"Службени гласник РС", број 53/2011

На основу члана 33. став 1. Закона о тајности података ("Службени гласник РС", број 104/09) и члана 42. став 1. Закона о Влади ("Службени гласник РС", бр. 55/05, 71/05 - исправка, 101/07, 65/08 и 16/11),

Влада доноси

УРЕДБУ

о посебним мерама заштите тајних података у информационо-телекомуникационим системима

I. УВОДНА ОДРЕДБА

Члан 1.

Овом уредбом утврђују се посебне мере заштите тајних података у информационо-телекомуникационим системима.

II. ПОСЕБНЕ МЕРА ЗАШТИТЕ ТАЈНИХ ПОДАТАКА У ИНФОРМАЦИОНО-ТЕЛЕКОМУНИКАЦИОНИМ СИСТЕМИМА

Члан 2.

Посебне мере заштите тајних података у информационо-телекомуникационим системима (у даље тексту: систем) могу бити техничке и организационе, а предузимају се у циљу спречавања случајних грешака, неправилног и недозвољеног прикупљања, чувања, обраде, коришћења, оштећења, уништења, као и фалсификовања и злоупотребе тајних података.

Посебне мере заштите тајних података у систему односе се на: објекат у коме је смештен систем (опрема, документи, програмска подршка и мрежа); простор, просторије, односно безбедносне зоне у којима се обрађују тајни подаци у систему; овлашћена лица за управљање безбедношћу система; све учеснике у раду система; коришћење система за потребе рада са тајним подацима; режим рада система; заштиту тајних података приликом обраде и чувања у систему; заштиту од ризика компромитујућег електромагнетног зрачења, као и инсталирање уређаја за чување тајних података.

Члан 3.

Техничке мере из члана 2. став 1. ове уредбе нарочито се односе на:

1) физичку заштиту објеката, простора, просторије, односно безбедносне зоне у којима се обрађују тајни подаци у систему, као и средстава и докумената из система;

2) противпожарну заштиту;

3) обезбеђивање и заштиту опреме (избор одговарајуће и поуздане опреме, обезбеђивање опреме током њеног рада, редовно сервисирање и снабдевање резервним деловима) и докумената при њиховом коришћењу и чувању;

4) заштиту програмске подршке (у фази пројектовања, развоја и коришћења програмског система);

5) заштиту мреже (приликом пројектовања и рада).

Организационе мере из члана 2. став 1. ове уредбе нарочито се односе на:

1) организацију технологије рада у систему при пројектовању (израда прелиминарне студије о развоју којом се утврђује степен тајности података који се обрађују у систему и степен тајности самог система, идејног пројекта, главног пројекта, извођачког пројекта и увођења пројектованих решења) и при оперативним раду система (планирање рада и вођење евиденција о извршавању свих поступака у раду система и кретању документације);

2) утврђивање поступака у случају ванредних околности;

3) остале услове за успешно функционисање система (контрола приликом заснивања радног односа, утврђивање послова и задатака учесника у раду система, стручна обука запослених и др.).

Члан 4.

Простор, просторије, односно безбедносне зоне у којима се обрађују тајни подаци у систему одређују се у складу са прописом којим се утврђују посебне мере физичко-техничке заштите тајних података.

Члан 5.

Орган јавне власти, односно правно лица које по основу уговорног односа пружа услуге органу јавне власти (у даљем тексту: правно лице), одређују овлашћено лице за управљање безбедношћу система.

Овлашћено лице за управљање безбедношћу система у органу јавне власти, односно правном лицу, прати и оцењује безбедносне карактеристике система.

Приликом одређивања овлашћених лица за управљање безбедношћу система, орган јавне власти, односно правно лице, дужни су да обезбеде да једно лице не контролише све важне елементе безбедности система, као и да та лица поседују одговарајући сертификат за приступ тајним подацима.

Члан 6.

Систем мора да испуњава услове за:

1) заштиту од неауторизованог приступа, која подразумева идентификовање и поуздано гарантовање идентитета (аутентикација) лица која имају приступ систему;

2) контролу и вођење евиденције о приступу систему;

3) континуирано бележење (аутоматизовано, ручно или комбиновано) о безбедносном стању система (безбедносни запис), активностима система, као и изменама постојећег стања система;

4) проучавање безбедносних записа од стране овлашћених лица;

5) одређивање овлашћења корисницима у вези са безбедношћу система;

6) одређивање овлашћења корисницима у вези са коришћењем система;

7) обезбеђивање безбедног начина означавања степена тајности;

8) идентификацију корисника који врши измене, штампање, преснимавање или брисање тајног документа;

9) бележење измене, штампање, преснимавање или брисање тајног податка од стране корисника;

10) заштиту важних техничких и програмских елемената, системских могућности и функционалности система;

11) обезбеђење резервних архива тајних података, за случај губитка постојећих архива, као и вођење евиденција о приступу архивама.

