НАЦРТ

ЗАКОН О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ

I. ОСНОВНЕ ОДРЕДБЕ

Предмет уређивања

Члан 1.

Овим законом се уређују мере заштите од безбедносних ризика у информационо-комуникационим системима, одговорности правних лица приликом управљања и коришћења информационо-комуникационих система и одређују се надлежни органи за спровођење мера заштите, координацију између чинилаца заштите и праћење правилне примене прописаних мера заштите.

Значење појединих термина

Comment [GZ1]: Додати и дефинисати појам сертификације –акредитације и стим у вези ново настале појмове акредитовани руководилац ИКТ система, сертификовани ИКТ систем, и слично

Члан 2.

Поједини термини у смислу овог закона имају следеће значење:

1) *информационо-комуникациони систем* (ИКТ систем) може бити:

(1) електронска комуникациона мрежа у смислу закона који уређује електронске комуникације;

(2) уређај или група међусобно повезаних уређаја, такав да се у оквиру тог уређаја, односно у оквиру барем једног из те групе уређаја, врши аутоматска обрада података у складу са рачунарским програмом;

(3) рачунарски подаци који се похрањују, обрађују, претражују или преносе помоћу средстава из подтачака (1) и (2) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;

2) *руковалац ИКТ система* је орган јавне власти или организациона јединица органа јавне власти, односно правно лице одговорно за рад ИКТ система;

3) *информациона безбедност* представља скуп мера и радњи које омогућавају да ИКТ систем заштити тајност, интегритет, расположивост, аутентичност и непорецивост података којима се рукује путем тог система, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;

4) *тајност* је својство података, односно информација, које захтева одређен начин поступања ~~са податком који обезбеђује да~~ током обраде, и чувања и дистрибуције није како не би постао доступан неовлашћеним лицима;

5) *интегритет* значи очуваност изворног садржаја и комплетности података и информација;

6) *расположивост* је својство података које значи да се податкомцима и информацијама управља на начин који обезбеђује да је су податкомци и информације доступани и употребљиви на захтев овлашћених лица онда када им је потребан;

7) *аутентичност* је својство података које значи да се податкомцима и информацијама управља на начин који омогућава проверу и потврду да је податке, односно информације створио или послао онај за кога је декларисано да је назначену операцију извршио;

8) *непорецивост* представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;

9) *ризик* значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података и информација или нарушавања исправног функционисања ИКТ система;

10) *управљање ризиком* је систематичан скуп мера који укључује планирање, организовање и усмеравање активности како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;

11) инцидент је свака околност или догађај којим се остварује неповољан ефекат на информациону безбедност;

12) *мере заштите ИКТ система* су нормативне (правне, организационе и кадровске), физичко-техничке, логичке и криптолошке ~~техничке и организационе~~ мере за управљање безбедносним ризицима ИКТ система;

13) *тајни податак* значи тајни податак у смислу прописа којима се уређује област заштите тајних података, односно информација;

14) *ИКТ систем за рад са тајним подацима, односно информацијама* је ИКТ систем који је у складу са законом одређен за рад са тајним подацима, *односно информацијама*;

15) *орган јавне власти* је државни орган, орган територијалне аутономије, орган јединице локалне самоуправе, организација којој је поверено вршење јавних овлашћења, правно лице које оснива државни орган, орган територијалне аутономије или локалне самоуправе, као и правно лице које се претежно, односно у целини финансира из буџета;

16) *служба безбедности* је служба безбедности у смислу закона којим се уређују основе безбедносно-обавештајног система Републике Србије;

17) *самостални руковаоци ИКТ система* су министарство надлежно за послове одбране, министарство надлежно за унутрашње послове, министарство надлежно за спољне послове и службе безбедности;

18) *компромитујуће електромагнетно зрачење (КЕМЗ)* представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;

19) *криптобезбедност* је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите.

20) *криптозаштита* је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;

21) *криптографски производ* је софтвер или уређај путем кога се врши криптозаштита;

22) *криптоматеријали* су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;

23) *безбедносна зона* је зона у смислу прописа којима се уређује област заштите тајних података;

24) *информациона добра* обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште акте, процедуре и слично.

Начела

Члан 3.

