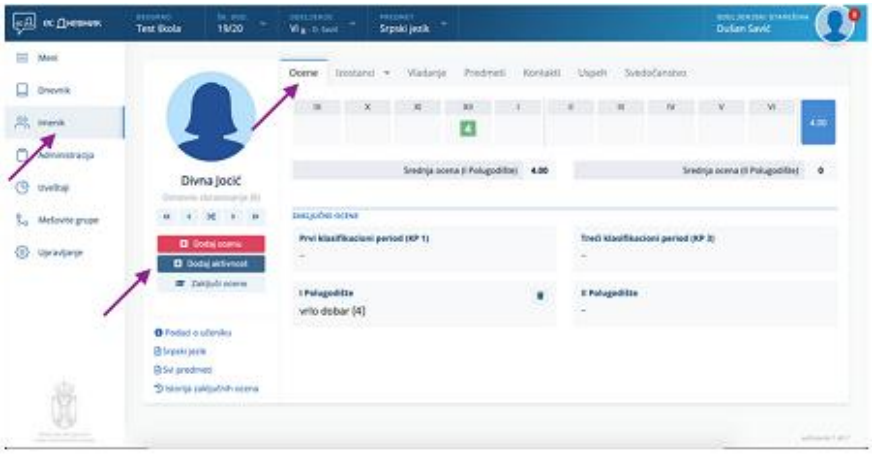
ДРЖАВНА
РЕВИЗОРСКА
ИНСТИТУЦИЈА

ИЗВЕШТАЈ
О РЕВИЗИЈИ СВРСИСХОДНОСТИ ПОСЛОВАЊА
Информациони систем „есДневник“

Број: 400-889/2021-03/06
Београд, 20. децембар 2021. године

ПОТРЕБНО ЈЕ ДА МИНИСТАРСТВО ПРОСВЕТЕ, НАУКЕ И ТЕХНОЛОШКОГ РАЗВОЈА УНАПРЕДИ УПРАВЉАЊЕ ИНФОРМАЦИОНИМ СИСТЕМОМ „есДНЕВНИК“ НА НАЧИН ДА ОБЕЗБЕДИ НЕОПХОДАН НИВО ПОУЗДАНОСТИ СИСТЕМА, И ЊЕГОВ ОДРЖИВИ РАЗВОЈ И ФУНКЦИОНИСАЊЕ

Информациони систем „есДневник“ је успостављен у школској 2018/2019, са циљем вођења евиденције о образовно-васпитном раду, успеху и владању ученика. Пружаоци услуга су „Телеком Србија“ Београд и „Тесла“ доо Загреб. Корисници приступају систему путем web странице. Проблеми који су идентификовани у досадашњем периоду коришћења система су: недовољан број рачунара, застарели рачунари и оперативни системи који су самим тим и небезбедни, није обезбеђено функционисање система у случају раскида сарадње са пружаоцима услуга, пружалац услуге има потпун приступ систему и продукционој бази, обрада података о личности коју врши пружалац услуга није у потпуности успостављена на законом прописан начин, није успостављен процес даљег развоја у складу са предлозима и потребама корисника итд.



У наредном периоду је потребно успоставити **управљање „есДневник“-ом** на начин да се процедурама уреде послови који се односе на овај систем, обезбеди прикупљање и анализа примедби и предлога од стране корисника и ако је потребно изврши надоградња система у складу са тим, а не само у складу са изменама закона, како би систем био ефикаснији, и финансијским плановима и њиховим извршењем омогући замена старих и небезбедних рачунара и оперативних система, и број уређаја прилагоди потребама школа.

Како би **континуитет пословања** у ванредним околностима био свеобухватан, потребно је дефинисати мере које ће обезбедити да систем функционише и у случају раскида сарадње са групом пружаоца услуга, што сада није случај.

Механизам **сарадње са пружаоцима услуга** потребно је уредити одговарајућим процедурама које треба да обезбеде доступност, поверљивост и интегритет података, и контролу примене примењених мера заштите. Такође, обраду података о личности треба уредити на начин заснован на примени законских одредби. Министарство треба да успостави управљање и администрирање информационим системом „есДневник“ на начин који подразумева да само министарство има администраторски приступ систему.

Препоруке

Државна ревизорска институција је након спроведене ревизије Министарству просвете, науке и технолошког развоја, између осталих, дала следеће препоруке:

- да усвоји и имплементира правила и процедуре за безбедност података када је у питању сарадња са пружаоцима услуга, што подразумева обавезну примену мера заштите података и успостављање механизма за праћење примене тих мера, и уреди процес обраде података од стране пружаоца услуга у информационом систему „есДневник“ на законом прописан начин,
- да уреди администрирање и управљање системом на начин да једино МПНТР има администраторска права, док ће пружаоц услуга и корисници моћи да систему приступе једино уз одобрење и контролу администратора,
- да приликом припреме финансијских планова осигура стабилно финансирање циљева кроз детаљно планирање средстава за развој, набавку и одржавање свих компоненти информационог система „есДневник“,
- да успостави континуитет пословања у ванредним околностима на начин да обезбеди функционисање система и у случају прекида сарадње са пружаоцима услуга, а што подразумева неопходан хардвер, апликативни софтвер, изворни код, стручно знање, базе података, управљање резервним копијама података, и процес тестирања планова континуитета пословања.

Садржај

Скраћенице и термини

Табела број 1: Најчешће коришћене скраћенице у извештају

Пун назив	Скраћеница
Јединствени информациони систем просвете	ЈИСП
Јединствени образовни број	ЈОБ
Електронски дневник	есДневник
Министарство просвете, науке и технолошког развоја	Министарство
Министарство просвете, науке и технолошког развоја	МПНТР
Информационе технологије	ИТ
Информациони систем	ИС
Информационо-комуникациони систем	ИКТ систем
Општа регулатива о заштити података о личности "General Data Protection Regulation"	ГДПР
Државна ревизорска институција	ДРИ

I Резиме и препоруке

Државна ревизорска институција је спровела ревизију сврсисходности „Информациони систем „есДневник“.

Информациони систем „есДневник“ је успостављен у школској 2018/2019 године, са циљем вођења евиденције о образовно-васпитном раду, успеху и владању ученика. Годину дана пре успостављања система покренут је пилот пројект у 60 школа у току 2017/2018 године.

Пружаоци услуга су „Телеком Србија“ Београд и „Тесла“ доо Загреб.

По информацијама добијеним у Министарству просвете, науке и технолошког развоја, Апликативни софтвер, као и база података и резервне копије су смештене на серверима у „Телеком Србија“ Београд, док на развоју и одржавању апликације ради фирма „Тесла“ доо Загреб.

Сви корисници приступају систему путем web странице, са одговарајућим функционалностима/извештајима, и дефинисаним правима. Приступ је могућ преко рачунара, али и мобилних уређаја, попут таблета или мобилног телефона. Корисници система су координатори система, директор, наставни кадар, родитељи. Иако је, укључујући и годину дана у којем је имплементиран пилот пројекат, ово четврта година како се систем користи, још увек нису све школе укључене у систем, углавном због недостатака у хардверском делу – рачунара, интернета итд., али и због непостојања вишејезичне подршке у неким срединама.

У току предстудије, и у току коришћења система идентификовани су проблеми везани за недовољан број рачунара, и скоро па половину од укупног броја рачунара који су застарели, узимајући у обзир и оперативни систем који користе, јер су оперативни системи који више немају подршку што се тиче безбедоносних закрпа самим тим и небезбедни, затим, није обезбеђено функционисање система у случају раскида сарадње са пружаоцима услуга, пружалац услуге има потпун приступ систему и продукционој бази, обрада података о личности коју врши пружалац услуга није у потпуности успостављена на законом прописан начин, није успостављен процес даљег развоја у складу са предлозима и потребама корисника итд.

Циљ ревизије је да се оцени ефективност увођења информационог система „есДневник“ у основно и средње образовање у Србији.

Законом о основама система образовања и васпитања, прописано је да Министарство просвете, науке и технолошког развоја Републике Србије обезбеђује функционисање система образовања и васпитања, а нарочито успоставља и управља ЈИСП-ом, и да у оквиру школске управе обезбеђује све услове да установе несметано уносе, попуњавају, ажурирају и одржавају базу података о образовању и васпитању у оквиру ЈИСП-а; Правилником о ЈИСП-у је прописано да Министарство обезбеђује потребне ресурсе за функционисање ЈИСП-а, чији је „есДневник“ практично део. Уколико установа, високошколска установа, установа ученичког и студентског стандарда, односно јавно признати организатор активности води евиденцију у електронском облику у оквиру ЈИСП-а, у складу са овим и посебним законом, Министарство је обрађивач података у погледу администрирања система, чувања и заштите података. Како би се препоруке могле свеобухватно и системски имплементирати, МПНТР је одабрано за субјект ревизије.

У току ревизије је спроведена анкета која је обухватила све школе чије смо контакт податке добили од Министарства просвете, обављен је већи број интервјуа,

анализирано преко 1100 докумената, и коришћени су јавно доступни подаци. У току ревизије школе обухваћене анкетом су биле извори информација.

Након спроведене ревизије утврдили смо:

Потребно је да Министарство просвете, науке и технолошког развоја успостави управљање информационим системом „есДневник“ на начин да обезбеди неопходан ниво поузданости система, и његов одрживи развој и функционисање

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

1. Ефективно управљање информационим системом „есДневник“ није у потпуности успостављено, зато што планирање средстава у ревидираном периоду није обезбедило неопходно инвестиционо улагање у све компоненте информационог система, нису успостављене процедуре за ИТ управљање, и није успостављен адекватни систем хелп-деск услуге, што за последицу има неадекватан и небезбедан хардвер, и отежан даљи развој система у складу са потребама корисника.

Због непостојања детаљних анализа хардверских и софтверских ресурса и потреба школа приликом набавке система и у току његовог коришћења, није обезбеђено стабилно финансирање информационог система „есДневник“, што за последицу има недовољан број рачунара, застареле рачунаре и застареле, самим тим и небезбедне оперативне системе. Како је прописано Законом о основама система образовања и васпитања Министарство обезбеђује потребне ресурсе за функционисање ЈИСП-а, чији је део „есДневник“. (Препорука број 1)

Због непостојања подзаконских прописа који се односе на „есДневник“ и преусмерене приоритетне активности министарства на успостављање ЈИСП-а, нису усвојене процедуре за управљање ИТ пословима, што онемогућава или отежава контролу ових послова од стране руководства или континуитет обављања послова у случају замене запослених на ИТ пословима. (Препорука број 2)

Због тога што МПНТР није успоставило хелп-деск услугу и није успостављена размена података између пружаоца услуга и МПНТР у делу прикупљања и пријављивања проблема и захтева за изменама система од стране корисника, није успостављен процес измене информационог система у складу са потребама корисника, што за последицу може имати смањену ефикасност система која се огледа у успостављеним функционалностима и корисничким улогама. (Препорука број 3)

2. Нису усвојене и примењене свеобухватне мере заштите информационог система „есДневник“, јер МПНТР није успоставило управљање информационом безбедношћу система кроз неопходну процену ИТ ризика, организациону структуру и усвајање одговарајућих правила и процедура, управљање процесом континуитета пословања што обухвата и управљање резервним копијама и контролу примене мера заштите, што је неопходно како би била осигурана поузданост система.

Организација ИТ безбедности, због недостатка довољно стручног знања и недостатка кадровских капацитета, није успостављена тако да обухвата питања усвајања и примене адекватних докумената која уређују ову област, организациону структуру ИТ безбедности, управљање инцидентима, приступ систему и примену

других мера заштите ИКТ система, што за последицу има већи степен рањивости информационог система. (Препорука број 4)

МПНТР, због тога што не располаже потребним ресурсима, није у потпуности успоставило мере које обезбеђују континуитет пословања у ванредним околностима, што у случају прекида сарадње са пружаоцем услуга за последицу може имати нефункционисање информационог система у дужем временском периоду. (Препорука број 5)

МПНТР, због непознавања ове проблематике, недовољно искуства и обученог ИТ кадра, није успоставило управљање ИТ ризицима, што за последицу може имати стварање непотребно великих трошкова у случају настанка нежељеног догађаја, а који се могао спречити, или великих нефинансијских губитака (података на пример) због неблаговременог предузимања мера. (Препорука број 6)

3. Министарство није успоставило ефективан механизам сарадње са пружаоцима услуге, зато што није усвојило и имплементирало правила и процедуре када је у питању ова област, није успоставило администрирање система на законима прописан начин и није процес обраде података о личности уредило на јасан, законом прописан начин.

Због тога што нису прописане мере безбедности и заштите података из евиденција, МПНТР није усвојило правила и процедуре које се односе на безбедност података када су у питању уговори са пружаоцима услуга, тако да и поред тога што у уговорима са пружаоцима услуга постоји део који се односи на поверљивост података, није успостављен механизам за контролу да ли пружалац услуга поштује обавезе у вези поверљивости података, и није обезбедило обраду података о личности на законом прописан начин, што за последицу може имати смањени степен поузданости система. (Препорука број 7)

Због тога што нису прописане мере безбедности и заштите података из евиденција, МПНТР није успоставило управљање и администрирање информационим системом „есДневник“ на начин који подразумева да само МПНТР има администраторски приступ систему, што за последицу може имати нарушавање поверљивости и интегритета података. (Препорука број 8)

Државна ревизорска институција, након спроведене ревизије „Информациони систем „есДневник““, даје следеће препоруке:

Министарству просвете, науке и технолошког развоја да:

1. приликом припреме финансијских планова осигура стабилно финансирање циљева кроз детаљно планирање средстава за развој, набавку и одржавање свих компоненти информационог система „есДневник“ (приоритет 2[1]);

2. успостави процедуре које ће дефинисати функционисање информационог система „есДневник“ када је у питању управљање системом, начин уноса, обраде и ажурирања података који се уносе у систем, и обезбедити континуитет обављања послова у случају замене запослених на ИТ пословима (приоритет 2);

3. уреди процес прикупљања предлога за изменама система и пријављене проблеме од стране корисника успостављањем хелп-деск услуге или механизма

[1] ПРИОРИТЕТ 2 - Несврсисходности које је могуће отклонити у року до годину дана

размене ових информација са пружаоцем услуга уколико он врши хелп-деск услугу који ће обезбедити да све прикупљене информације МПНТР добије у истом тренутку када и пружалац услуге и по потреби у систем уведе и друге кориснике система и имплементира додатне функционалности и креирање додатних врста извештаја (приоритет 2);

4. успостави мере информационе безбедности које обухватају усвајање и имплементацију аката која уређују ову област, укључујући и процес одобравања и укидања приступа информационом систему „есДневник“, адекватну организациону структуру ИТ безбедности, управљање инцидентима, и друге неопходне мере безбедности и заштите података из евиденција информационог система „есДневник“ (приоритет 2);

5. успостави континуитет пословања у ванредним околностима, на начин да обезбеди функционисање система и у случају прекида сарадње са пружаоцима услуга, а што подразумева неопходан хардвер, апликативни софтвер, изворни код, стручно знање, базе података, управљање резервним копијама података, и процес тестирања планова континуитета пословања (приоритет 2);

6. успостави управљање ИТ ризицима, што подразумева евидентирање, класификацију, анализу ИТ ризика и дефинисање стратегије за смањивање/отклањање ризика (приоритет 2);

7. усвоји и имплементира правила и процедуре за безбедност података када је у питању сарадња са пружаоцима услуга, што подразумева обавезну примену мера заштите података и успостављање механизма за праћење примене тих мера, и уреди процес обраде података од стране пружаоца услуга у информационом систему „есДневник“ на законом прописан начин (приоритет 2);

8. уреди администрирање и управљање системом на начин да једино МПНТР има администраторска права, док ће пружалац услуга и корисници моћи да систему приступе једино уз одобрење и контролу администратора (приоритет 2).

Генерални државни ревизор

_____

Др Душко Пејовић
Државна ревизорска институција
Макензијева 41
11000 Београд, Србија
20. децембар 2021. године

II Увод

Државна ревизорска институција спровела је ревизију сврсисходности на тему „Информациони систем „есДневник““. Ревизија је спроведена у складу са Законом о Државној ревизорској институцији[2], Пословником Државне ревизорске институције[3] и Програмом ревизије Државне ревизорске институције за 2021. годину. Поступци ревизије су спроведени у периоду од априла до октобра 2021. године.

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

1. Проблем

Пројекат имплементације електронског дневника („есДневник“), почео је пилот пројектом у школској 2017/2018. години, а настављен је главним пројектом у школској 2018/2019. години, склапањем Уговора о набавци софтверског решења за вођење евиденција у основним и средњим школама (електронски дневник) са групом понуђача и то: „Телеком Србија“ ад Београд, „МТС Системи и интеграције“ доо Београд и „Тесла“ доо Загреб.

Циљ пројекта „есДневник“-а је објективније и ефикасније вођење евиденција о образовно-васпитном раду ученика, успеху и владању ученика. Пуна примена „есДневник“-а подразумева непостојање двоструког уноса евиденција у папирни и електронски дневник.

Евиденција (база података) у овом систему садржи податке дефинисане Законом о основама система образовања и васпитања, а који обухватају податке за одређивање идентитета ученика, податке за одређивање образовног статуса ученика, податке за одређивање социјалног статуса ученика и податке за одређивање функционалног статуса ученика.

У претходном периоду, установљено је да су постојали проблеми везани за информациону безбедност у више области:

• Многе школе у Србији не располажу довољним бројем рачунара како би обезбедили да у сваком одељењу постоји по један уређај који би се користио за рад у електронском дневнику. Чак је и добар број рачунара који се користе застарео, као и оперативни системи на њима.

• Није обезбеђен континуитет пословања у случају раскида уговора, сервери на којима се извршава систем нису у власништву Министарства, био би јако отежан процес поновног успостављања система на другим серверима, због недостатка стручног знања и скоро сигурних проблема са миграцијом база података.

• Пружалац услуге има приступ систему и продукционој бази података, иако је уговорима предвиђено да има приступ са минималним могућим правима. Законска је обавеза да министарство управља и администрира информационим системом.

[2] „Службени гласник РС“, бр. 101/05, 54/07, 36/10 и 44/18-др.закон
[3] „Службени гласник РС“, број 9/09

• Није успостављен процес даљег развоја у складу са предлозима и потребама корисника, јер МПНТР није успоставило систем да преузима податке о томе од пружаоца услуга, који врши услугу подршке.

• Обрада података о личности коју врши пружалац услуга није у потпуности успостављена на законом прописан начин, пре свега због недоумица ко је руковалац подацима у електронском дневнику.