Члан 7.

Систем ради у једном од следећих безбедносних режима:

1) "НЕСЕЛЕКТИВНИ";

2) "СЕЛЕКТИВНИ";

3) "СА ВИШЕ НИВОА".

Руководилац органа јавне власти, односно одговорно лице у правном лицу посебним актом одређује безбедносни режим рада система.

Члан 8.

У систему који ради у безбедносном режиму "НЕСЕЛЕКТИВНИ", сва лица која имају приступ том систему морају да имају сертификат за приступ тајним подацима највишег

степена тајности података који се обрађују у систему и имају приступ свим тајним подацима који се обрађују у систему.

У систему који ради у безбедносном режиму "СЕЛЕКТИВНИ", сва лица која имају приступ том систему морају да имају сертификат за приступ тајним подацима највишег степена тајности података који се обрађују у систему и могу приступати само одређеним тајним подацима.

У систему који ради у безбедносном режиму "СА ВИШЕ НИВОА", лица која имају приступ том систему не морају да имају сертификат за приступ тајним подацима највишег степена тајности података који се обрађују у систему и имају приступ само одређеним тајним подацима који се обрађују у систему.

Селективан приступ систему и селективан приступ тајним подацима у систему спроводи се помоћу одговарајућег хардвера и софтвера.

Члан 9.

Тајни податак не сме се преносити кроз систем изван безбедносних зона без примене метода и средстава криптозаштите, који су одобрени од стране органа надлежног за спровођење послова у области криптозаштите.

Члан 10.

Ради одржавања безбедности система у току његовог коришћења, орган јавне власти, односно правно лице спроводи:

1) периодичну проверу система, свих његових делова и медија за чување и пренос тајних података, као и сагледавање достигнутих услова за обезбеђење поверљивости, расположивости, интегритета и аутентичности тајних података у систему;

2) чување података који се односе на систем, као и тајних података који се обрађују у систему на посебним документима, уз обавезно вођење резервних евиденција и примену мера заштите које су предвиђене за податке са највишим степеном тајности података који се налазе у систему;

3) инсталирање хардвера, софтвера и конфигурисање система од стране овлашћених лица;

4) примењивање нових техничких и програмских средстава у систему у складу са одговарајућим техничким стандардима СРПС ИСО/ИЕЦ 27001 и СРПС ИСО/ИЕЦ 17799;

5) сервисирање и поправку средстава из система на начин који не нарушава безбедност система;

6) контролни преглед на средствима из система која су била на сервисирању и поправци изван органа јавне власти, односно правног лица од утицаја компромитујућег електромагнетног зрачења од стране стручних лица;

7) одговарајући поступак приликом неовлашћеног откривања тајности документа или губитка документа који садржи тајни податак;

8) одговарајући поступак приликом откривања неовлашћеног упада у систем;

9) планирање мера безбедности у случају ванредних ситуација.

Члан 11.

Преносива информационо-телекомуникациона средства и документа која се користе у систему, сматрају се тајним податком и могу се укључити у систем само ако је претходно извршена провера могућег угрожавања система од стране стручних лица органа јавне власти, односно правног лица.

Ако орган јавне власти, односно правно лице нема стручна лица за проверу из става 1. овог члана, провера се врши у органу јавне власти који има стручна лица, на основу међусобног споразума.

Члан 12.

Документа која се користе у систему, означена различитим степенима тајности, означавају се вишим степеном тајности, у складу са законом.

Документи који обезбеђују приступ систему (шифре, лозинке, елементи идентификације и др.) штите се мерама предвиђеним за заштиту података који се налазе у систему, означеним са највишим степеном тајности.

Члан 13.

Приватна информационо-телекомуникациона средства и преносиви документи (лични рачунари, преносиви рачунари, дискете, меморијски модули и др) не могу се користити за обраду тајних података.

Члан 14.

Ако се тајном податку степена тајности "ДРЖАВНА ТАЈНА" или "СТРОГО ПОВЕРЉИВО" промени или укине степен тајности, документу на којем је тај податак био записан у електронском облику, не може се променити или укинути степен тајности.

Ако се тајном податку степена тајности "ПОВЕРЉИВО" или "ИНТЕРНО" промени или укине степен тајности, документу на којем је тај податак био записан у електронском облику, може се променити или укинути степен тајности, само кад је тај податак избрисан на начин да га је немогуће обновити софтверским алатом.

Документа из ст. 1. и 2. овог члана морају се уништити након истека рока њихове употребе или након истека рока употребе система у којем су се користили, у складу са прописом којим се утврђују посебне мере физичко-техничке заштите тајних података.

Члан 15.

Технички застарела или оштећена документа на којима су чувани тајни подаци уништавају се, у складу са прописом којим се утврђују посебне мере физичко-техничке заштите тајних података.

Члан 16.

