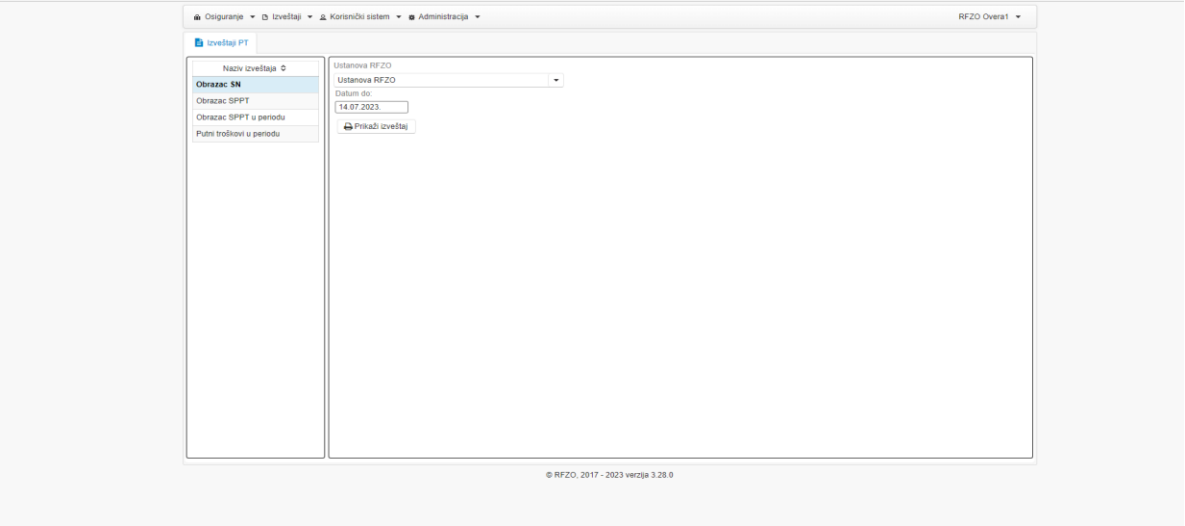
[25] скраћеница за групу образаца. УП је скраћеница за обрасце „коришћење здравствене заштите у пуном износу на терет средстава обавезног здравственог осигурања“. С је скраћеница од Стоматологија и односи се на „потврда за прегледе и лечење болести уста и зуба“.

Слика број 3: Основни изглед прозора ИС МЕОП за преглед УП/С образаца[26]



Апликација цМЕОП такође садржи модул за креирање извештаја. Постоји преко 50 извештаја који су разврстани по категоријама.

Слика број 4: Основни изглед прозора за преглед извештаја



Електронска размена података са интерним системима

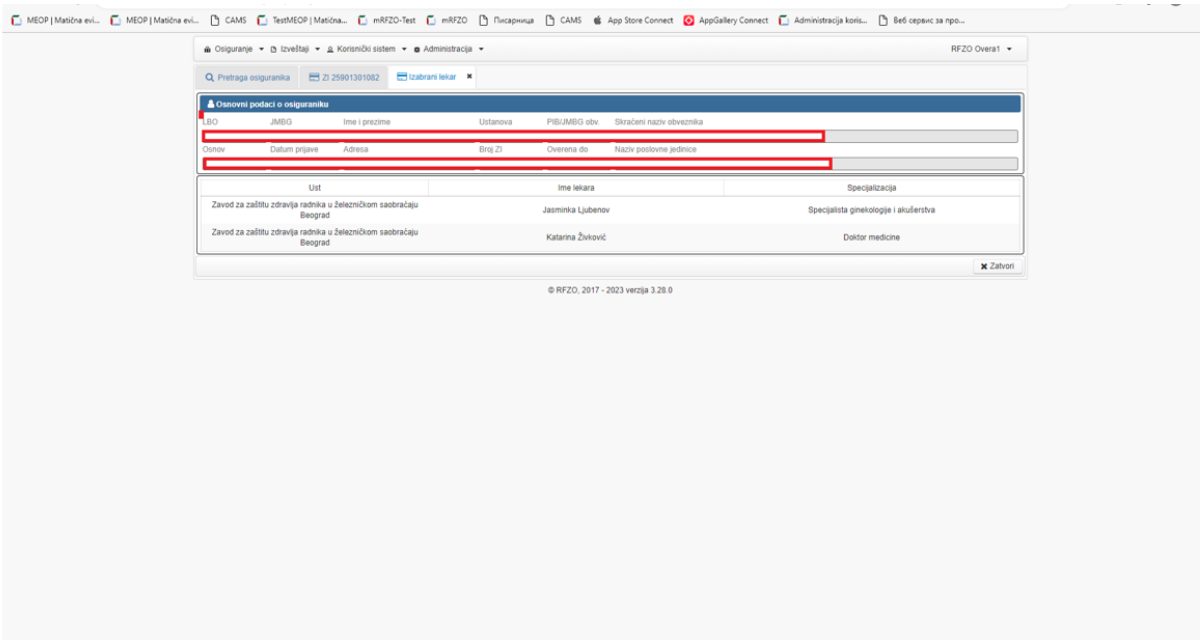
За потребе различитих пословних процеса РФЗО-а, цМЕОП размењује податке са више различитих интерних подсистема и апликација.

Размену података можемо груписати у следеће подсистеме:

Подсистем за размену података са РИЛ системом (Регистар изабраних лекара) – у оквиру цМЕОП апликације могуће је извршити проверу да ли осигураник има изабраног лекара док РИЛ користи податке о осигурању у процесу контроле регистрације изабраног лекара осигураника.

[26] лични подаци осигураника су засенчени.

Слика број 5: Основни изглед прозора ИС МЕОП за размену података са РИЛ системом



Извоз поништених књижица – из ИС МЕОП се једном недељно извозе подаци о поништеним књижицама у XML формату за потребе објављивања на порталу РФЗО и учитавања у системе електронских фактура[27].

Читање података о осигураницима из система Писарнице.

Провера уплате доприноса – подсистем за проверу уплате доприноса обвезника у односу на податке добијене из ПУ и вођење евиденције измирених доприноса за период пре 2013. године као и податке о доприносима самосталаца.

Подсистем за извоз података о обрачунатим боловањима намењен интерном финансијско-рачуноводственом систему РФЗО као и порталу РФЗО.

Читање података о осигураницима из апликације за добровољно здравствено осигурање[28].

Електронска размена података са спољним институцијама

РФЗО комуницира са неколико система у циљу електронске размене података као што су ЦРОСО, еУправа и различите ЗУ.

Размену података можемо груписати у следеће подсистеме:

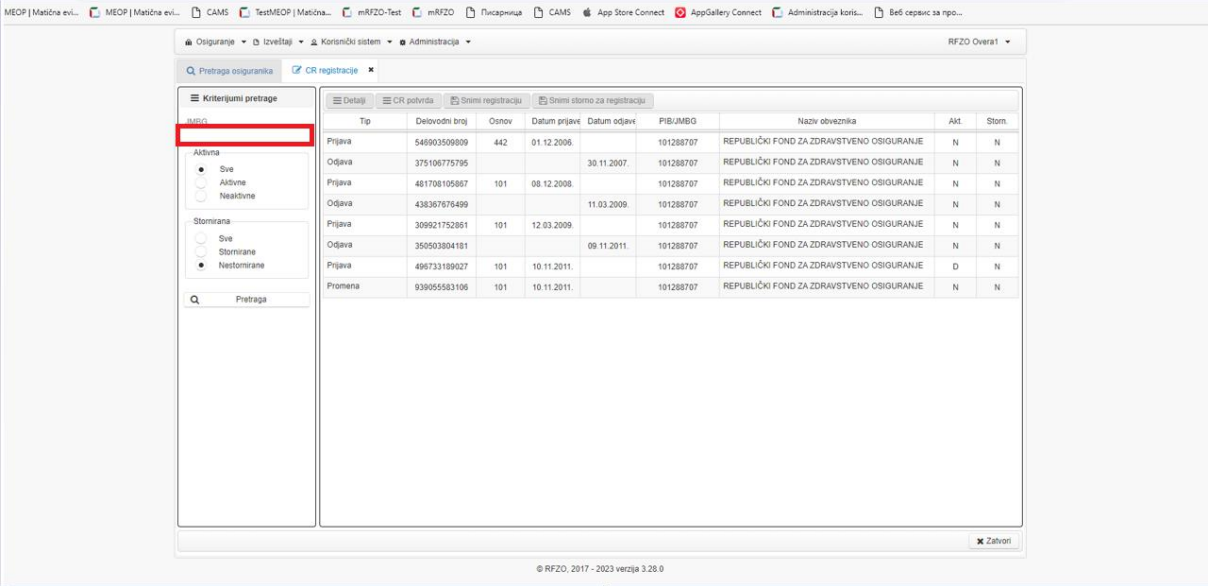
Подсистем за интеграцију са системом ЦРОСО - овај систем обезбеђује размену пријава између РФЗО и ЦРОСО. Систем обухвата и преузимање података о обвезницима из

[27] подаци преузети из документа „Опис и спецификација предмета, услови испоруке или извршења“, Партија 1 – Матична евиденција и остваривање права (цМЕОП), јавна набавка број 404-1-208/22-116, покренута у 2022. години под називом „Услуга одржавања дела софтверских система РФЗО“, страна 9 од 16.

[28] подаци преузети из документа „Опис и спецификација предмета, услови испоруке или извршења“, Партија 1 – Матична евиденција и остваривање права (цМЕОП), јавна набавка број 404-1-208/22-116, покренута у 2022. години под називом „Услуга одржавања дела софтверских система РФЗО“, страна 9 од 16.

система ЦРОСО-а у систем РФЗО, као и података о уплаћеним доприносима. ЦРОСО од РФЗО преузима податке о овереним здравственим исправама.

Слика број 6: Основни изглед прозора ИС МЕОП за интеграцију са системом ЦРОСО



Подсистем за интеграцију са системом еУправа – преузимање личних података за новорођену децу при креирању КЗО захтева као и слање података о осигураницима за потребе подношења захтева за КЗО кроз систем еУправе.

Подсистем за добијање података са КЗО – подсистем се састоји од десктоп апликације КЗО Читач, јавног веб сервиса и интерне базе података са подацима о КЗО картицама. КЗО Читач чита податке са картице убачене у читач на локалном рачунару или веб сервиса који пружа информације о последњим подацима са КЗО.

Веб сервис за проверу података о осигураницима - здравствене установе (домови здравља, болнице, апотеке, ИЗИС[29], еРецепт итд.) имају потписан уговор о коришћењу података из система цМЕОП, у циљу провере статуса осигураника и исправности његове здравствене исправе[30].

Величина система

Апликација цМЕОП је централна апликација која се користи у 29 филијала и око 150 испостава РФЗО и има око 1.500 активних корисника. Кроз апликацију је евидентирано преко 8.000.000 осигураника који остварују или су остваривали своја права из обавезног здравственог осигурања.

На месечном нивоу, у просеку се изврши око 500.000 пријава/промена/одјава осигураника, 800.000 овера здравствених исправа, обрачуна и евидентира 30.000

[29] Интегрисани здравствени информациони систем.

[30] подаци преузети из документа „Опис и спецификација предмета, услови испоруке или извршења“, Партија 1 – Матична евиденција и остваривање права (цМЕОП), јавна набавка број 404-1-208/22-116, покренута у 2022. години под називом „Услуга одржавања дела софтверских система РФЗО“, страна 10 од 16.

боловања и унесе око 120.000 одлука лекарских комисија. У оквиру осталих остваривања права, изда се или евидентира око 150.000 докумената и налаза месечно.[31]

Величина подсистема за електронску размену података са спољним институцијама.

Из ИС МЕОП РФЗО, дневно се у просеку пошаље око 5.000 регистрација према ЦРОСО. Са друге стране, РФЗО систем прихвата више од 20.000 пријава од стране ЦРОСО.

ЦРОСО просечно дневно дохвати податке за око 50.000 оверених здравствених исправа.

На дневном нивоу од стране здравствених установа, упути се око 400.000 позива ка веб сервису за проверу података о осигураницима[32].

Техничке карактеристике система

Технологија коришћена за развој цМЕОП апликације је Java SE 8, JAVA EE 8, Wildfly 13 и Microsoft Server SQL 2016. Преглед технологија по подсистемима:

- презентациони слој - MVC архтектура базирана на JSF и PrimeFaces библиотеци компонената,
- слој пословне логике – EJB, JPA, Eclipselink
- подсистем извештавања – JasperReports,
- цМЕОП подсистем ка делу спољних системима - SOAP веб сервиси у оквиру апликације и WSO2 ентерприсе сервис бус (WSO2ESB 4.9.0) који комуницира директно са спољним корисницима кроз SOAP веб сервисе.

Поред ових технологија коришћене су и друге технологије за развој појединачних, одвојених модула. Подсистем за размену података са ЗУ и еУправом је базиран ја на SOAP веб сервисима и имплементиран је са Java 6, Tomcat 6 и MS SQL Server 2012. Размена се одвија коришћењем HTTPS протокола. Подсистем за администрацију КЗО је базиран на Sybase Powerbuilder 10.5 и MS Server 2008[33].

3) Исправа о осигурању

Према одредбама члана 25 став 1 Закона о здравственом осигурању, лицу коме је утврђено својство осигураног лица матична филијала издаје, односно активира исправу о осигурању. Исправа о осигурању је КЗО и потврда о здравственом осигурању (члан 25 став 2 Закона о здравственом осигурању). КЗО садржи:

1. видљиве податке: име, презиме, датум рођења, лични број осигураног лица (у даљем тексту: ЛБО), број здравствене картице и серијски број ЧИП-а (према одредбама члана 26 ст. 1 и 2 Закона о здравственом осигурању) и
2. податке које садржи контактни микроконтролер (у даљем тексту: ЧИП). ЧИП садржи следеће идентификационе податке о осигуранику: име, име једног родитеља, презиме, адреса (улица и број, место и општина), јединствени матични

[31] Подаци преузети из документа „Опис и спецификација предмета, услови испоруке или извршења“ Партија 1 – Матична евиденција и остваривање права (цМЕОП), јавна набавка број 404-1-208/22-116, покренута у 2022. години под називом „Услуга одржавања дела софтверских система РФЗО“, страна 10 од 16.

[32] подаци преузети из документа „Опис и спецификација предмета, услови испоруке или извршења“, Партија 1 – Матична евиденција и остваривање права (цМЕОП), јавна набавка број 404-1-208/22-116, покренута у 2022. години под називом „Услуга одржавања дела софтверских система РФЗО“, страна 10 од 16.

[33] подаци преузети из документа „Опис и спецификација предмета, услови испоруке или извршења“, Партија 1 – Матична евиденција и остваривање права (цМЕОП), јавна набавка број 404-1-208/22-116, покренута у 2022. години под називом „Услуга одржавања дела софтверских система РФЗО“, страна 10 од 16.

број грађана (у даљем тексту: ЈМБГ), односно евиденциони број за стране држављане, датум рођења, ЛБО, пол, основ осигурања, податке о обвезнику плаћања доприноса (члан 26 став 4 Закона о здравственом осигурању). ЧИП садржи следеће податке о члану породице осигураника: име, име једног родитеља, презиме, адреса (улица и број, место и општина), ЈМБГ, односно евиденциони број за стране држављане, датум рођења, ЛБО, пол, идентификационе податке о осигуранику, основ осигурања (према одредбама члана 26 ст. 4 и 5 Закона о здравственом осигурању). Подаци које садржи ЧИП користе се само у случају да давалац здравствене услуге нема техничке могућности да приступи подацима из матичне евиденције (према одредбама члана 26 став 6 Закона о здравственом осигурању).

РФЗО општим актом уређује садржај и облик исправе о осигурању, начин овере, категорије осигураних лица за коју преузима обавезу трошкова издавања картице здравственог осигурања, као и друга питања од значаја за коришћење исправе (према одредбама члана 26 став 7 Закона о здравственом осигурању).

Права из обавезног здравственог осигурања остварују се на основу оверене исправе о осигурању. Оверу исправе о осигурању врши матична филијала на основу доказа да је уплаћен доспели допринос, као и на основу других доказа, у складу са законом. Ако исправа о осигурању није оверена због тога што доспели допринос није плаћен, извршиће се накнадна овера када тај допринос буде уплаћен (према одредбама члана 125 ст. 1, 2 и 3 Закона о здравственом осигурању).

IV Закључци

У овом поглављу износимо закључке до којих смо дошли спроводећи ревизију сврсисходности на тему „Ефективност информационог система Матична евиденција и остваривање права (МЕОП) у Републичком фонду за здравствено осигурање", код субјекта ревизије РФЗО.

Донети закључци представљају одговоре на постављена ревизијска питања, дефинисана у делу извештаја II Увод – 3. Ревизорска питања. Закључци су донети на основу утврђених налаза – сваки закључак је изведен на основу припадајућих налаза.

У наставку извештаја наводимо закључке са одговарајућим налазима.

ЗАКЉУЧАК 1: РФЗО није у потпуности успоставио ефективно ИТ управљање због недостатка кадровских капацитета, непрепознавања могућих ИТ ризика и управљања подацима из матичне евиденције осигураника.

Циљ овог дела извештаја је да одговоримо на прво ревизијско питање, односно да ли је успостављено ефективно ИТ управљање у РФЗО. Ради постизања да ИТ управљање буде ефективно, потребно је да организација има одговарајуће кадрове, врши препознавање ИТ ризика и планира и спроводи мере за њихово ублажавање ради заштите ИТ система. Поред кадрова и ИТ ризика, за нашу ревизију је значајна и синхронизација и заштита података о осигураницима путем КЗО.

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

Налаз 1.1: РФЗО није донео ИТ стратегију за период 2022–2024. године.

Стратегија се по правилу усваја за период од пет до седам година, а остваривање њених циљева планира се и прати посредством акционог плана за спровођење стратегије.

РФЗО није израдио ИТ стратегију за период 2022-2024. године и пратећи акциони план ради спровођења мера из ИТ стратегије. РФЗО је усвојио ИТ стратегију за период 2019-2021. године.

РФЗО наводи да због пандемије вируса COVID 19 и додатних послова и задатака није усвојио нову стратегију, за период 2022-2024. године.

Влада доноси Стратегију развоја здравствене заштите ради обезбеђивања и спровођења друштвене бриге за здравље на нивоу Републике Србије. Влада доноси програме здравствене заштите ради спровођења Стратегија развоја здравствене заштите (чл. 18 и 19 Закона о здравственој заштити). Друштвена брига за здравље на нивоу Републике Србије обухвата и обезбеђивање услова за развој ИЗИС. ИС МЕОП је саставни део ИЗИС-а. Влада није донела Стратегију развоја здравствене заштите.

Користи од усвајања ИТ стратегије и акционог плана јесу олакшано планирање развоја ИТ, сврсисходно коришћење расположивих финансијских средстава и унапређено ИТ управљање и тиме остваривање пословних циљева РФЗО.

Законом о планском систему Републике Србије[34] уређује се плански систем Републике Србије, односно управљање системом јавних политика и средњорочно планирање, врсте и садржина планских докумената које у складу са својим надлежностима предлажу, усвајају и спроводе сви учесници у планском систему, међусобна усклађеност планских докумената, поступак утврђивања и спровођења јавних политика и обавеза извештавања о спровођењу планских докумената, као и сходна примена обавезе спровођења анализе ефеката на прописе и на вредновање учинака тих прописа.

Према одредбама члана 10 став 1 Закона о планском систему Републике Србије прописано је да је документ јавних политика плански документ којим учесници у планском систему, у складу са својим надлежностима, утврђују или разрађују већ утврђене јавне политике, док је ставом 2 истог члана прописано да су врсте докумената јавних политика: 1) стратегија; 2) програм; 3) концепт политике и 4) акциони план.

[34] „Службени гласник РС“, бр. 30/18.

Стратегија је основни документ јавне политике, којим се на целовит начин утврђују стратешки правац деловања и јавне политике у конкретној области планирања и спровођења јавних политика утврђених прописом Владе. Стратегија по правилу усваја за период од пет до седам година, а остваривање њених циљева планира се и прати посредством акционог плана за спровођење стратегије[35].Стратегија по правилу има један општи циљ и до пет посебних циљева који доприносе остварењу тог општег циља. Општи и посебни циљеви морају бити јасно одређени, мерљиви, прихватљиви, реални и временски одређени.

Акциони план јесте документ јавне политике највишег нивоа детаљности, којим се разрађују стратегија, у циљу управљања динамиком спровођења мера јавних политика које доприносе остваривању посебних циљева стратегије, односно програма. Акциони план је саставни део стратегије и по правилу се усваја истовремено са тим документима јавних политика. Акциони план, по правилу, усваја за период примене стратегије, односно програма који разрађује.[36]

РФЗО је у 2019. години спровео јавну набавку „Услуге дефинисања ИКТ стратегије и софтверске архитектуре ИКТ система РФЗО“[37]. Позив за подношење понуда објављен је 4. октобра 2019. године, а уговор о јавној набавци додељен и закључен са привредним друштвом „Egzakta“ доо[38]. Добављач је израдио, а РФЗО усвојио ИКТ стратегију РФЗО под називом „Дефинисање ИКТ стратегије и софтверске архитектуре ИКТ система РФЗО“[39]. ИКТ стратегија РФЗО се односи на период 2019-2021. године.