• Нису донете процедуре које уређују ИТ послове, информациону безбедност итд. Због тога исти послови се на различит начин обављају у школама, онако како то тумаче директор и координатори система у школи. Без процедура није могуће успоставити систем контроле и преноса знања у случају замене запослених.

2. Циљ ревизије

Циљ ревизије је да се оцени у којој мери је успостављено ефективно управљање информационим системом „есДневник“.

Изабрана тема је повезана са циљем 1 из Стратешког плана ДРИ за период 2019-2023 године, да ће ДРИ одговорити на тренутне и хитне изазове у раду корисника јавних средстава, односно потциљем 1.9: Образовање (Функционална буџетска категорија 900): ДРИ ће кроз свој рад утврдити недостатке и предложити решења како би помогла остваривању циљева и задатака државе везаних за образовање. Такође, и са циљем 2 Утврдити проблеме и предложити решења за међусекторске проблеме на свим нивоима, ради унапређења одговорности и транспарентности, односно у оквиру тога потциљ 2.5: Унапредити јавно управљање и коришћење информационих технологија (ИТ)[4].

ИТ системи су од кључног значаја за пословање у оквиру јавног сектора и активности постају све скупље, сложеније и као и степен осетљивости података које оне садрже. Иницијативе е-Управе у Србији имају за циљ унапређење коришћења ИТ и интернета широм јавне управе да би се обезбедиле информације грађанима и привредним друштвима. ДРИ је кроз своје ревизије ранијих година утврдила да неки субјекти ревизије нису предузели неопходне мере у области безбедности ИТ система – укључујући и право на приступ подацима и поверљивост података. Нису спровели неопходне процене ризика, нити су усвојили стратегије које регулишу развој ИТ технологија. Ово неадекватно планирање ИТ развоја довело је до кашњења у реализацији пројеката, укључујући и нови интегрисани пословни ИТ систем и резултирало је у додатним трошковима[5]. Рад ДРИ ће помоћи да се унапреди способност ИТ система да сви јавни програми постану ефикаснији, а да се при томе штите кључно пословање и осетљиве информације.

3. Ревизијска питања

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

1. У којој мери је успостављено ефективно управљање информационим системом „есДневник“?

[4] Стратешки план Државне ревизорске институције за период 2019-2023. *http://www.dri.rs/upload/documents/Opsti_dokumenti/DRI%20Strateski%20plan%202018-2023.pdf*
[5] Стратешки план Државне ревизорске институције за период 2019-2023. *http://www.dri.rs/upload/documents/Opsti_dokumenti/DRI%20Strateski%20plan%202018-2023.pdf*

- Да ли је МПНТР успоставило оквир за управљање информационим системом у смислу планирања, финансирања, успостављања неопходне организационе структуре и процедура које уређују ове послове и континуиране обуке?
- Да ли МПНТР спроводи обуке везане за управљање и коришћење информационог система и како управља хардверским ресурсима?
- Да ли МПНТР прикупља и анализира проблеме корисника, да ли је успостављена хелп-деск услуга, да ли се и како прикупљају, анализирају, одобравају и имплементирају захтеви за измене система?
- На који начин се управља рачунарском опремом у школама која се користи за информациони систем „есДневник“?

2. У којој мери успостављене мере информационе безбедности обезбеђују поузданост информационог система „есДневник“?
   - Да ли постоје имплементирана правила и процедуре за информациону безбедност?
   - Да ли је и на који начин у МПНТР успостављена организација ИТ безбедности?
   - На који начин су успостављене мере физичке заштите и контроле логичког приступа систему?
   - На који начин се управља континуитетом пословања у ванредним околностима?
   - На који начин се спроводи управљање ИТ ризицима?
   - На који начин се у систему управља инцидентима?
3. У којој мери је успостављен механизам сарадње са пружаоцима услуга испунио све неопходне циљеве, укључујући и доступност података?
   - Да ли постоје правила и процедуре које се односе на безбедност података када су у питању уговори са пружаоцима услуга?
   - Да ли постоји механизам којим се осигурава да је пружалац услуге усвојио услове за заштиту и безбедност података и да ли их спроводи?
   - Да ли су могућности софтвера искоришћене у потпуности, имајући у виду извештавање на свим нивоима?
   - На који начин МПНТР прати реализацију извршења уговора?
   - Да ли су неопходне (улазно/излазне) информације доступне свим (потенцијалним) корисницима у информационом систему?

Питања која смо формулисали се односе на три најризичније области, на основу процене ризика коју смо спровели на бази доступних, тј. прикупљених података у предстудији.

Прво питање се односи на ИТ управљање. Адекватно ИТ управљање је неопходно како би се управљало целим системом, тачније свим његовим компонентама почевши од планирања, израде и усвајања стратегије, акционог плана за примену стратегије, измене закона у складу са стратегијом итд., адекватног финансирања система, што подразумева претходно урађене анализе, и усклађеност са акционим плановима за

спровођење стратегије, затим јасно дефинисану организацију и правила и процедуре за ИТ послове, и редовно спроведене ИТ обуке, управљање изменама система што обухвата идентификације захтева, одобрења, имплементације измена, такође и управљање системом, што се у овом случају посебно односи на хардверски део – рачунаре и интернет.

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

Треће питање се односи на успостављање ефективног механизма сарадње са пружаоцима услуга. Као и у случају претходна два питања, најпре се анализирају правила и процедуре које се односе на сарадњу са пружаоцима услуга, а посебно када је у питању ИТ безбедност, тј. заштита података. Такође, потребно је анализирати механизам за контролу спровођења уговора, нарочито у погледу поверљивости. Анализом треба утврдити да ли је могуће увођење нових, корисних функционалности у систему, нарочито ако је то могуће спровести у оквиру постојеће инфраструктуре, апликације и уговорних обавеза Министарства.

4. Обим и ограничења ревизије

Ревизијом смо обухватили активности Министарства у периоду од 2017. до 2020. године.

Предмет испитивања су биле области:

1) ИТ управљање – може се сматрати целокупним оквиром који води 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 ли примењује неопходне политике и процедуре који се односе на ИТ систем[6];

[6] WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions

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[7];

3) Успостављање ефективног механизма сарадње са пружаоцима услуга како би се осигурало да се услуге пружају према очекивањима субјекта. Субјект ревизије треба да има процесе у циљу обезбеђивања периодичног праћења статуса пројекта, квалитета услуге и тестирања производа пре увођења у оперативно окружење. Осим тога, као део процеса праћења извршења обавеза пружаоца услуга, субјект ревизије може такође вршити ревизију интерног процеса осигурања квалитета пружених услуга, како би се обезбедило да кадар пружаоца услуга прати уговорно одобрену политику и планове за све своје послове.[8]

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

5. Методологија у поступку рада

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[9]), као и све податке добијене од субјекта ревизије и извора информација – школа. Анализирали смо податке и информације за период од 2017. до 2020. године.

У вези са системом „есДневник“-а анализиране су области ИТ управљање, информациона безбедност и успостављање ефективног механизма сарадње са пружаоцима услуга.

У циљу потврђивања информација из документације и прикупљања података који нису доступни у документима, обавили смо интервјуе и послали анкету и упитнике корисницима информационог система „есДневник“.

Детаљнији опис коришћене методологије дат је у Прилогу 1.

[7] Члан 7. став 3. Закона о информационој безбедности
[8] WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions
[9] INTOSAI Радна група за ИТ ревизију

III Опис предмета ревизије

„ЕсДневник“ је саставни део јединственог информационог система просвете, који је уведен у употребу 2017/18. школске године, као пилот пројекат, а настављен је главним пројектом у школској 2018/19. години. „ЕсДневник“ садржи личне податке малолетних лица, образовни статус деце и ученика, социјални статус деце и ученика, родитеља, старатеља и хранитеља, здравствени статус деце и ученика.

1. Законодавни и институционални оквир

Законодавни оквир

Закон о основама система образовања и васпитања[10], у члану 30. прописује да Министарство обезбеђује функционисање система образовања и васпитања, у складу са општим принципима и циљевима образовања и васпитања, посебно планира и прати унапређивање квалитета образовања на основу релевантних чињеница информационог система у образовању, истраживања, анализа и вредновања образовања, односно планира развој квалитета образовања заснован на чињеницама и успоставља и управља јединственим информационим системом просвете у Републици Србији, стара се о несметаном протоку података и обезбеђује доступност и заштиту података. У члану 31. је прописано да Министарство у оквиру школске управе обезбеђује све услове да установе несметано уносе, попуњавају, ажурирају и одржавају базу података о образовању и васпитању у оквиру јединственог информационог система просвете. Чланом 126. Закона о основама система образовања и васпитања прописано је да је директор одговоран за благовремен и тачан унос и одржавање ажурности базе података о установи у оквиру јединственог информационог система просвете.

Део IX Закона о основама система образовања и васпитања уређује Јединствени информациони систем просвете.

Чланом 175. наведеног закона прописано је да уколико установа води евиденцију у електронском облику Министарство је обрађивач података у погледу администрирања система, чувања и заштите података.

Чланом 184. овог закона прописано је да Министарство обезбеђује мере заштите од неовлашћеног приступа и коришћења података у ЈИСП-у. Послове администрирања ЈИСП-а и регистара из члана 175. става 4. овог закона обавља посебно овлашћено лице у Министарству. Мере безбедности и заштите података из евиденција и регистара прописује министар.

Законом о основама система образовања и васпитања, Законом о основном образовању и васпитању[11] и Законом о средњем образовању и васпитању[12] прописано је да установа води прописану евиденцију у штампаном и/или електронском облику и издаје јавне исправе, у складу са овим и посебним законом.

У складу са Правилником о оцењивању ученика у основном образовању и васпитању[13], школе су обавезне да личне податке из евиденције о ученицима и податке

[10] „Службени гласник РС“, бр. 88/17, 27/18 – др. закон 10/19, 27/18 – др. закон и 6/20
[11] „Службени гласник РС“, бр. 55/13, 101/17, 27/18 – др. закон и 10/19
[12] „Службени гласник РС“, бр. 55/13, 101/17, 27/18 – др. закон и 6/20
[13] „Службени гласник РС“, број 34/19

из евиденције о успеху ученика који се односе на закључне оцене на крају школске године и резултате на завршном испиту чувају трајно.

Према члану 87. Закона о основном образовању и васпитању у школи може да се води евиденција електронски, у оквиру јединственог информационог система просвете и на обрасцима. Врсту, назив, садржај и изглед образаца евиденција и јавних исправа и начин њиховог вођења, попуњавања и издавања, прописује министар, у складу са Законом.

У складу са Законом о информационој безбедности[14] ИКТ системи од посебног значаја су и системи који се користе у обављању делатности од општег интереса, између осталих и у обављању послова у органима власти. Истим законом прописане су мере заштите ИКТ система од посебног значаја. Оператор ИКТ система од посебног значаја одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система.

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

Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја ближе се уређују мере заштите информационо-комуникационих система од посебног значаја.[15]

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

Уредбом о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја, ближе се уређује садржај акта о безбедности информационо-комуникационих система од посебног значаја.[16]

Закон о заштити података о личности уређује право на заштиту физичких лица у вези са обрадом података о личности и слободни проток таквих података, начела обраде, права лица на које се подаци односе, обавезе руковалаца и обрађивача података о личности, кодекс поступања, пренос података о личности у друге државе и међународне организације, надзор над спровођењем овог закона, правна средства, одговорност и казне у случају повреде права физичких лица у вези са обрадом података о личности, као и посебни случајеви обраде.[17]

[14] „Службени гласник РС“, бр. 6/16, 94/17 и 77/19
[15] „Службени гласник РС“, број 94/16
[16] „Службени гласник РС“, број 94/16
[17] „Службени гласник РС“, број 87/18

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

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

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

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

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

Члан 45. овог закона прописује да ако се обрада врши у име 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 (став 1).

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

Обрада од стране обрађивача мора бити уређена уговором или другим правно обавезујућим актом, који је закључен, односно усвојен у писменом облику, што обухвата и електронски облик, који обавезује обрађивача према 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 (став 3).

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

1) обрађује податке о личности само на основу писмених упутстава 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. овог закона;

4) поштује услове за поверавање обраде другом обрађивачу из ст. 2. и 7. овог члана;

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 овог закона;

6) помаже руковаоцу у испуњавању обавеза из члана 50. и чл. 52. до 55. овог закона, узимајући у обзир природу обраде и информације које су му доступне;

7) после окончања уговорених радњи обраде, а на основу одлуке 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 става 4. тачка 8) овог члана, обрађивач је дужан да без одлагања упозори руковаоца ако сматра да писмено упутство које је од њега добио није у складу са овим законом или другим законом којим се уређује заштита података о личности.

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

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

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

Приликом процењивања одговарајућег нивоа безбедности из става 1. овог члана посебно се узимају у обзир ризици обраде, а нарочито ризици од случајног или незаконитог уништења, губитка, измене, неовлашћеног откривања или приступа

подацима о личности који су пренесени, похрањени или обрађивани на други начин (став 3).

Руковалац и обрађивач дужни су да предузму мере у циљу обезбеђивања да 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 (став 5).

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

Институционални оквир

Министарство просвете, науке и технолошког развоја обавља послове државне управе који се односе на: истраживање, планирање и развој предшколског, основног, средњег и високог образовања и ученичког и студентског стандарда; допунско образовање деце домаћих држављана у иностранству; управни надзор у предшколском, основном, средњем и високом образовању и ученичком и студентском стандарду; учешће у изградњи, опремању и одржавању објеката предшколског, основног, средњег и високог образовања и ученичког и студентског стандарда од интереса за Републику Србију; стручно-педагошки надзор у предшколском, основном и средњем образовању и ученичком стандарду; организацију, вредновање рада и надзор над стручним усавршавањем запослених у просвети; признавање јавних исправа стечених у иностранству; унапређење друштвене бриге о обдареним ученицима и студентима; унапређење друштвене бриге о ученицима и студентима са посебним потребама, стварање услова за приступ и реализацију пројеката из делокруга тог министарства који се финансирају из средстава претприступних фондова Европске уније, донација и других облика развојне помоћи, као и друге послове одређене законом.

Министарство просвете, науке и технолошког развоја обавља послове државне управе који се односе на: систем, развој и унапређење научноистраживачке делатности у функцији научног, технолошког и привредног развоја; предлагање и реализацију политике и стратегије научног и технолошког развоја; утврђивање и реализацију програма научних, технолошких и развојних истраживања; усавршавање кадрова за научноистраживачки рад; предлагање и реализацију иновационе политике; предлагање и реализацију политике и програма у области вештачке интелигенције; подстицање технопредузетништва, трансфера знања и технологија у привреди; развој и унапређење иновационог система у Републици Србији; развој функционисања система научно-технолошких информација и програма развоја научно-технолошке инфраструктуре; истраживање у области нуклеарне енергије; сигурност нуклеарних објеката; производњу и привремено складиштење радиоактивних материјала, изузев у нуклеарним енергетским постројењима, као и друге послове одређене законом.[18]

Како је у надлежности Министарства просвете, науке и технолошког развоја успостављање и управљање јединственим информационим систем просвете, самим тим

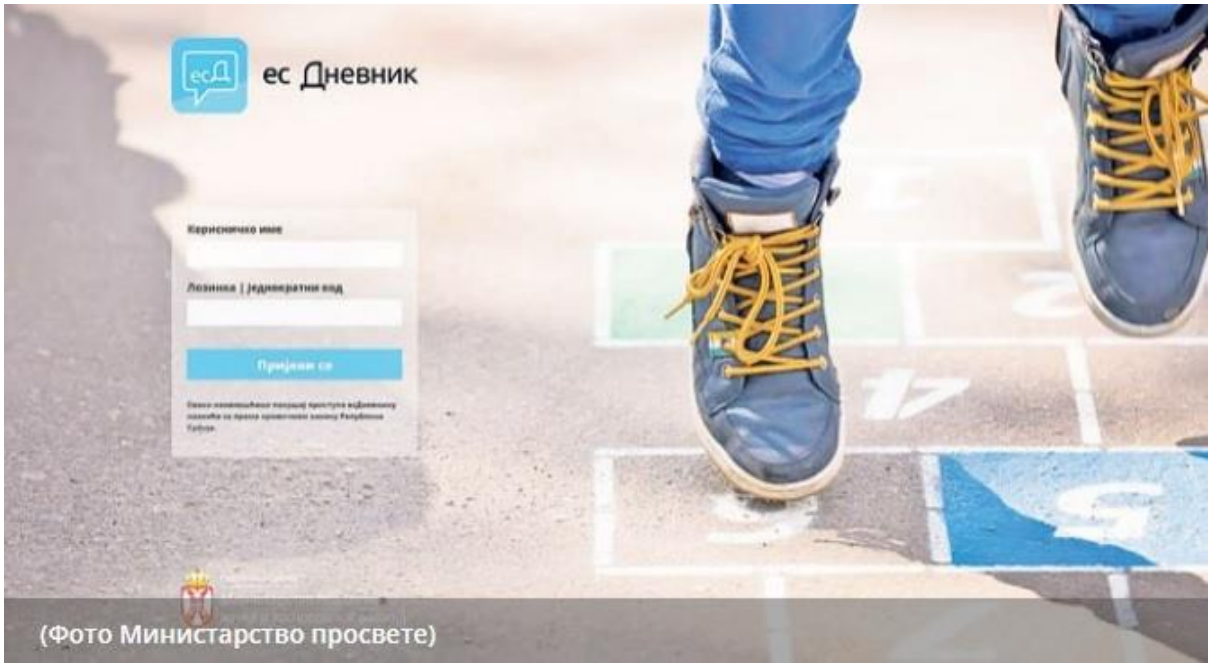
[18] члан 17. Закона о министарствима („Службени гласник РС“, број 128/20)

и електронским дневником, као и обезбеђење протока података, доступности и заштите података, ревизијом је као субјект одабрано Министарство, како би се препоруке могле имплементирати.

2. Информациони систем „есДневник“

ЕЛЕКТРОНСКИ ДНЕВНИК („есДНЕВНИК“)

Електронски дневник службено се зове „есДневник“, што је скраћеница од „електронски систем дневник”. Систем „есДневник“ јесте јединствено и централно решење Министарства просвете, науке и технолошког развоја Републике Србије (даље: МПНТР или Министарство), које замењује све досадашње начине вођења евиденције у основним и средњим школама.



Илустрација 1. *Изглед портала „есДневник“*

Циљ пројекта електронског дневника је објективније и ефикасније вођење евиденције о образовно-васпитном раду ученика. Повећање објективности се односи на реалније оцењивање, јер је наставницима онемогућен увид у оцене из других предмета, а тиме и стицање предрасуда о знању ученика. Ефикасност се огледа и у смањењу административног рада наставника, јер се све потребне евиденције налазе на једном месту. Постигнут је и увид у наставни процес у реалном времену и тиме омогућено превентивно деловање.