Приликом планирања и примене мера заштите ИКТ система треба се руководити начелима:

1) *начело управљања ризиком* – избор и ниво примене мера се заснива на процени ризика, потреби за превенцијом ризика и отклањања последица ризика који се остварио, укључујући све врсте ванредних околности;

2) *начело целовите заштите* – мере се примењују на свим организационим, физичким и техничко-технолошким нивоима, као и током целокупног животног циклуса ИКТ система;

3) *начело стручности и добре праксе* – мере се примењују у складу са стручним и научним сазнањима и искуствима у области информационе безбедности;

4) *начело свести и оспособљености* – сва лица која својим поступцима ефективно или потенцијално утичу на информациону безбедност треба да буду свесна ризика и поседују одговарајућа знања и вештине.

5) *Načelo upravljivosti* – Informaciona bezbednosna rešenja, primenjena u IKT sistemima, moraju biti u potpunosti upravljiva od strane korisnika.

Надлежни орган

Члан 4.

Орган државне управе надлежан за безбедност ИКТ система је министарство надлежно за послове информационог друштва (у даљем тексту: Надлежни орган).

Тело за координацију послова информационе безбедности

Члан 5.

У циљу остваривања сарадње и усклађеног обављања послова у функцији унапређења информационе безбедности, као и иницирања и праћења превентивних и других активности у области информационе безбедности Влада образује Тело за координацију послова информационе безбедности (у даљем тексту: Тело за координацију), као координационо тело Владе, у чији састав улазе представници министарства надлежних за послове информационог друштва, одбране, унутрашњих послова, спољних послова, правде, представници служби безбедности, Канцеларије Савета за националну безбедност и заштиту тајних података, Генералног секретаријата Владе, Управе за заједничке послове републичких органа и Националног ЦЕРТ-а.

Актом Владе ближе се уређује организација и начин рада Тела за координацију и образују се стручне радне групе за потребе Тела за координацију.

Одговорност за безбедност ИКТ система

Члан 6.

Руковаоци свих ИКТ система у Републици Србији одговорни су за предузимање одговарајућих мера заштите ИКТ система којима се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају

Comment [GZ2]: Начело управљивости ИБ

Comment [U3]: Погрешо писмо, латиница уместо ћирилице

Comment [GZ4]: Надлежност Министарства

Comment [GZ5]: Министарство задужено за регулисање области је Министарство надлежно за послове информационог друштва (у даљем тексту Министарство, мада је под условом да се информациона безбедност посматра на нивоу националног кибер простора онда ово пре свега домен министарстава силе, пре свега МО)
Овде треба навести надлежности Министарства у области информационе безбедности таксативно:
- Предлаже Влади уредбе из ИБ
- Доноси подзаконске акте из ИБ
-Доноси Националну Стратегију из ИБ
- Дефинише критичну инфраструктуру из ИБ
- Прописује обавезе власника и управљача критичне инфраструктуре
- Врши надзор функционисања система ИБ у државним органима и организацијама као и свим осталим управљачима и власницима критичне инфраструктуре
- Доноси планове активности и развоја из области ИБ
- Врши инспекцијски надзор над применом законске регулативе из области ИБ и свих других законских оквира који директно или индиректно утичу на ИБ
-Врши акредитацију- сертификацију ИКТ система и свих других чинилаца из области ИБ
-Спроводи хармонизацију и усаглашава све Прописе и акта донета на основу овог закона
- …..

Comment [GZ6]: У циљу хармонизације и усаглашености свих битних чинилаца из области ИБ на пословима непрекидног унапређења и усаглашавања са светским трендовима области ИБ Министарство пре предлагања и доношење аката из своје надлежности консултује и прибавља мишљења МО, МУП, МСП, МП, служби безбедности, Канцеларије Савета за националну безбедност, ген. Секретаријата владе, управе за заједничке послове Владе, националног ЦЕРТ-а.
У противном одговорност за функционисање, спровођење мера и ефикасност из ИБ не постоји и није транспарентно.

Comment [GZ7]: Ускладити са изменама у члану 5

вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

Ближе услове за мере из става 1. овог члана уређује Влада на предлог Надлежног органа, уважавајући међународне стандарде и стандарде који се примењују у одговарајућим областима рада.