ИКТ стратегије РФЗО се састоји из два дела, и то:

Први део: Дефинисање софтверске архитектуре ИКТ система РФЗО. Резултат ове фазе је дефинисана софтверска архитектура РФЗО.

Други део: Дефинисање ИКТ стратегије РФЗО, која садржи три основна корака: анализу постојећег Система ИКТ и усклађеност са стратегијом РФЗО, дефинисање стратешких планова ИКТ, дефинисање Акционих планова за имплементацију[40].

Анализирајући информационе системе РФЗО-а креатор стратегије „Егзакта“ доо је утврдио да апликативни портфолио РФЗО показује добре и лоше стране у појединим областима. ИКТ систем РФЗО упоређен је са стандардима за апликативни портфолио кроз 17 димензија и то је била основа за дефинисање смерница за унапређење[41].

РФЗО у току поступка ревизије није доставио/донео акциони план за спровођење ИКТ стратегије РФЗО. РФЗО није усвојио ИКТ стратегију за период 2022-2024. године, нити акциони план за претходну ИКТ стратегију (за период 2019-2021. година) и као објашњење навео да због пандемије вируса COVID 19 и додатних задужења нису били у могућности да донесу ИКТ стратегију (и припадајући акциони план за спровођење стратегије) за период од 2022-2024. године, већ су поступали по претходно донетој стратегији.

[35] Чланови 11 и 13 Закона о планском систему Републике Србије.
[36] Члан 18 Закона о планском систему.
[37] редни број јавне набавке у 2019. години: 404-22-208/19-27.
[38] као представнику понуђача у заједничкој понуди: „Egzakta“ доо и „Standardi i rešenja“ доо. Уговор је закључен 18. октобра 2019. године.
[39] Одлуком в.д. директора РФЗО 01 број 404-2-27/19-16 од 18. новембра 2019. године.
[40] преузето из конкурсне документације за јавну набавку „Услуга дефинисања ИКТ стратегије и софтверске архитектуре ИКТ система РФЗО“, стр. 6-7
[41] „Дефинисање ИКТ стратегије и софтверске архитектуре ИКТ система РФЗО“.

Користи од усвајања ИТ стратегије и акционог плана су фокус на план развоја ИТ, коришћење расположивих финансијских средстава и унапређено ИТ управљање.

Препоручујемо Републичком фонду за здравствено осигурање да донесе стратешки документ (ИТ стратегију) и акциони план, којим би се планирао развој и управљање информационим системима, рачунарским апликацијама, базама података и континуираном обуком запослених.

Налаз 1.2: ИТ управљање није успостављено на адекватан начин због непрепознавања свих ИТ ризика и недовољних кадровских капацитета.

ИТ управљање представља целокупни оквир који води ИТ операције у организацији како би се обезбедило да организација задовољава потребе пословања данас и да укључује планове за будуће потребе и раст. ИТ управљање је интегрални део управљања организацијом и обухвата организационо вођење, институционалне структуре и процесе и друге механизме (извештавање и повратне информације, спровођење, ресурсе итд.) који обезбеђују да ИТ системи подржавају организационе циљеве и стратегију, док балансирају ризике и ефективно управљају ресурсима. ИТ управљање има кључну улогу у одређивању контролног окружења и поставља темеље за успостављање најбољих пракси интерне контроле и извештавања.[42]

Корисници јавних средстава успостављају финансијско управљање и контролу у складу са одредбама Закона о буџетском систему. Према одредбама Закона о информационој безбедности (члан 3 став 1 тачка 1), приликом планирања и примене мера заштите ИКТ система треба се руководити начелом управљања ризиком. Управљање ризицима обухвата идентификовање, процену и контролу над потенцијалним догађајима и ситуацијама које могу утицати на остварење циљева корисника јавних средстава, обезбеђујући разумно уверавање да ће ти циљеви бити остварени (члан 7 став 1 Правилника о заједничким критеријумима и стандардима за успостављање, функционисање и извештавање о систему ФУК у јавном сектору). Оператор ИКТ система утврђује, у оквиру организационе структуре, послове и одговорности запослених за управљање ризицима у области информационе безбедности (члан 2 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја).

РФЗО није идентификовао све ИТ ризике, а последично ни планове и мере за умањење ризика. РФЗО је усвојио Стратегију управљања ризицима, а за период ревизије 2020-2022. године утврдио три ИТ ризика која се понављају сваке године.

У Сектору за развој и ИТ у Дирекцији РФЗО у Београду на 34 систематизована радна места, запослено је 15 лица. У 29 филијала РФЗО, попуњеност радних места на ИТ пословима је 63%.

РФЗО није препознао све ИТ ризике због мањка ИТ кадрова и неучествовања запослених на ИТ пословима у филијалама РФЗО у идентификовању ИТ ризика при изради Стратегије управљања ризицима.

Значајно ограничење у развоју ИКТ система је и недовољан број запослених у Сектору за развој и ИТ и смањена могућност запошљавања нових кадрова, што последично утиче и на спровођење мера за умањење ИТ ризика.

[42] IDI WGITA – IDI Приручник за ИТ ревизију врховних ревизорских институција (енг. WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions.

Последице непрепознавања ИТ ризика могу бити непотребно велики трошкови у случају настанка нежељеног догађаја (који се могао спречити) или велики нефинансијски губици (у првом реду података) због немогућности благовременог предузимања мера.

Финансирање развоја и одржавања информационог система МЕОП

ИС МЕОП је кључна апликација за пословање РФЗО. Ради се о информационом систему који је у изворном облику (коду) развио Електротехнички факултет из Београда (у даљем тексту: ЕТФ).

ИС МЕОП постоји од 2006. године као дистрибуирана десктоп апликација, инсталирана у свим испоставама, филијалама и Дирекцији РФЗО[43]. У периоду до краја 2015. године ЕТФ је вршио одржавање и унапређење ИС МЕОП као једини понуђач. У периоду од 2016. до 2022. године ЕТФ је био члан групе привредних субјеката која је одржавала ИС МЕОП. Од 2022. године, ЕТФ није више члан групе привредних субјеката са којима се закључује поменути уговор, што је приказано у табели која следи.

Табела број 2. Преглед јавних набавки одржавања ИС МЕОП у периоду 2020-2023. године

Година	Назив набавке	Референтни број набавке	CPV ознака	Добављач коме је додељен уговор	Уговорена вредност[44]	Уговор закључен на период
1	*2*	*3*	*4*	*6*	*7*	*8*
2020.	Услуга одржавања дела софтверских система РФЗО	404-1208/19-76	72260000 - Услуге повезане са софтвером	Soneco d.o.o, као представника понуђача у заједничкој понуди: 1. Soneco d.o.o. 2. Електротехнички факултет Универзитета у Београду 3. Heliant d.o.o"	23.424.480	12 месеци
2021.	Услуга одржавања дела софтверских система	404-1-208/20-97	72267000 - Услуге одржавања и поправке софтвера	Soneco доо Београд, као носилац групе привредних субјеката: 1. Soneco d.o.o, ул. Макензијева бр. 24, Београд 2. Heliant d.o.o, ул. Макензијева бр. 24, Београд 3. Електротехнички факултет Универзитета у Београду, Булевар краља Александра бр. 73, Београд	23.424.480	12 месеци
2022.	Услуга одржавања софтверских система РФЗО	404-1-208/21-101	72267000 - Услуге одржавања и поправке софтвера	Soneco доо Београд, као носилац групе привредних субјеката: 1. Soneco d.o.o, ул. Макензијева бр. 24, Београд 2. Heliant d.o.o, ул. Макензијева бр. 24, Београд	23.424.480	12 месеци

[43] Пројектни задатак цМЕОП- унапређење постојећег система за матичну евиденцију и остваривања права (новембар 2014. године).

[44] податак се односи на вредност уговора са ПДВ-ом за Партију 1 - Матична евиденција и остваривање права. Износ исказан у динарима.

Година	Назив набавке	Референтни број набавке	CPV ознака	Добављач коме је додељен уговор	Уговорена вредност[44]	Уговор закључен на период
1	*2*	*3*	*4*	*6*	*7*	*8*
2023.	Услуга одржавања дела софтверских система РФЗО	404-1-208/22-116	72267000 - Услуге одржавања и поправке софтвера	Soneco доо Београд, као носилац групе привредних субјеката: 1. Soneco d.o.o, ул. Макензијева бр. 24, Београд 2. Heliant d.o.o, ул. Макензијева бр. 24, Београд	28.376.640	12 месеци

У оквиру техничке спецификације из конкурсне документације јавне набавке „Услуга одржавања дела софтверских система РФЗО“ у 2020. години, за партију 1 – М1 Матична евиденција и остваривање права, предмет уговора је набавка услуге одржавања ИС МЕОП , која подразумева да пружалац услуге:

„Да одржава предметне софтверске системе у функционално исправном стању;

Да врши корективно одржавање софтверских система које подразумева:

унапређење софтверског производа у циљу исправљања откривених већих и мањих нерегуларности у раду, скривених мана и грешака,

унапређење софтверског решења у циљу ефикаснијег рада и коришћења, као резултат властитих идеја и концепата Извршиоца;

да у року не дужем од једног радног дана од пријема захтева, отклони проблем који доводи до потпуног застоја у раду или до губитка кључних функционалности неопходних за вршење обавезних дневних активности, и да у року не дужем од 3 радна дана отклони остале проблеме у раду;

Да врши превентивно одржавање, које подразумева:

модификацију софтверских система у циљу откривања и отклањања потенцијалних проблема пре него што они доведу до нерегуларности у раду;

Да врши адаптивно одржавање, које подразумева:

промену или допуну функционалности софтверског система, као последицу промене окружења (хардверског окружења, системског софтвера, мрежног окружења) у року не дужем од 10 радних дана;

адаптацију софтверског система због промене законске и друге регулативе које утичу на софтверске системе, у року који је у складу са законски дефинисаним терминима спровођења;

адаптацију софтверског система у смислу промене или допуне функционалности софтверског система, на захтев наручиоца.

Да, уколико је неопходно, према процени дирекције РФЗО изврши обуку корисника за коришћење нових измењених делова програмских модула;

Да овлашћеним представницима корисника пружи сву потребну подршку у коришћењу софтверских система, телефоном, електронском поштом, у својим просторијама или на локацији корисника. Одржавање удаљеним приступом дозвољено је само уз експлицитну дозволу Сектора за развој и информационе технологије у складу са безбедносном политиком рачунарске мреже РФЗО;

Да према инструкцијама Дирекције и у формату који дефинише дирекција РФЗО у софтверским системима обезбеди интерфејс за аутоматско преузимање података из других информационих подсистема РФЗО;

Да пруже остале стручне информатичке подршке приликом решавања поремећаја у раду предметних система који настану услед проблема са хардвером, системским софтвером, базом података, или приликом коришћења самих софтверских система.“[45]

У оквиру техничке спецификације из конкурсне документације јавне набавке „Услуга одржавања дела софтверских система РФЗО“ у 2022. години, за партију 1 – М1 Матична евиденција и остваривање права, поред услуга наведених у тексту изнад, додата је и следећа алинеја:

„Да на месечном нивоу доставе последње верзије изворних кодова свих софтверских система који су предмет одржавања, односно превентивног, адаптивног и корективног унапређења.“[46]

Поред развоја и одржавања ИС МЕОП за РФЗО је такође битна и број и старост рачунара који су у употреби, оперативни систем и антивирус програми. У поступку ревизије РФЗО нам је доставио преглед рачунара (број и старост), оперативни систем и антивирус програм који се користи на тим рачунарима. Одговоре приказујемо у следећој табели.

Закључак је да РФЗО у филијалама и испоставама филијала користи рачунаре који су старији од 5 година, што представља пробијање предвиђеног рока употребе рачунара и сигнал за замену рачунарима новије генерације.

Табела број 3. Преглед броја, старости рачунара, оперативног система и антивирус програма у РФЗО на дан 31.12.2022. године

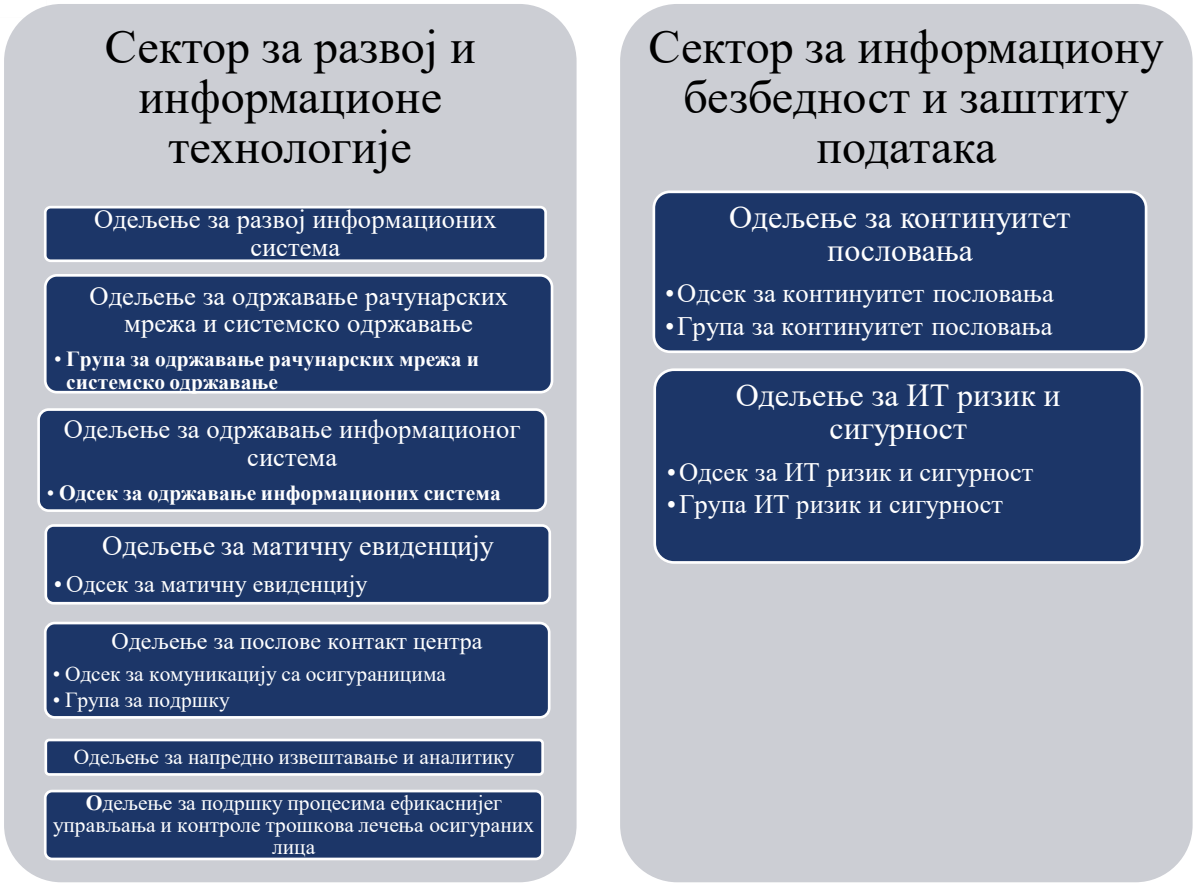
РБ	Питање	Дирекција	Покрајински фонд	Филијале	Испоставе
1	Број активних рачунара (који се користе за ИС МЕОП)	41	4	877	630
2	Година набавке рачунара	2017-2021	2018-2019	2013-2021	2013-2021
3	Оперативни систем који се користи	Windows 10	Windows 10	Windows 10 и 11	Windows 10
4	Антивирус програм који се користи	Kaspersky			

Кадровски капацитети Сектора за развој и информационе технологије

Увидом у Правилник о организацији и систематизацији послова у Републичком фонду за здравствено осигурање[47], утврђено је да се информационим системима у Дирекцији РФЗО управља тако што се у оквиру унутрашњих организационих јединица: „Сектор за развој и информационе технологије“ и „Сектор за информациону безбедност и заштиту података“, образују одељења, одсеци и групе.

[45] страна 9-10/65 конкурсне документације за јавну набавку „Услуга одржавања дела софтверских система РФЗО“, јавна набавка број: 404-1-208/19-76.
[46] страна 8/16 конкурсне документације за јавну набавку „Услуга одржавања дела софтверских система РФЗО“, јавна набавка број: 404-1-208/21-101.
[47] 12 бр. 110-5/20 од 31.01.2020. године.

Слика број 7: Приказ организационе структуре Дирекције РФЗО (сектори који су одговорни за ИТ управљање, безбедност и развој)

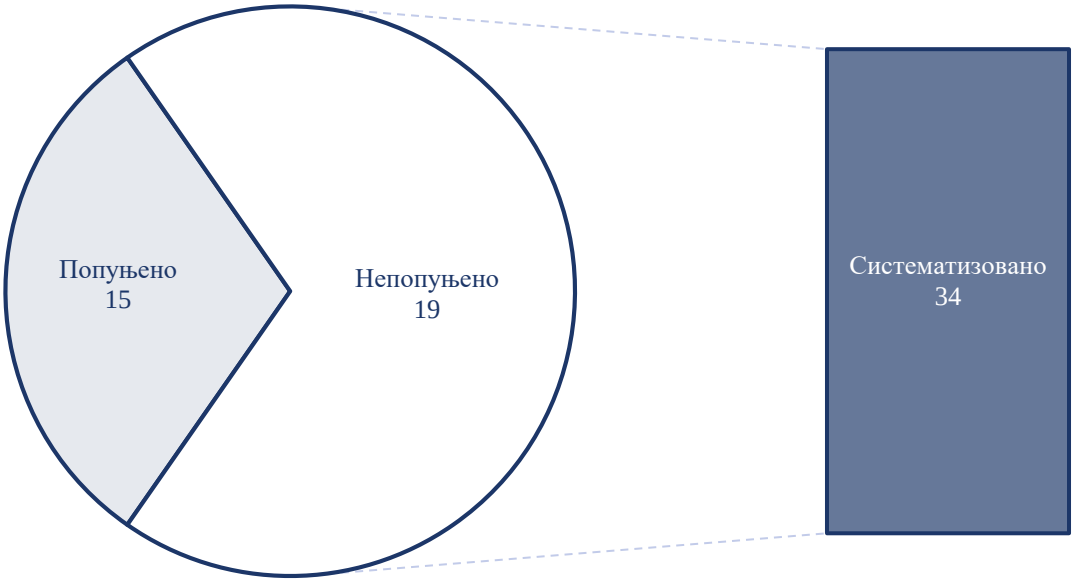


У Дирекцији РФЗО у Београду, у оквиру Сектора за развој и информационе технологије од систематизована 34 радна места[48], попуњено је 15 радних места, што чини 44% попуњености кадровских капацитета. Укупан број запослених у РФЗО на дан 28.6.2023. године износи 2.148 запослених[49].

[48] запослени у Одељењу за послове контакт центра, које је формално у оквиру Сектора за развој и информационе технологије, нису урачунати с обзиром да није реч о техничким лицима (информатичарима), већ о лицима која пружају подршку осигураницима у вези са остваривањем права на здравствену заштиту и генерално услугама које пружа РФЗО.

[49] податак добијен од РФЗО.

Слика број 8: Кадровски капацитет у Сектору за развој и информационе технологије Дирекције РФЗО

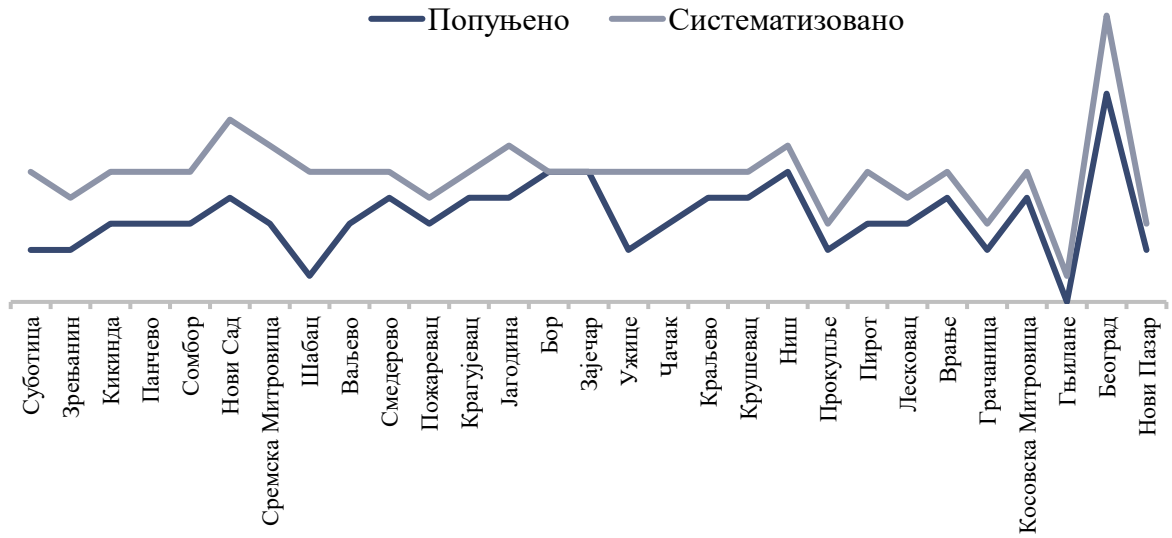


Као што је објашњено у Налазу 2.2 и приказано у Табели број 4 овог извештаја, у Сектору за информациону безбедност и заштиту података није запослено ниједно лице, иако су у том сектору систематизована радна места.