Коришћење аутоматизованих информационо-телекомуникационих средстава која раде без присуства оператера заснива се на процени ризика безбедности система, коју врши руководилац органа јавне власти, односно одговорно лице у правном лицу.

Члан 17.

Сви делови система који се користе за обраду тајних података степена тајности "ДРЖАВНА ТАЈНА", "СТРОГО ПОВЕРЉИВО" или "ПОВЕРЉИВО" морају бити заштићени од компромитујућег електромагнетног зрачења, применом техничких, односно оперативних мера за заштиту од утицаја тог зрачења, у складу с проценом ризика од компромитујућег електромагнетног зрачења.

Члан 18.

Инсталирање уређаја и софтвера у систему врши овлашћено лице за управљање безбедношћу система у органу јавне власти, односно правном лицу.

Члан 19.

Ако се тајни подаци размењују са страном државом или међународном организацијом, поред посебних мера предвиђених овом уредбом, примењују се и стандарди за безбедност мрежа, уређаја за пренос, међусобну повезаност система и криптозаштиту тајних података, предвиђени међународним споразумом.

III. КОРИШЋЕЊЕ СИСТЕМА ЗА ПОТРЕБЕ РАДА СА ТАЈНИМ ПОДАЦИМА

Члан 20.

Орган јавне власти, као и правно лице које намерава да користи систем за обраду и чување тајних података, претходно извршава процену могућег угрожавања безбедности тајних података од упада у систем, као и процену угрожавања употребе и уништавања тајних података који су обрађени и сачувани у систему (у даљем тексту: процена ризика безбедности система).

Процена ризика безбедности система односи се на утврђивање ризика, процену ризика који се не могу избећи, процену угрожености система, као и претње и могуће последице

реализације претњи за систем, укључујући и ризике у вези са окружењем у којем се систем користи.

Процена ризика безбедности система врши се периодично, у складу са планом за процену ризика система који доноси руководилац органа јавне власти, односно одговорно лице у правном лицу.

Члан 21.

Ако орган јавне власти, односно правно лице имају потребу да повежу своје системе, закључују споразум о повезивању тих система.

Члан 22.

Уз процену ризика безбедности система руководилац органа јавне власти, односно одговорно лице у правном лицу доноси акт којим прописује безбедносни поступак за пријем, обраду, пренос, чување и архивирање тајних података у електронском облику, као и чување пројектне документације (прелиминарне студије о развоју система, идејни пројекат, главни пројекат и извођачки пројекат).

Члан 23.

Процена ризика безбедности система врши се за систем у коме се обрађују, преносе и чувају тајни подаци степена тајности "ДРЖАВНА ТАЈНА", "СТРОГО ПОВЕРЉИВО" и "ПОВЕРЉИВО".

За систем у коме се обрађују тајни подаци који су означени степеном тајности "ИНТЕРНО", орган јавне власти, односно правно лице обезбеђује одржавање одговарајућег нивоа безбедности тајних података (поверљивости, целовитости, аутентичности или доступности), у складу са прописима којима се уређује информациона безбедност.

Проверу спровођења нивоа безбедности из става 2. овог члана, врши орган јавне власти или правно лице, односно овлашћено лице за управљање безбедношћу система.

IV. УПРАВЉАЊЕ РИЗИКОМ БЕЗБЕДНОСТИ СИСТЕМА

Члан 24.

Управљање ризиком безбедности система састоји се од трајног процењивања и обраде ризика, ради спречавања уништења, отуђења, губитка и неовлашћеног приступа тајним подацима.

Орган јавне власти, односно право лице доноси одлуку о управљању ризиком безбедности система.

Члан 25.

Обрада ризика безбедности система представља активност у којој се за сваки процењени ризик утврђује степен прихватљивости ризика, у циљу његовог прихватања, смањења или избегавања.

Ризик се сматра прихватљивим ако би настала штета била мања од штете која би настала услед неспровођења безбедносних мера.

Смањивање ризика спроводи се применом безбедносних мера, у циљу спречавања уништења, отуђења, губитка и неовлашћеног приступа тајним подацима.

Избегавање ризика подразумева предузимање безбедносних мера, у циљу избегавања радњи које би могле изазвати ризик.

Члан 26.

После доношења одлуке о обради ризика, орган јавне власти, односно правно лице, доноси акт о обради ризика којим се утврђује спровођење потребних безбедносних мера.

Резултати процењивања и обраде ризика редовно се ревидирају, у складу са потребама органа јавне власти, односно правних лица, на основу насталих унутрашњих или спољашњих промена система.

V. ЗАВРШНА ОДРЕДБА

Члан 27.

Ова уредба ступа на снагу осмог дана од дана објављивања у "Службеном гласнику Републике Србије".

05 број 110-5619/2011
У Београду, 14. јула 2011. године

Влада

Први потпредседник Владе -
заменик председника Владе,
Ивица Дачић, с.р.