Обавеза достављања података

Comment [GZ8]: Члан 7 треба прецизно дефинисати водећи рачуна о свим законима на снази који уређују поступање са подацима укључујући и све податке од значаја за ИБ ВРЛО ОСЕТЉИВ ЧЛАН И ВАЖАН ЗА УСАГЛАШАВАЊЕ СА ЕУ!!!!!!! Овако написан је штетан и треба га брисати

Члан 7.

На захтев безбедносних служби и министарства надлежног за унутрашње послове, руковалац ИКТ система је дужан да стави на располагање податке од значаја за информациону безбедност, који су службама безбедности и министарству надлежном за унутрашње послове потребни при обављању послова из њихове надлежности у складу са законом.

II. БЕЗБЕДНОСТ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА

ИКТ системи од посебног значаја

Comment [GZ9]: У ИКТ системе од посебног интереса морају се посебно истаћи и системи који се користе у пословима одбране и безбедности

Comment [GZ10]: Јако је важно дефинисати појмове и одреднице критичне ИКТ инфраструктуре кибер националног простора која је у суштини предмет уређења овог закона

Члан 8.

ИКТ системи од посебног значаја су системи који се користе у:

1) обављању послова у органима јавне власти;
2) обављању делатности од општег интереса;
3) обављању послова финансијских институција;
4) обављању послова у здравственој заштити;
5) обављању делатности пружања услуга информационог друштва којима се омогућавају друге услуге информационог друштва.

Влада, на предлог министарства надлежног за послове информационог друштва, ближе уређује листу послова и делатности из става 1. овог члана.

Мере заштите ИКТ система од посебног значаја

Члан 9.

Руковаоци ИКТ система од посебног значаја дужни су да предузимају одговарајуће мере 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.

Ближе услове за мере из става 1. овог члана уређује Влада на предлог Надлежног органа, уважавајући међународне стандарде и стандарде који се примењују у одговарајућим областима рада.

Акт о безбедности ИКТ система од посебног значаја

Члан 10.

Руковалац ИКТ система од посебног значаја дужан је да донесе акт о безбедности ИКТ система.

Акт о безбедности ИКТ система одређује мере заштите ИКТ система, а нарочито принципе, начин и процедуре постизања и одржавања адекватног нивоа безбедности овог система, као и овлашћења и одговорности у вези са овом безбедношћу и ресурсима тог система.

Акт о безбедности ИКТ система мора да буде усклађен с променама у окружењу и у самом ИКТ систему.

Руковалац ИКТ система од посебног значаја дужан је да врши интерну проверу ИКТ система најмање једном годишње и о томе сачини извештај.

Ближе услове за садржај акта о безбедности ИКТ система, начин интерне провере ИКТ система и садржај извештаја о интерној провери ИКТ система уређује Влада на предлог Надлежног органа.

Comment [GZ11]: Дефинисати појам сертификације, интерна провера не значи ништа ако није транспарентна а што се остварује давањем акредитације од стране надележног органа . Даје се након темељне провере свих процедура, софтвера и хардвера.

Поверавање активности у вези са ИКТ системом од посебног значаја трећим лицима

Члан 11.

Руковалац ИКТ система од посебног значаја може поверити активности у вези са ИКТ системом трећим лицима, у ком случају је обавезан да уреди однос са тим лицима на начин који обезбеђује предузимање мера заштите тог ИКТ система у складу са законом.

Comment [GZ12]: Под условом да је треће лице акредитовано од стране Министарства

Активностима из става 1. овог члана (у даљем тексту: поверене активности) сматрају се све активности које укључују обраду, чување, односно могућност приступа подацима којима располаже руковалац ИКТ система од посебног значаја, а односе се на његово пословање, као и активности развоја, односно одржавања софтверских и хардверских компоненти од којих непосредно зависи његово исправно поступање приликом вршења послова из надлежности, односно пружања услуга.

Под трећим лицем из става 1. овог члана сматра се и привредни субјекат који је имовинским и управљачким односима (лица са учешћем, чланице групе друштава којој тај привредни субјект припада и др.) повезан са руковаоцем ИКТ система од посебног значаја.