Покрајински фонд за здравствено осигурање (Дирекција Нови Сад), као организациона јединица РФЗО, нема сектор ни одељење које би било задужено за ИТ послове, тиме ни запослене задужене за ИТ послове.[50]

У 29 филијала РФЗО укупно је систематизовано 150 радних места за ИТ послове, од чега је попуњено 95 радних места, то чини 63% попуњености кадровских капацитета.

Слика број 9: Кадровски капацитет систематизованих и попуњених ИТ радних места по филијалама РФЗО



[50] податак добијен од одговорних лица РФЗО у току поступка ревизије.

На одређено време у РФЗО је запослено укупно седам лица (пет саветника за информациону безбедност, један софтвер инжењер и један техничар одржавања информационих система и технологија)[51]. Имајући у виду значај и потребе за сталним унапређењем ИС, последице недостатка ИТ кадрова утичу на остваривање радних и пословних циљева организације, што отежава свакодневни рад са осигураницима, ЗУ и другим организацијама (привредом и јавним сектором).

РФЗО је у току поступка ревизије доставио доказе о слању „Пријаве о потреби за запошљавањем“ из фебруара и новембра 2022. године Националној служби за запошљавање ради новог запошљавања на више од десет радних места на пословима информационих технологија у Републичком фонду за здравствено осигурање.

Препоручујемо Републичком фонду за здравствено осигурање да у циљу успостављања организационе структуре за ИТ управљање, предузме мере за јачање кадровских капацитета кроз повећање броја и/или стручних знања запослених.

Управљање ИТ ризицима

Према одредбама члана 81 Закона о буџетском систему[52] корисници јавних средстава успостављају финансијско управљање и контролу, које се спроводи политикама, процедурама и активностима са задатком да се обезбеди разумно уверавање да ће своје циљеве остварити кроз: 1) пословање у складу са прописима, унутрашњим актима и уговорима; 2) реалност и интегритет финансијских и пословних извештаја; 3) економично, ефикасно и ефективно коришћење средстава и 4) заштиту средстава и података (информација).

Према одредбама члана 3 Правилника о заједничким критеријумима и стандардима за успостављање, функционисање и извештавање о систему финансијског управљања и контроле у јавном сектору[53], финансијско управљање и контрола је систем политика, процедура и активности које успоставља, одржава и редовно ажурира руководилац корисника јавних средстава, а којим се управљајући ризицима обезбеђује уверавање у разумној мери да ће се циљеви корисника јавних средстава остварити на правилан, економичан, ефикасан и ефективан начин. Према члану 5 истог правилника, финансијско управљање и контрола обухвата пет међусобно повезаних елемената:

1) контролно окружење;
2) управљање ризицима;
3) контролне активности;
4) информисање и комуникација;
5) праћење и процена система.

Управљање ризицима обухвата идентификовање, процену и контролу над потенцијалним догађајима и ситуацијама које могу утицати на остварење циљева корисника јавних средстава, обезбеђујући разумно уверавање да ће ти циљеви бити остварени (члан 7 став 1). Руководилац корисника јавних средстава усваја стратегију управљања ризиком, која се ажурира сваке три године, као и у случају када се контролно окружење значајније измени (члан 7 став 2). Управљање ризицима обухвата следеће принципе:

[51] податак добијен од одговорних лица РФЗО у току поступка ревизије.
[52] „Службени гласник РС“, бр. 54/09, 73/10, 101/10,.. 118/21, 138/22 и 118/21 - др. закон.
[53] „Службени гласник РС“, бр. 89/19.

1) Корисник јавних средстава утврђује циљеве на начин који је довољно јасан да би се омогућила идентификација и процена ризика који се односе на те циљеве;
2) Анализу ризика у оквиру корисника јавних средстава као основ за одлучивање о начину управљања ризицима;
3) Процену ризика од могућности преваре;
4) Идентификовање и анализу промена у оквиру корисника јавних средстава које би могле значајније утицати на систем интерне контроле. (члан 7 став 3)[54].

Према одредбама члана 3 став 1 тачка 1) Закона о информационој безбедности, приликом планирања и примене мера заштите ИКТ система треба се руководити начелом управљања ризиком. Избор и ниво примене мера се заснива на процени ризика, потреби за превенцијом ризика и отклањања последица ризика који се остварио, укључујући све врсте ванредних околности.

Сва питања разматрана у овој ревизији у основи имају процену одређених ризика (ИТ управљање, ИТ безбедност, приступ подацима од стране пружаоца услуга итд.). Процена самих ризика посматра се кроз термине утицај и вероватноћа док се њихово рангирање изводи укрштањем утицаја и вероватноће. Процена утицаја обухвата процену ефекта који би неповољан догађај имао на организацију уколико би се остварио. Код процене вероватноће дешавања процењује се колика је вероватноћа настанка одређеног ризика унутар неког периода (нпр. 1 година). Из процене утицаја и вероватноће произилази процена укупне изложености ризику коју је неопходно извршити како би се утврдили приоритети, односно како треба управљати најзначајнијим ризицима[55].

У Уредби о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја[56], у члану 2 прописано је да оператор ИКТ система утврђује, у оквиру организационе структуре, послове и одговорности запослених за заштиту информационих добара, односно средстава и имовине за надзор над пословним процесима од значаја за информациону безбедност, за управљање ризицима у области информационе безбедности, као и за послове предвиђене процедурама у области информационе безбедности.

РФЗО је доставио Стратегију управљања ризицима из јула 2021. године, која представља стратешки документ који употпуњује даљи развој система финансијског управљања и контроле и има за циљ да се у РФЗО уведе пракса управљања ризицима и успостави оквир којим ће се и у будућем периоду развијати сам процес управљања. Овом стратегијом одређен је процес идентификовања ризика, процена идентификованих ризика, рангирање, као и активности које треба предузети како би се ефекти ризика (укупна изложеност ризику) ублажили. Такође, одређује се и који запослени учествују у процесу управљања, начину извештавања о евидентираним ризицима и њиховом статусу. Ризици се евидентирају у Регистру ризика. Регистар ризика је „база података“ за све информације о ризицима. Регистар ризика се ажурира сваке године. Ризици који се тичу ИТ и осталих система подршке, смештени су у оквиру „Унутрашњих ризика“, у групу која носи назив „Ризици који се односе на планирање, процесе и системе“.[57]

[54] члан 7 Правилника о заједничким критеријумима и стандардима за успостављање, функционисање и извештавање о систему финансијског управљања и контроле у јавном сектору („Службени гласник РС“, бр. 89/19).
[55] Смернице за управљање ризицима, Министарство финансија.
[56] „Службени гласник РС“, бр. 94/16.
[57] Стратегија управљања ризицима, јул 2021. године.

У поступку ревизије, извршен је увид у извод из документа „Регистар ризика“ за 2020, 2021. и 2022. годину, у делу који се односи на IT ризике. Утврђено је да је РФЗО идентификовао иста три ризика за сваку годину, и то:

1) Непостојање резервних копија база података у моменту хаварије и немогућност приступа подацима;
2) Прекид у раду „core“ система РФЗО-а;
3) Прекид у раду система за извештавање и апликација чије процедуре врше упит над подигнутим базама.

РФЗО је успоставио Општи модел управљања ризицима, који се састоји од пет корака:

- дефинисање циљева;
- утврђивање ризика;
- анализа и процена ризика;
- реаговање на ризик - поступање у случајевима ризика;
- праћење и извештавање о ризицима.[58]

Наведена три IT ризика су од стране РФЗО вреднована, односно рангирана са аспекта вероватноће и утицаја, предложене су одговарајуће мере за ублажавање тих ризика, наведена су лица која су одговорна за превентивне мере којима се третира идентификовани ризик и у Регистру ризика евидентиране су конкретне активности на третирању ризика.

РФЗО не врши се годишње ажурирање регистра ризика како је предвидео Стратегијом управљања ризицима. Последица непрепознавања ИТ ризика може проузроковати немогућност брзог и адекватног реаговања на инцидент или хаварију, дужи период опоравка ИС након инцидента/хаварије и у крајњој мери непостизање пословних циљева и резултата. Последице могу бити и велики трошкови услед нежељених догађаја (инцидент/хаварија) или велики нефинансијски губици (података), због немогућности благовременог реаговања.

Препоручујемо Републичком фонду за здравствено осигурање да успостави управљање ИТ ризицима, што подразумева евидентирање, класификацију, анализу свих ИТ ризика и дефинисање стратегије за смањивање/отклањање ризика.

Налаз 1.3: РФЗО није успоставио правила управљања подацима из матичне евиденције осигураника, којима би онемогућио приступ личним подацима осигураника и без њиховог физичког присуства.

Исправа о осигурању је КЗО и потврда о здравственом осигурању (члан 25 и 26 Закона о здравственом осигурању). Према одредбама Правилника о исправи о осигурању (члан 10 став 2 и 3) ако се промене подаци садржани у ЧИП-у картице, осигураном лицу се не издаје нова картица, већ се електронским путем врши промена података у матичној евиденцији и на усмени захтев осигураног лица, у случају промене података (осигураног лица), матична филијала врши физичку синхронизацију података садржаних у ЧИП-у картице са подацима који су измењени у матичној евиденцији.

РФЗО синхронизацију података на контактном микроконтролору (у даљем тексту: ЧИП) КЗО не врши електронским путем, већ је потребна физичка синхронизација података на ЧИП-у.

[58] Стратегија управљања ризицима Републичког фонда за здравствено осигурање, јул 2021. године, страна 5

КЗО се не користи у свим ЗУ на идентичан начин, јер се подацима матичне евиденције може приступити без идентификације корисника (учитавањем КЗО или коришћењем минимум два податка - ЈМБГ и ЛБО/број здравствене исправе).

РФЗО није обезбедио да ЗУ приступају подацима матичне евиденције осигураника на јединствен начин, који би обезбедио већу поузданост и заштиту личних података осигураника.

КЗО су почеле да се користе 2013. године и за претходних 10 година је технолија израде картица значајно напредовала. У пракси ЗУ КЗО користи као „обичну" књижицу и само један податак (ЛБО или број ЗИ), а не минимум два ради идентификације осигураника.

Последице приступа матичној евиденцији осигураника без уноса минимум два податка (или учитавањем КЗО) оставља могућност да се од стране корисника система оствари увид у личне податке осигураника и у случајевима када он није присутан, идентификован на други начин или када то уопште није потребно.

Према одредбама члана 25 став 1 Закона о здравственом осигурању, лицу коме је утврђено својство осигураног лица матична филијала издаје, односно активира исправу о осигурању.

Према одредбама члана 25 став 2 Закона о здравственом осигурању, исправа о осигурању је КЗО и потврда о здравственом осигурању.

Према одредбама члана 26 став 1 Закона о здравственом осигурању, КЗО садржи видљиве податке и податке које садржи ЧИП, док према одредбама става 2 истог члана Закона о здравственом осигурању, видљиви подаци су: име, презиме, датум рођења, лични број осигураног лица (у даљем тексту: ЛБО), број здравствене картице и серијски број ЧИП-а.

Према одредбама члана 26 став 4 Закона о здравственом осигурању, ЧИП садржи следеће идентификационе податке о осигуранику: име, име једног родитеља, презиме, адреса (улица и број, место и општина), ЈМБГ, односно евиденциони број за стране држављане, датум рођења, ЛБО, пол, основ осигурања, податке о обвезнику плаћања доприноса.

Према одредбама члана 26 став 7 Закона о здравственом осигурању, РФЗО општим актом уређује садржај и облик исправе о осигурању, начин овере, категорије осигураних лица за коју преузима обавезу трошкова издавања картице здравственог осигурања, као и друга питања од значаја за коришћење исправе.

Према одредбама члана 2 став 2 Правилника о исправи о осигурању[59], лицу коме је утврђено својство осигураног лица филијала РФЗО издаје, односно активира исправу о осигурању, док је чланом 5 став 1 прописано да се КЗО издаје на основу захтева за издавање КЗО. КЗО садржи видљиве податке и податке које садржи ЧИП, у коме се подаци уносе из матичне евиденције (члан 7 ст. 1 и 4 Правилника о исправи о осигурању).

КЗО не садржи податке о пруженим услугама у здравственим установама, податке о лековима добијеним на рецепт, као ни друге податке о остваривању права из здравственог осигурања.[60]

Према одредбама члана 10 Правилника о исправи о осигурању, ако се промене видљиви подаци на КЗО, осигурано лице је дужно да поднесе захтев за издавање нове картице (став 1) као и да, ако се промене подаци садржани у ЧИП-у картице, осигураном лицу се

[59] „Службени гласник РС", бр. 1/21.
[60] https://rfzo.rs/index.php/osiguranalica/ekartica/ekartica-podaci-menu

не издаје нова картица, већ се електронским путем врши промена података у матичној евиденцији (став 2). Према члану 10 став 3 истог правилника, на усмени захтев осигураног лица, у случају промене података садржаних у ЧИП-у, матична филијала врши физичку синхронизацију података садржаних у ЧИП-у КЗО са подацима који су измењени у матичној евиденцији.

РФЗО нема усвојену процедуру за физичку синхронизацију података садржаних у ЧИП-у КЗО са подацима који су измењени у матичној евиденцији. У пракси овлашћено лице РФЗО на шалтеру РФЗО прихвата захтев од стране осигураног лица и примењује одређене кораке у ИС МЕОП који се могу описати на следећи начин: Кликом на поље „Синхронизација CAMS-а и картице“ ради се поређење података у CAMS бази и података на КЗО. Уколико се неки подаци разликују, биће приказани подаци са CAMS-а. Кликом на дугме „Упис промењених података на КЗО“, подаци се шаљу на CAMS и врши се синхронизација са CAMS базом тј. упис података на КЗО. За упис података на картицу потребно је на рачунару имати два читача картица. У једном читачу треба да буде КЗО, а у другом картица која на себи има квалификовани електронски сертификат. Одговорна лица РФЗО су нагласила да је ажурирање података на ЧИП-у била учестала пракса до тренутка када је ИС МЕОП унапређен технолошки, а што је омогућило кориснику (осигураном лицу или овлашћеном лицу ЗУ) да посредством веб сервиса на један клик (приликом очитавања КЗО у читачу) направи увид у најажурније податке садржане на КЗО, без потребе претходног одласка на шалтер РФЗО у циљу синхронизације података на чипу.[61]

Слика број 10: Изглед и подаци на КЗО

Према одредбама члана 19 ст. 1 и 2 Правилника о исправи о осигурању, до издавања КЗО, матична филијала осигураном лицу издаје потврду која се штампа из матичне евиденције на српском језику ћириличким, односно латиничким писмом.

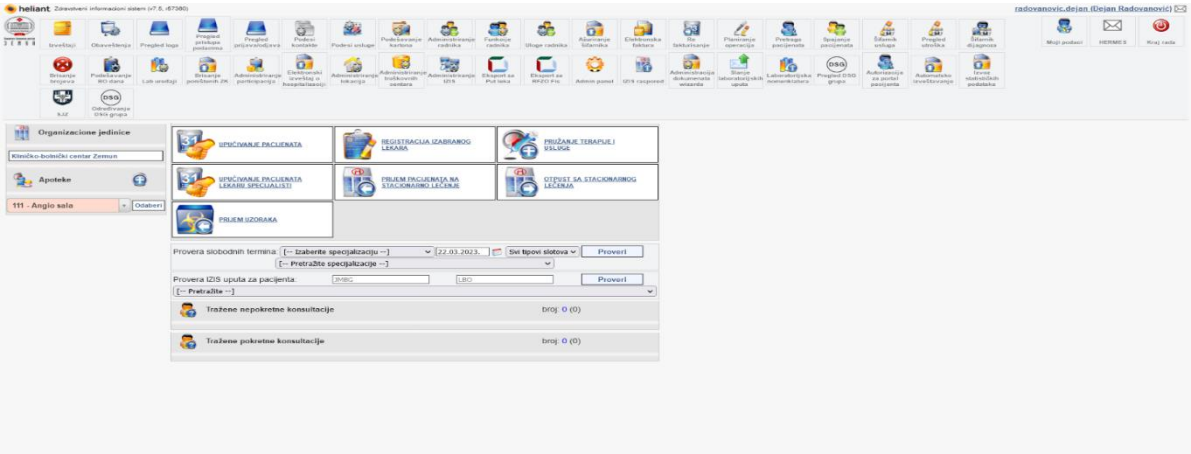
Број уручених КЗО на дан 31.12.2022. године износи 7.894.641 КЗО[62].

У поступку ревизије, тим за ревизију је одржао састанак са две ЗУ и то: Клиничко-болничким центром Земун (у даљем тексту: КБЦ Земун) и Домом здравља Младеновац (у даљем тексту: ДЗ Младеновац). Том приликом, извршен је увид у здравствене информационе системе који ове ЗУ користе у свом раду.

[61] извор: подаци добијени од субјекта ревизије у току поступка ревизије.
[62] податак добијен од субјекта ревизије.

КБЦ Земун од децембра 2021. године користи „Heliant Health“ информациони систем, уз напомену да је пре овог информационог система коришћен HIS (енгл. Hospital Information System) – болнички информациони систем.

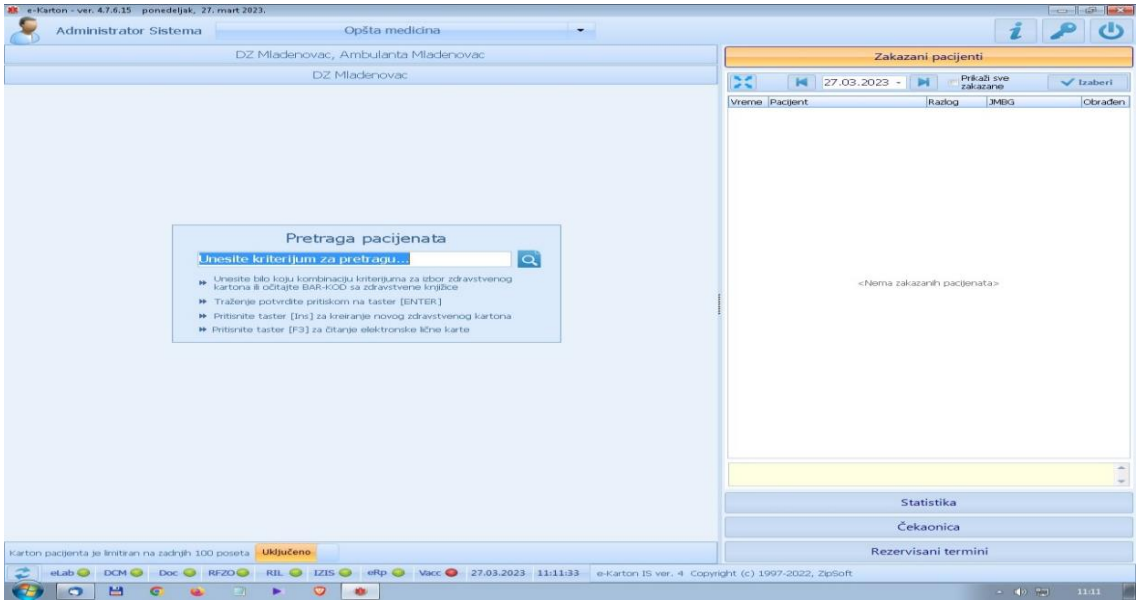
Слика број 11: Слика екрана апликације „Heliant Health“ у КБЦ Земун



Када је у питању одабир осигураника у информационом систему „Heliant Health”, одабир се врши на основу једног податка (ЈМБГ, ЛБО или броја здравствене исправе) и након уноса приступа се подацима садржаним на КЗО тј. основним подацима (име, презиме, број ЛБО, адреса, број телефона, а могу се налазити и други подаци као што је назив обвезника итд.). На овај начин је могуће без присуства пацијента, без очитане његове КЗО, извршити одабир пацијента и остварити увид у његове податке.

Запослени у ДЗ Младеновац користе „ZipSoft“ информациони систем за здравствене установе.

Слика број 12: Слика екрана апликације „ZipSoft“ у ДЗ Младеновац



Када је у питању одабир осигураника у информационом систему „ZipSoft”, одабир се врши на основу једног податка (ЈМБГ, ЛБО или броја здравствене исправе) и након уноса приступа се подацима садржаним на КЗО тј. основним подацима (име, презиме, број ЛБО, адреса, број телефона, а могу се налазити и други подаци као што је назив обвезника итд.).

Увођење КЗО (укључујући и два податка које су повезане са њом – ЛБО и број КЗО) су између осталог за циљ имале и једнозначну идентификацију здравственог осигураника, што се у пракси показало да није увек случај. Процес подразумева да се осигураник приликом пријема идентификује учитавањем КЗО и да на тај начин буде потврђено лично присуство осигураника, што треба да осигура да ће се његовим подацима приступити само када осигураник буде лично присутан.