Додатно, приликом интересовања родитеља о напретку детета, наставнику је у електронском дневнику омогућено да показује евиденције само о том детету. Такође, примењено решење омогућава родитељима индивидуални увид у евиденције о ученику путем Интернета.

Пројекат имплементације електронског дневника почео је пилот пројектом у школској 2017/2018. години, а настављен је главним пројектом у школској 2018/2019. години.

Пилот пројекат је започео у 60, а завршио са више од 500 основних и средњих школа.

По завршетку пилот пројекта одлучено је да се све школе укључе у главни пројекат у школској 2018/19. години.

Систем „есДневник“ јесте софтверско решење. У раду „есДневник“ сервиса користи се мрежна инфраструктура технолошког партнера „Телеком Србије“. Сви сервери и друга ИКТ опрема се налазе у заштићеном рачунарском центру.

Систему „есДневник“, веб апликацији, корисници приступају путем Интернета са било којег рачунара у школи или код куће, али искључиво са оног који приступа апликацији из адресног опсега ИП адреса Републике Србије.

ХАРДВЕРСКИ И СОФТВЕРСКИ ПРЕДУСЛОВИ

Систем „есДневник“ конструисан је да функционише на стоном, преносном или таблет рачунару са инсталираним једним од подржаних оперативних система (Windows 7 или виши, Linux, MacOS, Android 5.0 или виши, и OS 9.0 или виши) и једним од подржаних Интернет претраживача (Google Chrome, FIrefox, Internet Explorer 11.0 или виши/ Edge, Safari, Opera). Минимална димензија екрана таблет рачунара је 10 инча. Све друге комбинације рачунара, оперативних система и Интернет претраживача нису подржане.

За функционисање система „есДневник“-а неопходна је стална веза са Интернетом (жична или бежична), минималне брзине 10 Mbit/c.

КОРИСНИЦИ „есДневник“ СИСТЕМА

Школе самостално управљају системом „есДневник“ у смислу уноса и обраде података. Школски координатори управљају корисницима система, а корисници система управљају подацима о ученицима и образовно-васпитном евиденцијом.

Илустрација 2. *Складиштење таблета у школи*

Илустрација 3. *Приказ десктоп рачунара у учионици*

Наставници за потребе вођења електронске евиденције о успеху и владању ученика користе десктоп и лаптоп рачунаре, као и таблете. У највећем броју случајева, у учионицама се налази по један рачунар који се користи поред осталог и за „есДневник“, док се из разумљивих разлога у школама у којима наставници користе таблети, таблети за време одмора чувају у зборници.

УЛОГЕ У СИСТЕМУ „есДневник“

За сваку школу у „есДневник“ систему су дефинисане следеће улоге: школски координатор, одељењски старешина, наставник, директор школе, замена директора и стручне службе. Свака рола има специфична права и обавезе.

ШКОЛСКИ КООРДИНАТОР

Школски координатор јесте улога у систему са највише права и обавеза. Свака школа дефинише минимално два (2) школска координатора. Школски координатор подешава параметре своје школе, уноси кориснике (одељењске старешине, наставнике, директоре и ППС), генерише њихова корисничка имена и иницијалне шифре, ресетује шифре.

Такође, школски координатор може да уноси и ученике, да додељује ученике одељењима/разредима, одељењским старешинама, наставницима, да им додељује предмете, односно да обавља администрацију везану за ученике. Ово није његова главна улога, јер се ученицима првенствено баве одељењски старешина и наставници.

ОДЕЉЕЊСКИ СТАРЕШИНА

Одељењски старешина (даље: ОС) обавља администрацију везану за ученике из свог одељења. Односно, може да уноси ученике у систем, да додељује ученике одељењима/разредима, наставницима, да им додељује предмете, уноси оцене из предмета који предаје, регулише изостанке, види све оцене из свих предмета за своје

одељење, да исписује ученике из одељења/школе, да види све извештаје о одељењу и својим ученицима.

Такође, ОС уноси евиденцију о родитељима/старатељима ученика, има право да показује делове система „есДневник“-а за време индивидуалних посета родитеља/старатеља, штампања картица (извештаја) за родитеље/старатеље. Поред тога, ОС уноси контакте (родитеља/старатеља) ученика, креира родитељске налоге за Портал родитеља и ученика „мој.есДневник“, ресетује лозинку за родитељски налог, а све у складу са захтевом родитеља.

НАСТАВНИК

Наставник уноси евиденцију везану за свој предмет, ученика и одељење. Наставник види и може да уноси евиденцију само о ученицима/одељењима којима он предаје – не види друге предмете нити оцене.

ДИРЕКТОР ШКОЛЕ

Директор школе уз могућност прегледа свих ученика, предмета, одељења, наставника, и свих специфичних извештаја на нивоу целе школе, има и функцију одобравања брисања погрешно уписаних оцена. Захтев за брисање прослеђује предметни наставник, информацију да постоји захтев за брисање оцене добија Школски координатор, а само Директор може да одобри (или не одобри) брисање оцена.

СТРУЧНЕ СЛУЖБЕ

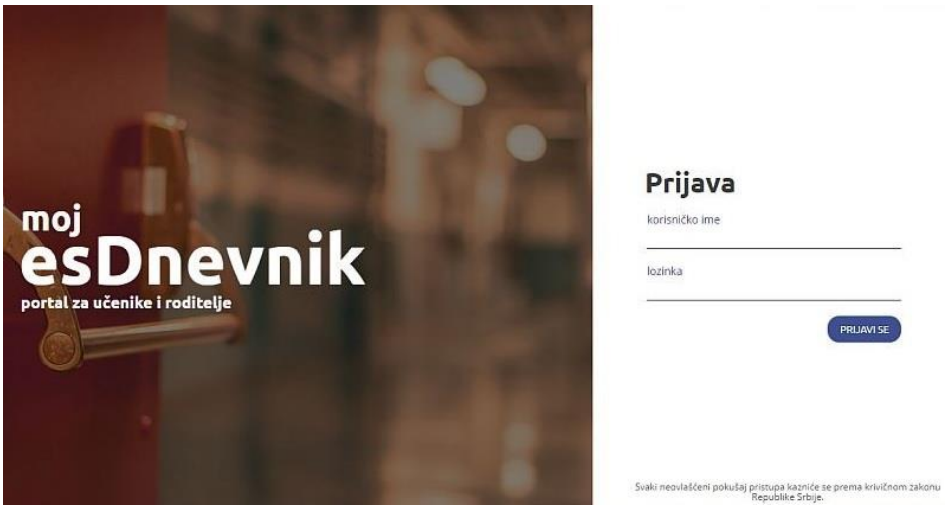
Стручне службе имају могућност праћења напретка и поређења свих ученика, одељења, наставника, ОС кроз посебно дефинисане извештаје.

ПРИСТУП СИСТЕМУ И УНОС ПОДАТАКА О УЧЕНИЦИМА

Веб апликацији „есДневник“ корисници приступају путем корисничког имена, лозинке и/или једнократног кода (токена).

ПРИСТУП РОДИТЕЉА „есДНЕВНИК“-У

Родитељске налоге за приступ евиденцијама издају школе, према динамици коју саме одреде.



Илустрација 4. *Изглед портала за ученике и родитеље „мој есДневник“*

IV Закључци

У овом поглављу износимо закључке до којих смо дошли спроводећи ревизију сврсисходности на тему „есДневник“, код субјекта ревизије:

1. Министарство просвете, науке и технолошког развоја, Београд

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

ЗАКЉУЧАК 1: Ефективно управљање информационим системом „есДневник“ није у потпуности успостављено, зато што планирање средстава у ревидираном периоду није обезбедило неопходно инвестиционо улагање у све компоненте информационог система, нити су успостављене процедуре које обезбеђују управљање и контролу свих процеса, и континуитет обављања послова у случају замене запослених на ИТ пословима, и што због непостојања адекватног система хелп-деск услуге није осигуран даљи развој система у складу са потребама корисника

Информациони систем „есДневник“ покрива основно и средње образовање у Србији, са потенцијално преко 1,3 милиона корисника (ученика, родитеља, наставника), и за циљ има објективније и ефикасније вођење евиденција о образовно-васпитном раду ученика, успеху и владању ученика, са крајњим циљем да пуна примена „есДневник“-а подразумева непостојање двоструког уноса евиденција у папирни и електронски дневник. Сви корисници приступају систему путем web странице, са одговарајућим функционалностима/извештајима, и дефинисаним правима. Приступ је могућ преко рачунара, али и мобилних уређаја, попут таблета или мобилног телефона. Корисници система су координатори система, директор, наставни кадар, родитељи.

Успостављање Информационог система „есДневник“ је покренуто у школској 2017/2018. години, покретањем пилот пројекта у оним школама које задовољавају критеријуме за увођење „есДневник“-а, односно поседују како техничку опремљеност, тако и заинтересованост запослених да се укључе у пројекат. Од 2019. године је покренут главни пројекат, који подразумева успостављање система у свим школама у Републици Србији.

У току успостављања овог система јављали су се проблеми везани за управљање информационим системом. Најпре, постоје проблеми са опремљеношћу школа за коришћење система (недовољан број расположивих рачунара, проблеми са интернет конекцијом). Чак и данас многе школе у Србији не располажу довољним бројем рачунара како би обезбедили да у сваком одељењу постоји по један уређај који би се користио за рад у електронском дневнику. Добар број рачунара који се користе је застарело, као и оперативни системи на њима. Неке школе не користе систем јер не могу да обезбеде интернет. Такође, постоје проблеми што у једном броју школа које обављају своју делатност и на језику националних мањина систем није у употреби, јер није обезбеђена подршка за систем на језику одређене националне мањине.

Установљено је и да не постоје усвојена правила и процедуре које се односе на ИТ послове, иако је то и законска обавеза, а како је након успостављања „есДневник“-а

уследило и успостављање ЈИСП-а, Правилником који је уредио ближе услове за успостављање ЈИСП-а практично „есДневник“ није ни обухваћен.

Приликом увођења система, и дефинисања функционалних и техничких захтева, приоритетни задатак је био да електронски дневник има све „функције“ као и стари, папирни дневник. Поред тога, дефинисане су и неке функционалности које папирни дневник не омогућава – креирање одређених извештаја, рад са удаљене локације итд. Међутим, у току коришћења система испоставило се да постоји још пуно могућих функционалности које би користиле у раду. Међутим, МПНТР није успоставило размену података у том смислу са пружаоцем услуга, који пружа подршку корисницима, тако да ти предлози нису прикупљани и анализирани, самим тим ни имплементирани.

Имајући у виду све ове уочене проблеме, неправилности и ризике у овој ревизији, између осталог, наш циљ је био да у оквиру првог ревизијског питања утврдимо у којој мери су успостављени системи управљања информационим системом „есДневник“ омогућили испуњење пословних циљева, успостављање јасно дефинисане организационе структуре.

Како би одговорили на ово питање, разматрали смо да ли је обезбеђено стабилно финансирање одржавања и развоја информационог система у складу са стратешким документима. Анализирали смо и да ли су усвојена и да ли се примењују правила и процедуре у вези управљања ИТ операцијама, као и да ли је и на који начин успостављен процес измене система у циљу повећања његове ефикасности.

Наш закључак заснивамо на следећим налазима:

Налаз 1.1: Није обезбеђено стабилно финансирање информационог система „есДневник“

Због непостојања детаљних анализа хардверских и софтверских ресурса и потреба школа приликом набавке система и у току његовог коришћења, није обезбеђено стабилно финансирање информационог система „есДневник“, што за последицу има недовољан број рачунара, застареле рачунаре и застареле, самим тим и небезбедне оперативне системе. Законом о основама система образовања и васпитања, прописано је да МПНТР обезбеђује функционисање система образовања и васпитања, а нарочито успоставља и управља јединственим информационим системом просвете, и да у оквиру школске управе обезбеђује све услове да установе несметано уносе, попуњавају, ажурирају и одржавају базу података о образовању и васпитању у оквиру јединственог информационог система просвете; Правилником о јединственом информационом систему просвете је прописано да Министарство обезбеђује потребне ресурсе за функционисање ЈИСП-а, чији је део „есДневник“.

Финансирање једног информационог система, у најширем смислу, обухвата набавку и одржавање хардвера (рачунара, сервера, штампача, мрежне опреме и других уређаја), набавку и развој софтвера (набавку оперативних система, апликативног софтвера – често набавку одржавања софтвера, када су у питању специфични послови), одржавање база података и чување резервних копија, људске ресурсе и обуке, и у неким случајевима израду одговарајућих правних аката којима се рад тог система уређује.

Зато је у овој ревизији циљ био да се анализира, поред података о финансирању система и хардверско-софтверским ресурсима у школама, и организациони део који се односи на ИТ послове везане за „есДневник“, у МПНТР и у школама, и спроведене обуке запослених који раде на тим пословима.

Како је дефинисано Законом о основама система образовања и васпитања, у члану 30., Министарство обезбеђује функционисање система образовања и васпитања, у складу са општим принципима и циљевима образовања и васпитања, а нарочито успоставља и управља јединственим информационим системом просвете у Републици Србији, стара се о несметаном протоку података и обезбеђује доступност и заштиту података. Исти закон, у члану 175., прописује да је Јединствени информациони систем просвете (у даљем тексту: ЈИСП) скуп база података и рачунарских програма, потребних за прикупљање и обраду података у евиденцијама и регистрима, уз обезбеђивање заштите података о личности.

Установа, високошколска установа, односно установа ученичког и студентског стандарда води евиденцију о деци, ученицима, одраслима и студентима обухваћеним формалним образовањем, о родитељима, односно другим законским заступницима и о запосленима, а јавно признати организатор активности о полазницима и кандидатима обухваћеним неформалним образовањем, у складу са овим и посебним законом, законом којим се уређује високо образовање и законом којим се уређује ученички и студентски стандард. Уколико установа, високошколска установа, установа ученичког и студентског стандарда, односно јавно признати организатор активности води евиденцију у електронском облику у оквиру ЈИСП-а, у складу са овим и посебним законом, Министарство је обрађивач података у погледу администрирања система, чувања и заштите података.

Министарство, у оквиру ЈИСП-а води, између осталих, и регистар деце, ученика, одраслих, полазника, кандидата и студената. У тај регистар се уносе подаци из евиденција које води установа, високошколска установа, установа ученичког и студентског стандарда, односно јавно признати организатор активности.

Члан 186. истог закона прописује да се средства за финансирање делатности установа обезбеђују у буџету Републике Србије, аутономне покрајине и јединице локалне самоуправе. Такође, установе могу да остваре и сопствене приходе по основу проширене делатности, као и друге приходе у складу са законом.

Правилник о јединственом информационом систему просвете, у члану 2. прописује: Јединствени информациони систем просвете (у даљем тексту: ЈИСП) успоставља и њиме управља министарство надлежно за послове образовања и васпитања (у даљем тексту: Министарство). Министарство обезбеђује услове за безбедност и сигурност техничке опреме и софтвера, као и потребне ресурсе за функционисање ЈИСП-а. Такође, прописано је да МПНТР обезбеђује и техничке услове у установама за безбедан, сигуран, заштићен, аутентификован и ауторизован приступ ЈИСП-у.

Правилником је у члану 3. прописано да основна и средња школа воде прописану евиденцију на основу закона којим се уређују основе система образовања и васпитања (у даљем тексту: Закон) и посебних закона којима се уређују основно образовање и васпитање и средње образовање и васпитање и да је дужна да обезбеди унос и ажурирање података у регистре, у складу са Законом, посебним законом, односно законом којим се уређује високо образовање.

Сходно наведеном, јасно је да је „есДневник“ евиденција коју води школа и која чини део регистра ЈИСП-а, те да је МПНТР у обавези да обезбеди све неопходне техничке услове за рад у информационом систему „есДневник“. Информациони систем „есДневник“, под тим називом није дефинисан у законима који уређују основно и средње образовање у Србији.

У овој ревизији, циљ у овом делу је био да се анализира како је са финансијског аспекта успостављан систем из године у годину, какви су ресурси и потребе школа. Анализирана је документација коју је доставило МПНТР и подаци прикупљени од 632 школе који се односе на „есДневник“.

Правилником о номенклатури нематеријалних улагања и основних средстава са стопама амортизације[19], прописано је да је годишња стопа амортизације за ставку „Електронски рачунари и остала опрема за обраду података“ износи 20%. То практично значи да је књиговодствена вредност рачунара после пет година коришћења нула динара. Другачије речено, сматра се да су рачунари након пет година 100% амортизовани.

Век употребе рачунара је обрнуто пропорционалан његовој поузданости и то и у хардверском и у софтверском смислу и то треба имати у виду приликом планирања средстава за набавку новог хардвера. Планирање, када је у питању информациони систем „есДневник“ обухвата планирање на републичком нивоу и планирање на нивоу сваке школе, с обзиром да школе набављају рачунаре из више извора – из сопствених средстава, уз помоћ локалне самоуправе, и оне које добију од МПНТР.

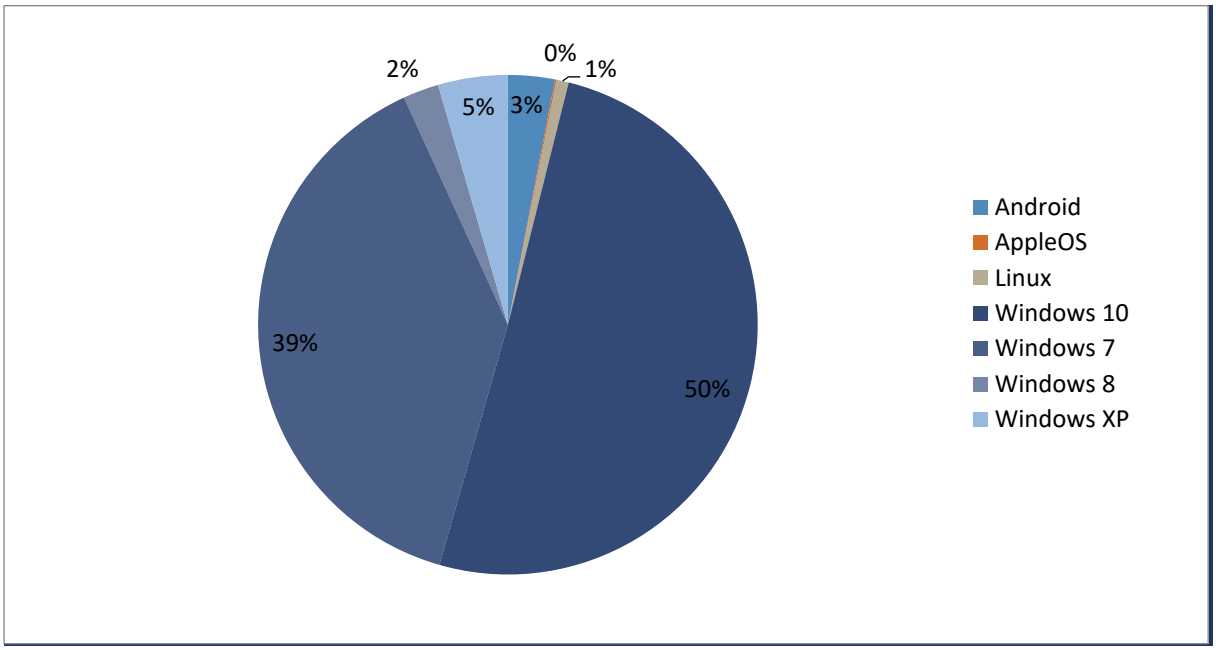
Подршка за оперативни систем Windows XP је укинута 2014. године. Анализом прикупљених података од укупно 632 школе, установљено је да 5% рачунара користи овај оперативни систем. Подршка за оперативни систем Windows 7 је укинута почетком 2020. године. У анализи коју смо спровели, од укупног броја рачунара који се користе за „есДневник“, 39% рачунара има овај оперативни систем. Око 2% рачунара користи оперативни систем Windows 8, за који не постоји подршка од 2016. године. Најављени датум укидања подршке од стране Microsoft-а за оперативни систем Windows 10 је октобар 2025. године.