Поверавање активности врши се на основу уговора закљученог између руковаоца ИКТ система од посебног значаја и лица коме се те активности поверавају или посебним прописом.

Руковалац ИКТ система од посебног значаја одговара у целини за безбедност ИКТ система и предузимање мера заштите ИКТ система и у случају када су одређене активности у вези са тим ИКТ системом поверене трећим лицима.

Comment [GZ13]: Овде је јако важно дефинисати одговорност управе лица од посебног значаја, тј одговорност директора, УО, и слично, одговорни руководилац ИКТ система мора бити одговоран али као другостепени у хијерархији,

Члан 12.

Изузетно од одредаба члана 11, уколико су активности у вези са ИКТ системом поверене прописом, тим прописом се могу другачије уредити обавезе и одговорности руковаоца ИКТ система од посебног значаја у вези поверених активности.

Comment [GZ14]: Овај члан је нејасан и као такав непрецизан ? ваљда су за све ИКТ системе који припадају скупу критичне инфраструктуре прописане активности , обавезе а самим тим и одговорност?

Обавештавање Надлежног органа о инцидентима

Члан 13.

Руковаоци ИКТ система од посебног значаја обавезни су да обавесте Надлежни орган о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности.

Изузетно од става 1, руковаоци ИКТ система за рад са тајним подацима обавештења из става 1. упућују органу надлежном за обезбеђење примене стандарда и прописа у области заштите тајних података, финансијске институције обавештења упућују Народној банци Србије, а телекомуникациони оператори регулаторном телу за електронске комуникације.

Одредбе ст. 1 и 2. овог члана не односе се на самосталне руковаоце ИКТ система.

Листу инцидената и начин обавештавања из става 1. ближе уређује Надлежни орган.

Ако је инцидент од интереса за јавност, Надлежни орган, односно орган из става 2. коме се упућују обавештења о инцидентима, може наложити његово објављивање.

Ако је инцидент везан за извршење кривичних дела која се гоне по службеној дужности, Надлежни орган, односно орган из става 2. коме се упућују обавештења о инцидентима, обавештава надлежно јавно тужилаштво, односно министарство надлежно за унутрашње послове.

Ако је инцидент повезан са нарушавањем права за заштиту података о личности, Надлежни орган, односно орган из става 2. коме се упућују обавештења о инцидентима, о томе обавештава и Повереника за информације од јавног значаја и заштиту података о личности.

Овлашћења Надлежног органа

Члан 14.

Надлежни орган има овлашћења да испита да ли руковаоци ИКТ система од посебног значаја доследно спроводе обавезе прописане од чл. 8. до чл. 13. овог закона.

Надлежни орган у погледу овлашћења из става 1. овог члана може захтевати од руковалаца ИКТ система од посебног значаја да доставе све неопходне информације о свом ИКТ систему, интерне акте о безбедности ИКТ система и извештаје о интерној провери ИКТ система.

Одредбе ст. 1. и 2. овог члана не односе се на ИКТ системе самосталних руковалаца и ИКТ системе за рад са тајним подацима.

Међународна сарадња и рана упозорења о ризицима и инцидентима

Comment [GZ15]: Треба прецизно дефинисати ко обавештава национални ЦЕРТ и како

Comment [GZ16]: И они такође треба да буду обухваћени обавезом извештавања о инцидентима, пре свега нападима јер само тако имамо принцип свобухватности.

Comment [GZ17]: Опет имамо непотрбно гранање чиме се свобухватност извештавања губи, нека финансијске институције обавештавају НБС али нека обавештавају и национални ЦЕРТ јер је у информационој безбедности време детекције и реакције пресудно.

Comment [GZ18]: И овде онда немамо принцип свеобухватности …морамо имати јединствену базу инцидената- напада! Не извештава се о евентуалној штети или упаду у систем већ о покушају – претпоставка је да се критична инфраструктура ефикасно штити!

Comment [GZ19]: Као и раније и овде треба дефинисати сертификацију ИКТ система, усаглашеност са стандардима и прописима донетим на основу овог закона али и других закона који директно или индиректно уређују и утичу на домен информационе безбедности

Comment [GZ20]: Обавезно дефинисати начин контроле руководилаца ИКТ система укључујући и самосталне и друге – мора постојати механизам контроле контролора….