РФЗО на свом сајту[63] ради провере КЗО (датума до кога је оверена или поништена КЗО) тражи унос два податка, броја ЗИ и ЛБО.

Последице приступа матичној евиденцији осигураника без уноса минимум два податка (или учитавања КЗО), оставља могућност да се од стране корисника система оствари увид у личне податке осигураника и у случајевима када он није присутан, идентификован на други начин или када то уопште није потребно.

Препоручујемо Републичком фонду за здравствено осигурање да успостави правила управљања подацима матичне евиденције осигураника којима би се, уз обавезно физичко присуство осигураника, омогућио приступ личним подацима осигураника.

ЗАКЉУЧАК 2: РФЗО није у потпуности успоставио управљање информационом безбедношћу ИС МЕОП јер није попунио радна места у Сектору за информациону безбедност и заштиту података и не прати и не контролише додељена права приступа ИС МЕОП, што може довести до неовлашћеног приступа подацима осигураника и оствареним правима у здравственој заштити.

Циљ овог дела извештаја је да одговоримо на друго ревизијско питање, односно у којој мери успостављене мере безбедности података у ИС МЕОП обезбеђују поверљивост, заштиту и интегритет података (поузданост ИС). Безбедност података у ИС МЕОП подразумева да РФЗО успостави јасна и ефикасна правила и процедуре контроле физичког и логичког приступа и управљања лог фајловима и инцидентима. Такође је важно да информациона безбедност буде кадровски успостављена како би се безбедносне улоге и одговорности дефинисале у складу са правилима и процедурама за безбедност информација. Безбедност података подразумева и праћење и контролу приступа ИС МЕОП од стране ЗУ и запослених у РФЗО.

Према одредбама члана 8 став 1 Закона о информационој безбедности, оператор ИКТ система дужан је да донесе акт о безбедности ИКТ система, док је ставом 2 истог члана прописано да се тим актом одређују мере заштите, а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

Закон о информационој безбедности ступио је на снагу 5. фебруара 2016. године, док су уредбе које ближе уређују примену закона донете 17. новембра 2016. године. У року од 90 дана требало је донети акт о безбедности ИКТ система, што значи да је последњи рок за то био 17. фебруар 2017. године.

РФЗО је усвојио акт о безбедности информационог система под називом „Акт о безбедности информационо-комуникационог система Републичког фонда за

[63] https://www.rfzo.rs/index.php/osiguranalica/provera-overe-zdrisp

здравствено осигурање“, који је заведен под бројем 01 Бр. 450-3007/22 од 12. маја 2022. године[64]. Овим актом су, у складу са Законом о информационој безбедности, ближе уређене мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационог система РФЗО. Мере заштите ИКТ система које су ближе уређене наведеним актом служе превенцији од настанка инцидената и минимизацији штете од инцидената и њихова примена је обавезна за све запослене. Директор Сектора за информациону безбедност и заштиту података одговоран је за праћење примене мера безбедности, као и за проверу да су подаци заштићени на начин који је утврђен тим актом и интерним процедурама.

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

Налаз 2.1: РФЗО није у потпуности успоставио логички приступ ИС МЕОП који обезбеђује поузданост информационог система (контролу права приступа).

Према одредби члана 10 став 1 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, оператер ИКТ система је у обавези да предвиди процедуру за одобравање и укидање овлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа, тако што предвиђа услове за одобравање и укидање овлашћеног приступа, проверу адекватности одобреног нивоа приступа и доделу јединствене идентификационе ознаке лицу којем се одобрава приступ.

Додела и коришћење администраторских права приступа треба да буде ограничена и контролисана (члан 10 став 4 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја).

Према одредбама члана 14 Акта о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање, РФЗО управља приступом ИКТ систему и услугама кроз употребу корисничких идентификатора. Истим актом је предвиђено да се додељивање привилегованих (администраторских) права на приступ врши на основу одлуке Сектора за развој и информационе технологије (у даљем тексту: Сектора за развој и ИТ).

У поступку ревизије смо утврдили да РФЗО није успоставио контролне механизме да:

- додела и коришћење администраторских права приступа буде ограничена и контролисана и

- креирање, додељивање, измена и деактивирања корисничких имена (корисничких идентификатора) у ИС МЕОП буде у складу са одредбама Акта о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање.

Након издавања Нацрта извештаја РФЗО је доставио доказе да је извршио анализу матрице привилегија администаторских и корисничких налога у ИС МЕОП (додељених права приступа) и ускладио права приступа ИС МЕОП у складу са Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја и Актом о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање и важећим политикама и процедурама.

Узроци непотпуне контроле и праћења додељених права приступа ИС МЕОП су

[64] У поступку ревизије, одговорна лица РФЗО су навела да Акт о безбедности ИКТ система у РФЗО у примени од маја 2022. године, а да су питања информационе безбедности, пре тог датума била регулисана процедурама и политикама у складу са стандардом ИСО-27001.

- недовољна координација између Сектора за развој и ИТ и запослених на ИТ пословима у филијалама,

- огранизациона структура у којој су запослени на ИТ пословима у филијалама одговорни директорима филијала.

Последице доделе администаторских без знања и одобрења Сектора за развој и ИТ, су могућност неовлашћеног приступа подацима осигураника и остваренима правима у здравственој заштити.

Физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему

Према одредбама члана 17 Акта о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање[65], РФЗО је дужан да предузме мере ради спречавања неовлашћеног физичког приступа објектима, простору, просторијама и зонама, у којима се налазе средства и документи ИКТ система, као и спречавање оштећења и ометања информација, сходно „Политици контроле физичког приступа“, ПОЛ-1014. Безбедносне области морају бити заштићене одговарајућим контролама уласка како би се осигурало да је само овлашћеним појединцима дозвољен приступ. РФЗО обезбеђује и примењује одговарајућу контролу приступа, чиме се омогућава физичка безбедност канцеларија, просторија и средстава. Такође, безбедним конфигурисањем се онемогућава приступ кључној опреми а у циљу спречавања видљивости поверљивих информација, активностима споља. Физичка заштита се мора планирати и за случајеве природних катастрофа, непријатељских напада или несрећа. [66]

Политика контроле физичког приступа, референтни број ПОЛ-1014

Политика контроле физичког приступа усвојена је дана 20.6.2013. године (последња верзија[67]). Циљ наведене политике је да обезбеди физичку сигурност свих ресурса који су у власништву РФЗО. Сагласно тачки 2 поменуте политике, политика се примењује на све запослене, укључујући и привремено запослене, запослене по уговору, трећа лица и све оне који долазе у контакт са ресурсима, просторијама, информацијама или информационим системима организације.

Према тачки 3 Политике контроле физичког приступа, права физичког приступа су усклађена са одговорностима, тако да сва лица имају приступ само ресурсима који су им потребни за испуњавање пословних обавеза, односно најмања могућа права приступа која су им неопходна (принцип „least privileges“).

Према тачки 4.1 поменуте политике, приступ просторијама РФЗО мора да буде ограничен како би се обезбедило да само ауторизовани корисници или посетиоци имају право приступа. Евиденција посетилаца мора постојати, било у папирној било у електронској евиденцији, као и да, где год је могуће, постоји физичка контрола приступа просторијама организације у виду физичко-техничког обезбеђења које ће бележити све посетиоце који приступају просторијама. Према тачки 4.2 политике, у хитним случајевима (пожар, поплава, земљотрес, терористички напад, улични нереди и слично), уколико је неопходно да неауторизована лица приступе ресурсима и просторијама организације за која немају додељено право, обезбеђење објекта и дежурно особље

[65] 01 број 450-3007/22 од 12. маја 2022. године.
[66] члан 17 Акта о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање.
[67] верзија: 2.00, заводни број: 54-2913/12-84.

обавештава лица одговорна за физичку сигурност организације и/или релевантне чланове руководства.

У току поступка ревизије, одговорна лица су истакла да РФЗО има закључен Уговор бр. 44-1/21 о пружању услуге физичко-техничког обезбеђења пословних објеката РФЗО (29 објеката укључујући и зграду Дирекције РФЗО) за период од 24 месеца од 20. јула 2021. године, који за циљ има осигурање безбедности и здравља на раду и обезбеђење сигурности људи и имовине, а све у складу са позитивноправним прописима из предметне области. Напомињу и да постоји одређени број објеката где се просторије РФЗО налазе у просторијама других корисника објеката (општине, домови здравља, Републичког фонда за пензијско и инвалидско осигурање, Националне службе за запошљавање и других) који већ поседују своје физичко-техничко обезбеђење. РФЗО је такође навео да имају закључен Уговор бр. 32-1/22 од 23. фебруара 2022. године о пружању услуге контроле противпожарних апарата, хидраната, паник расвете и противпожарних централа за потребе организационих јединица РФЗО.

У поступку ревизије извршили смо увид у просторије где се налазе сервери и пратећа комуникациона опрема и закључили да су просторије обезбеђене одговарајућом физичком-техничком заштитом.

Логички приступ

Према одредби члана 10 став 1 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, оператер ИКТ система је у обавези да предвиди процедуру за одобравање и укидање овлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа, тако што предвиђа услове за одобравање и укидање овлашћеног приступа, проверу адекватности одобреног нивоа приступа и доделу јединствене идентификационе ознаке лицу којем се одобрава приступ.

Оператор ИКТ система води евиденцију о додељеним и одузетим ознакама, утврђује услове за коришћење заједничке идентификационе ознаке у случајевима када је то неопходно, дефинише начин и услове онемогућавања и уклањања јединствених идентификационих ознака, као и услове за доделу и коришћење администраторских права (члан 10 став 2 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја).

Лицима којима се одобрава овлашћени приступ омогућује се приступ на основу података за аутентификацију (лозинке, криптографски кључеви, подаци складиштени на токенима и сл.) (члан 10 став 3 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја).

Додела и коришћење администраторских права приступа треба да буде ограничена и контролисана (члан 10 став 4 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја).

Оператор ИКТ система дужан је да обезбеди механизам за укидање права приступа у случајевима промене радног места, престанка радног односа и, по потреби, у другим случајевима (члан 10 став 5 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја).

Према одредбама члана 14 Акта о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање, РФЗО управља приступом ИКТ систему и услугама кроз употребу корисничких идентификатора. Управљање идентификаторима врши се уз поштовање следећих принципа:

- Кориснички идентификатори су јединствени, тако да се корисници могу везати уз њих и учинити одговорним за своје активности;
- Коришћење заједничких идентификатора дозвољава се само онда када је то погодно за обављање посла уз претходно одобрење;
- Корисницима којима је престао радни однос или период ангажовања тренутно се онемогућавају или уклањају кориснички идентификатори;
- Периодично идентификовање и уклањање или онемогућавање вишеструких корисничких идентификатора;
- Вишеструки идентификатори неког корисника се не издају другим корисницима.

Сваком кориснику се додељује право приступа ИКТ систему у складу са радним задацима које обавља. Кориснику се додељују јединствени подаци за логовање и јединствена шифра за логовање, који се не смеју делити са другим корисницима. Додељивање привилегованих (администраторских) права на приступ врши се на основу одлуке Сектора за развој и информационе технологије. Привилегована права на приступ додељује се посебно за сваки системски објекат уз дефинисан рок трајања тих права. Привилегована права на приступ које треба доделити корисничком идентификатору другачија су од оних која се користе за редовне активности. Редовне пословне активности не треба вршити из привилегованих корисничких идентификатора. Компетенције корисника са привилегованим правима на приступ се редовно преиспитују ради провере да ли су у складу са њиховим обавезама. Забрањено је неовлашћено коришћење општих корисничких идентификатора администратора. Шифре за приступ општим корисничким идентификаторима администратора се мењају променом корисника. РФЗО периодично врши преиспитивање права корисника на приступ, као и након сваке промене (унапређење, разрешење и крај запослења). Запосленима, другим радно ангажованим и екстерним корисницима информација и опреме за обраду информација по престанку запослењу или истеку уговора, укида се право на приступ[68].

Политика управљања корисничким улогама, референтни број ПОЛ-1011

Политика управљања корисничким улогама[69] дефинише начин управљања корисничким налозима и привилегијама и то путем:

- Ауторизације за управљање корисничким налозима и привилегијама,
- Квалификације за налоге који користе информационе ресурсе,
- Управљање корисничким налозима и привилегијама и
- Управљање лозинкама.

Према тачки 5 наведене политике, лица која су одговорна за креирање корисничких налога морају да обезбеде да налози буду креирани само за оне особе које су квалификоване да имају налог и чији је идентитет потврђен, као и да приступ информационим ресурсима мора бити ауторизован и морају постојати адекватни записи о одобреним правима приступа. Такође, наведеном политиком уређено је и да приступ корисника информационим ресурсима мора бити контролисан и преиспитан од стране одговорних лица кад дође до значајних промена околности или најмање једном годишње.

[68] члан 14 Акта о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање.
[69] ПОЛ-1011 од 20.6.2013. године.

Политика контроле логичког приступа, референтни број ПОЛ-1013

Политика контроле логичког приступа усвојена је дана 20.6.2013. године (последња верзија[70]). Контрола логичког приступа се састоји из три процеса: идентификације (провере корисничког имена), аутентификације (провере комбинације корисничког имена и лозинке) и ауторизације (провере права приступа функције система). Политика контроле логичког приступа за циљ има да установи стандард за креирање јаких лозинки, њихову заштиту и учесталост мењања. Политика контроле логичког приступа обухвата све запослене и трећа лица која имају право приступа информацијама или информационим системима организације и примењује се у свим организационим јединицама РФЗО и важи за све системе и све запослене.[71]

Према одредбама Акта о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање, РФЗО дозвољава рад на даљину и употребу мобилних уређаја од стране запослених, уколико је осигурана безбедност рада у случају обављања послова ван просторија послодавца, узимајући у обзир и ризике до којих може доћи услед неадекватног коришћења мобилних уређаја[72].

У поступку ревизије је од одговорних лица РФЗО тражен списак администраторских и корисничких налога у оквиру ИС МЕОП, као и записници о праћењу и ревидирању приступа корисника (корисничких права приступа) информационим ресурсима (са посебним акцентом на ИС МЕОП) у току 2021. и 2022. године, како је то прописано Политиком управљања корисничким улогама ПОЛ-1011.

Слика број 13: Списак администраторских и корисничких налога у ИС МЕОП

Сагласно тачки 3.2 Политике контроле логичког приступа, власник система има крајњу одговорност за креирање, имплементацију, документовање и комуникацију формалне политике која омогућава следеће контролисане активности:

- креирање и измену корисничких имена;
- деактивирање корисничких имена приликом престанка коришћења истих.

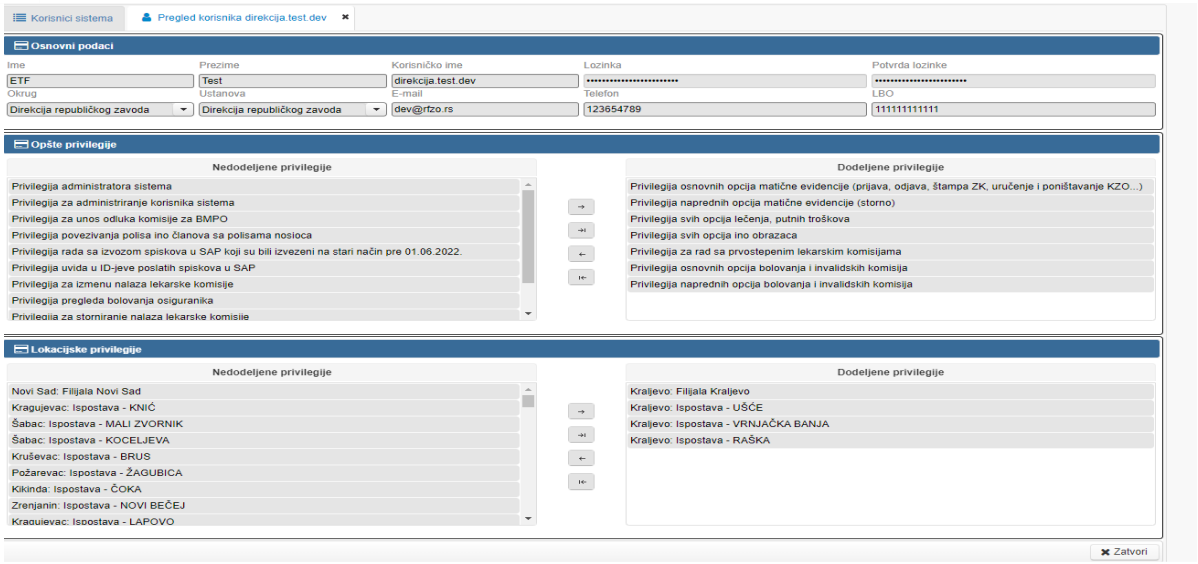
Укупан број активних налога у апликацији МЕОП износи 1.832 налога[73].

Сви захтеви за креирање, измену или деактивирање корисничког имена морају бити документовани, за шта се користе обрасци ОБИ-1006 (Захтев за регистрацију и одјаву корисника) и ОБИ-1010 (Захтев за регистрацију, промену и одјаву корисника информационих система РФЗО).[74]

У поступку ревизије, тражени су обрасци ОБИ-1006 и ОБИ-1010 за корисничка имена (кориснички идентификатори) која су заједничка односно специфична.

[70] верзија 2.00, заводни број: 54-2913/12-83.
[71] Политика контроле логичког приступа, ПОЛ-1013 од 20.6.2013. године.
[72] члан 7 Акта о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање.
[73] податак добијен од субјекта ревизије.
[74] Обрасци ОБИ-1006 и ОБИ-1010 прописани су тачком 3.2 Политике контроле логичког приступа ПОЛ-1013.

Слика број 14: Преглед додељених системских и локацијских привилегија за изабраног корисника „direkcija.test.dev“



РФЗО је у поступку ревизије доставио обрасце ОБИ-1006 и ОБИ-1010 за тражена корисничка имена.

Анализом матрице привилегија (списка администраторских и корисничких налога) у оквиру ИС МЕОП, утврдило смо да креирање (измену и деактивирање) администраторских и корисничких налога раде одговорна лица у Дирекцији РФЗО, у оквиру Сектора за развој и ИТ. Такође, дозволу за креирање администраторских и корисничких налога имају и информатичари у филијалама РФЗО (уз сагласност директора филијале). Међу администраторским налозима у филијалама РФЗО утврдили смо да у појединим случајевима иста особа поседује администраторски налог који је отворен од стране Дирекције и администраторски налог који је отворио сам администратор уз сагласност директора филијале.

У току спровођења ревизије РФЗО је извршио анализу матрице привилегија администаторских и корисничких налога у ИС МЕОП (додељених права приступа) и ускладио права приступа ИС МЕОП у складу са Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја и Актом о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање и важећим политикама и процедурама.

Према одредбама члана 14 Акта о безбедности информационо-комуникационог система РФЗО, додељивање привилегованих (администраторских) права на приступ врши се на основу одлуке Сектора за развој и ИТ, што у овим случајевима није испоштовано.

У току ревизије смо посетили и три филијале РФЗО: Београд, Панчево и Зрењанин и на њиховим примерима закључили следеће:

1. да се додела корисничких налога код све три филијале врши од стране ИТ администратора филијале, уз сагласност директора филијале (путем ОБИ обрасца 1006 и 1010),

2. да се додела администраторских налога код све три филијале врши од стране Сектора за развој и ИТ, а да су у једној филијали отворени и администраторски налози од стране самог ИТ администратора у тој филијали;
3. ОБИ обрасци се не чувају (архивирају) на идентичан начин и не контролише се могућност да запослени имају више активних налога.
4. према наводима представника филијала, ОБИ обрасци не одговарају у потпуности ИС цМЕОП, односно одговарају старој верзији ИС МЕОП.[75]

У току поступка ревизије, РФЗО је доставио Решење о преносу овлашћења за обављање одређених послова на директора Филијале Панчево, 12 број 031-458/16 од 29.12.2016. године, у коме је у тачки 7) наведено да директор филијале обавља и послове вођења матичне евиденције осигураних лица са подацима потребним за спровођење обавезног здравственог осигурања и за обезбеђивање и контролу остваривања права из тог осигурања.

Узроци непотпуне контроле и праћења додељених права приступа ИС МЕОП су
- недовољна координација између Сектора за развој и ИТ и запослених на ИТ пословима у филијалама,
- организациона структура у којој су запослени на ИТ пословима у филијалама одговорни директору филијале и
- географска разуђеност филијала и тиме различито поступање при примени интерних аката РФЗО.

Додела администраторских права од стране информатичара у филијалама РФЗО без сагласности и контроле Сектора за развој и ИТ потенцијално може угрозити податке о осигураницима и остварeним правима.

Мера предузета у поступку ревизије

РФЗО је у току поступка ревизије доставио Извештај о контролама управљања корисничким налозима за филијале Београд, Зрењанин и Панчево, као и матрицу привилегија администраторских и корисничких налога за ИС МЕОП након извршене анализе администраторских и корисничких налога.