Укупно, на бази података прикупљених од 632 школе, анализа је показала да 46% рачунара користи застареле оперативне системе, тачније системе за које више не постоји ажурирање и инсталација безбедоносних закрпа. 50% рачунара користи оперативни систем Windows 10.

Оперативни систем	Број рачунара	Процентуално
Android	321	3%
AppleOS	10	0%
Linux	84	1%
Windows XP	478	5%
Windows 7	4106	39%
Windows 8	246	2%
Windows 10	5352	50%

Илустрација 5. *Број рачунара и оперативних система*

[19] „Службени лист СРЈ“, бр. 17/97 и 24/00

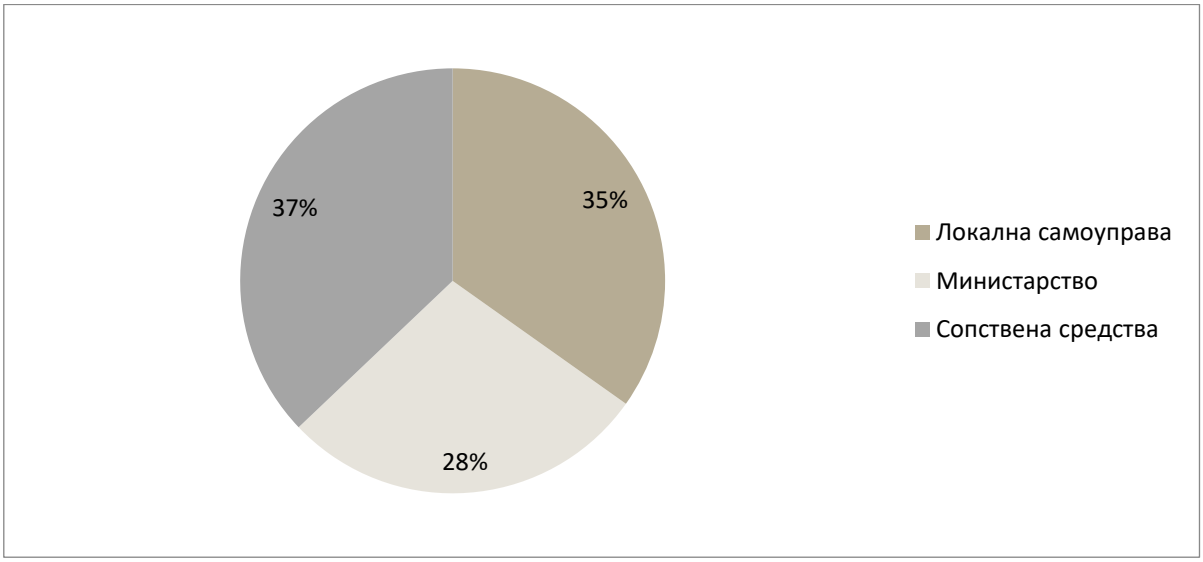


Илустрација 6. *Који оперативни систем користе школе у Републици Србији?*

Анализа података добијених од 632 школе је показала да је МПНТР у ревидираном периоду обезбедило 28% од укупног броја рачунара који се користе за рад у „есДневник“-у. 35% рачунара су школама набавиле локалне самоуправе, док су школе из сопствених средстава обезбедиле 37% рачунара.

Извор финансирања	Број рачунара	Процентуално
Министарство	2.942	28%
Локална самоуправа	3.647	35%
Сопствена средства	3.886	37%

Илустрација 7. *Извор финансирања рачунара у Републици Србији*

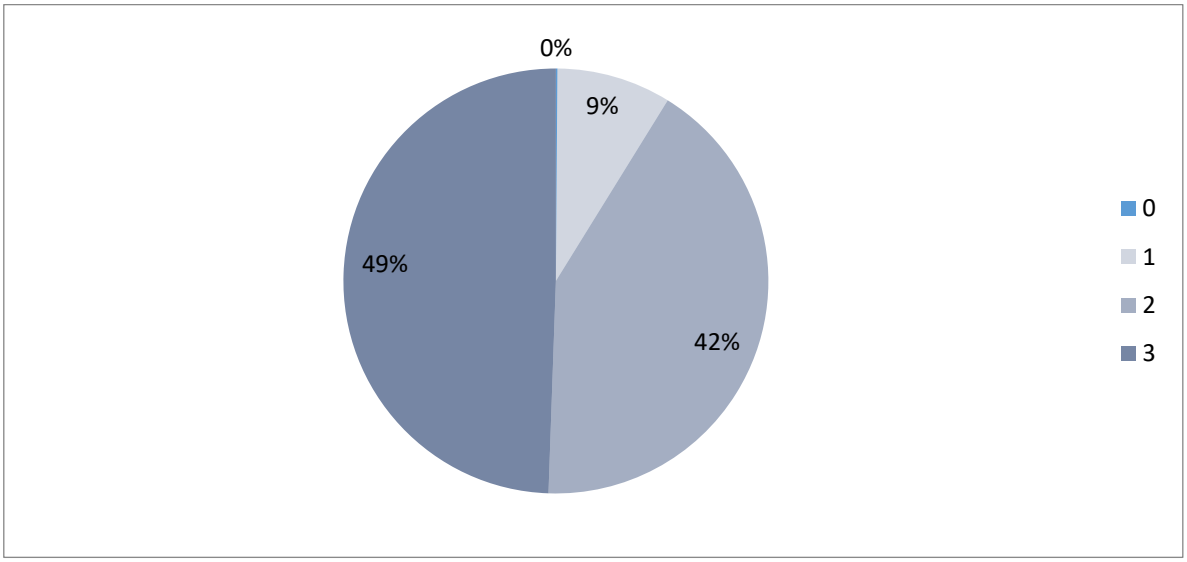


Илустрација 8. *Како су прикупљена средства за куповину уређаја у Републици Србији?*

У посматраном периоду, на бази података добијених од 632 школе, може се уочити пад у проценту броја рачунара које је МПНТР набавило. Наиме, у 2018. години, МПНТР је набавило 846 рачунара, или 49% од укупног броја, у 2019. години 714 уређаја што чини 42% од укупног броја, а у 2020. години 149 рачунара, или 9% од укупног броја.

Година	Број рачунара	Процентуално
0	2	0%
1	149	9%
2	714	42%
3	846	49%

Илустрација 9. *Набавка уређаја од стране МПНТР у последње три године*

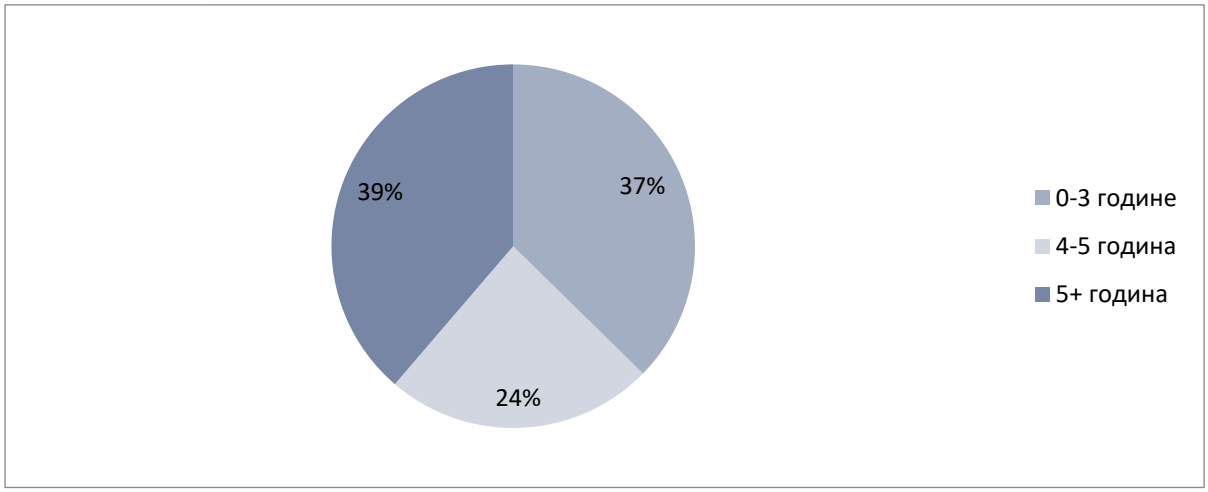


Илустрација 10. *Набавка уређаја од стране Министарства у последње три године*

Када је у питању старост рачунара, анализа прикупљених података од 632 школе је показала да је 37% уређаја набављено у претходне три године, да је 24% рачунара старо између четири и пет година, што је према претходно наведеном Правилнику о номенклатури нематеријалних улагања и основних средстава са стопама амортизације, граница када се сматра да су рачунари 100% амортизовани, а 39% је старије од пет година, има случајева да су још увек у употреби рачунари стари 12 година.

Старост уређаја	Број рачунара	Процентуално
0-3 године	3.933	37%
4-5 година	2.522	24%
5+ година	4.077	39%

Илустрација 11. *Старосна структура рачунара у Републици Србији*



Илустрација 12. *Старост уређаја у Републици Србији*

Када је у питању интернет конекција, анализом прикупљених података од 632 школе установљено је да је у 266 интернет конекцију обезбедило МПНТР, 296 школа је интернет обезбедило из сопствених средстава, док у осталим случајевима нису достављени подаци о томе.

Анализа добијених података од школа је показала да је у осам округа половина од укупног броја рачунара застарела, јер је старост рачунара и до 12 година, и то су окрузи где је проценат набављених рачунара од стране МПНТР био испод 25%. Треба поново напоменути, како се не ради о школама које су обухваћене анкетом на бази узорковања, јер узорковање није коришћено у овој ревизији. Добијени резултати се не могу генерализовати, и у том проценту не одражавају стање у целој популацији, тачније за све школе у Србији укупно.

МПНТР није документовало процес покретања и реализацију пилот пројекта у склопу којег је у школској 2017/2018. години Пилот пројекат започео у 60, а завршио са више од 500 основних и средњих школа. По завршетку пилот пројекта одлучено је да се све школе укључе у главни пројекат у школској 2018/19. години. Пилот пројекат је реализован као донација, односно софтвер је бесплатно уступљен да би се пилот пројекат реализовао. Пројекат је реализовала фирма „Тесла“ доо из Загреба.

У 2018. години Министарство просвете, науке и технолошког развоја (Наручилац) је спровело отворени поступак Јавне набавке, број ОП/Д/02/18, чији је предмет набавка софтверског решења за вођење евиденције у основним и средњим школама (електронски дневник).

С обзиром да је била само једна понуда од Групе понуђача и то: Предузеће за телекомуникације „Телеком Србија“ ад, Таковска 2, Београд, „МТС Системи и интеграције“ доо, Милутина Миланковића 9ж, Нови Београд и „Тесла“ доо, Присавље 2, Загреб, Наручилац је са наведеном Групом понуђача закључио Уговор број 404-02-71/2018-17 од 24. августа 2018. године у периоду трајања од једне године. Укупна уговорена вредност износи: 162.235.000 динара без ПДВ-а, односно 194.682.000 динара са ПДВ-ом.

Министарство просвете, науке и технолошког развоја (Наручилац) је закључило са Групом понуђача Уговоре о пружању услуге – Подршка, одржавање и хостовање софтверског решења за вођење евиденције у основним и средњим школама („есДневник“), број 404-02-114/2019-18 од 9. децембра 2019. године и број 404-02-90/2020-17 од 25. децембра 2020. године, у трајању од 12 месеци. Уговори су

закључени у месечном износу од 6.354.083 динара без ПДВ-а, односно 7.624.900 динара са ПДВ-ом. Укупна уговорена вредност за цео период је фиксна и износи 76.249.000 динара без ПДВ-а, односно 91.498.800 динара са ПДВ-ом.

Уговор о набавци софтверског решења за вођење евиденције у основним и средњим школама („есДневник“) број 404-02-71/2018-17 од 24. августа 2018. године закључен је у периоду трајања од једне године, тј. до 24. августа 2019. године. Чланом 2. наведеног Уговора, прописано је да одржавање и корисничка подршка важи до трајања Уговора.

Уговор о пружању услуге – Подршка, одржавање и хостовање софтверског решења за вођење евиденције у основним и средњим школама („есДневник“), број 404-02-114/2019-18 закључен је 9. децембра 2019. године, што није у складу са наведеним Уговором, јер је закључен три месеца касније.

Број предмета ЈН	ОП/Д/02/18	**Процењена вредност ЈН**	162.250.000,00
Група понуђача: Предузеће за телекомуникације Телеком Србија ад, Таковска 2, Београд – МТС Системи и интеграције доо, Милутина Миланковића 9ж, Нови Београд – Тесла доо, Присавље 2, Загреб		**Вредност Уговора без ПДВ-а**	**Вредност Уговора са ПДВ-ом**
Број и датум Уговора о набавци софтверског решења за вођење евиденције у основним и средњим школама (есДневник)	404-02-71/2018-17 од 24. 8. 2018. год.	162.235.000,00	194.682.000,00
Одржавање софтверског решења			
Број и датум Уговора о пружању услуге - Подршка, одржавање и хостовање софтверског решења за вођење евиденције у основним и средњим школама (есДневник)	404-02-124/2019-18 од 9.12.2019. год.	76.249.000,00	91.498.800,00
Број и датум Уговора о пружању услуге - Подршка, одржавање и хостовање софтверског решења за вођење евиденције у основним и средњим школама (есДневник)	404-02-90/2020-17 од 25.12.2020. год.	76.249.000,00	91.498.800,00
Укупно:		**152.498.000,00**	**182.997.600,00**

Илустрација 13. *Финансирање система „есДневник“*

Када је у питању организациона ИТ структура у МПНТР која обавља послове везане за „есДневник“, анализиран је Правилник о унутрашњем уређењу и систематизацији радних места, у Сектору за дигитализацију у просвети и науци, у којем је систематизовано шест радних места у чијем опису послова се налазе и они делови који се односе на евиденције које воде школе, као што је информациони систем „есДневник“. У групи за е-Просвету су руководилац групе, администратор сервиса е-Просвете и администратор портала е-Просвете и пружалац помоћи и подршке корисницима, док су у групи за дигитализацију у образовању руководилац групе, саветник за примену дигитализације у образовању и за праћење дигитализације у образовању.

Анализа описа послова показује да су, између осталих, предвиђени послови:

– организације и координирања обављања послова у вези са успостављањем, функционисањем и ажурирањем дигитализованих података и евиденција, између осталих, и у области основног и средњег образовања,

– припреме финансијских аката и докумената у вези са успостављањем ЈИСП-а,

– праћење реализације пројеката,

– спровођење прописа из области ИКТ система, прописа о заштити података о личности,

– администрирање успостављања и коришћења система е-Просвете,

– израде пројектних захтева за надоградњу и надзор над доступности и коришћења дигитализованог ЈИСП-а,

– активности за унапређење информационог система,

– вођење интерне евиденције позива корисника и отварање тикета за проблеме које ће решавати програмери и техничка подршка,

– давање препорука и предлога за унапређење на нивоу система,

– образовање за ИКТ и развој дигиталних компетенција,

– праћење ефеката и извештавање о активностима и реализацији циљева из акционих планова,

– обука запослених у школама за коришћење информатичке обуке,

– анализа планираних и евалуација примењених процедура које се односе на дигитализацију у образовању,

– праћење реализације програма модернизације ИКТ инфраструктуре у основним и средњим школама.

У школама, поред корисника система, као што су директор и наставни кадар, послове које обављају координатори „есДневник“-а обухватају следеће активности:

– Похађање обуке за координаторе,
– Праћење и редовно усвајање знања и компетенције везане за надоградњу и измену система „есДневник“-а,
– Реализација обука за наставнике своје школе, пружање потребне подршке и увођење у рад нових наставника,
– Администрирање дела УПРАВЉАЊЕ НА НИВОУ ШКОЛЕ који се односи на Подешавање школе, Кориснике система (наставнике, предмете које предају, њихова овлашћења), Разредна одељења, Табелу трајања часова, Увид у захтеве за брисањем оцене,
– Пренос података у наредну школску годину,
– У сарадњи са одељењским старешином, пружање подршке приликом уноса замена за предметног наставника (проверава датум са којим се замена завршава).

У опису послова запослених који обављају посао координатора у школама нису наведени послови везани за „есДневник“ које они свакодневно обављају. Такође, треба напоменути да координатори овај посао обављају без додатне надокнаде.

Анализа података прикупљених од 632 школе је показала да постоје школе у којима ради само по један координатор, да је у највећем броју школа тај број два, а као што је приказано у табели, постоје и школе које су навеле да имају чак пет координатора система „есДневник“. У 19 случајева школе нису навеле податак о броју координатора.

Број координатора	Број школа
0	1
1	24
2	439
3	76
4	23
5	6

Илустрација 14. *Број координатора у школама*

Уговором о набавци предвиђено је да ће пружалац услуге обуку координатора у првих 600 школа које ће користити „есДневник“ спровести у року од 45 дана од почетка коришћења система у школској 2018/2019 години, тј. од 01. септембра 2018. године. Обуку преосталих координатора обавезан је да спроведе до 31. децембра 2018. године. Није дефинисана обавеза обучавања координатора који након тог рока преузму обављање тог посла у школама.