Члан 15.

Надлежни орган је дужан да успостави и одржава међународну билатералну и мултилатералну сарадњу на пољу безбедности ИКТ система, а поготово да пружи рана упозорења о ризицима и инцидентима који испуњавају најмање један од следећих услова:

1. брзо расту или имају тенденцију да постану високи ризици;
2. превазилазе или могу да превазиђу националне капацитете;
3. могу да имају негативан утицај на више од једне државе.

Уколико је инцидент у вези са извршењем кривичног дела, по добијању обавештења од Надлежног органа, министарство надлежно за унутрашње послове ће у званичној процедури проследити пријаву надлежном телу Европске полицијске канцеларије (ЕУРОПОЛ).

III. ПРЕВЕНЦИЈА И ЗАШТИТА ОД БЕЗБЕДНОСНИХ РИЗИКА У ИКТ СИСТЕМИМА У РЕПУБЛИЦИ СРБИЈИ

Национални центар за превенцију безбедносних ризика у ИКТ системима (Национални ЦЕРТ)

Члан 16.

Национални центар за превенцију безбедносних ризика у ИКТ системима (у даљем тексту: Национални ЦЕРТ) обавља послове координације превенције и заштите од безбедносних ризика у ИКТ системима у Републици Србији на националном нивоу.

За послове Националног ЦЕРТ-а надлежна је Регулаторна агенција за електронске комуникације и поштанске услуге.

Члан 17.

Национални ЦЕРТ прикупља и размењује информације о ризицима за безбедност ИКТ система, као и догађајима који угрожавају безбедност ИКТ система и у вези тога обавештава, упозорава и саветује лица која управљају ИКТ системима у Републици Србији, као и јавност, а посебно:

1. прати стање о инцидентима на националном нивоу,
2. пружа рана упозорења, узбуне и најаве и информише релевантна лица о ризицима и инцидентима,
3. реагује по пријављеним инцидентима, тако што пружа савете на основу расположивих информација лицима која су погођена инцидентом и предузима друге потребне мере из своје надлежности на основу сазнања из пријаве,
4. континуирано израђује анализе ризика и инцидената, које чини јавно доступним,
5. подиже свест код грађана, привредних субјеката и органа јавне власти о значају информационе безбедности, о ризицима и мерама заштите, укључујући спровођење кампања у циљу подизања те свести,
6. води евиденцију Посебних ЦЕРТ-ова.

Национални ЦЕРТ непосредно сарађује са Надлежним органом, Посебним ЦЕРТ-овима у Републици Србији, сличним организацијама у другим земљама, са јавним и привредним субјектима, ЦЕРТ-овима самосталних руковаоца ИКТ система, као и са ЦЕРТ-ом републичких органа.

Comment [GZ21]: Ова надлежност има и добрих и лоших особина. Треба дискутовати и наћи баланс. Може Рател под условом да учешће у управљању као и директне приступе серверу националног ЦЕРТ у Рателa имају битне националне институције. Такође, јако је важно да се унутар Рателa онда национални ЦЕРТ устроји по принципима и правилима која важе за рад нпр Канцеларије за националну безбедност као и других националних центара којима је домен рада национални ниво безбедности. Национални ЦЕРТ, без обзира ако је у Рателу мора бити у потпуности инегрисан у национални систем безбедности по свим критеријума. Ако оде у Рател само зато што Рател може да обезбеди континуитет у раду ЦЕРТ-а довољно високим платама које претпостављају дугорочна и квалитетна кадровска решења онда то није довољно добар избор. Притом не требе сигурно рачунати на благонаклоност ЕУ јер се на крају крајева мора одржати статус независности Рателa а то је јако компликован модел када је у питању НАЦИОНАЛНИ НИВО БЕЗБЕДНОСТИ, практично немогућ модел.

Comment [GZ22]: Осим евиденције могао би да има и контролну функцију али не инспекцијску

Национални ЦЕРТ промовише усвајање и коришћење прописаних и стандардизованих правила за:

1. управљање и санирање ризика и инцидената,
2. класификацију информација о ризицима и инцидентима,
3. класификацију озбиљности инцидената и ризика
4. дефиницију формата и модела података за размену информација о ризицима и инцидентима и дефиницију правила по којима ће се именовати значајни системи.