Налаз 2.2: РФЗО није попунио радна места у Сектору за информациону безбедност и заштиту података.

Према одредби члана 7 став 3 тачка 1) Закона о информационој безбедности, мере заштите ИКТ система односе се на успостављање организационе структуре са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система. Такође, оператор ИКТ система дужан је да у оквиру организационе структуре, у складу са природом, обимом и сложеношћу пословања, утврди послове и одговорности запослених, у циљу управљања информационом безбедношћу (члан 2 став 1 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја).

РФЗО је успоставио организациону структуру са утврђеним пословима и одговорностима запослених за ИТ безбедност. Међутим, РФЗО није попунио радна места у Сектору за информациону безбедност и заштиту података, иако је Правилником о организацији и систематизацији послова је систематизовано 12 радних места.

[75] централизација ИС МЕОП извршена је у 2017. години, док део узоркованих ОБИ образаца потиче из периода када је ИС МЕОП био децентрализован (радио на локалним серверима у филијалама РФЗО).

Запослени на ИТ пословима су учествовали на две обуке за ИТ безбедност у периоду ревизије (2020-2022. година).

Узроци су мањи број запослених од предвиђеног броја (систематизованог), већина запослених у опису послова имају задужење везано за информациону безбедност, а да им то није превасходни радни задатак и неучествовање на обукама из информационе безбедности.

Организација ИТ безбедности у РФЗО није успостављена тако да обухвата примену адекватних прописа која уређују ову област – Закона о информационој безбедности, Закона о здравственој документацији и евиденцијама у области здравства, Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, Акта о информационој безбедности и других интерних аката, као и примену других мера заштите ИКТ система, што за последицу има већи степен рањивости информационог система.

Одредбом члана 1 Уредбе о утврђивању листе делатности у којима се обављају делатности од општег интереса и у којима се користе информационо-комуникациони системи од посебног значаја[76] утврђује се Листа делатности у областима у којима се обављају делатности од општег интереса и у којима се користе ИКТ системи. Истом уредбом (Прилог 1) прописано је да је здравствена делатност коју обављају ЗУ и друга правна лица која обављају здравствену делатност, делатност од општег интереса и у којој се користи ИКТ системи.

Према одредби члана 7 став 3 тачка 1) Закона о информационој безбедности, мере заштите ИКТ система односе се на успостављање организационе структуре са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система.

Према одредби члана 2 став 1 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, оператор ИКТ система дужан је да у оквиру организационе структуре, у складу са природом, обимом и сложеношћу пословања, утврди послове и одговорности запослених, у циљу управљања информационом безбедношћу.

Према одредби члана 2 став 2 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, оператор ИКТ система утврђује у оквиру организационе структуре, послове и одговорности запослених за заштиту информационих добара, односно средстава и имовине за надзор над пословним процесима од значаја за информациону безбедност, за управљање ризицима у области информационе безбедности, као и за послове предвиђене процедурама у области информационе безбедности .

Према одредби члана 2 став 3 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, подела одговорности запослених треба да се изврши тако да се онемогући неовлашћена или ненамерна измена, оштећење или злоупотреба средстава, односно информационих добара оператора ИКТ система, као и да се онемогући приступ, измена или коришћење средстава без овлашћења и без евиденције о томе .

Према одредби члана 51 Закона о здравственој документацији и евиденцијама у области здравства ЗУ, приватна пракса и друга правна лица дужни су да успоставе и одржавају систем безбедности који обухвата мере за обезбеђење сигурности података које оне

[76] „Службени гласник РС“, бр. 94/19.

поседују у складу са тим законом и законом којим се уређује заштита података о личности.

РФЗО је у поступку ревизије доставио извод из Правилника о организацији и систематизацији послова у РФЗО у делу који се односи на информационе технологије-Дирекција РФЗО, Покрајински фонд, филијале РФЗО[77]. У наредној табели се налази приказ систематизованих радних места Дирекције РФЗО у оквиру Сектора за информациону безбедност и заштиту података.

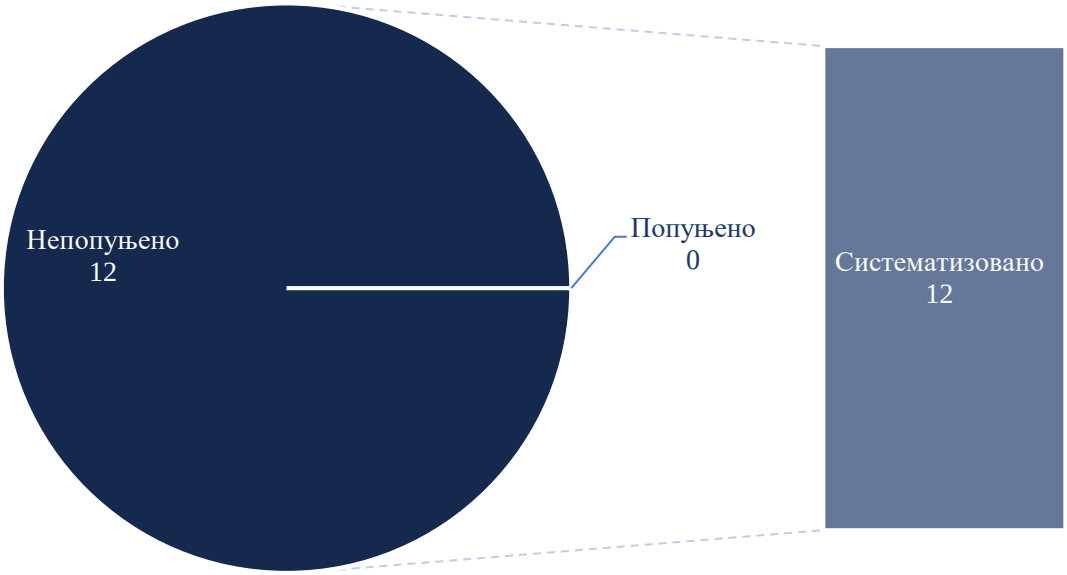
Табела број 4. Приказ систематизованих радних места Дирекције РФЗО у оквиру Сектора за информациону безбедност и заштиту података

XV СЕКТОР ЗА ИНФОРМАЦИОНУ БЕЗБЕДНОСТ И ЗАШТИТУ ПОДАТАКА	Систематизовано	Попуњено
Директор сектора	1	0
Заменик директора Сектора	1	0
	УКУПНО: 2	0
XV/1. ОДЕЉЕЊЕ ЗА КОНТИНУИТЕТ ПОСЛОВАЊА	Систематизовано	Попуњено
Начелник одељења	1	0
XV/1.1. Одсек за континуитет пословања	Систематизовано	Попуњено
Шеф Одсека	1	0
Група за континуитет пословања	Систематизовано	Попуњено
Руководилац групе	1	0
Самостални организатор процеса	1	0
Саветник за информациону безбедност	1	0
	УКУПНО: 5	0
XV/2. ОДЕЉЕЊЕ ЗА ИТ РИЗИК И СИГУРНОСТ	Систематизовано	Попуњено
Начелник одељења	1	0
XV/2.1. Одсек за ИТ ризик и сигурност	Систематизовано	Попуњено
Шеф Одсека	1	0
Група ИТ ризик и сигурност	Систематизовано	Попуњено
Руководилац групе	1	0
Самостални организатор процеса	1	0
Саветник за информациону безбедност	1	0
	УКУПНО: 5	0
	УКУПНО СИСТЕМАТИЗОВАНО: 12	0

Од систематизованих 12 радних места у оквиру Сектора за информациону безбедност и заштиту података, није попуњено ниједно радно место.

[77] 12 бр. 110-5/20 од 31.1.2020. године.

Слика број 15: Искоришћеност кадровских капацитета у Сектору за информациону безбедност и заштиту података Дирекције РФЗО



У одговору на упитник о стању ИТ у РФЗО[78], као одговор на питање да ли РФЗО има запослено лице одговорно за безбедност информационог система, одговорна лица РФЗО су истакла да је начелник Одељења за одржавање рачунарских мрежа и системско одржавање, у оквиру Сектора за развој и ИТ, одговоран за безбедност информационог система.

У поступку ревизије, извршен је увид у уговор о раду[79] и анекс уговора[80] са наведеном запосленом. Том приликом је утврђено да поред стандардних послова које обавља начелник Одељења за одржавање рачунарских мрежа и системско одржавање, у анексу уговора је наведено да запослена обавља и следеће послове:

- обезбеђивање безбедности и заштите података информационог система РФЗО;
- обезбеђивање заштите информационог система од неовлашћеног упада и приступа подацима.

Анализирајући извод из Правилника о организацији и систематизацији послова у РФЗО у делу који се односи на информационе технологије - Дирекција РФЗО, Покрајински фонд и филијале РФЗО, достављеног у току поступка ревизије, утврђено је да су послови „обезбеђивања безбедности и заштите података информационог система РФЗО“ и послови „обезбеђивања заштите информационог система од неовлашћеног упада и приступа подацима“, у опису делокруга рада већине систематизованих радних места[81] у оквиру Сектора за развој и ИТ Дирекције РФЗО.

Управљање информационом безбедношћу је изузетно важна област и захтева одговарајућу организацију и запослене који могу заштитити ресурсе РФЗО, како опреме

[78] послатог РФЗО електронском поштом, дана 21. фебруара 2023. године.
[79] 02/11 број: 112-3089/13 од 26. јула 2013. године.
[80] 12/3 број: 112-1569/14 од 25. маја 2014. године.
[81] радна места: заменик директора Сектора за развој информационих система; заменик директора Сектора за послове одржавања рачунарских мрежа и системско одржавање; начелник Одељења за развој информационих система; помоћник начелник Одељења за развој информационих система; начелник Одељења за одржавање информационих система; шеф Одсека за одржавање информационих система.

тако и информационог система од неовлашћеног упада и приступа подацима. Неадекватно управљање информационом безбедношћу може имати дугорочни утицај на циљеве организације, а у ИТ делу рањивост информационог система и могућност злоупотреба података из ИС МЕОП.

Препоручујемо Републичком фонду за здравствено осигурање да предузме мере на кадровском јачању Сектора за информациону безбедност и заштиту података.

Обуке запослених на ИТ пословима везане за безбедност ИТ

У току поступка ревизије, тим за ревизију је прикупио податке о спроведеним обукама у вези са ИТ безбедношћу у 2020, 2021. и 2022. години.

РФЗО није доставио предлоге планова и планове стручног усавршавања за 2020. и 2021. годину.

План стручног усавршавања за 2022. годину (Табела број 5) усвојен је од стране руководства РФЗО, али планиране обуке нису спроведене током 2022. године.

Табела број 5. Предлог плана стручног усавршавања за 2022. годину (део који се односи на област информационих технологија)[82]

ОБЛАСТ ИНФОРМАЦИОНИХ ТЕХНОЛОГИЈА				
1	*2*	*3*	*4*	*5*
Курс	Филијала Крагујевац	20486B Developing ASP.NET MVC 5 Web Applications	Online курс	CET- Beograd
Конференција	Филијала Крагујевац	Заштита и сигурност података, Рачунарске мреже и телекомуникације, Информациони и ЕРП системи	13.-.16.03.2022. Копаоник- хотел Гранд	YU INFO
Курс	Филијала Крагујевац	MCSA Windows Server 2016	Online курс	CET- Beograd
Курс	Филијала Крагујевац	20741 Networking with Windows Server 2016	Online kurs	CET- Beograd
Курс	Филијала за зајечарски округ	MCSE: Data Management and Analytics (SQL 2016)	(8 дана/ 64 часова), Београд	CET d.o.o. Beograd
Курс	Филијала за зајечарски округ	MCSE: Cloud Platform and Infrastructure (Windows Server 2016)	(37 дана / 148 часова), Београд	CET d.o.o. Beograd
Курс	Чачак	MSCA Windows server 2019	Накнадно ће бити утврђено	Образовни центар Академија Чачак
Курс	Чачак	MCSA: SQL 2019 Database Development	Накнадно ће бити утврђено	Образовни центар Академија Чачак
Курс	Филијала Крагујевац	20486B Developing ASP.NET MVC 5 Web Applications	Online курс	CET- Beograd
Конференција	Филијала Крагујевац	Заштита и сигурност података, Рачунарске мреже и телекомуникације, Информациони и ЕРП системи	2022. Копаоник- хотел Гранд	YU INFO
Курс	Дирекција – Сектор за ИТ	MCSA SQL 2016 Database Development	Београд	CET
Курс	Дирекција – Сектор за ИТ	MCSA SQL 2016 Business Intelligence Development	Београд	CET
Курс	Дирекција – Сектор за ИТ	MCSA SQL 2016 Database Administration	Београд	CET
Курс	Дирекција – Сектор за ИТ	Kurs 20761 A	Београд	CET
Курс	Дирекција – Сектор за ИТ	Kurs 20762 B	Београд	CET
Курс	Дирекција – Сектор за ИТ	CCNP - Enterprise	Београд	RCUB
Курс	Дирекција – Сектор за ИТ	CCNP - Обнова	Београд	RCUB
Курс	Дирекција – Сектор за ИТ	MCSA SQL 2016 Database Development	Београд	CET
Курс	Дирекција – Сектор за ИТ	MCSA SQL 2016 Business Intelligence Development	Београд	CET

[82] подаци добијени од одговорних лица РФЗО у току поступка ревизије.

ОБЛАСТ ИНФОРМАЦИОНИХ ТЕХНОЛОГИЈА				
1	*2*	*3*	*4*	*5*
Курс	Дирекција – Сектор за ИТ	MCSA SQL 2016 Database Administration	Београд	CET
Курс	Дирекција – Сектор за ИТ	MCSA Web Applications	Београд	CET
Курс	Дирекција – Сектор за ИТ	Java основни курс – припрема за OCA Java SE 8	Београд	CET
Курс	Дирекција – Сектор за ИТ	PHP Web Development	Београд	It-академија
Курс	Дирекција – Сектор за ИТ	ITIL V4	Београд	IT Центар
Курс	Дирекција – Сектор за ИТ	MCSA SQL 2016 Database Development	Београд	CET
Курс	Дирекција – Сектор за ИТ	Developing ASP.NET	Београд	CET
Курс	Дирекција – Сектор за ИТ	PHP Web Development	Београд	IT Центар

У току 2021. године, одржана је обука на тему „Компоненте 2: Проширење информационог система централне Матичне евиденције и остваривања права, Ставке 5.2.7 Модул за замену (mockup) екстерних сервиса за тестно окружење“[83], о чему је као доказ достављен записник о извршеној обуци са списком учесника.

У току 2022. годину, РФЗО одржана је обука на тему „Упознавање запослених са стандардом ISO/IEC 27001 Информационе технологије – Технике безбедности – Системи менаџмента безбедношћу информација – Захтеви“. То је била једина обука на тему информационе безбедности одржана у 2022. години.

У поступку ревизије смо обишли и три филијале РФЗО: Београд, Панчево и Зрењанин, где смо констатовали да запослени на ИТ пословима нису учествовали на обукама из области информационих технологија у претходне три године.

Анализом достављене документације која се односи на стручно усавршавање запослених у секторима за ИТ РФЗО у 2020, 2021. и 2022. години, утврђено је да обуке које се односе на информационе технологије нису организоване довољно често, а и када су планиране нису спроведене (пример 2022. година), што ствара ризик да запослени из Сектора за ИТ и развој РФЗО и запослени на ИТ пословима у филијалама РФЗО нису у довољној мери информисани о актуелним ИТ питањима и могућим безбедносним претњама, као и о новим мерама за заштиту ИКТ система.

Препоручујемо Републичком фонду за здравствено осигурање да предузме активности у циљу континуиране едукације запослених који обављају ИТ послове.

Налаз 2.3: РФЗО није у потпуности успоставио процес праћења и контроле приступа ИС МЕОП од стране ЗУ и запослених у РФЗО.

Оператор ИКТ система треба да обезбеди да се у ИКТ систему формирају записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу, а који се морају чувати и редовно проверавати (члан 18 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја и члан 22 Акта о безбедности информационо-комуникационог система РФЗО).

РФЗО бележи приступ ИС МЕОП (од стране запослених у РФЗО-у и ЗУ) путем записа о догађајима (логови фајлова).

[83] датум одржавања обуке: 3. децембар 2021. године.

РФЗО нема успостављена правила и процедуре редовног праћења и контроле записа о догађајима (лог фајлова) у одређеном периоду, већ се зависно од случаја до случаја ради проверу записа о догађајима (лог фајлова).

Записи о догађајима (лог фајлови) су веома обимни и захтевају редовно праћење и контролу.

Користи од праћења и редовне контроле записа о догађајима (лог фајлова) су брже откривање/реаговање на инциденте/нежељене догађаје а тиме и мања могућност злоупотреба података из ИС МЕОП.

Креирање лог фајлова

Према одредбама члана 18 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, оператор ИКТ система треба да обезбеди да се у ИКТ систему формирају записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу, а који се морају чувати и редовно проверавати.

Средства за записивање и записи треба да буду заштићени од неовлашћеног приступа и промене.

У оквиру ИКТ система записују се активности администратора и корисника и редовно преиспитују у циљу заштите.

У циљу обезбеђивања поузданости записа, времена у свим подсистемима ИКТ система морају бити синхронизована међусобно, као и са референтним тачним временом[84].

Чување података о догађајима који могу бити од значаја за безбедност ИКТ система

Према члану 22 Акта о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање, у ИКТ систему РФЗО формирају се записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу.

Записивање догађаја

Према члану 22 Акта о безбедности информационо-комуникационог система, РФЗО прави записе о догађајима и бележи активности корисника, грешке и догађаје у вези са информационом безбедношћу, који се морају чувати и редовно преиспитивати. Истим чланом је прописано да администратори система немају дозволу да бришу или деактивирају дневнике о сопственим активностима.

Записи о догађајима садрже:

- идентификаторе корисника;
- активности система;
- датуме, време и детаље кључних догађаја, нпр. пријављивања и одјављивања;
- идентитет или локацију уређаја, ако је могуће, и идентификатор система;
- записе о успешним и одбијеним покушајима приступа систему;
- записе о успешним и одбијеним покушајима приступа подацима и другим ресурсима;
- промене у конфигурацији система;

[84] члан 18 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја.

- коришћење привилегија;
- коришћење системских помоћних функција и апликација;
- датотеке којима се приступало и врсте приступа;
- мрежне адресе и протоколе;
- аларме које је побудио систем за контролу приступа;
- активирање и деактивирање система заштите, као што су антивирусни системи и системи за откривање упада.[85]

Записи администратора и оператера

Активности администратора и оператера система се записују а записи штите и редовно преиспитују. Власници привилегованих корисничких налога могу бити у стању да управљају записима на опреми за обраду информација која је под њиховом директном контролом, на који начин се штите и прегледају записи да би се одржала одговорност за привилеговане кориснике. За чување података о догађајима који могу бити од значаја за безбедност ИКТ система задужен је Сектор за информациону безбедност и заштиту података[86].

У поступку ревизије извршен је увид у узорак лог фајлова приступа ИС МЕОП од стране запослених и ЗУ.

Од одговорних лица РФЗО у поступку ревизије тражени су записи о догађајима (лог фајлови) ИС МЕОП за 2021. и 2022. годину. РФЗО је доставио доказе односно записе о догађајима (лог фајлова) за тражени узорак.

РФЗО бележи приступ ИС МЕОП (од стране запослених у РФЗО-у и ЗУ) путем записа о догађајима (логови фајлова). РФЗО не врши редовно праћење и контролу записа о догађајима (лог фајлова) у одређеном периоду, већ зависно од случаја до случаја ради проверу записа о догађајима (лог фајлова).

РФЗО није успоставио правила за редовно праћење и контролу записа о догађајима (лог фајлова) због времена која је потребно за анализу обимних лог фајлова и недостатка кадрова. РФЗО спроводи контролу лог фајлова од случаја до случаја. РФЗО није препознао чињеницу да је за руковање подацима о остваренима правима из обавезног здравственог осигурања потребно овластити посебно лице у РФЗО.

Користи од праћења и редовне контроле записа о догађајима (лог фајлова) су брже откривање/реаговање на инциденте/нежељене догађаје а тиме и мања могућност злоупотреба података из ИС МЕОП.

Препоручујемо Републичком фонду за здравствено осигурање да успостави правила и процедуре за редовну контролу и праћење приступа ИС МЕОП.

[85] Члан 22 Акта о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање.
[86] Члан 22 Акта о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање.

ЗАКЉУЧАК 3: РФЗО није у потпуности успоставио ефективан механизам сарадње, односно није у потпуности уредио правилима и процедурама однос са пружаоцем услуге одржавања ИС МЕОП и мере којима обезбеђује континуитет пословања у случају прекида сарадње са пружаоцем услуге одржавања ИС МЕОП.