Анализа података добијених од 632 школе је показала да је у периоду од 2017.-2021. године 300 школа било обухваћено обуком координатора за вођење „есДневник“-а, док је у истом периоду организована обука наставника и других корисника система у 241 школи.

Датум последње обуке координатора	Број школа чији су координатори похађали обуку	Датум последње обуке наставника и других корисника система	Број школа чији су наставници похађали обуку
2017. година	25	**2017. година**	19
2018. година	177	**2018. година**	53
2019. година	46	**2019. година**	70
2020. година	11	**2020. година**	48
2021. година	41	**2021. година**	51
Укупно:	**300**	**Укупно:**	**241**

Илустрација 15. *Обуке координатора, наставника и других корисника система*

На основу приказаних података, може се закључити да процесу увођења информационог система „есДневник“ није претходила анализа стања хардвера и софтвера у школама, нити је постојао акциони план који би пратио обнављање ИТ инфраструктуре у школама. То је за последицу проузроковало неадекватно финансирање система, што се може закључити на основу броја и старости рачунара и

оперативних система, разлике у броју набављених рачунара од стране МПНТР по годинама, где је тај број уместо да се увећава био у паду, разлике у броју (проценту) набављених рачунара по окрузима, недовољног обухвата обуке координатора система по школама, и недовољног броја координатора у неким школама.

Препоручујемо Министарству просвете, науке и технолошког развоја да приликом припреме финансијских планова осигура стабилно финансирање циљева кроз детаљно планирање средстава за развој, набавку и одржавање свих компоненти информационог система „есДневник“.

Налаз 1.2: Непостојање процедура онемогућава контролу обављања послова и пренос знања на новозапослене

Због непостојања подзаконских прописа који се односе на „есДневник“ и преусмерене приоритетне активности МПНТР на успостављање ЈИСП-а, нису усвојене процедуре за управљање ИТ пословима, што онемогућава или отежава контролу ових послова од стране руководства или континуитет обављања послова у случају замене запослених на ИТ пословима. Како је у систему дозвољен рад на даљину и употребу мобилних уређаја, како је потребно обезбедити одговарајући ниво образовања и способности лицима који управљају и користе систем, како је неопходно успоставити праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу потребно је процедурама уредити ове и друге послове како је прописано Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја. Правилником о јединственом информационом систему просвете је требало уредити и вођење евиденције, као што је „есДневник“.

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

Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја прописано је да оператор ИКТ система од посебног значаја, у овом случају МПНТР, између осталог, успоставља организациону структуру, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система од посебног значаја, обезбеђивање да лица која користе ИКТ систем, односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност; заштиту од ризика који настају при променама послова или престанка радног ангажовања лица запослених; идентификовање информационих добара и одређивање одговорности за њихову заштиту итд. У том смислу, успостављају се неке од следећих процедура: Процедура развоја и одржавања информационог система, Процедура за ажурирање информационог система, Процедура за пријављивање и отклањање застоја у раду информационог система, Процедура о коришћењу мобилних уређаја, Процедура за поступање, обраду, складиштење и пренос података итд.

У току ревизије, у вези процедура и политика у ИТ, МПНТР је доставило документацију која се односи на ова питања. Анализом је утврђено да:

Директивом о поступању са рачунарском опремом од 4. јула 2018. године МПНТР је дефинисало начин евидентирања рачунарске опреме коју купује, добија на поклон или добија на привремено коришћење, задуживања и раздуживања рачунарске опреме, као и пријаве и поправке рачунарске опреме. Ова директива се не односи на рачунаре које користе школе и које су набавиле на раније у извештају наведене начине.

Процедуром П01 – Експлоатација и одржавање информационих система од 15. новембра 2018. године, дефинисан је начин и поступак експлоатације и одржавања информационих система, са подручјем примене како у МПНТР, тако, између осталог, и у школама.

Анализом наведене процедуре, уочено је да се не примењује на информациони систем „есДневник“, јер између осталог:

– у члану 6.1.1 Експлоатација системског софтвера на серверима је, између осталог, прописано да уколико запослени констатује било какву неправилност везану за функционисање сервера (констатује прекид рада системског софтвера), дужан је да уради припрему за уклањање и уклања грешку у раду сервера. Међутим, расположиви ресурси не обухватају сервере на којима се извршава систем „есДневник“.

– у члану 6.1.2 Експлоатација апликативних решења прописано је да у случају неправилности функционисања апликативних решења корисник о томе преко електронске поште обавештава запослене на радном месту Администратор портала е-Просвете и пружалац помоћи и подршке корисницима и Администратор портала е-Науке и пружалац помоћи и подршке корисницима. Међутим, корисници система се у случају проблема обраћају хелп-деску пружаоца услуге, а не некоме у МПНТР (осим у појединачним и ретким случајевима). Такође, у члану 6.1.2.6 Пружање корисничке подршке корисницима информационог система је прописано да организатори информационог система из СДПН пружају подршку корисницима радним данима у току радног времена. Корисници се обраћају путем електронске поште где прецизно наводе манифестовање проблема. Међутим, овакву врсту подршке пружа пружалац услуге.

– у члану 6.1.4.1 BACKUP података (сигурносна копија) је прописано да Backup података на серверима извршава запослени на радним местима везаним за администрацију сервиса е-Просвете и администрацију сервиса е-Науке (или запослени у складу са овлашћењима и одговорностима наведеним у уговору). Међутим, овај посао обавља пружалац услуге. Такође, у члану 6.2.3 Одржавање базе података је прописано да одржавање базе података врши запослени у складу са овлашћењима и одговорностима наведеним у уговору. И овај посао обавља пружалац услуге.

Из ове процедуре произлазе следећа упутства: за издавање приступних параметара и за израду извештаја по потреби, такође и записи Захтев за израду извештаја у ИС, за израду генерисаних извештаја, за доделу приступних параметара за информационе системе, за измену или допуну апликативног решења и за пуштање апликативног решења у продукционо окружење.

Координатори и други корисници система у форми упутства су информисани да је увођењем дневника у електронском облику промењена само форма, а да су овлашћења, коришћење и управљање подацима о ученицима и вођењу просветно-васпитне евиденције остала у складу са досадашњим обавезама и одговорностима.

Како су истакли запослени који раде у „есДневник“-у, постоје недоумице у вези тога када се из система брише наставник коме је престао радни однос, шта радити са налогом запосленог који је привремено замењен другим наставником због, на пример боловања итд. Око тога није било недоумица када се користио папирни дневник, јер је приступ папирном дневнику био могућ само физичким путем. У случају електронског дневника, приступ је наставницима омогућен и са локација које су удаљене, па је могуће, између осталог, тако уписивати и часове (чак и ретроактивно тј. са закашњењем), оцене итд. Такође, постоје и недоумице око тога због чега је омогућено брисање оцена „уназад“, тачније са кашњењем од више дана, па и недеља итд.

У току спровођења ревизије, испоставило се да се од школе до школе неки од послова у „есДневник“-у обављају на различите начине, тј. онако како је о томе одлучио директор самостално или заједно са координаторима.

Правилником о јединственом информационом систему просвете, који је донет 29. октобра 2019. године, прописани су ближи услови и начин успостављања Јединственог информационог система просвете, регистара установа, акредитованих високошколских установа, акредитованих студијских програма, запослених у установама и високошколским установама, деце, ученика, одраслих и студената, вођења, прикупљања, уноса, ажурирања и доступности података који се уносе у регистре, као и врсте статистичких извештаја на основу података из регистара. Вођење евиденције, као што је „есДневник“ није уређено у правилнику, иако се начин рада са класичним дневником и електронским дневником у неким пословима разликују – у електронски дневник се подаци могу уносити и удаљеним приступом итд. Зато је те послове неопходно уредити процедурама.

Укупно гледано, може се закључити да у систему не постоје усвојене и имплементиране процедуре које уређују ИТ послове везане за информациони систем „есДневник“, тачније да се постојеће процедуре или не односе на тај систем или се не примењују. Самим тим, није могуће успоставити одговарајући систем контроле или „преношења знања“, што је неопходно у случајевима кадровских замена на овим пословима.

Препоручујемо Министарству просвете, науке и технолошког развоја да успостави процедуре које ће дефинисати функционисање информационог система „есДневник“ када је у питању управљање системом, начин уноса, обраде и ажурирања података који се уносе у систем, и обезбедити континуитет обављања послова у случају замене запослених на ИТ пословима.

Налаз 1.3: Није успостављен процес измене информационог система у складу са потребама корисника

Због тога што МПНТР није успоставило хелп-деск услугу и није успостављена размена података између пружаоца услуга и МПНТР у делу прикупљања и пријављивања проблема и захтева за изменама система од стране корисника, није успостављен процес измене информационог система у складу са потребама корисника, што за последицу може имати смањену ефикасност система, која се огледа у успостављеним функционалностима и корисничким улогама. Надоградња система, како у смислу усклађивања са законским нормама, тако и у смислу надоградње додатних функционалности је дефинисана Уговором о набавци софтверског решења за вођење евиденције у основним и средњим школама (електронски дневник).

Уговором о набавци софтверског решења за вођење евиденције у основним и средњим школама (електронски дневник), од 24. августа 2018. године, пружалац услуге (тачније група пружаоца услуге) се, између осталог, у члану 2. обавезао да ће пружати техничку и корисничку подршку у току трајања уговора. При идентификовању захтева за „есДневник“ МПНТР је у документу Врста, техничке карактеристике, количина и опис добра који је био саставни део Уговора о набавци софтверског решења за вођење евиденције у основним и средњим школама (електронски дневник), од 24. августа 2018. године, у члану 2.1.1 Усклађеност са законом прописало да је неопходно да решење буде у потпуности усклађено са Законом о основама система образовања и васпитања, са Законом о основном образовању и васпитању, са Законом о средњем образовању и васпитању, Законом о заштити података о личности, као и свим релевантним подзаконским актима. Такође, у делу уговора 5.3.1. дефинисана је и надоградња система, како у смислу усклађивања са законским нормама, тако и у смислу надоградње додатних функционалности.

У истом документу у делу 2.4.1. Основна функционалност дефинисане су све основне функционалности које треба да има решење, тј. информациони систем „есДневник“:

- класификациони периоди,
- дневник,
- именик,
- планирање часова,
- извештаји и записници,
- вишејезичност,
- сведочанства,
- списак уџбеника и друге литературе за наставу.

Такође, у делу 2.4.2. Додатне функционалности дефинисане су и додатне функционалности, не као обавезне:

- управљање профилом корисника,
- групно оцењивање писмених радова на истом екрану,
- директорска контролна табла,
- опциона функционалност дневника,
- опциона функционалност именика,
- опциони извештаји.

Корисничко упутство је дефинисано као обавезна функционалност.

Није документован процес консултовања са „заинтересованим“ странама, тј. будућим корисницима система у периоду дефинисања (функционалних) захтева који ће постати део техничке спецификације. Приликом идентификовања (и нових) пословних ИТ процеса, руководство мора имати довољно информација о захтевима и евентуалним проблемима, како би захтев одобрило или одбило, тј. како би управљало ИТ пословима.

Уговорима о пружању услуге подршка, одржавање и хостовање софтверског решења за вођење евиденције у основним и средњим школама (електронски дневник) од 09. децембра 2019. и 25. децембра 2020. године, у члану 2. пружалац услуге се обавезује да пружа услуге подршке, и у складу са Техничким карактеристикама предмета набавке дужан је да обезбеди барем један начин пријаве проблема, примарно путем електронске поште.

У Сектору за дигитализацију у просвети и науци, Правилником о унутрашњем уређењу и систематизацији радних места је у групи за е-Просвету систематизовано радно место администратор портала е-Просвете и пружалац помоћи и подршке корисницима, коме у опису послова, између осталог, стоји: води интерну евиденцију позива корисника и отвара тикете за проблеме које ће решавати програмери и техничка подршка. МПНТР није документовало да су се ови послови обављали када је у питању „есДневник“.

Након интервјуисања једног броја корисника система у току ревизије, и прикупљања података путем упитника и електронске поште, евидентиран је један број предлога за измене постојећих функционалности и увођење нових. Могу се груписати у неколико категорија:

- Штампање докумената,
- Извештавање,
- Оцењивање,
- Вођење евиденција,
- Рад са мешовитим одељењима,
- Додатне функције,
- Остало.

Такође, тренутно решење „есДневник“-а није омогућило коришћење на свим језицима на којима се обавља образовни рад, а што је наведено као обавезна функционалност, зато постоји и предлог за изменама у том смислу од стране једног броја школа.

Ни у Уговору о набавци софтверског решења за вођење евиденције у основним и средњим школама (електронски дневник), ни у Уговорима о пружању услуге подршка, одржавање и хостовање софтверског решења за вођење евиденције у основним и средњим школама (електронски дневник) од 09. децембра 2019. и 25. децембра 2020. године није предвиђено и дефинисано да ће пружалац услуге све прикупљене примедбе и предлоге проследити Министарству ради даље анализе.

У току вршења ревизије установљено је да у ревидираном периоду, МПНТР није прикупљало предлоге од заинтересованих страна, у конкретном случају корисника система (директора, координатора, наставника итд.), ни у периоду израде апликативног решења, ни у току коришћења система, што је неопходно како би процес развоја софтвера довео до ефикаснијег информационог система.

Препоручујемо Министарству просвете, науке и технолошког развоја да уреди процес прикупљања захтева за изменама система и пријављене проблеме од стране корисника успостављањем хелп-деск услуге или механизма размене ових информација са пружаоцем услуга, уколико он врши хелп-деск услугу, који ће обезбедити да све прикупљене информације МПНТР добије у истом тренутку када и пружалац услуге и по потреби у систем уведе и друге кориснике система и имплементира додатне функционалности и креирање додатних врста извештаја.

ЗАКЉУЧАК 2: Нису усвојене и примењене свеобухватне мере заштите информационог система „есДневник“, јер МПНТР није успоставило управљање информационом безбедношћу система кроз неопходну процену ИТ ризика, организациону структуру и усвајање одговарајућих правила и процедура, управљање процесом континуитета пословања, што обухвата и управљање резервним копијама и контролу примене мера заштите, што је неопходно како би била осигурана поузданост система

Информациона безбедност је једно од најважнијих питања које треба уредити и дефинисати мере заштите, а основа за то је управо акт о информационој безбедности.

Поједини послови у овој области треба да су уређени одговарајућим процедурама, то је и законска обавеза, зато што акт о безбедности, као општи акт, обично не садржи детаљне инструкције како се неки процес спроводи и ко је за то одговоран.

Спровођење мера је посао добро обучених, стручних ИТ кадрова. Организацијски треба да буду уређени тако да омогућавају јасну поделу дужности и одговорности, али и контролу свих тих послова.

Посебна пажња се треба посветити питањима приступа систему: физичком и логичком приступу, одговарајућим процедурама, упутствима, евиденцијама, а затим и практичном имплементацијом тих докумената и контролом.

Уколико неке послове обавља пружалац услуге, то је потребно дефинисати уговором. Између осталог, обавезно је дефинисати све обавезе пружаоца услуга када је у питању информациона безбедност.

Законом о информационој безбедности уређени су критеријуми мере заштите од безбедносних ризика у информационо-комуникационим системима (ИКТ). 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. Оператери ИКТ система од посебног значаја су обавезни да донесу мере заштите ИКТ система, које се односе на превенцију и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама, као и мере које обезбеђују континуитет обављања посла у ванредним околностима.

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

Уредбом о утврђивању листе делатности у областима у којима се обављају делатности од општег интереса и у којима се користе информационо-комуникациони системи од посебног значаја се утврђује Листа делатности у областима у којима се обављају делатности од општег интереса и у којима се користе информационо-комуникациони системи.

Законом о основама система образовања и васпитања, у члану 30. прописано је да је надлежност МПНТР да се стара о несметаном протоку података и обезбеђује доступност и заштиту података. Чланом 175. прописано је да уколико установа, високошколска установа, установа ученичког и студентског стандарда, односно јавно признати организатор активности води евиденцију у електронском облику у оквиру

ЈИСП-а, у складу са овим и посебним законом, Министарство је обрађивач података у погледу администрирања система, чувања и заштите података. Истим чланом је прописано и да су установе, високошколске установе, установа ученичког и студентског стандарда, односно јавно признати организатор активности, дужни да у регистар деце, ученика, одраслих, полазника, кандидата и студената (један од регистара у ЈИСП-у) уносе и ажурирају податке из евиденција које воде (што је у овом случају „есДневник“). Министарство успоставља ЈИСП и њиме управља уз техничку подршку службе Владе надлежне за пројектовање, усклађивање, развој, функционисање система електронске управе и друге послове прописане законом (у даљем тексту: Служба Владе). Служба Владе је обрађивач података када обавља послове који се односе на чување, спровођење мера заштите и обезбеђивања сигурности и безбедности података из регистара, у државном центру за чување и управљање података, у складу са прописима којима се уређује електронска управа и информациона безбедност. Ближе услове и начин успостављања ЈИСП-а, регистара, вођења, обраде, уноса, ажурирања, доступности података који се уносе у регистре, као и врсти статистичких извештаја на основу података из регистара, прописује министар. Чланом 184. који се односи на заштиту података прописано је да установа, високошколска установа, установа ученичког и студентског стандарда, односно јавно признати организатор активности обезбеђује мере заштите од неовлашћеног приступа и коришћења података из евиденција које води. Министарство обезбеђује мере заштите од неовлашћеног приступа и коришћења података у ЈИСП-у, када служба Владе не обавља послове из члана 175. Послове администрирања ЈИСП-а и регистара из члана 175. овог закона обавља посебно овлашћено лице у Министарству. Мере безбедности и заштите података из евиденција и регистара прописује министар, како је то прописано чланом 184.

У члану 2. Правилника о јединственом информационом систему просвете прописано је да Министарство обезбеђује и техничке услове у установама за безбедан, сигуран, заштићен, аутентификован и ауторизован приступ ЈИСП-у. Овлашћено лице Министарства (у даљем тексту: Администратор) обавља послове администрирања система, у складу са законом.

Све то, у посматраном периоду ревизије 2017-2020. године, није на адекватан начин препознато од стране МПНТР, почевши од неусвајања основног акта о информационој безбедности, процедура које уређују ту област, а односе се на систем „есДневник“, и непрописивања мера безбедности и заштите података из евиденција и регистара.

Уговором о набавци софтверског решења за вођење евиденције у основним и средњим школама је дефинисано да ће пружалац услуга обезбедити висок степен поузданости решења (доступност од најмање 99,95%), као и функционисање система на секундарној локацији која је физички удаљена од примарне, и са временом успостављања пуне функционалности од три сата, као и редовно формирање резервних копија.