Циљ овог дела извештаја је да одговоримо на треће ревизијско питање, односно у којој мери је уговорни однос са пружаоцем услуге одржавања ИС МЕОП обезбедио испуњење пословних циљева и неопходни ниво поузданости ИС. Уговор са пружаоцем услуге подразумева да се дефинишу правила и процедуре које се односе на безбедност и заштиту података када се спроводи развој или одржавање ИС. Правила и процедуре за безбедност и заштиту података обухватају контролне механизме приступа подацима, обраде података и надзора над коришћењем података. Важан аспект односа са пружаоцем услуга је и обезбеђивање континуитета пословања а тиме и наставак коришћења ИС у случају отказа или непродужења уговора са пружаоцем услуге.

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

Налаз 3.1: РФЗО није успоставио (уредио) однос са пружаоцем услуга одржавања ИС МЕОП у делу дефинисања нивоа доступности и врсте информација, средстава којима могу приступити пружаоци услуга, начина приступа информацијама и средствима и надзора над приступом.

РФЗО је дужан да споразумом регулише обавезе пружаоца услуге у вези са информацијама и средствима која су доступна пружаоцима услуге (према одредби члана 26 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја).

РФЗО је такође у обавези да именује лице које је:

- задужено за праћење реализације пружања услуга и контролу испуњености нивоа информационе безбедности (према одредби члана 27 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја).
- одговорно за информациону безбедност и контролу приступа и надзора над извршењем уговорних обавеза, као и поштовање одредби правилника којима су такве активности дефинисане (према одредби члана 30 Акта о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање).
- одговорно за информациону безбедност које редовно прати, анализира, преиспитује и проверава извршене услуге и усаглашеност са уговореним услугама (према одредби члана 31 Акта о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање).

РФЗО није дефинисао правила и процедуре којима се уређује сарадња са пружаоцем услуге одржавања ИС МЕОП, у делу нивоа доступности и врсте информација којима може да приступи пружалац услуге, начине приступа информацијама и средствима и надзора над приступом. Регулисање односа са пружаоцем услуга одржавања ИС МЕОП у овом делу подразумева управљање информационом безбедношћу за шта је потребно јачати кадровске капацитете и стручна знања.

Као што смо навели у Налазу 2.2 овог извештаја, информациона безбедност није кадровски успостављена у РФЗО, што може имати утицаја на реализацију уговора о

одржавању ИС МЕОП, квалитет извршених услуга, контролу приступа ИС, надзор над извршењем уговорних обавеза и заштиту података.

Мере заштите ИКТ система су уређене одредбама члана 7 Закона о информационој безбедности. Оператор ИКТ система одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система. Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

Мере заштите ИКТ система се, између осталог, односе на:

- заштиту средстава оператора ИКТ система која су доступна пружаоцима услуга (став 3 тачка 25) и
- одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга (став 3 тачка 26).

Према одредбама члана 26 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, оператор ИКТ система у својим процедурама предвиђа:

- ниво доступности и врсту информација и средства којима могу да приступе пружаоци услуга,
- начине приступа информацијама и средствима и
- надзор над приступом.

Оператор ИКТ система треба да идентификује и успостави процедуре безбедности информација које се конкретно баве приступом информацијама пружаоца услуга унутар организације (члан 26 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја).

Обавезе пружаоца услуга у вези са информацијама и средствима која су доступна пружаоцима услуга оператора ИКТ система, регулишу се споразумом између оператора ИКТ система и пружаоца услуга, чијим одредбама се обезбеђује адекватан ниво заштите информација и средстава, у складу са прописима и техничким стандардима (члан 26 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја).

Оператор ИКТ система дужан је да обезбеди да пружалац услуга обавља поверене активности у складу са актом о безбедности ИКТ система, односно другим актима којима се уређује безбедност његовог информационог система (члан 26 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја).

Према одредбама члана 27 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, у циљу одржавања уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга, оператор ИКТ система успоставља механизме надзора над пружањем услуга, именује лице које је задужено за праћење реализације пружања услуга и контролу испуњености нивоа информационе безбедности, применом одговарајућих процедура и успоставом надзора.

Према одредбама члана 27 Акта о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање, заштита података који се преносе комуникационим средствима унутар РФЗО, између РФЗО и лица ван РФЗО, обезбеђује се утврђивањем одговарајућих правила, процедура, потписивањем уговора и споразума, као и применом адекватних контрола. У оквиру истог члана дефинисани су споразуми о

поверљивости или не откривању који за циљ имају заштиту информација РФЗО и обавезују потписнике да информације штите, користе и објављују их на одговоран и ауторизован начин.

Према одредбама члана 30 Акта о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање, уговори који се закључују са пружаоцима услуга који имају приступ информацијама, средствима или опреми за обраду информација РФЗО морају садржати уговорну одредбу о заштити и чувању поверљивости информација, података и документације. Такође је дефинисано да РФЗО успоставља контролу безбедности информација које се односе на процесе и процедуре које ће спроводити пружаоци услуга.

Пре отпочињања преговора, потенцијални пружалац услуга у обавези је да потпише изјаву о поверљивости и заштити података, информација и документације, која садржи обавезу за пружаоца услуге да достављене или на други начин учињене доступним информације и подаци могу бити коришћени искључиво на начин претходно одобрен од стране РФЗО, а за потребе извршења предмета преговора. Изјава о поверљивости, односно уговор о пружању услуга треба да садржи одредбу о поверљивости са јасно утврђеним обавезама и одговорношћу пружаоца услуге уз претњу раскидом уговора и накнаде штете у корист РФЗО-а у случају повреде ове одредбе. Пружаоци услуга дужни су да захтеве РФЗО у погледу безбедности информација прошире и на своје подуговараче за додатне услуге или производе. Лице одговорно за информациону безбедност је одговорно за контролу приступа и надзор над извршењем уговорних обавеза, као и поштовање одредби правилника којима су такве активности дефинисане (члан 30 Акта о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање).

Према члану 31 Акта о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање, када је у питању одржавање и обезбеђивање уговорног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга, РФЗО успоставља мере надзора и заштите за време пружања услуга и након извршеног посла.

Лице одговорно за информациону безбедност редовно прати, анализира, преиспитује и проверава извршене услуге и усаглашеност са уговореним услугама. Такође је предвиђено да приликом закључења уговора са пружаоцем услуга неопходно јасно дефинисати квалитативне, оперативне и финансијске критеријуме оцене; утврдити поступак извештавања, праћења и поступања у складу са захтевима РФЗО у поступку извршења уговорених услуга и извршити оцену извршених услуга и квалитета пружаоца услуга (члан 31 Акта о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање).

У поступку ревизије утврђено је да је РФЗО усвојио процедуре којима се ближе уређују услови екстернализације услуга (пружање услуга од стране добављача), а што је предвиђено чланом 26 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја и то:

1. Политика за „аутсорс“ (референтни број: ПОЛ-1024);
2. Политика контроле приступа рачунарској мрежи (референтни број: ПОЛ-1015).

Политика за „аутсорс“, референтни број ПОЛ 1024

Политика за „аутсорс“ описује начин контролисања „аутсорс“ фирми како би се максимално умањио ризик. Према одредбама политике, организација може да „аутсорсује“ више врста услуга (софтвер и хардвер, пројектовање и развој ИТ система, дизајн, ФТО, финансијске услуге, итд). Политиком су прописани уговори и изјаве о поверљивости између РФЗО и „аутсорс“ фирме како би се обе стране заштитиле. Уговор треба да садржи дефинисане типове информација које ће се размењивати, као и сврху њихове размене. Уколико су информације које се размењују осетљиве, у уговору ће бити дефинисана и изјава о поверљивости информација између РФЗО и „аутсорса“. Информације ће бити поверљиве и контролисане у складу са политиком РФЗО. Било која информација коју РФЗО добије од „аутсорса“ биће заштићена изјавом о поверљивости. Пре раскида уговора, поверљивост ће се проверити како би се утврдило да ли треба да се додатно прошире услови наведени у уговору. Даље је политиком дефинисано да у зависности од процене ризика, разне додатне контроле могу бити додате у уговор:

- Правне, регулаторне или друге обавезе трећих лица, као што су заштита/поверљивост података и слично;
- Обавезе и контролисање заштите и сигурности информација као што су:
  - Политике, процеси, стандарди и упутства за заштиту информација које се налазе у оквиру ИСМС-а[87];
  - Провера запослених или трећих лица која раде по уговору;
  - Контрола приступа како би се забранило неовлашћено откривање, модификација или уништавање информација, укључујући физичке и логичке контроле приступа, процедуре за додељивање, ревидирање, ажурирање и укидање приступа систему, подацима, просторијама и слично;
  - Процедуре за управљање инцидентима у циљу заштите и сигурности информација, укључујући обавезно пријављивање инцидената;
  - Враћање или уништавање ресурса од стране „аутсорса“ по завршетку активности или када имовина није више потребна за даље обављање „аутсорс“ активности;
  - Права, патенти и друга заштита интелектуалне својине која се дели са „аутсорсом“ или је „аутсорс“ развија наводи се као део захтева у уговору;
  - Управљање променама у ИТ окружењу, укључујући управљање рањивошћу, закрпама и верификацију контрола сигурности система пре стављања у продукцију;
- Споразум о континуитету пословања, укључујући управљање кризним ситуацијама, инцидентима и опоравком.

Политика контроле приступа рачунарској мрежи, референтни број ПОЛ-1015

Политика контроле приступа рачунарској мрежи усвојена је дана 20.6.2013. године (последња верзија[88]) и описује сигурносне захтеве за спољни (удаљени) приступ рачунарској мрежи и покрива широк спектар технологија укључујући мобилне телефоне, модемско повезивање и VPN (virtual private network) приступ.

Приступ рачунарској мрежи РФЗО од стране запослених или овлашћених трећих лица (владиних или невладиних) са удаљене локације (укључујући кућу, хотелске собе,

[87] Information security management system.
[88] верзија. 2.00, заводни број: 54-2913/12-85.

канцеларије клијената или VPN конекције преко интернета), морају бити одобрене пре него што се технички омогући успостава конекције. Та врста удаљеног приступа није неопходна у свим случајевима и одобрење може у сваком тренутку бити повучено уколико дође до нежељених последица и/или неусаглашености са сигурносним политикама РФЗО (тачка 4 политике).

Према тачки 5 политике, у строго контролисаним условима, РФЗО ће дозволити трећим лицима (који су дефинисани као добављачи, односно произвођачи хардвера/софтвера, запослени по уговору и друга лица која нису стално запослена у РФЗО**)** да приступе рачунарској мрежи РФЗО. Власник информација за чије информације је треће лице добило одобрење приступа биће обавештен и даће формално одобрење за приступ трећем лицу пре него што га оно успостави. Процес доношења одлуке за одобравање права приступа може да укључи и проверу контрола система који ће се повезати, сигурносне политике трећег лица и резултате провере самог трећег лица. Привилегије за трећа лица ће бити строго ограничене на системе и информације које су потребне да би се спровели предефинисани пословни циљеви или задаци.

Према тачки 7 политике, сва трећа лица која желе да удаљено приступе рачунарској мрежи РФЗО односно тачно одређеним компјутерима/серверима морају да потпишу или на други начин дају изјаву о прихватању обавеза и услова коришћења пре него што им се изда кориснички налог. Уколико одређено треће лице већ има кориснички налог за приступ рачунарској мрежи, такође ће морати да прихвате/потпише изјаву пре него што му се обнови кориснички налог. Потписивање изјаве о прихватању обавеза и услова коришћења значи да је корисник разумео и пристао да поштује политике и процедуре РФЗО које су у вези са информационом сигурношћу.

РФЗО је доставио Уговор бр. 18-1/22[89] о пружању услуге одржавања софтверских система РФЗО за партије 1-11. Одредбама члана 3 став 2 наведеног уговора, уређено је да се извршилац обавезује да уз рачун из става 1 тог члана, РФЗО односно организационој јединици РФЗО достави извештај који садржи опис и обим извршене услуге, место и време извршења услуге, као и број непосредно ангажованих извршилаца, за сваку појединачно извршену услугу у претходном месецу, за који РФЗО даје сагласност. Према ставу 3 наведеног члана, уколико извршилац у претходном месецу није извршио ниједну појединачну услугу, уз испостављени рачун доставља извештај који садржи напомену да у претходном месецу није извршио ниједну појединачну услугу.

У поступку ревизије извршен је увид у рачун[90] за извршене услуге одржавања ИС МЕОП за месец октобар 2022. године привредног субјекта „Soneco d.o.o.“. У прилогу наведеном рачуну, достављен је и „Извештај о активностима тима Soneco d.o.o. за период од 1.10.2022. до 31.10.2022. године, а по уговору бр. 18-1/22“, који садржи, између осталог преглед активности на основу Ticket система и преглед активности ван Ticket система. Међутим, наведени извештај не садржи број непосредно ангажованих извршилаца за сваку појединачно извршену услугу у претходном месецу, за који РФЗО даје сагласност.

РФЗО је у обавези да:

- успостави механизме надзора над пружањем услуга,

[89] датум: 3. фебруар 2022. године.
[90] број: 5213-2022-TU-0374 од 31. октобра 2022. године, испостављен на основу Уговора бр. 18-1/22 од 3. фебруара 2022. године.

- именује лице које је задужено за праћење реализације пружања услуга и контролу испуњености нивоа информационе безбедности,
- именује лице које ће бити одговорно за контролу приступа и надзор над извршењем уговорних обавеза, као и поштовање одредби правилника којима су такве активности дефинисане (одговорно лице за информациону безбедност),
- да редовно прати, анализира, преиспитује и проверава извршене услуге и усаглашеност са уговореним услугама (одговорно лице за информациону безбедност).

У поступку ревизије смо утврдили да РФЗО и пружалац услуге одржавања ИС МЕОП сваке године закључују уговор о пружању услуге одржавања софтверских система РФЗО. Осим уговора, РФЗО и пружалац услуге нису закључили споразум чијим би се одредбама обезбедио адекватан ниво заштите информација и средстава, у складу са прописима и техничким стандардима.

Регулисање односа са пружаоцем услуга одржавања ИС МЕОП у овом делу подразумева управљање информационом безбедношћу. Као што смо навели информациона безбедност није кадровски успостављена у РФЗО, што може имати утицаја на реализацију уговора о одржавању ИС МЕОП, квалитет извршених услуга, контролу приступа ИС, надзор над извршењем уговорних обавеза и заштиту података.

Препоручујемо Републичком фонду за здравствено осигурање да успостави правила и процедуре сарадње са пружаоцем услуга развоја и одржавања ИС МЕОП, што подразумева дефинисање нивоа доступности и врсте информација, средстава којима могу приступити пружаоци услуга, начина приступа информацијама и средствима и надзора над приступом.

Налаз 3.2: РФЗО је обезбедио заштиту осетљивих података о осигураницима тако да врши псеудонимизацију података базе МЕОП.

ИС МЕОП је основни информациони систем РФЗО и саставни део ИЗИС-а (према одредби члана 44 став 2 Закона о здравственој документацији и евиденцијама у области здравства). ИЗИС чине здравствено-статистички систем, информациони систем организација здравственог осигурања и информациони системи здравствених установа, приватне праксе и других правних лица.

Институт за јавно здравље РС „Др Милан Јовановић Батут“ је руковалац подацима који чине ИЗИС (члан 44 став 1 Закона о здравственој документацији и евиденцијама у области здравства).

РФЗО и ЗУ, као обрађивачи података, у обавези су да за поверавање обраде података трећој страни добију сагласност од Института за јавно здравље „Др Милан Јовановић Батут“ (према одредбама члана 45 став 2 Закона о заштити података о личности). Између РФЗО и ЗУ, у делу матичне евиденције осигураника постоји однос зависности. ЗУ има могућност приступа ИС МЕОП, ради провере матичних података осигураника.

Представници РФЗО су навели да пружалац услуге одржавања ИС МЕОП не врши обраду података о личности, већ врши псеудонимизацију базе података МЕОП.

У поступку ревизије одржали смо састанак са представницима привредног друштва „Soneco“ доо (пружалац услуге одржавања ИС МЕОП) на коме нам је презентован модул за псеудонимизацију података базе МЕОП.

Закон о заштити података о личности

Према одредбама члана 4 став 1 Закона о заштити података о личности[91], поједини изрази у овом закону имају следеће значење:

1) „податак о личности“ је сваки податак који се односи на физичко лице чији је идентитет одређен или одредив, непосредно или посредно, посебно на основу ознаке идентитета, као што име и идентификациони број, података о локацији, идентификатора у електронским комуникационим мрежама или једног, односно више обележја његовог физичког, физиолошког, генетског, менталног, економског, културног и друштвеног идентитета;

2) „лице на које се подаци односе“ је физичко лице чији се подаци о личности обрађују;

3) „обрада података о личности“ је свака радња или скуп радњи које се врше аутоматизовано или неаутоматизовано са подацима о личности или њиховим скуповима, као што су прикупљање, бележење, разврставање, груписање, односно структурисање, похрањивање, уподобљавање или мењање, откривање, увид, употреба, откривање преносом, односно достављањем, умножавање, ширење или на други начин чињење доступним, упоређивање, ограничавање, брисање или уништавање (у даљем тексту: обрада).

Према одредбама члана 42 став 1 Закона о заштити података о личности, узимајући у обзир ниво технолошких достигнућа и трошкове њихове примене, природу, обим, околности и сврху обраде, као и вероватноћу наступања ризика и ниво ризика за права и слободе физичких лица који произилазе из обраде, руковалац је приликом одређивања начина обраде, као и у току обраде, дужан да:

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

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

Осим тога, одредбама члана 42 став 2 Закона о заштити података о личности прописано је да је руковалац дужан да сталном применом одговарајућих техничких, организационих и кадровских мера обезбеди да се увек обрађују само они подаци о личности који су неопходни за остваривање сваке појединачне сврхе обраде. Та се обавеза примењује у односу на број прикупљених података, обим њихове обраде, рок њиховог похрањивања и њихову доступност.

Такође, одредбама члана 42 став 3 Закона о заштити података о личности прописано је да се овим мерама мора увек обезбедити да се без учешћа физичког лица подаци о личности не могу учинити доступним неограниченом броју физичких лица.

Према одредбама члана 45 став 1 Закона о заштити података о личности, ако се обрада врши у име руковаоца, руковалац може да одреди као обрађивача само оно лице или орган власти који у потпуности гарантује примену одговарајућих техничких, организационих и кадровских мера, на начин који обезбеђује да се обрада врши у складу са одредбама овог закона и да се обезбеђује заштита права лица на које се подаци односе.

Према одредбама члана 45 став 2 Закона о заштити података о личности, обрада се може поверити другом обрађивачу само ако га руковалац за то овласти на основу општег или

[91] „Службени гласник РС“, бр. 87/18.

посебног писменог овлашћења. Ако се обрада врши на основу општег овлашћења, обрађивач је дужан да информише руковаоца о намераваном избору другог обрађивача, односно о замени другог обрађивача, како би руковалац имао могућност да се супротстави таквој промени.

Према одредбама члана 45 став 3 Закона о заштити података о личности, обрада од стране обрађивача мора бити уређена уговором или другим правно обавезујућим актом, који је закључен, односно усвојен у писменом облику, што обухвата и електронски облик, који обавезује обрађивача према руковаоцу и који уређује предмет и трајање обраде, природу и сврху обраде, врсту података о личности и врсту лица о којима се подаци обрађују, као и права и обавезе руковаоца.

Према одредбама члана 45 став 4 Закона о заштити података о личности, уговором или другим правно обавезујућим актом обрађивач дужан да:

1) обрађује податке о личности само на основу писмених упутстава руковаоца, укључујући и упутство у односу на преношење података о личности у друге државе или међународне организације, осим ако је обрађивач законом обавезан да обрађује податке. У том случају, обрађивач је дужан да обавести руковаоца о тој законској обавези пре започињања обраде, осим ако закон забрањује достављање тих информација због потребе заштите важног јавног интереса;

2) обезбеди да се физичко лице које је овлашћено да обрађује податке о личности обавезало на чување поверљивости података или да то лице подлеже законској обавези чувања поверљивости података;

3) предузме све потребне мере у складу са чланом 50 Закона о заштити података о личности;

4) поштује услове за поверавање обраде другом обрађивачу из члана 45 ст. 2 и 7 Закона о заштити података о личности;

5) узимајући у обзир природу обраде, помаже руковаоцу применом одговарајућих техничких, организационих и кадровских мера, колико је то могуће, у испуњавању обавеза руковаоца у односу на захтеве за остваривање права лица на које се подаци односе из Главе III. тог закона;

6) помаже руковаоцу у испуњавању обавеза из члана 50 и чл. 52 до 55 Закона о заштити података о личности, узимајући у обзир природу обраде и информације које су му доступне;

7) после окончања уговорених радњи обраде, а на основу одлуке руковаоца, избрише или врати руковаоцу све податке о личности и избрише све копије ових података, осим ако је законом прописана обавеза чувања података;

8) учини доступним руковаоцу све информације које су неопходне за предочавање испуњености обавеза обрађивача прописаних овим чланом, као и информације које омогућавају и доприносе контроли рада обрађивача, коју спроводи руковалац или друго лице које он за то овласти.

У случају из члана 45 став 4 тачка 8) Закона о заштити података о личности, обрађивач је дужан да без одлагања упозори руковаоца ако сматра да писмено упутство које је од њега добио није у складу са тим законом или другим законом којим се уређује заштита података о личности.

Одбредбама члана 50 став 1 Закона о заштити података о личности прописана је безбедност обраде тако да у складу са нивоом технолошких достигнућа и трошковима њихове примене, природом, обимом, околностима и сврхом обраде, као и вероватноћом наступања ризика и нивоом ризика за права и слободе физичких лица, руковалац и

обрађивач спроводе одговарајуће техничке, организационе и кадровске мере како би достигли одговарајући ниво безбедности у односу на ризик.

У складу са одредбама члана 50 став 2 Закона о заштити података о личности, према потреби, мере нарочито обухватају: 1) псеудонимизацију и криптозаштиту података о личности; 2) способност обезбеђивања трајне поверљивости, интегритета, расположивости и отпорности система и услуга обраде; 3) обезбеђивање успостављања поновне расположивости и приступа подацима о личности у случају физичких или техничких инцидената у најкраћем року и 4) поступак редовног тестирања, оцењивања и процењивања делотворности техничких, организационих и кадровских мера безбедности обраде.

Према одредбама члана 50 став 3 Закона о заштити података о личности, приликом процењивања одговарајућег нивоа безбедности посебно се узимају у обзир ризици обраде, а нарочито ризици од случајног или незаконитог уништења, губитка, измене, неовлашћеног откривања или приступа подацима о личности који су пренесени, похрањени или обрађивани на други начин.

У складу са одредбама члана 50 став 5 Закона о заштити података о личности, руковалац и обрађивач дужни су да предузму мере у циљу обезбеђивања система по којем свако физичко лице које је овлашћено за приступ подацима о личности од стране руковаоца или обрађивача, обрађује ове податке само по налогу руковаоца или ако је на то обавезано законом.

Закон о здравственој документацији и евиденцијама у области здравства

Према члану 44 став 1 Закона о здравственој документацији и евиденцијама у области здравства, ИЗИС се организује и развија ради планирања и ефикасног управљања системом здравствене заштите, системом здравственог осигурања, као и ради прикупљања и обраде података у вези са здравственим стањем становништва, финансирањем здравствене заштите и функционисањем здравствене службе, док према члану 44 став 2 Закона о здравственој документацији и евиденцијама у области здравства, ИЗИС чине: здравствено-статистички систем, информациони систем организација здравственог осигурања и информациони системи здравствених установа, приватне праксе и других правних лица. Завод за јавно здравље основан за територију Републике Србије је, према члану 44 став 4 Закона о здравственој документацији и евиденцијама у области здравства, руковалац подацима који чине ИЗИС.

Слика број 16: Илустративни приказ система који чине ИЗИС

Политика заштите информација, референтни број ПОЛ-1004

Политика заштите информација усвојена је дана 20.6.2013. године (последња верзија[92]). РФЗО је усвојио ову политику са циљем да сви запослени буду упознати са захтевима и обавезама у вези са заштитом информација, да би се постигао задовољавајући ниво заштите информација.

Према тачки 2.1 наведене политике, све информације се могу класификовати у три категорије: информације од јавног значаја; интерне информације и нарочито осетљиви подаци о личности, док у зависности од класификације односно нивоа поверљивости, различите мере се могу применити да би се информације заштитиле. Четири основне компоненте заштите информација су: Физичка сигурност, Заштита рачунарске опреме, рачунарске мреже и софтвера, Заштита документат и Заштита запослених.

Тачка 2.3 наведене политике, предвиђа да РФЗО рукује нарочито осетљивим подацима о личности и примењује високе мере заштите, као што је ограничена доступност, техничке, кадровске и организационе мере заштите. Примери за нарочито осетљиве податке су лозинке и лични подаци о запосленима, подаци о осигураницима РФЗО, споразуми о поверљивости са корисницима. Нарочито осетљивим подацима рукују запослени који обављају послове остваривања права из обавезног здравственог осигурања, управног поступка, надзорника осигурања, заштитника права осигураних лица, контроле електронске фактуре, лекарских комисија, администратора базе података.

Према тачки 4.5 наведене политике, приступ рачунарској мрежи РФЗО могу имати само запослени, док за екстерне запослене приступ пословној мрежи мора бити одобрен од стране директора Сектора за развој и ИТ и директора Сектора за здравствено осигурање и правне послове, а на предлог директора сектора у Дирекцији РФЗО или директора филијала РФЗО.

Важно је напоменути да се Политика заштите информација позива на одредбе Закона о заштити података о личности[93], који није у примени од 20. августа 2019. године.

Контроле приступа (*извод из Политике за „аутсорс“, референтни број ПОЛ-1024*)

Политиком контроле приступа дефинисано је да су неопходне одговарајуће сигурносне контроле како би се спречио неовлашћени приступ ресурсима РФЗО од стране „аутсорса“. Детаљи контроле зависе од природе ресурса и припадајућих ризика, што имплицира потребу да се изврши процена ризика и осмисли одговарајућа архитектура контрола.

Такође је дефинисано да техничка контрола приступа треба да обухвати: идентификацију и аутентификацију корисника и ауторизацију пре приступа..

Такође је дефинисано да ће РФЗО осигурати да сви информациони ресурси који су доступни „аутсорсу“ током трајања уговора (додатно, све копије које су касније направљене, укључујући бекап и архиве) буду на правилан начин враћени или уништени после одређеног периода након истека или раскида уговора. У случају када су у питању веома поверљиви информациони ресурси, „аутсорс“ мора формално да прихвати одговорност за одређене ресурсе од тренутка преузимања до тренутка враћања.

[92] верзија: 2.01, заводни број: 54-2913/12-74.
[93] „Службени гласник РС“, бр. 97/08, 104/09 - др. закон, 68/12 - одлука УС и 107/12.

Псеудонимизација података у информационом систему МЕОП

У складу са ИКТ стратегијом Републичког фонда за здравствено осигурање – Стратегија развоја и дефинисаном „high-level“ архитектуром система, РФЗО је имао потребу за унапређењем и проширењем ИС цМЕОП, који ће обезбедити ефикасан рад на пословима вођења централне евиденције осигураника и осигураних лица, као и евидентирању и контроли остваривања права.

Представници РФЗО су на питање тима за ревизију да ли је извршена имплементација Модула за псеудонимизацију, изјавили да се модул за псеудонимизацију података базе ИС МЕОП користи за формирање базе за тест окружење, као што је и предвиђено документацијом новог ИС МЕОП. С тим у вези, РФЗО је у 2020. години спровео јавну набавку под називом „Услуга развоја софтверског система за матичну евиденцију и остваривање права РФЗО уз реинжењеринг постојећих пословних процеса и алгоритама на којима се заснивају сви подсистеми остваривања права на здравствену заштиту осигураних лица“.[94] Уговор о јавној набавци додељен је „Unicom-Telecom“ d.o.o. као представнику понуђача у заједничкој понуди: „Unicom-Telecom“ d.o.o, „Heliant“ d.o.o, „Soneco“ d.o.o. и „Infolab“ d.o.o.

Увидом у конкурсну документацију (страна 10 од 41) поменуте јавне набавке, утврђено је да је у оквиру исте предвиђен „модул за псеудонимизацију података базе МЕОП“, који се за формирање базе за тест окружење. Извод из конкурсне документације наводимо у тексту који следи:

„За потребе континуираног одржавања и унапређења ИС Матична евиденција и остваривања права, формирано је и перманентно се одржава тестно окружење. Задатак тестног окружења је да служи за тестирање и прихватање нових и унапређених функционалности система, за репродуковање пријављених грешака са продукционог система, као и за тестирање перформанси система под реалним оптерећењем. Да би се обезбедио реалан обим података за тест окружење потребно је омогућити да се база података тест окружења формира од продукционе базе података, али уз одговарајуће мере заштите података о личности.

Модул за псеудонимизацију података треба да има идентификоване све типове података о личности и одређене технике за заштиту сваког од тих типова. Модул треба да обезбеди обраду копије базе са циљем да се формира нова база у којој ће адекватно бити заштићени подаци о личности. Обрада базе података мора да као резултат има базу која је истог обима као и улазна база и да је очувана логичка конзистенција података у складу са правилима пословних процеса.

Перформансе модула морају да омогуће да се формирање нове базе тест окружења обавља како у редовним циклусима, тако и према ванредним потребама, а да период недоступности тест окружења при новом формирању буде мањи од 6 сати.“

Према наводима представника РФЗО, тестно окружење се користи у свакодневном раду за тестирање и прихватање нових и унапређених функционалности, репродуковање пријављених грешака са продукционог система и тестирање перформанси под реалним оптерећењем. Псеудонимизација базе на тесту се врши након „освежавања“ подацима са продукције (RESTORE DATABASE), када се сви идентификовани лични подаци у бази псеудонимизују.

У поступку ревизије одржали смо састанак са представницима привредног друштва „Soneco“ доо (пружалац услуге одржавања ИС МЕОП) на коме нам је презентован модул за псеудонимизацију података базе МЕОП. Путем видео линка представници

[94] редни број јавне набавке у 2020. години: 404-1-208/20-50.

привредног друштва „Soneco“ доо су нам објаснили коришћење три окружења ИС и то: тестног, развојног и продукционог и процеса псеудонимизације података.

Представници привредног друштва „Soneco“ доо су навели да техника „псеудонимизације“ мора да буде увек присутна у пракси „освежавања података“ развојне базе. База података развојног окружења представља копију тестног окружења РФЗО, а база развојног окружења се повремено ажурира тако што се повуку подаци из продукцијске базе РФЗО, али се подаци обавезно претходно псеудонимизирају (примењујући различите алгоритме). Такође су навели и да, када се ради псеудонимизација података, псеудонимизирају (маскирају) се обавезно следећи подаци: име, презиме и средње име осигураника. Од преосталих података као што је ЛБО и ЈМБГ, маскира се ЈМБГ (применом различитих алгоритама), док се ЛБО не маскира.

Уговор о пружању услуге одржавања софтверских система РФЗО[95]

Према одредбама члана 9 уговора, извршилац се обавезује да поверљиве информације које је сазнао у вези са извршењем овог уговора неће користити у друге сврхе, осим за испуњење уговорних обавеза, као и да их неће открити трећем лицу, осим уколико је то неопходно за извршење предмета овог уговора, уз претходну сагласност РФЗО.

Обавеза из става 1 тог члана не односи се на информације које је извршилац дужан да саопшти у складу са позитивноправним прописима.

У случају да дође до откривања поверљивих информација без претходне сагласности РФЗО, извршилац је дужан да без одлагања о томе обавести РФЗО, а у случају да је РФЗО том приликом претпрео штету, извршилац је дужан да је надокнади.

Одговорна лица РФЗО нису доставила уговоре о обради података о личности закључене у 2020, 2021. и 2022. години са пружаоцем услуге одржавања ИС МЕОП. Одговорна лица РФЗО су навела да се наведени уговори не закључују са пружаоцем услуге одржавања ИС МЕОП из разлога што пружалац наведене услуге не врши обраду података о личности.[96]

Као што је објашњено у Налазу 1.3 овог извештаја, тим за ревизију одржао је састанак са КБЦ Земун. Том приликом, извршен је увид у здравствени информациони систем „Heliant Health”, који ова ЗУ користи у раду. Тим за ревизију покушао је да приступи матичној бази осигураника, уносом само једног параметра у информациони систем „Heliant Health”. Приступ је био омогућен, иако није била физички учитана КЗО. Имајући у виду чињеницу да поменути осигураник никада није користио здравствене услуге у КБЦ Земун, поставља се питање како је омогућен приступ подацима матичне евиденције поменутог осигураника, а да претходно није учитана КЗО. Према наводима запослених лица у КБЦ Земун, КБЦ Земун од децембра 2021. године користи „Heliant Health“ информациони систем, па је могуће да је, приликом инсталације новог информационог система, испоручилац софтвера извршио интеграцију са постојећом (ажурном) базом података из неке друге ЗУ.

ИЗИС чине здравствено-статистички систем, информациони систем организација здравственог осигурања и информациони системи здравствених установа, приватне праксе и других правних лица. Институт за јавно здравље РС „Др Милан Јовановић Батут“ је руковалац подацима који чине ИЗИС.

[95] 03/5 број: 404-1-106/21-12 од 3. фебруара 2022. године.
[96] Одговор РФЗО на питање да ли потписују уговор о обради података о личности са пружаоцем услуге одржавања информационог система МЕОП.

РФЗО и ЗУ, као обрађивачи података, у обавези су да за поверавање обраде података трећој страни добију сагласност од Института за јавно здравље „Др Милан Јовановић Батут“, (према одредбама Закона о заштити података о личности). Између РФЗО и ЗУ у делу матичне евиденције осигураника постоји однос зависности. ЗУ има могућност приступа ИС МЕОП ради провере матичних података осигураника.

Према изјави одговорних лица РФЗО, пружалац услуге одржавања ИС МЕОП не врши обраду података о личности, већ се врши псеудонимизација базе података МЕОП.

Налаз 3.3: РФЗО није предвидео мере које обезбеђују континуитет пословања у случају прекида сарадње са пружаоцем услуге одржавања ИС МЕОП.

Према одредбама члана 7 Законом о информационој безбедности, прописано је, између осталог да оператор ИКТ система одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система. Мере заштите ИКТ система односе се и на континуитет пословања у ванредним околностима (Закон о информационој безбедности).
Такође, одредбама члана 29 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, прописане су мере које обезбеђују континуитет обављања посла у ванредним околностима.
Мерама заштите ИКТ система се обезбеђује превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима. За РФЗО је од великог значаја анализа процеса континуитета пословања у случају прекида сарадње са пружаоцем услуге одржавања ИС МЕОП.

РФЗО је знатно зависан од добављача, тј пружаоца услуге развоја и одржавања ИС МЕОП и у случају раскида/отказа уговора, РФЗО у дужем временском периоду неће бити у стању да врши неопходне измене ИС МЕОП. Такође, у уговору о одржавању ИС МЕОП није дефинисан миграција података у случају да РФЗО промени пружаоца услуга развоја ИС.

Поред тога што је то законска обавеза, план континуитета пословања пружа значајан одговор на ризике који постоје у вези са губитком података и треба да буде успостављен и периодично тестиран. Ризик је већи када је у питању раскид сарадње са пружаоцима услуга одржавања информационог система, јер у том случају недостаје неопходно знање потребно за наставак одржавања и развоја, а нарочито у случају потенцијалног преласка на нови систем и неопходну миграцију података.

Према одредбама члана 7 Законом о информационој безбедности, прописано је, између осталог да оператор ИКТ система одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система. Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима. Према одредбама члана 7 став 3 тачка 28) Закона о информационој безбедности, мере заштите ИКТ система односе се на мере које обезбеђују континуитет обављања посла у ванредним околностима.

Одредбама члана 29 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, прописане су мере које обезбеђују континуитет обављања посла у ванредним околностима и то:

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

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

За РФЗО је од великог значаја анализа процеса континуитета пословања у случају прекида сарадње са пружаоцем услуге одржавања информационог система МЕОП.

План континуитета пословања треба да обухвати: донета правила и процедуре које уређују континуитет пословања, успостављање плана опоравка од катастрофе, управљање резервним копијама и тестирање ових планова и резервних копија.

РФЗО има усвојен План и стратегију континуитета пословања Дирекције РФЗО[97], усвојен 11. новембра 2022. године. Сврха овог документа је да се одреди начин на који ће РФЗО осигурати све предуслове да може наставити са пословањем у случају кризних ситуација.

Према тачки 3 Политике континуитета пословања, а у складу са анализом утицаја на пословање, утврђене су критичне функције и сервиси који представљају приоритет за очување и које је потребно у кризним ситуацијама прво вратити, и то: непрекидно напајање електричном енергијом; непрекидна веза ка сервис провајдеру телекомуникационих услуга; отказ у раду активне мрежне опреме; отказ у раду сервера; отказ у рада storage уређаја. Сагласно тачки 3.2 наведене политике, сценарији који потенцијално могу да угрозе критичне функције и обухваћени су у процесу управљања континуитетом пословања: прекид у снабдевању електричном енергијом услед квара или испада мреже; прекид у пружању услуга провајдера телекомуникационих услуга услед квара или испада мреже; прекид рада активне мрежне опреме услед квара; прекид рада сервера услед квара; прекид рада сториџ (storage) уређаја услед квара.

Према тачки 3.3 наведеног документа, сврха Плана опоравка од хаварије је да се, за случај појаве хаварије или другог прекида у пословању, детаљно одреди на који начин ће РФЗО опоравити ИТ инфраструктуру и ИТ услуге у заданом року.

РФЗО у Политици континуитета пословања није предвидео као могућност непродужење/раскид уговора са пружаоцем услуга одржавања ИС, односно начин наставка пословања у измењеним/отежаним условима.

ИС МЕОП инсталиран је и ради на серверу који се налази у РФЗО.

Увидом у Уговор о услузи одржавања дела софтверских система РФЗО за 2022. годину[98] (који се односи на партију 1 - М1: Матична евиденција и остваривање права), чланом 18 уговорено је да се исти може раскинути са отказним роком од 30 дана од дана достављања писаног обавештења о отказу другој уговорној страни, као и да наручилац има право једностраног раскида уговора у свако доба и без отказног рока, уколико извршилац не извршава уговорене обавезе на уговорени начин, о чему ће писмено

[97] верзија: 2.00, заводни број: 54-2913/12-105.
[98] број: 404-1-106/21-12 од 3. фебруара 2022. године.

обавестити извршиоца. Другим речима, није прописана обавеза пружаоца услуге одржавања ИС МЕОП да обезбеди континуитет пословања за ИКТ системе.

На тај начин, присутан је ризик да у случају једностраног раскида од стране пружаоца услуге одржавања ИС МЕОП, РФЗО неће бити у могућности да одржава и даље развија ИС МЕОП на начин да тај информациони систем прати промене у пословању РФЗО. Из тог разлога, потребно је обезбедити да план континуитета пословања обухвати и случај прекида сарадње са пружаоцем услуге одржавања ИС.

На основу прикупљених података и обављене анализе, може се закључити да континуитет пословања није на адекватан начин успостављен у РФЗО у делу сарадње са пружаоцима услуга, а посебно ИС МЕОП-а као основног информационог система у РФЗО. Поред тога што је то законска обавеза, план континуитета пословања пружа значајан одговор на ризике који постоје у вези са губитком података и треба да буде успостављен и периодично тестиран. Ризик је већи када је у питању раскид сарадње са пружаоцима услуга одржавања информационог система, јер у том случају недостаје неопходно знање потребно за наставак одржавања и развоја, а нарочито у случају потенцијалног преласка на нови систем и неопходну миграцију података.

Препоручујемо Републичком фонду за здравствено осигурање да предузме активности у циљу успостављања континуитета пословања у делу измена/доградње информационог система МЕОП и евентуалне миграције података, у случају прекида сарадње са пружаоцем услуге.

V Прилози

Прилог 1 – Методологија у поступку рада

Ревизија је спроведена у складу са Методолошким правилима и смерницама за ревизију сврсисходности пословања.

Да бисмо одговорили на ревизијска питања, анализирали смо законску и подзаконску регулативу, користили стручну литературу (WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions 15), Методолошка правила и смернице за ИТ ревизију као и све податке добијене од субјекта ревизије и извора информација – здравствених установа. Анализирали смо податке и информације за период од 2020. до 2023. године. На основу прикупљених података у току предстудије и у складу са Приручником за спровођење ревизије, одабране су три ИТ области у оквиру којих су обављени поступци ревизије: ИТ управљање, Информациона безбедност и Сарадња са пружаоцем услуга.

ИТ области

ИТ области						
ИТ управљање	Развој и набавка	ИТ операције	Сарадња са пружаоцима услуга	План континуитета и опоравка	Информациона безбедност	Апликативне контроле

У фази планирања ревизије, са представницима РФЗО смо обавили разговор (интервју) на којем су постављена следећа питања:

1. Информациони системи који се користе у обављању пословне делатности РФЗО
* тражен је списак информационих система које РФЗО користи у свом раду

2. Описати намене за које се користе информациони системи из претходног питања
* тражена су корисничка упутства за све информационе системе који се користе у раду РФЗО

3. Да ли је задржан децентрализовани приступ организовању информационих технологија[1]
* централизација и консолидовање информативног система ствара могућност за уклањање неправилности у раду, повећање информационе безбедности, успостављање ефикасног плана континуитета пословања и ефективнијег и јефтинијег пословања.

4. Да ли постоји IT стратегија или други стратешки документ

5. Да ли се апликација матичне евиденције осигураника (МЕОП) и даље користи
* ради се о софтверу за евиденцију осигураника Фонда и евиденције свих остварених права у систему здравственог осигурања (обрачун и контролу боловања, рад лекарских комисија Фонда, обрачун путних трошкова…
* тражено је упутство за коришћење МЕОП апликације

6. Разлог из ког ЕТФ више није део заједничке понуде одржавања матичне евиденције
* веза: јавна набавка „Услуга одржавања софтверских система РФЗО“ 2021. и 2022. година

7. Да ли је вршена ревизија информационог система у претходном периоду (IT ревизија)

8. Уколико је вршена ревизија информационог система, када је последњи пут иста вршена и на коју годину се односи

У току планирања ревизије Републичком фонду за здравствено осигурање послат је и упитник са следећим питањима.