Ризик у области управљања континуитета пословања је велики. МПНТР не располаже властитом ИКТ инфраструктуром нити другим ресурсима потребним за рад система „есДневник“, као нити за рад других система које МПНТР користи, а која су сличног нивоа сложености. Из тог разлога МПНТР се ослања на пружаоце услуга којима је таква врста услуге основна делатност. У случају да пружалац услуга, који је и власник ауторских права на изворном коду, више није у могућности да пружа услугу одржавања, Уговором је предвиђено да Министарство добија сва потребна права да

организује наставак одржавања на други начин. Међутим, у конкретном случају, МПНТР није обезбедило континуитет пословања, јер поред софтверског решења треба обезбедити и одговарајуће техничке услове – хардвер, инфраструктуру итд., али и потребно стручно знање за инсталацију софтвера, базе података, техничку и стручну подршку корисницима итд.

Једно од начела Закона о информационој безбедности је управо процена ИТ ризика. Сва питања разматрана у овој ревизији у основи имају процену одређених ризика (континуитет пословања, приступ подацима од стране пружаоца услуга, организација ИТ безбедности итд.).

Циљ у оквиру другог ревизијског питања је анализа система у области информационе безбедности која треба да да оцену примењених мера заштите, да ли је у информационом систему „есДневник“ успостављен ефективан оквир за континуитет пословања у случају ванредних околности, и да ли је МПНТР успоставило свеобухватно управљање ИТ ризицима.

Наш закључак заснивамо на следећим налазима:

Налаз 2.1: Није у потпуности успостављена организација ИТ безбедности

Организација ИТ безбедности, због недостатка довољно стручног знања и недостатка кадровских капацитета, није успостављена тако да обухвата питања усвајања и примене адекватних докумената која уређују ову област, организациону структуру ИТ безбедности, управљање инцидентима, приступ систему и примену других мера заштите ИКТ система, што за последицу има већи степен рањивости информационог система. Мере заштите од безбедносних ризика треба да буду донете и примењене као што је то прописано Законом о информационој безбедности и Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја.

У овом делу циљ је био да се изврши анализа да ли су усвојена и примењена одговарајућа документа која се односе на информациону безбедност – акт о безбедности информационог система и одговарајуће процедуре, да ли је успостављено управљање инцидентима и примена других мера заштите ИКТ система, што је и законска обавеза свих оператора ИКТ система од посебног значаја, да ли је успостављена организациона ИТ структура са утврђеним пословима и одговорностима запослених за управљање информационом безбедношћу и да ли су запослени оспособљени за посао који раде и разумеју своју одговорност.

Без успостављања адекватне организације ИТ безбедности није могуће управљати подацима на начин прописан законима. Организација ИТ безбедности обухвата више послова које треба уредити, у смислу успостављања управљачке и организационе структуре, обученог и стручног ИТ кадра, процене ИТ ризика, обезбеђивања континуитета пословања у случају ванредних ситуација и у склопу тога управљања резервним копијама података, усвајања и имплементације правила и процедура за све ИТ послове, уређивање обавеза пружаоца услуга у складу са законом и подзаконским актима, контроле логичког и физичког приступа систему, управљања улазним и излазним подацима итд.

Законом о основама система образовања и васпитања прописано је у члану 184. да установа, високошколска установа, установа ученичког и студентског стандарда, односно јавно признати организатор активности обезбеђује мере заштите од неовлашћеног приступа и коришћења података из евиденција које води. Министарство

обезбеђује мере заштите од неовлашћеног приступа и коришћења података у ЈИСП-у, када служба Владе не обавља послове из члана 175. став 9. овог закона. За потребе научноистраживачког рада и приликом обраде података и израде анализа лични подаци користе се и објављују на начин којим није омогућено њихово откривање. Послове администрирања ЈИСП-а и регистара из члана 175. става 4. овог закона обавља посебно овлашћено лице у Министарству. Мере безбедности и заштите података из евиденција и регистара прописује министар како је то прописано чланом 184.

Министар није прописао мере безбедности и заштите података из евиденција и регистара.

МПНТР је донело Директиву о безбедности информационо-комуникационог система Министарства просвете, науке и технолошког развоја 25. августа 2021. године, као меру предузету у току ревизије. У односу на овај документ, потребно је ажурирати и ускладити постојеће правилнике, директиве, процедуре и упутства која се односе на ИТ послове, имајући посебно у виду члан 6. и то:

– Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених којом се остварује управљање информационом безбедношћу у оквиру Министарства, јер је потребно да МПНТР донесе одговарајућа појединачна акта у складу са Правилником о унутрашњем уређењу и систематизацији радних места и да додефинише Директиву о поступању са рачунарском опремом, како би она садржала све наведено у последњем ставу члана 6.1.,

– Постизање безбедности рада на даљину и употребе мобилних уређаја, јер МПНТР није документовало Евиденцију о уређајима намењеним за рад на даљину, што је неопходно имајући у виду одржавање „есДневника“ од стране пружаоца услуга,

– Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа,

– Обезбеђивање исправног и безбедног функционисања средстава за обраду података, јер МПНТР није документовало лог записе који се односе на ревидирани период,

– Заштита од губитака података, јер према важећем уговору процесом израде резервних копија управља пружалац услуга,

– Чување података о догађајима који могу бити од значаја за безбедност ИКТ система, јер МПНТР није документовало лог записе који се односе на ревидирани период,

– Безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система, јер се позива на процедуре које не обухватају „есДневник“,

– Одржавање уговореног нивоа информационе безбедности и пружаних услуга у складу са условима који су уговорени са пружаоцем услуга, јер није дефинисано на који начин МПНТР извршава мере надзора, нити је повезано са процедурама које ово питање уређују,

– Мере које обезбеђују континуитет обављања посла у ванредним околностима.

Поред свега наведеног, не постоји део који се односи на процену ризика, а процена ИТ ризика с једне стране не само што је можда најважније начело Закона о информационој безбедности због своје важности, већ је и основа од које се полази приликом израде свих других процедура за ИТ послове.

Од шест радних места систематизованих Правилником о унутрашњем уређењу и систематизацији радних места, у Сектору за дигитализацију у просвети и науци, у групи за е-Просвету у опису послова руководилац групе је дефинисано између осталог: стара се о спровођењу прописа из области безбедности ИКТ система, у опису послова администратора сервиса е-Просвете стоји: стара се о исправности успостављених процедура које обезбеђују одржавање квалитета и безбедности података у оквиру ЈИСП-а („есДневник“ је практично део ЈИСП-а), док у групи за дигитализацију у образовању опису послова радног места за примену дигитализације у образовању, између осталог, стоји: стара се о благовременом поступању по прописима из области безбедности ИКТ система.

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

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

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

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

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

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

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

Нису организоване обуке за запослене у школама који користе информационе системе, што ствара ризик да они нису у довољној мери информисани о могућим безбедносним претњама, нити довољно обучени да на њих одговоре правовременим предузимањем мера (вируси, фишинг итд.).

МПНТР није усвојило све неопходне процедуре које се односе на информациону безбедност, а анализа достављених – постојећих процедура показује да се не односе на безбедност система „есДневник“.

Када су у питању школе и систем „есДневник“, осим упутства које су добили, координатори у школама који отварају налоге корисницима у складу са улогама немају дефинисане процедуре које ова питања уређују, што није у складу са чланом 10. Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја. Такође, ови послови нису наведени у опису послова радних места на којима раде координатори.

Закон о основама система образовања и васпитања, у члану 126. тачка 12., прописује: директор установе је одговоран за благовремен и тачан унос и одржавање ажурности базе података о установи у оквиру јединственог информационог система просвете.

Закон о основном образовању и васпитању, у члану 88. прописује: директор школе се стара и одговоран је за благовремен и тачан унос података и одржавање ажурности евиденција и безбедност података, без обзира на начин њиховог вођења.

Закон о средњем образовању и васпитању, у члану 77. прописује: директор школе се стара и одговоран је за благовремен и тачан унос података и одржавање ажурности евиденција и безбедност података, без обзира на начин њиховог вођења.

Практично, одговорност директора је различито прописана у овим законима, јер се у Закону о основама система образовања и васпитања не наводи да је одговоран за безбедност података без обзира на начин њиховог вођења.

Имајући у виду да школе нису уговарале коришћење система „есДневник“ и да не могу имати утицај на безбедност података у том систему, јер су само корисници који приступају путем web приступа, директори школа не могу у потпуности одговорити обавези да су одговорни за безбедност података у систему „есДневник“, јер се подаци не похрањују у школама.

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

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

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

Циљ управљања инцидентима је успостављање механизама да се најпре инциденти евидентирају, а затим и да се правовремено реагује. Како се инцидент може десити било где у систему, запослени који уочи настали проблем треба обавестити надлежно лице, које ће предузети даље кораке, или дати инструкције. Уколико се не врши

евидентирање инцидената, и не спроводе мере како се такав инцидент не би поновио, то може као последицу имати понављање инцидената, које није морало да се деси, самим тим и настанак додатне штете у систему (оштећење, нестанак рачунарске опреме, штете настале активирањем малициозног кода, неовлашћен приступ систему, покушаји упада у систем итд.)

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

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

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

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

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

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

Сходно томе, МПНТР треба да овај процес уреди поштујући управо наведене одредбе Закона, али и одредбе Директиве о безбедности ИКТ система од посебног значаја. Али, то не значи само да се свим корисницима система доделе параметри приступа и улоге у систему. Потребно је и обезбедити механизам контроле тог процеса, како би се у сваком тренутку могло установити да ли листа корисника одговара тренутној листи корисника система, са одговарајућим улогама.

На сличним принципима се уређује и физички приступ, дакле обухвата одређивање лица која могу да приступе сервер собама, разлоге за то, тј. улоге тих лица, и механизам контроле тог процеса.

На основу свега наведеног, може се закључити да организација ИТ безбедности није успостављена тако да обухвата питања усвајања и примене адекватних докумената (процедуре, директиве итд.) која уређују ову област, а односи се на организациону структуру ИТ безбедности, управљање инцидентима, приступ систему и примену других мера заштите ИКТ система, што за последицу има већи степен рањивости информационог система.

Препоручујемо Министарству просвете, науке и технолошког развоја да успостави мере информационе безбедности које обухватају усвајање и имплементацију аката која уређују ову област, укључујући и процес одобравања и укидања приступа информационом систему „есДневник“, адекватну организациону структуру ИТ безбедности, управљање инцидентима и друге неопходне мере безбедности и заштите података из евиденција информационог система „есДневник“.

Налаз 2.2: Не постоји план континуитета пословања у случају раскида уговора са пружаоцем услуга

Министарство просвете, науке и технолошког развоја, због тога што не располаже потребним ресурсима, није у потпуности успоставило мере које обезбеђују континуитет пословања у ванредним околностима, што у случају прекида сарадње са пружаоцем услуга за последицу може имати нефункционисање информационог система у дужем временском периоду. Мере које обезбеђују континуитет пословања у ванредним околностима, што укључује и случај раскида уговора/сарадње са пружаоцима услуга, треба да буду уређене како је прописано Законом о информационој безбедности, Уредбом о ближем уређењу мера заштите информационо-комуникационих система.

Један од циљева ревизије је био анализа процеса континуитета пословања у ванредним околностима. Анализа је обухватила све целине које чине делотворан план континуитета пословања: донета правила и процедуре која уређују континуитет пословања, успостављање плана опоравка од катастрофе, управљање резервним копијама и тестирање ових планова и резервних копија.

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

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

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

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

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

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

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

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

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

Уговором о набавци софтверског решења за вођење евиденције у основним и средњим школама („есДневник“) је прецизирано да пружалац услуге, између осталог, има обавезу припреме резервне копије система на удаљеној локацији коју обезбеди МПНТР и на којој ће се чувати резервна копија софтверског решења, као и обавезу редовног формирања резервних копија података. У документу који као прилог чини саставни део уговора – Врста, техничке карактеристике, количина и опис добра, у делу 2.1.6. – Поузданост решења, дефинисано је да је пружалац услуге дужан да обезбеди функционисање решења и на другој, ДР локацији (за опоравак у случају отказа примарне локације), која ће бити физички удаљена од примарне локације. ДР локација мора обезбедити очување пуне функционалности решења са евентуално умањеним капацитетом и временом успостављања пуне функционалности које не сме бити дуже од три сата од тренутка отказа примарне локације. И примарна локација и секундарна локација се налазе у Београду, секундарна локација је у функцији од марта 2019. године. Власник опреме је „Телеком Србија“ ад.

Уговором о пружању услуге – Подршка, одржавање и хостовање софтверског решења за вођење евиденције у основним и средњим школама („есДневник“), пружалац услуге се у складу са прилогом који је саставни део уговора – Техничке карактеристике (спецификација) премета набавке, између осталог, обавезао да ће формирати дневне криптоване резервне копије података са роком чувања од 180 дана, као и да ће резервне копије сместити и на ДР локацију, као и да ће обавити све неопходне радње како би се успоставила пуна функционалност у случају отказа система на примарној локацији.

Директивом о безбедности информационо-комуникационог система Министарства просвете, науке и технолошког развоја од 25. августа 2021. године, када је у питању процес континуитета пословања, између осталог, прописано је да у циљу заштите од губитка података МПНТР врши израду резервних копија које обухватају системске информације, апликације и податке који су неопходни за опоравак целокупног система у случају наступања последица изазваним ванредним околностима, и да је, између осталог, спровођење ових активности у делокругу рада Сектора за дигитализацију у просвети и науци МПНТР и групе за одржавање квалитета у интерној мрежи рачунара МПНТР.

Дакле, са једне стране, а према важећем уговору, процесом израде резервних копија управља пружалац услуга, а са друге стране, за овај посао су надлежни запослени у МПНТР.

Када је у питању „есДневник“ МПНТР нема активну улогу у процесу прављења резервних копија.

Истом Директивом је прописано да су мере које министарство примењује, а које обезбеђују континуитет пословања дефинисане Планом телекомуникационо-информатичког обезбеђења и заштите (криптозаштите) информација. Међутим, према

наводима овлашћених лица МПНТР, када је у питању план континуитета пословања, група пружаоца услуга има развијен план континуитета функционисања „есДневник“ система. План континуитета пословања темељи се на опоравку инфраструктуре, апликативног сервиса „есДневник“, те резервних копија података.

МПНТР не располаже властитом ИКТ инфраструктуром потребном за рад система „есДневник“, због чега се ослањају на пружаоце услуга којима је таква врста услуге основна делатност, тако да је приликом израде тендерске документације за набавку система за вођење евиденција МПНТР поставило критеријуме у смислу потребне озбиљности понуђача. МПНТР наводи да су понуђачи своју озбиљност, између осталог, доказивали организационом и техничком опремљеношћу и капацитетима, референцама, као и потребним људским ресурсима одређених профила.

МПНТР је као најповољнију понуду, која је задовољавала све задате услове, одабрао понуду конзорцијума којег предводи највећи пружалац ИКТ услуга у Србији, предузеће „Телеком Србија“ ад. Ово предузеће, којег је већински власник Република Србија, је уједно и власник опреме на којој се пружа уговорена услуга хостовања решења. У складу са озбиљношћу понуђача, МПНТР сматра да је ризик у смислу немогућности извршења уговорених услуга од стране пружаоца услуге сведена на минимум.

У случају да пружалац услуга, који је и власник ауторских права на изворном коду, више није у могућности да пружа услугу одржавања, Уговором је предвиђено да Министарство добија сва потребна права да организује наставак одржавања на други начин.

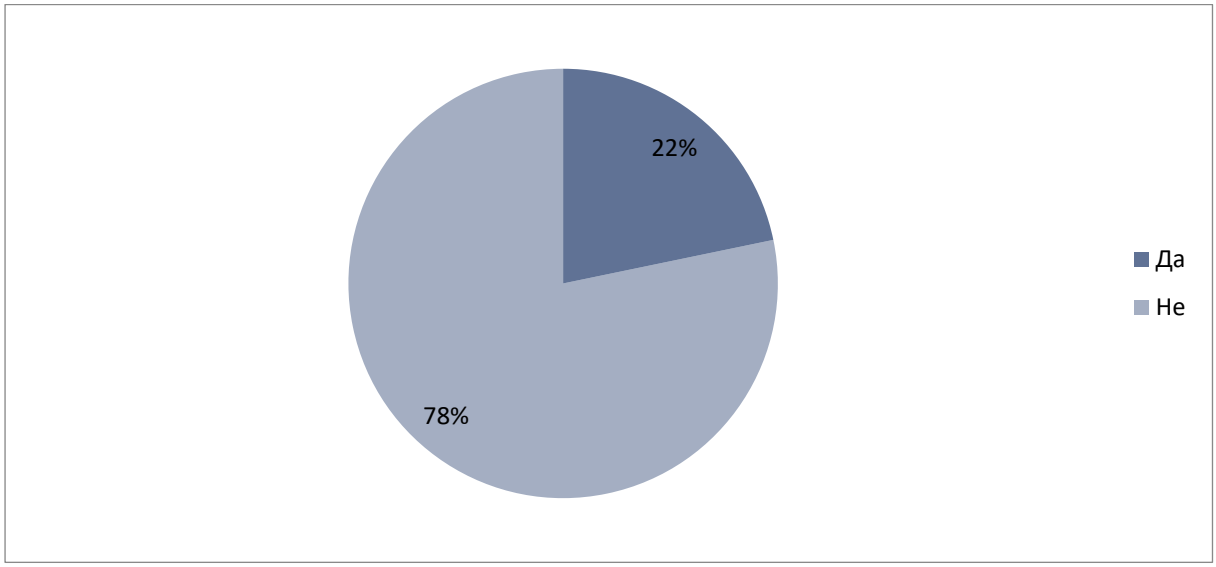
Уговором о набавци софтверског решења за вођење евиденције у основним и средњим школама („есДневник“) је дефинисано у члану 7. да Добављач преноси Наручиоцу право својине на испорученим и инсталираним софтверским решењем, као и право својине над свим измењеним верзијама софтверског решења које у току трајања овог уговора буду испоручене Наручиоцу.

Међутим, план континуитета пословања мора обухватити и ситуације када дође до раскида уговора између тренутног пружаоца услуга и МПНТР. У конкретном случају, МПНТР није обезбедило континуитет, јер поред софтверског решења треба обезбедити и одговарајуће техничке услове – хардвер, инфраструктуру итд., али и потребно стручно знање за инсталацију софтвера, базе података, техничку и стручну подршку корисницима итд.

Када су школе у питању, један од начина да школа обезбеди податке о образовно-васпитном раду у случају нефункционисања „есДневник“-а је и постојање папирне евиденције.

На питање да ли школе воде и паралелну, папирну евиденцију о успеху и владању ученика, 122 школе је одговорило да води и папирну евиденцију, односно 22% од укупног броја школа, док је 439 одговорило да не води, односно 78% од укупног броја школа.

Вођење папирне евиденције је битно, јер уколико дође до губитка података или нефункционисања „есДневник“-а дужи временски период, наставници би могли несметано да наставе активности, између осталог, и закључивање оцена. Школама је остављен простор да бирају да ли ће водити само папирну евиденцију, само електронску или и папирну и електронску евиденцију.



Илустрација 16. *Да ли школе воде и папирну евиденцију о успеху и владању ученика?*

Други начин који школама омогућава рад и у случају нефункционисања система је извоз података који је омогућен директору школе. Уколико би се подаци периодично извозили, наставници би имали увид у оцене чак и ако не би функционисао „есДневник“. Овако извезене податке је потребно заштитити од неодобреног увида, измене итд.

Препоручујемо Министарству просвете, науке и технолошког развоја да успостави континуитет пословања у ванредним околностима, на начин да обезбеди функционисање система и у случају прекида сарадње са пружаоцима услуга, а што подразумева неопходан хардвер, апликативни софтвер, изворни код, стручно знање, базе података, управљање резервним копијама података, и процес тестирања планова континуитета пословања.

Налаз 2.3: Није успостављено управљање ИТ ризицима

Министарство просвете, науке и технолошког развоја, због непознавања ове проблематике, недовољно искуства и обученог ИТ кадра, није успоставило управљање ИТ ризицима, што за последицу може имати стварање непотребно великих трошкова у случају настанка нежељеног догађаја, а који се могао спречити, или великих нефинансијских губитака (података на пример) због неблаговременог предузимања мера. Управљање ИТ ризицима треба да буде уређено како је прописано Законом о информационој безбедности и Уредбом о ближем уређењу мера заштите информационо-комуникационих система. То је и обавеза дефинисана Уговором о обради података о личности.

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

Разлози зашто је то тако су управо последице које могу настати или које су већ настале у информационим системима, а које стварају губитке, финансијске или

нефинансијске природе (података на пример), који се добром проценом ризика могу избећи.

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

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

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

Како је наведено у МПНТР, Одредбама Уговора о набавци софтверског решења, као и о одржавању, управљање ризицима је пренето на Добављача, па је његова одговорност да води рачуна о сигурности, безбедности и доступности система. Група пружаоца услуга спроводи управљање ИТ ризицима у складу са ISO стандардима, као и IT risk management framework-у који се користи приликом самог развоја, дистрибуције и инсталације апликативног решења. Процена ризика се, међутим, не може пренети на пружаоца услуга, не може се аутсорсовати, зато што могуће штетне последице, пре свега, погађају онога ко је власник система, у овом случају МПНТР, а не пружаоца услуга.

Уговором о обради података о личности, који је закључен 07. маја 2021. године између МПНТР и групе понуђача, у члану 5. који се односи на безбедност обраде је дефинисано да су уговорне стране дужне да спроводе одговарајуће мере заштите, како би био достигнут одговарајући ниво безбедности у односу на ризик итд. У истом члану је дефинисано да су уговорне стране дужне да засебно изврше процену вероватноће наступања ризика и ниво ризика, као и да одреде мере заштите, како би се умањио процењени ризик.

МПНТР није успоставило управљање ризицима, што подразумева евидентирање, класификацију, анализу ИТ ризика и дефинисање стратегије за смањивање/отклањање ризика. Из тог разлога, Министарству је дата одговарајућа препорука.

Препоручујемо Министарству просвете, науке и технолошког развоја да успостави управљање ИТ ризицима, што подразумева евидентирање, класификацију, анализу ИТ ризика и дефинисање стратегије за смањивање/отклањање ризика.

ЗАКЉУЧАК 3: Министарство није успоставило ефективан механизам сарадње са пружаоцима услуге, зато што није усвојило и имплементирало правила и процедуре када је у питању ова област, није успоставило администрирање система на законима прописан начин и није процес обраде података о личности уредило на јасан, законом прописан начин

Информациона безбедност је једно од најважнијих питања које треба уредити и дефинисати мере заштите. Основа за то је управо акт о информационој безбедности, или у случају МПНТР Директива о безбедности информационо-комуникационог система МПНТР, која је донета 25. августа 2021., и која није постојала у ревидираном периоду. Поједини послови у овој области треба да су уређени одговарајућим процедурама, то је и законска обавеза, зато што акт о безбедности као општи акт обично не садржи детаљне инструкције како се неки процес спроводи, и ко је за то одговоран.

Спровођење мера је посао добро обучених, стручних ИТ кадрова. Организацијски треба да буду уређени тако да омогућавају јасну поделу дужности и одговорности, али и контролу свих тих послова.

Уколико неке послове обавља пружалац услуге, то је потребно дефинисати уговором. Између осталог, обавезно је дефинисати све обавезе пружаоца услуга када је у питању информациона безбедност.

Посебна пажња се треба посветити питањима приступа систему: физичком и логичком приступу, али и успостављању континуитета пословања, нарочито у случају када је то уговором дефинисана обавеза пружаоца услуга, зато што у случају раскида уговора постоји ризик да систем неће моћи да функционише у дужем временском периоду.

МПНТР приликом покретања процеса набавке система „есДневник“, почев од покретања пилот пројекта, затим покретања јавне набавке система годину дана касније, а и касније током ревидираног периода није донело процедуре које уређују сарадњу са пружаоцима услуга, посебно када је у питању информациона безбедност. То је онемогућило свеобухватан механизам контроле извршења обавеза које у том смислу законски има и Министарство и пружалац услуге.

Када су у питању евиденције које воде школе, Законом о изменама и допунама Закона о основама система образовања и васпитања[20] чланом 8. извршено је брисање дотадашњег члана 174., који је прописивао да је руковалац подацима у евиденцији о ученицима школа. Није прописано ко је „нови“ руковалац подацима. Овакво решење уноси забуну у дефинисању односа руковалац-обрађивач, о чему ће бити речи у овом делу извештаја.

Наш закључак заснивамо на следећим налазима:

[20] „Службени гласник РС", број 6/20

Налаз 3.1: Сарадња са пружаоцем услуга није уређена процедурама, самим тим није успостављен неопходан механизам контрола, нити је процес обраде података уређен на законом прописан начин

Због тога што нису прописане мере безбедности и заштите података из евиденција, МПНТР није усвојило правила и процедуре које се односе на безбедност података када су у питању уговори са пружаоцима услуга, тако да и поред тога што у уговорима са пружаоцима услуга постоји део који се односи на поверљивост података, није успостављен механизам за контролу да ли пружалац услуга поштује обавезе у вези поверљивости података, и није обезбедило обраду података о личности на законом прописан начин, што за последицу може имати смањени степен поузданости система. Треба обезбедити заштиту средстава оператора ИКТ система која су доступна пружаоцима услуга и механизам који ће обезбедити одржавање уговореног нивоа информационе безбедности и пружених услуга, у складу са условима који су уговорени са пружаоцем услуга како је прописано Законом о информационој безбедности и Уредбом о ближем уређењу мера заштите информационо-комуникационих система. У Уговору о обради података о личности треба јасно бити дефинисано ко је руковалац подацима, а ко обрађивач како је прописано Законом о заштити података о личности.

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

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

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

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

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

оператор ИКТ система успоставља механизме надзора над пружањем услуга, именује лице које је задужено за праћење реализације пружања услуга и контролу испуњености нивоа информационе безбедности, применом одговарајућих процедура и успоставом надзора.

МПНТР није усвојило процедуре које се односе на одржавање уговореног нивоа информационе безбедности и пружених услуга, у складу са условима који су уговорени са пружаоцем услуга.

Између осталих, у складу са обавезама из Уговора о набавци система, није успостављена ни имплементирана процедура којом се контролише да се систему приступа само са локација које се налазе у Републици Србији. МПНТР није документовало да спроводи контролу приступа која се односи на то да ли се систему приступа и са локација ван Републике Србије.

МПНТР није успоставило процедуру која се односи на чување и депоновање изворног кода, што представља обавезу пружаоца услуге из Уговора о набавци система. МПНТР није документовало да врши контролу овог процеса.

Закон о основама система образовања и васпитања прописује у члану 15. да се када је у питању вођење евиденције у штампаном и/или електронском облику у установама, сви видови прикупљања, обраде, објављивања и коришћења података спроводе у складу са овим, посебним и законом којим се уређује заштита података о личности.

Када је у питању успостављање ЈИСП-а који чини скуп база података и рачунарских програма, потребних за прикупљање и обраду података у евиденцијама и регистрима, уз обезбеђивање заштите података о личности, прописано је чланом 175. да установа, високошколска установа, односно установа ученичког и студентског стандарда води евиденцију о деци, ученицима, одраслима и студентима обухваћеним формалним образовањем, о родитељима, односно другим законским заступницима и о запосленима, а јавно признати организатор активности о полазницима и кандидатима обухваћеним неформалним образовањем, у складу са овим и посебним законом. Уколико установа, високошколска установа, установа ученичког и студентског стандарда, односно јавно признати организатор активности води евиденцију у електронском облику у оквиру ЈИСП-а, у складу са овим и посебним законом, Министарство је обрађивач података у погледу администрирања система, чувања и заштите података. У оквиру ЈИСП-а, Министарство, између осталог, води регистар деце, ученика, одраслих, полазника, кандидата и студената у који се уносе подаци из евиденција које води установа, високошколска установа, установа ученичког и студентског стандарда, односно јавно признати организатор активности.

Министарство успоставља ЈИСП и њиме управља уз техничку подршку службе Владе надлежне за пројектовање, усклађивање, развој, функционисање система електронске управе и друге послове прописане законом (у даљем тексту: Служба Владе).

Ближе услове и начин успостављања ЈИСП-а, регистара, вођења, обраде, уноса, ажурирања, доступности података који се уносе у регистре, као и врсти статистичких извештаја на основу података из регистара, прописује министар.

У члану 176., у процесу доделе ЈОБ-а установа, високошколска установа, односно јавно признати организатор активности уноси податке у ЈИСП о идентитету детета, ученика, одраслог и студента: име, презиме, име једног родитеља, јединствени матични број грађана, други идентификациони број и опис идентификационог броја за страног

држављанина, лице без држављанства и тражиоца држављанства, односно лице које није уписано у матичну књигу рођених Републике Србије. Подаци о личности из става 4. овог члана обрађују се у сврху доделе ЈОБ-а детету, ученику, одраслом и студенту. Подаци о личности из става 4. овог члана могу да се обрађују и у сврху израде статистичких извештаја на начин којим није омогућено откривање података о личности, у складу са законом. Изузетно, подаци о личности из става 4. овог члана могу да се обрађују и у друге сврхе прописане законом. Министарство је руковалац подацима о личности из става 4. овог члана.

Чланом 4. Закона о заштити података о личности прописано је да 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 је 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).

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

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

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

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

Члан 45. овог закона прописује да ако се обрада врши у име 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 (став 1).

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

Обрада од стране обрађивача мора бити уређена уговором или другим правно обавезујућим актом, који је закључен, односно усвојен у писменом облику, што обухвата и електронски облик, који обавезује обрађивача према 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 (став 3).

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

1) обрађује податке о личности само на основу писмених упутстава 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. овог закона;

4) поштује услове за поверавање обраде другом обрађивачу из ст. 2. и 7. овог члана;

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. овог закона;

6) помаже руковаоцу у испуњавању обавеза из члана 50. и чл. 52. до 55. овог закона, узимајући у обзир природу обраде и информације које су му доступне;

7) после окончања уговорених радњи обраде, а на основу одлуке 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 става 4. тачка 8) овог члана, обрађивач је дужан да без одлагања упозори руковаоца ако сматра да писмено упутство које је од њега добио није у складу са овим законом или другим законом којим се уређује заштита података о личности.

Члан 50. овог закона уређује безбедност обраде тако да у складу са нивоом технолошких достигнућа и трошковима њихове примене, природом, обимом, околностима и сврхом обраде, као и вероватноћом наступања ризика и нивоом ризика за права и слободе физичких лица, руковалац и обрађивач спроводе одговарајуће

техничке, организационе и кадровске мере како би достигли одговарајући ниво безбедности у односу на ризик (став 1).

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

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

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

Руковалац и обрађивач дужни су да предузму мере у циљу обезбеђивања да 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 (став 5).

МПНТР је приликом потписивања Уговора о пружању услуге – Подршка, одржавање и хостовање софтверског решења за вођење евиденције у основним и средњим школама (електронски дневник) одредило лице које је одговорно за праћење и контролу извршења уговорних обавеза.

У уговору о набавци система „есДневник“, у члану 6. се пружалац услуге обавезао да ће обавезе које су предмет уговора извршавати у складу са прописима, док је у документу Врста, техничке карактеристике, количина и опис добра, који је саставни део уговора, дефинисано да решење мора бити потпуно усклађено са Законом о заштити података о личности. У уговору постоји одредба која наводи да школе рукују и обрађују податке – део 4.2. дефинише да свака школа прикупља, рукује и обрађује само своје податке, односно податке својих запослених, родитеља/старатеља и ученика који похађају конкретну школу, без могућности да види остале податке. Пружалац услуге је дужан да обезбеди да свака школа има могућност непосредног (директног) уноса података, без да школе податке у било каквом облику достављају понуђачу (пружаоцу услуге) или Наручиоцу (Министарству).

У Уговору о пружању услуге – Подршка, одржавање и хостовање софтверског решења за вођење евиденције у основним и средњим школама (електронски дневник), који је закључен 09. децембра 2019. године, у члану 6. се пружалац услуге обавезује да чува и штити све податке са којима буде упознат у току пружања услуга, а у делу који се односи на тајност података је дефинисан начин на који пружалац услуга и овлашћено лице министарства приступају систему.

У Уговору о пружању услуге – Подршка, одржавање и хостовање софтверског решења за вођење евиденције у основним и средњим школама (електронски дневник), који је закључен 25. децембра 2020. године, у члану 5. се пружалац услуге обавезује да услугу пружа у складу са законом и прописима који регулишу предметну област, у члану 6. да чува и штити све податке са којима буде упознат у току пружања услуга, и да ће међусобне радње у вези са обрадом података о личности регулисати Уговором о

обради података о личности. У делу који се односи на тајност података је дефинисан начин на који пружалац услуга и овлашћено лице министарства приступају систему.

Министарство је као обрађивач података када су у питању евиденције које води школа са групом пружаоца услуга закључило Уговор о обради података о личности 07. маја 2021. године, а предмет уговора је регулисање међусобних права и обавеза уговорних страна у вези са радњама обраде података о личности. То није у складу са чланом 45. Закона о заштити података о личности који прописује да 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 (став 1). Обрађивач из става 1. овог члана може поверити обраду другом обрађивачу само ако га руковалац за то овласти на основу општег или посебног писменог овлашћења.

МПНТР у ревидираном периоду није обезбедило обраду података о личности на законом прописан начин, јер школе као руковаоци подацима у евиденцији „есДневник“ нису у складу са наведеним одредиле нити повериле обраду података обрађивачу, у овом случају МПНТР, самим тим ни обрађивач није могао да обраду повери другом обрађивачу (у овом случају групи пружаоца услуга).

Препоручујемо Министарству просвете, науке и технолошког развоја да усвоји и имплементира правила и процедуре за безбедност података када је у питању сарадња са пружаоцима услуга, што подразумева обавезну примену мера заштите података, и успостављање механизма за праћење примене тих мера, и уреди процес обраде података од стране пружаоца услуга у информационом систему „есДневник“ на законом прописан начин.

Налаз 3.2: МПНТР није успоставило управљање и администрирање информационим системом „есДневник“ на начин који подразумева да само Министарство има администраторски приступ систему

Због тога што нису прописане мере безбедности и заштите података из евиденција, МПНТР није успоставило управљање и администрирање информационим системом „есДневник“ на начин који подразумева да само Министарство има администраторски приступ систему, што за последицу може имати нарушавање поверљивости и интегритета података. Министарство је обрађивач података у погледу администрирања система, чувања и заштите података, када установа води евиденцију у електронском облику у оквиру ЈИСП-а, како је то прописано Законом о основама система образовања и васпитања. Овлашћено лице Министарства (у даљем тексту: Администратор) обавља послове администрирања система, у складу са законом и Правилником о јединственом информационом систему просвете. Уговором о пружању услуге – Подршка, одржавање и хостовање софтверског решења за вођење евиденције у основним и средњим школама (електронски дневник), пружалац услуга ће добити приступ систему путем налога са минималним неопходним привилегијама приступа за која се изјасни као неопходна. Не и администраторски налог.

Законом о основама система образовања и васпитања у члану 30. је прописано да МПНТР успоставља и управља јединственим информационим системом просвете у Републици Србији, стара се о несметаном протоку података и обезбеђује доступност и заштиту података. Када је у питању заштита података, чланом 184. је прописано да установа, високошколска установа, установа ученичког и студентског стандарда,

односно јавно признати организатор активности обезбеђује мере заштите од неовлашћеног приступа и коришћења података из евиденција које води.

Једина мера коју може установа да примени када је у питању заштита од неовлашћеног приступа јесте неодавање података за приступ које користе запослени у школи.

Међутим, у почетку коришћења система десило се да су ученици у четири наврата дошли у посед корисничких имена и лозинки које користе наставници. Како наводе у МПНТР, све уговорне стране, у сарадњи са крајњим корисницима, благовремено су детектовале те детаљно анализирале сваку такву појаву, а у складу с тиме и правовремено реаговале на неутрализацију штете. Овде се ради искључиво о грешци наставника, крајњих корисника система „есДневник“, који су непажњом омогућили ученицима да дођу у посед њихових креденцијала. Свим наставницима, по узору на улоге већег степена комплексности у систему, омогућена је и напреднија аутентификација у два корака (двофакторска). Овакав начин пријаве није обавезан, и не користи се у довољној мери.

Министарство обезбеђује мере заштите од неовлашћеног приступа и коришћења података у ЈИСП-у, када служба Владе не обавља послове из члана 175. став 9. овог закона. За потребе научноистраживачког рада и приликом обраде података и израде анализа лични подаци користе се и објављују на начин којим није омогућено њихово откривање. Послове администрирања ЈИСП-а и регистара из члана 175. става 4. овог закона обавља посебно овлашћено лице у Министарству. Чланом 184. је прописано да мере безбедности и заштите података из евиденција и регистара прописује министар. Наведене мере нису прописане.

Правилником о јединственом информационом систему просвете прописано је да тај систем успоставља и њиме управља МПНТР, и да обезбеђује услове за безбедност и сигурност техничке опреме и софтвера, као и потребне ресурсе за функционисање ЈИСП-а. Министарство обезбеђује и техничке услове у установама за безбедан, сигуран, заштићен, аутентификован и ауторизован приступ ЈИСП-у. Овлашћено лице Министарства (у даљем тексту: Администратор) обавља послове администрирања система, у складу са законом. Подаци из ЈИСП-а доступни су искључиво у сврху прописану законом.