I. ИТ управљање

- Да ли организација има стратешки план (или план највишег нивоа управљања) којим се планира употреба и развој ИТ капацитета?
- Наведите износ буџета за ИТ за 2022. годину.
- Да ли су правилником о унутрашњој организацији и систематизацији радних места обухваћени послови у вези ИТ?
- Наведите организациону јединицу које је надлежна за питања у вези са информационим системом (сектори, одељења, службе…) и број запослених у тој организационој јединици.
- Да ли имате лице које је одговорно за функционисање ИС/ИТ? (лице које обавља функцију CIO-Chief information officer)
- Да ли имате лице које је одговорно за безбедност информационог система? (Лице које обавља функцију CISO-Chief information security officer)
- Да ли вршите обуку запослених у вези са ИТ темама (приступ и коришћење програма, електронска пошта, безбедност…)?
- Да ли су у систему управљања ризицима обухваћени и ИТ ризици?
- Да ли имате интерну ревизију ИС/апликације/ИТ?
- Да ли имате акт којим се уређује процес управљање пројектима који су у вези са ИС/апликацијом/ИТ и ко је задужен за управљање ИТ пројектима у Вашој организацији?

II. Развој и набавка

- Навести најзначајније информационе системе које користите.
- Да ли су информациони системи наведени у одговору на претходно питање, набављени/купљени од екстерног добављача или су развијени интерно (од стране ИТ Сектора)?
- Да ли организација има оперативне планове развоја ИТ капацитета (план, праћење рокова и имплементација пројекта) ?
- Да ли се развој/одржавање информационих система одвија у оквиру Сектора за ИТ РФЗО или се врши екстерна набавка услуге развоја/одржавања?
- Уколико се спроводи интерни развој/одржавање информационих система, да ли имате довољно стручних особа за развој/одржавање истих?
- Да ли је обезбеђена раздвојеност развојног, тестног и продукционог окружења информационих система?
- Да ли се промене у информационим системима које тражите ви као организација документују?
- Да ли се неке од активности које су поверене трећим лицима реализују уз употребу cloud технологија?
- Ко покреће захтеве за набавку или промену/допуну на информационом систему/апликацији?

- Наведите назив радног места са којег се најчешће иницира набавка или промена.
- Да ли су планиране значајније промене на информационим системима у 2023. години и да ли су биле значајне промене на информационим системима у 2021. и 2022. години?

III. ИТ операције

- Да ли постоји ажурна евиденција свих хардверских и софтверских компоненти информационих система?
- Да ли је успостављена функција хелп деска за МЕОП апликацију?
- Ако је одговор ДА, доставите последњи извештај о активностима.
- Да ли се периодично прати и извештава о стању искоришћености ИТ ресурса?
- Да ли имате процедуру за управљање променама у ИС/апликацијама/ИТ?

IV. Уговори са добављачима

- Да ли је уређен процес праћења и анализе квалитета пружених услуга од стране добављача?
- Да ли постоји процедура/акт којим се уређује питања информационе безбедности, заштите пословних или личних података којима имају приступ добављачи услуга (развоја и одржавања информационих система) ?
- Да ли су права за заштиту и приступ подацима уграђени у уговорима о набавци и одржавању информационих система ?
- На који начин и да ли РФЗО обезбеђује континуитет пословних операцију у случају не продужења уговора/престанка пружања услуге од стране добављача?

V. Планови континутета и опоравка

- Да ли постоји План за ванредне ситуације?
- Да ли постоји План континуитета пословања (BCP)?
- Да ли је, у склопу управљања континуитетом пословања, усвојен план опоравка активности у случају хаварије (DRP) или постоји као одвојен план ?
- Да ли се спроводи тестирање планова?
- Да ли постоји посебно задужен тим/ лице за управљање континуитетом пословања ?
- Да ли постоји посебно задужен тим/ лице за управљање активностима у случају хаварије ?
- Да ли су усвојене процедуре и дефинисане одговорности у вези с креирањем резервних копија података?
- Да ли су резервне копије смештене у безбедан простор за одлагање ван објекта?
- Да ли је у последње две године било тежих инцидената који би могли угрозити пословање РФЗО-а или личних података осигураника?

VI. Информациона безбедност

- Да ли сте усвојили Акт о информационој безбедности?
- Да ли је обезбеђено да су сви корисници информационог система упознати са садржином политике безбедности?
- Да ли је ради контроле приступа информационом систему успостављен систем управљања корисничким правима приступа?

- Да ли је омогућен удаљени приступ информационом систему?
- Да ли је обезбеђено генерисање логова свих значајних догађаја и активности у ИС/апликацији/ИТ?
- Да ли се примењује физичко-техничка заштита ресурса ИС (физички приступ, непрекидно напајање електричном енергијом, климатизација…)?
- Да ли се редовно одржавају обуке у циљу едукације запослених у вези са информационом безбедношћу?
- Да ли је обавезна промена корисничких лозинки и колико често се исте мењају?
- Да ли су примењене контроле за заштиту информационог система од малициозног програмског кода (вирус...)?
- Да ли је на рачунарима омогућена употреба екстериних уређаја за складиштење података (DVD, USB fleš, HDD…)

VII. Апликативне контроле

- Да ли право приступа МЕОП апликацији имају само овлашћена лица? (сви запослени, и/или постоје одређена ограничења
- Да ли је могућ извоз података о осигураницима у неким од стандардих формата (excel, word, pdf, hml)
- Да ли је могућ извоз збирних података о осигураницима по неком одређеном критеријуму (нпр дијагноза, годиште осигураника идт) у неким од стандардих формата (excel, word, pdf, hml)
- Да ли је на корисничким рачунарима омогућена употреба штампача (ако је Да у које сврхе?)

Након тога послат је и захтев за допуну података са следећим питањима:

- Шта је од ИТ пројеката предвиђених Финансијским планом за 2022. годину покренуто?
- Шта је од ИТ пројеката предвиђених Финансијским планом за 2023. годину планирано да се спроведе (питање 1002);
- На који период је донета ИКТ Стратегија РФЗО ?
- Да ли је усвојена од стране највишег руководства РФЗО ? (у прилогу доставити одлуку о усвајању).
- Колико је од систематизованих IT радних места попуњено у Дирекцији РФЗО ?
- Колико је од систематизованих IT радних места попуњено у Покрајинском Фонду РФЗО ?
- Колико је од систематизованих IT радних места попуњено по филијалама Дирекције РФЗО ?
- Колико је од систематизованих IT радних места попуњено по филијалама Покрајинског фонда РФЗО ?
- У одговору на питање 1004 навели сте да је Сектор за развој и информационе технологије при Дирекцији РФЗО надлежан за питања у вези са информационим системом, као и да је укупан број информатичара у Сектору 14, док је преостали члан Сектора правне струке. Каква је ситуација у филијалама Дирекције и филијалама Покрајинског Фонда по питању броја запослених информатичара и њихових задужења ?
- Шта је био предмет ревизије у оквиру ревизије Сектора за развој и информационе технологије у 2021/2022. години (питање 1009) ?
- доставити извештај о ревизији

- На питање 4002 (да ли постоји процедура/акт којим се уређује питања информационе безбедности, заштите пословних или личних података којима имају приступ добављачи услуга (развоја и одржавања информационих система)) сте одговорили са „ДА“.
- Да ли се Акт о информационој безбедности (као одговор на питање 6001) сматра процедуром/актом којим се уређује питања информационе безбедности, заштите пословних или личних података којима имају приступ добављачи услуга (развоја и одржавања информационих система) или је то неки други акт ?
- Да ли је Модул за псеудонимизацију базе података имплементиран у оквиру МЕОП система и да ли се користи у свакодневном раду/реалном времену? (питање 4003)
- На који софтверски систем РФЗО се мисли у одговору на питање 4004 („….Како би обезбедио континуитет пословних операција које покрива предметни софтверски систем РФЗО ће морати да дефинише нови пројекат функционалног и технолошког реинжењеринга који ће првенствено технолошки бити савременији и на тај начин сигурно прихватљивији информатичким добављачима.)?
- Да ли је постојао Акт о информационој безбедности пре маја 2022. године ? (питање 6001)
- Да ли постоје процедуре генерисања логова свих значајних догађаја и активности у ИС ?
- На који временски период се логови чувају ? (питање 6005)
- Да ли постоји процедура којом се прописује обавезна промене корисничких лозинки на 30 дана ? (питање 6008)

У току планирања ревизије били смо на састанку у КБЦ Земун, на којем смо разговарали са одговорним лицима за информационе технологије и размотрили следеће области:

1. Извршити увид у здравствени болнички информациони систем који запослени у КБЦ Земун користе у свом раду.

1а. начин на који се МЕОП апликација ажурира подацима из информационог система КБЦ Земун

2. Која је процедура када у КБЦ Земун нестане струје, на који начин се обезбеђује ажурирање болничког информационог система а затим и МЕОП апликације

3. Да ли се користи здравствена исправа (КЗО) приликом провере да ли је осигураник заиста осигуран ?

3а. да ли постоје случајеви да запослени КЗО Земун директно са сајта CROSO проверавају статус осигураног лица ?

4. Да ли се картону осигураника може приступити само уносом ЈМБГ или неког другог параметра?

У току планирања ревизије били смо на састанку и у ДЗ Младеновац, на којем смо разговарали са одговорним лицима за информационе технологије и поставили следећа питања:

1. Извршити увид и тражити објашњење о апликацији „Регистар изабраних лекара“. *Да ли се примењује у раду ДЗ Младеновац? Послати приказ (screenshot) почетне странице апликације и приказ након логовања*
2. Извршити увид у здравствено-информациони систем који запослени у ДЗ Младеновац користе у свом раду.
   информација о тренутку од кад се информациони систем примењује у ДЗ Младеновац.
   Послати приказ екрана почетне стране и стране где се претражује осигураник
3. Да ли постоји (директна) веза између базе информационог система коју користи ДЗ Младеновац и база података које користе друге здравствене установе *(у смислу да лекари ДЗ Младеновац могу да виде податке о здравственим услугама осигураном лицу пруженим у другим домовима здравља/болницама/клиничко-болничким центрима/институтима)* ?
4. Објаснити начин на који се и да ли се МЕОП апликација РФЗО ажурира са подацима из информационог система ДЗ Младеновац *(подаци унети од стране изабраног лекара ДЗ Младеновац о прописаној терапији, боловању, упуту на специјалистичко лечење и сл.).*
   Колико често се то ажурирање ради (на сваких сат времена, два сата, ноћу и сл. ?)
5. Да ли се користи здравствена исправа *(картица здравственог осигурања)* приликом провере да ли је осигураник заиста осигуран?
   да ли се користи читач здравствене картице
   да ли се користи апликација „Преглед картице здравственог осигурања“ (израђена од запослених у Сектору за ИТ РФЗО)
6. Да ли се матичној бази МЕОП или из информационог система ДЗ Младеновац може приступити само уносом ЈМБГ или само уносом неког другог параметра (нпр. ЛБО осигураника) за појединачно осигурано лице ?
7. Да ли запослени, *по учитавању података за конкретног осигураника из МЕОП апликације*, исте могу да извезу и похране на сопствене уређаје који имају могућност складиштења (преносиви рачунари, смарт телефони, USB меморијски дискови)?
8. Да ли се матичној бази МЕОП може приступити само употребом здравствено информационог система ДЗ Младеновац или и на неки други начин (директно логовање на МЕОП)?
9. Да ли су у пракси постојали случајеви и да ли постоје случајеви да запослени ДЗ Младеновац директно на сајту CROSO[99] проверавају статус осигураног лица?
10. Која је процедура када у ДЗ Обреновац нестане струје, на који начин се обезбеђује ажурирање здравствено-информационог система ДЗ Младеновац а затим и МЕОП апликације ?
    да ли установа располаже са UPS уређајима
    да ли установа располаже са агрегатом
11. Да ли се креира и чува лог приступа МЕОП бази матичне евиденције РФЗО од стране запослених ДЗ Младеновац?
    Колико дуго се чува лог приступа МЕОП апликацији ?

На почетку фазе спровођења ревизије обавили смо почетни састанак са представницима РФЗО.

[99] https://portal.croso.gov.rs/criscr/faces/Login.jspx;jsessionid=9NkOliT7WsiBVIUo616oW80mZrxdGLd6mQpElJN3cftzxQpApHm-!-270911603

Обавили смо интервјуе са одговорним лицима РФЗО, као и у филијалама РФЗО које смо посетили у току спровођења ревизије.

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

Ревизијско питање 1:

- Анализа ИТ стратегије или интервјуисање руководства да би се утврдили неопходни ресурси информационог система МЕОП и на који начин су исти утврђени и одобрени.
- Анализа белешки са састанака руководства да би се осигурало да су стратешке ИТ одлуке донете на највишем нивоу.
- Интервјуисање руководства или других одговорних лица да би се утврдило како организација анализира, успоставља приоритете и управља захтевима корисника информационог система.
- Интервјуисање руководства или других одговорних лица за одобравање пројеката да би се утврдило да су они узели у обзир ИТ организационе способности, вештине, ресурсе и обуку, и могућност да се користе нови алати, методе или процедуре.
- Анализа одобрених или одбијених захтева за покретање поступака набавки да би се осигурало да су оне у складу са усвојеном Стратегијом и акционим планом.
- Анализа организационе шеме да би се утврдило да је ИТ организација успостављена на стратешком нивоу.
- Анализа ИТ организационе шеме да би се утврдило да је усклађена тако да пружа потребну подршку и да је у складу са законским обавезама.
- Анализа извештаја о планираним и спроведеним обукама у вези са ИТ темама (укључујући и пратећу документацију која се тиче захтева за одржавање обуке, распореда одржавања и сл.).
- Анализа докумената да би се утврдило да ли су ИТ ризици део општег оквира за управљање ризицима и усклађености.
- Анализа плана за управљање ризицима или осталих докумената да би се осигурало да су одговорности за управљање ризицима јасно и недвосмислено додељене.
- Интервјуисање руководства или преглед белешки са састанака да би се утврдило да је руководство свесно и осталих ризика и да периодично прати њихов статус.

Ревизијско питање 2:

- Анализа да ли Стратегија ИТ безбедност идентификује: улоге и одговорности руководства и свих корисника, свест и обуку о безбедности.
- Анализа да ли акт о безбедности ИКТ система и политике и процедура за ИТ идентификују: улоге и одговорности руководства и свих корисника, свест и обуку о безбедности.
- Анализа механизама (електронске, физичке поште, обука, итд.) да би се осигурало да су правила о безбедности ИТ система дистрибуирана запосленима онда када се ажурирају или када за то постоји потреба.
- Анализа правилника о унутрашњем уређењу и систематизацији радних места у делу који се односи на информациону безбедност (утврђивање да ли је одговорност за ИТ безбедност формално и јасно наведена).
- Анализа извештаја о спроведеним ефективним обукама запослених са темом информационе безбедности (распоред обука, резултати завршних тестова, оцена ефективности обуке).

- Анализа да ли постоји документована процедура за реаговање на безбедносне инциденте и да ли су корисници упознати са процедуром и опасностима од угрожавања безбедности информација.
- Анализа извештаја о безбедносним инцидентима и докумената за праћење како би се утврдило које активности организација предузима када појединци крше безбедносна правила и процедуре.
- Анализа извештаја о безбедносним инцидентима да би се идентификовао број кршења безбедности информација од стране запослених или трећих лица у датом периоду, у циљу процене ефективности правила и процедура.
- Анализа да ли постоји адекватно обучен тим за реаговање у случају инцидента који има адекватан алат, ресурсе и подршку вишег руководства за решавање инцидента
- Анализа процедуралних мера које је организација предузела да би се ускладила са захтевима поверљивости података.
- Анализа матрица улога за утврђивање одговорности за администрирање конфигурације и опсега контроле конфигурације у оквиру информационог система МЕОП.
- Утврђивање да ли су се у прошлости јављали проблеми због конфигурацијских недоследности. Ако је тако, интервјуи са руководиоцима да би се проверило који су поступци примењени при променама конфигурације.
- Анализа процедура у циљу утврђивања колико често се прегледају различити приступи и привилегије које запослени или корисници имају у организацији.
- Одабир узорка корисничких и системских налога да би се утврдило постојање јасно дефинисане улоге и/или привилегије мапиране према функцијама посла као и овлашћење власника података и руководства (тј. потписане/ писане сагласности).
- Интервјуи са узорком корисника и провера упутства да би се утврдило како су корисници упознати са својим одговорностима за заштиту осетљивих информација или имовине, када им се одобри приступ.
- Провера да ли су квалитативни захтеви за лозинке дефинисани и примењени системом за управљање мрежом и/или оперативним системима заснованим на локалним захтевима/ организационим правилима и процедурама или најбољој пракси.
- Анализа документације везане за пријаву и решавање проблема корисника у коришћењу информационог система МЕОП.
- Анализа шта су контроле физичке безбедности субјекта ревизије (заштита од физичких и еколошких ризика, приступи објекту само од овлашћеног особља, борба против упада и сл.). Провера да ли одговарају најновијој анализи ризика.
- Прегледање локацијских и физичких мера предострожности у смислу кључних елемената ИТ инфраструктуре. Провера какве су контроле за заштиту животне средине успостављене (апарат за гашење пожара, аларм, системи за напајање, итд.).
- Провера приватности и безбедности поступања са излазним информацијама и процедура задржавања. Процена да ли су процедуре дефинисане тако да захтевају евидентирање потенцијалних грешака и њихово решавање пре дистрибуције извештаја.
- Провера да ли постоје документоване процедуре за обележавање осетљивих излазних информација апликација и, где је то потребно, слање осетљивих излазних информација на посебне уређаје са контролом приступа.

Ревизијско питање 3:

- Процена да ли организација има адекватна правила и процедуре за ангажовање спољних сарадника (пружалаца услуга).
- Анализа докумената да би се проценило да су израђене детаљне процедуре за одговарајући ниво доступности и врсту информација и средства којима могу да приступе пружаоци услуга, начине приступа информацијама и средствима и надзор над приступом.
- Анализа докумената да би се проценило да правила и процедуре узимају у обзир захтеве за заштиту средстава оператора ИКТ система која су доступна пружаоцима услуга, ради обезбеђивања информационе безбедности.
- Анализа докумената да би се проценило које матрице основних услуга су обухваћене уговором између РФЗО и добављача услуге одржавања ИС МЕОП.
- Преглед или интервјуисање запослених да би се утврдило поштовање акта о информационој безбедности у делу односа са пружаоцем услуга одржавања информационог система МЕОП.
- Анализа да ли уговорни услови и обавезе дефинишу безбедносна ограничења и обавезе које контролишу како ће извођачи користити имовину организације и приступати информационим системима и услугама.
- Анализа захтева за изменом информационог система у циљу сагледавања да ли се приликом измене/ажурирања информационог система примењују правила и процедуре заштите осетљивих података о личности (псеудонимизација, енкрипција и сл.).
- Анализа да ли су добављачи услуге одржавања и развоја ИС МЕОП извршили повреде безбедности информација. Провера активности руководства у погледу таквих кршења.
- Анализа да ли се организација постарала да је континуитет пословања (у смислу задржавања пословног знања и власништва над пословним процесом) садржан у споразуму о пружању услуге са добављачем.
- Анализа да ли је организација упозната са повезаним ризицима код могућег непродужења/отказивања пружања услуге одржавања и развоја ИС МЕОП.

У току спровођења ревизије обишли смо три филијале РФЗО (Београд, Панчево и Зрењанин), одржали састанке са директорима филијала и запосленима у ИТ одељењима и поставили следећа питања:

1. На основу чега се додељују права у цМЕОП апликацији, постоје ли правила и процедуре која се том приликом морају поштовати?
2. Колико има администратора МЕОП апликације у филијали за Град Београд/Панчево/Зрењанин и шта је њихова улога а колико корисника и ко им додељује права приступа МЕОП-у? Ко одређује које роле (улоге) имају корисници и на основу ког документа се та права додељују?
3. Да ли су запослени у филијали упознати са процедурама које се тичу логичког приступа ИКТ систему РФЗО-а ?
4. Која права има администратор филијале по ОБИ обрасцу?
5. Колико често запослени мењају лозинке за приступ МЕОП-у, односно на колико им се мењају лозинке (како се документује промена лозинки)?
6. Која је процедура заступљена у пракси приликом промене лозинке ?
7. Да ли запослени имају приступ свим филијалама или је приступ ограничен само на властиту филијалу (тј. филијалу у којој запослени ради)?

8. Каква је процедуре за активирање новог корисника МЕОП-а, измену права приступа постојећим корисницима, укидање права приступа?
9. Процедура за доделу корисничких и администраторских права.
10. Ко одобрава администраторска права за МЕОП? Дирекција или филијала?
11. Да ли су запослени у филијали похађали обуке везане за ИТ или ИТ безбедност од 2020. до данас ?
12. Лице одговорно за ИТ безбедност у филијали? Коме се обраћају уколико се деси инцидент, хаварија?
13. Да ли запосленима позната Стратегија управљања ризицима? Да ли су били укључени у процену ИТ ризика ?
14. Контрола физичког приступа серверима/базама података и безбедности просторија.