За потребе пружања услуга, а како је то дефинисано Уговором о пружању услуге – Подршка, одржавање и хостовање софтверског решења за вођење евиденције у основним и средњим школама (електронски дневник), пружалац услуга ће добити приступ систему путем налога са минималним неопходним привилегијама приступа за која се изјасни као неопходна. Уколико пружалац услуге накнадно утврди постојање потребе за вишим нивоом привилегија од оног који је дефинисан Записником, пружалац ће приступ спровести у сарадњи са лицем које овласти Министарство. Истим уговором, пружалац услуге се обавезао да ће систему приступати искључиво у сврху инсталације, нових верзија решења, подешавања, надоградње, дораде и одржавања система, те да неће вршити неовлашћен приступ подацима који се чувају у оквиру решења.

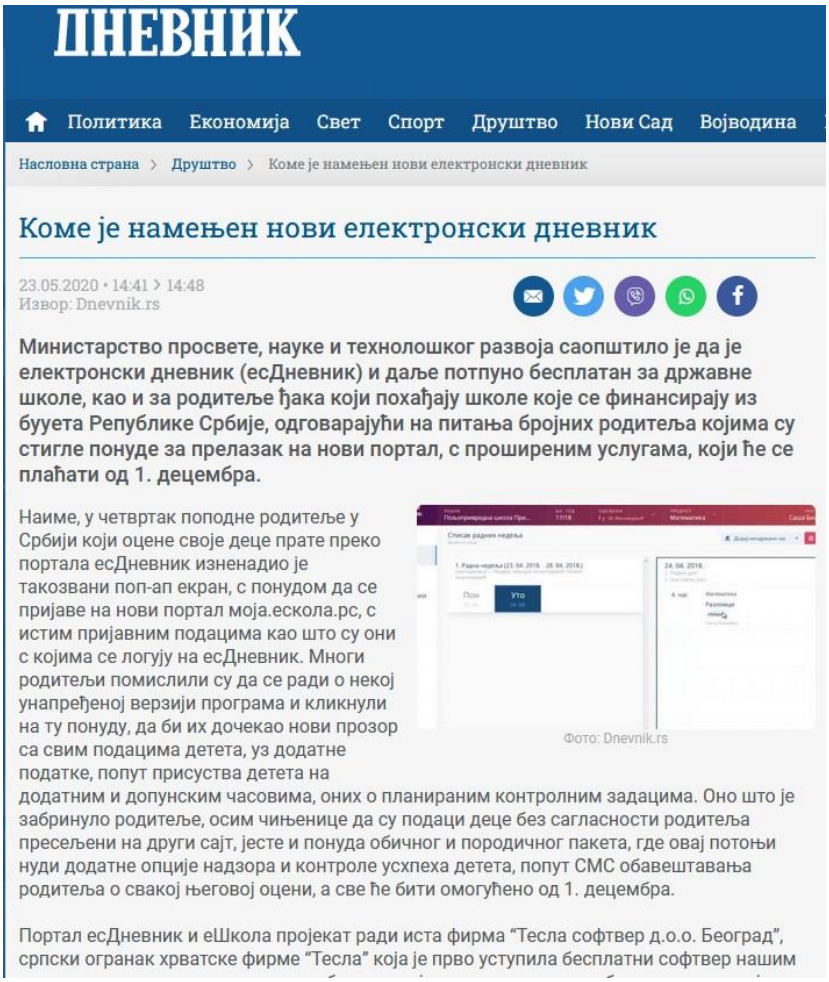
МПНТР није документовало да је потписан записник о минималним привилегијама које ће пружалац услуге имати приликом приступа систему.

Уговор о набавци система „есДневник“ није у складу са наведеним правилником, јер је у уговору дефинисано да ће пружалац обављати послове администрирања система, док је правилником дефинисано да ће те послове обављати овлашћено лице Министарства. Такође, како је дефинисано Уговором о пружању услуге – Подршка,

одржавање и хостовање софтверског решења за вођење евиденције у основним и средњим школама (електронски дневник), пружалац услуга ће добити приступ систему путем налога са минималним неопходним привилегијама приступа за која се изјасни као неопходна. Не и администраторски налог.

У мају 2020. године дошло је до неовлашћене могућности приступа подацима ученика преко портала „moja.eskola.rs“, који је у власништву фирме „Tesla software“ д.о.о. Београд, дакле фирме која није члан групе пружалаца услуге.

Вести о овом догађају пренели су и многи медији, а у вези са овим покренут је надзор од стране Повереника за информације од јавног значаја и заштиту података о личности.



ДНЕВНИК

Политика Економија Свет Спорт Друштво Нови Сад Војводина

Насловна страна › Друштво › Коме је намењен нови електронски дневник

Коме је намењен нови електронски дневник

23.05.2020 • 14:41 › 14:48
Извор: Dnevnik.rs

Министарство просвете, науке и технолошког развоја саопштило је да је електронски дневник (есДневник) и даље потпуно бесплатан за државне школе, као и за родитеље ђака који похађају школе које се финансирају из буџета Републике Србије, одговарајући на питања бројних родитеља којима су стигле понуде за прелазак на нови портал, с проширеним услугама, који ће се плаћати од 1. децембра.

Наиме, у четвртак поподне родитеље у Србији који оцене своје деце прате преко портала есДневник изненадио је такозвани поп-ап екран, с понудом да се пријаве на нови портал моја.ескола.рс, с истим пријавним подацима као што су они с којима се логују на есДневник. Многи родитељи помислили су да се ради о некој унапређеној верзији програма и кликнули на ту понуду, да би их дочекао нови прозор са свим подацима детета, уз додатне податке, попут присуства детета на додатним и допунским часовима, оних о планираним контролним задацима. Оно што је забринуло родитеље, осим чињенице да су подаци деце без сагласности родитеља пресељени на други сајт, јесте и понуда обичног и породичног пакета, где овај потоњи нуди додатне опције надзора и контроле усхпеха детета, попут СМС обавештавања родитеља о свакој његовој оцени, а све ће бити омогућено од 1. децембра.

Фото: Dnevnik.rs

Портал есДневник и еШкола пројекат ради иста фирма "Тесла софтвер д.о.о. Београд", српски огранак хрватске фирме "Тесла" која је прво уступила бесплатни софтвер нашим

Илустрација 17. *Вест о догађају објављена на порталу „Дневник“-а*

Како су навели представници МПНТР, приликом приступа порталу „есДневник“ појавила се реклама за приступ унапређеном порталу „еШкола“, којем су родитељи могли да приступе коришћењем већ додељених креденцијала за приступ „есДневник“-у, и на тај начин су родитељи могли да виде податке о оценама, владању итд. своје деце. Подаци, како су навели у МПНТР, нису пренети у други систем, већ се портал „еШкола“ систему „есДневник“ представио као „родитељ“ управо користећи креденцијале које је родитељ унео, и тако „повукао“ податке из система „есДневник“ и приказао их у новом облику.

Наведена реклама, и могућност приступа другом порталу нису биле уговорене функционалности између МПНТР и групе пружалаца услуге, самим тим увођење те функционалности није било одобрено од стране МПНТР. Уговором о одржавању, у делу 2.3.2 је дефинисано да ће понуђач обезбедити надоградњу система или појединих функционалности у смислу усклађивања са законским нормама, или које затраже наручилац и/или корисници решења, а које олакшавају или поспешују рад корисника, или које уносе нову вредност. У конкретном случају, наведена реклама/функционалност није затражена ни од стране наручиоца (МПНТР) нити од стране корисника решења. Такође, наведена реклама/функционалност не уноси нову вредност у „есДневник“, јер се ради о понуди за коришћење другог портала, у власништву фирме која није чланица групе пружалаца услуге.

Илустрација 18. *Почетна страница портала moja.eSkola.rs на дан 15.10.2021*

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

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

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

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

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

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

МПНТР није усвојило процедуру за одобравање и укидање овлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа која треба да овај процес уреди поштујући управо наведене одредбе. Али, то не значи само да се свим корисницима система доделе параметри приступа и улоге у систему. Потребно је и обезбедити механизам контроле тог процеса како би се у сваком тренутку могло установити да ли листа корисника одговара тренутној листи корисника система, са одговарајућим улогама.

Само на такав, свеобухватан начин управљања логичким приступом се може обезбедити неопходан степен безбедности система и података.

На сличним принципима се уређује и физички приступ, дакле обухвата одређивање лица која могу да приступе сервер собама, разлоге за то, тј. улоге тих лица, и механизам контроле тог процеса.

Као што је наведено, МПНТР треба да пропише и услове за доделу и коришћење администраторских права.

Препоручујемо Министарству просвете, науке и технолошког развоја да уреди администрирање и управљање системом на начин да једино МПНТР има администраторска права, док ће пружалац услуга и корисници моћи да систему приступе једино уз одобрење и контролу администратора

V Захтев за доставу одазивног извештаја

Субјект ревизије 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 умањење ризика од појављивања одређене несврсисходности у свом будућем пословању за чије предузимање субјект ревизије мора поднети уз одазивни извештај одговарајуће доказе.

Субјект ревизије је обавезни 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 оних који су отклоњени у току обављања ревизије и садржани у поглављу Мере предузете у поступку ревизије. За мере исправљања је дужан да уз одазивни извештај достави доказе према следећем:

1. За налазе, односно несврсисходности првог приоритета, односно које је могуће отклонити у року од 90 дана субјект ревизије је у обавези да достави доказе о отклањању несврсисходности односно предузимању мера исправљања;
2. За налазе, односно несврсисходности другог приоритета, односно које је могуће отклонити у року до годину дана субјект ревизије је у обавези 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;
3. За налазе, односно несврсисходности трећег приоритета, односно које је могуће отклонити у року од једне до три године субјект ревизије је у обавези 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 оцена да ли су мере исправљања исказане у одазивном извештају задовољавајуће.

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

Ако се оцени да одазивни извештај не указује да су откривене несврсисходности отклоњене на задовољавајући начин, сматра се да субјект ревизије крши обавезу доброг пословања. Ако се ради о незадовољавајућем отклањању значајне несврсисходности, сматра се да постоји тежи облик кршења обавезе доброг пословања. У овим случајевима Државна ревизорска институције је овлашћена да предузима мере сагласно члану 40. ст 7. до 13. Закона о Државној ревизорској институцији.

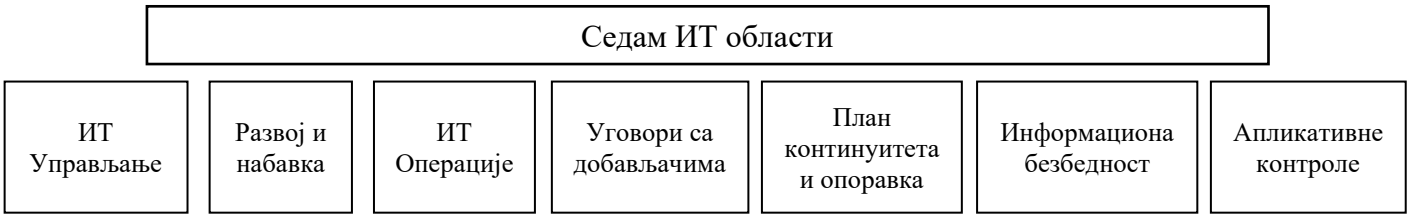
VI Прилог

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[21]), као и све податке добијене од субјекта ревизије и извора информација – школа. Анализирали смо податке и информације за период од 2017. до 2020. 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.



Илустрација 15. *ИТ области*

У циљу одговора на ревизијска питања, а имајући у виду законодавни и институционални оквир у периоду 2017 – 2020. године, за субјект ревизије изабрано је Министарство просвете, науке и технолошког развоја.

У циљу прикупљања података који нису доступни у документима, обавили смо интервјуе и послали упитнике корисницима информационог система „есДневник“.

У току спровођења ревизије школама је послат упитник, у коме су тражени следећи подаци:

- Да ли школа користи „есДневник“ (ДА/НЕ),
- Назив школе,
- Општина,
- Број ученика,
- Укупан број одељења у школској 2020/2021,
- Број истурених одељења,
- Број наставника-корисника система „есДневник“,
- Број десктоп рачунара који се користе (и) за рад у „есДневник“-у,
- Број лаптоп рачунара који се користе (и) за рад у „есДневник“-у,
- Број таблета који се користе (и) за рад у „есДневник“-у,

[21] INTOSAI Радна група за ИТ ревизију

- Број координатора система „есДневник“,
- Датум последње обуке координатора,
- Датум последње обуке наставника и других корисника система,
- Интернет обезбедила школа или министарство,
- Да ли имате предлоге/сугестије за побољшање система,
- Да ли водите и паралелну, папирну евиденцију о успеху и владању ученика,
- Врста уређаја (декстоп/лаптоп/таблет),
- Старост уређаја,
- Оперативни систем,
- Из којих средстава је набављен рачунар (сопствена средства/локална самоуправа/средства министарства).

Када су у питању школе, поред података добијених на основу упитника, обављени су и интервјуи и са једним бројем корисника система – директорима, координаторима и наставницима.

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

1. За прво ревизијско питање:

- Преглед ИТ стратегије или интервјуисање руководства да би се утврдило на који начин су утврђени и одобрени циљеви и неопходни ресурси система „есДневник“;
- 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 документације;
- Увид у евиденцију о рачунарској опреми по школама, и поређење са евиденцијама у изабраном узорку школа;
- Преглед одобрених или одбијених захтева за изменом система;
- Преглед документације везане за пријаву и решавање проблема корисника;
- Преглед ИТ организационе шеме да би се утврдило да је усклађена тако да пружа потребну подршку и у складу са законским обавезама;
- Разговори са запосленима који су одговорни за поштовање правила и процедура да би се утврдило колико често они извештавају више руководство о својим резултатима и на који начин они анонимно и независно траже податке о непоштовању;
- Разговори са руководиоцима и корисницима да би се разумело њихово виђење и став у вези са анализом правила и процедура.

2. За друго ревизијско питање:

- Анализа Акта о безбедности ИКТ система;

- Преглед докумената за процену да су правила и процедуре у складу са Законом о информационој безбедности и Уредбом о ближем уређењу мера заштите;
- 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;
- Преглед извештаја о спроведеним обукама који се односе на информациону безбедност;
- Анализа шта су примарне контроле физичке безбедности организације субјекта ревизије. Провера да ли одговарају најновијој анализи ризика;
- 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.);
- Анализа извештаја о инцидентима ради процене шта је предузето;
- Провера процедура у циљу утврђивања колико често се прегледају различити приступи и привилегије које запослени или корисници имају у организацији;
- Интервјуи са узорком корисника и провера упутства да би се утврдило како су корисници упознати са својим одговорностима за заштиту осетљивих информација или имовине, када им се одобри приступ;
- Анализа спискова корисника у школама и у МПНТР ради оцене ажурности;
- Провера процедуралних мера које је установа предузела да би се ускладила са захтевима поверљивости;
- Провера да ли уговорни услови и обавезе дефинишу безбедносна ограничења и обавезе које контролишу како ће извођачи користити имовину организације и приступати информационим системима и услугама;
- Провера да ли су извођачи извршили повреде безбедности информација. Провера активности руководства у погледу таквих кршења;
- Преглед докумената да би се проценило да правила и процедуре узимају у обзир захтеве за континуитет пословања кроз дефинисање организационих циљева за непредвиђене ситуације;
- Преглед или интервјуисање запослених да би се утврдило колико често се правила и процедуре за континуитет пословања ажурирају уколико се промене услови;
- Преглед докумената да би се проценило да план за прављење резервних копија садржи све кључне хардвере, податке, апликативне софтвере;
- Преглед докумената да би се проценило да су израђене детаљне процедуре за прављење резервних копија;
- Преглед докумената да би се проценило да се план за прављење резервних копија адекватно спроводи;
- Анализа евидентирања да би се проценило да је прављење резервних копија почело у утврђеним временским оквирима и да су резервне копије задржане за назначен временски период;

- Преглед докумената да би се проценило да су израђене детаље процедуре за опоравак и да садрже параметре за поновно постављање система, инсталационе закрпе, успостављајући поставку конфигурације, доступност системске документације и оперативних процедура, реинсталацију апликативних и системских софтвера, доступност најновијих резервних копија, тестирање система;

- Преглед докумената да би се проценило да је ИТ кадар обучен на пољу процедура за прављење резервних копија и опоравак;

- Преглед докумената да би се проценило да ли су све релевантне ставке обухваћене тестирањем;

- Преглед докумената да би се проценило да ли се реализују тестирања у одређеним временским интервалима, и благовремено;

- Провера да ли се организација постарала да је континуитет пословања садржан у споразуму о пружању услуге;

- Анализа стратегије за управљање ризицима;

- Провера поштовања примене упутстава/правилника који дефинишу унос оцена и других података у „есДневник“.

3. За треће ревизијско питање:

- Анализирати како је од стране пружаоца услуге уређен приступ „есДневник“-у и серверима на којима је „есДневник“ инсталиран, као и другим потребним ресурсима и да ли се то евидентира и где;

- Анализа механизма МПНТР за праћење извршења уговора са пружаоцима услуга;

- Проверити да ли се прати извршење обавеза пружаоца услуге када су у питању нивои услуга дефинисани уговором;

- Провера извештаја о безбедносним инцидентима и докумената за праћење како би се утврдило које активности МПНТР предузима када пружалац услуге крши безбедносна правила и процедуре;

- Провера процедура које је МПНТР предузело а које се односе на питања поверљивости;

- Провера да ли уговорни услови и обавезе дефинишу безбедносна ограничења и обавезе које контролишу како ће пружалац услуге користити имовину организације и приступати информационим системима и услугама;

- Провера да ли су пружаоци услуга извршили повреде безбедности информација. Провера активности руководства у погледу таквих кршења;

- Провера процедура у циљу утврђивања колико често се прегледају различити приступи и привилегије које запослени код пружаоца услуга имају;

- Добијање документације и процена пројекта, имплементације, приступа и прегледање;

- Проверити да ли је, уз нулте или минималне трошкове, могуће из постојећег система добити додатне услуге, превасходно у области извештавања (школске управе, министарство);

- Да ли постоје капацитети да се услуге које сада обезбеђује пружалац услуга реализују унутар МПНТР?

Обавили смо интервјуе са одговорним лицима Министарства просвете, науке и технолошког развоја, као и у школама које смо посетили.

Такође, у циљу прикупљања доказа и одговора на ревизијска питања, послат је велики број захтева за доставу одговора запосленима у школама, како би одвојено посматрали како је успостављен систем код субјекта ревизије, а како код школа.