Начин рада Националног ЦЕРТ-а ближе прописује Влада, на предлог Надлежног органа.

Члан 18.

Надзор над радом Националног ЦЕРТ-а врши Надлежни орган, који периодично проверава да ли Национални ЦЕРТ располаже одговарајућим ресурсима, његова овлашћења и учинак успостављених процеса за управљање сигурносним инцидентима.

Посебни центри за превенцију безбедносних ризика у ИКТ системима

Члан 19.

Посебан центар за превенцију безбедносних ризика у ИКТ системима (у даљем тексту: Посебан ЦЕРТ) обавља послове превенције и заштите од безбедносних ризика у ИКТ системима у оквиру одређеног правног лица, групе правних лица, области пословања и слично.

Посебан ЦЕРТ је правно лице или организациона јединица у оквиру правног лица, које је уписано у евиденцију посебних ЦЕРТ-ова коју води Национални ЦЕРТ.

Упис у евиденцију посебних ЦЕРТ-ова врши се на основу пријаве правног лица у оквиру кога се налази посебан ЦЕРТ.

Ближе услове за упис у евиденцију из става 3. доноси Надлежни орган.

Центар за безбедност ИКТ система у републичким органима (ЦЕРТ републичких органа)

Члан 20.

Центар за безбедност ИКТ система у републичким органима (у даљем тексту: ЦЕРТ републичких органа) обавља послове који се односе на заштиту од инцидената у ИКТ системима републичких органа, изузев ИКТ система самосталних руковаоца.

Послове ЦЕРТ-а републичких органа обавља Управа за заједничке послове републичких органа.

Послови ЦЕРТ-а републичких органа обухватају:

1) заштиту ИКТ система Рачунарске мреже републичких органа (у даљем тексту: РМРО);

2) координацију и сарадњу са руковаоцима ИКТ система које повезује РМРО у превенцији инцидената, откривању инцидената, прикупљању информација о инцидентима и отклањању последица инцидената;

3) издавање стручних препорука за заштиту ИКТ система републичких органа, осим ИКТ система за рад са тајним подацима.

Влада, на предлог министарства надлежног за послове информационог друштва, уређује мере заштите ИКТ система у републичким органима.

Члан 21.

Самостални руковаоци ИКТ система су у обавези да формирају сопствене центре за безбедност ИКТ система ради управљања инцидентима у својим системима.

Центри из става 1. овог члана међусобно размењују информације о инцидентима, као и са националним ЦЕРТ-ом и са ЦЕРТ-ом републичких органа, а по потреби и са другим организацијама.

IV. КРИПТОБЕЗБЕДНОСТ И ЗАШТИТА ОД КОМПРОМИТУЈУЋЕГ ЕЛЕКТРОМАГНЕТНОГ ЗРАЧЕЊА

Comment [GZ23]: У закону треба дефинисати стратешке послове и задатке а детаљну разраду урадити кроз подзаконске акте самог МО јер се тиме омогућује брже праћење и измене изузетно динамичне области!

Надлежност

Члан 22.

Министарство надлежно за послове одбране је надлежно за послове информационе безбедности који се односе на одобравање криптографских производа, дистрибуцију криптоматеријала и заштиту од компромитујућег електромагнетног зрачења и послове и задатке у складу са законом и прописима донетим на основу закона.

Послови и задаци

Члан 23.

Comment [GZ24]: У складу са претходним коментаром треба члан 23 генерализовати на ниво стратешких послова и задатака из овог домена, значи овде додати надлежност по питању КЕМЗ-а из следећих чланова, тј све следеће чланове треба на стратешком нивоу побројати у овом члану а даља детаљна разрада би била у надележности МО из разлога горе наведених у претходном коментару.

У складу са овим законом, министарство надлежно за послове одбране:

1) организује и реализује научноистраживачки рад у области криптографске безбедности и заштите од КЕМЗ;

2) развија, имплементира, верификује и класификује криптографске алгоритме;

3) истражује, развија, верификује и класификује сопствене криптографске производе и решења заштите од КЕМЗ;

4) верификује и класификује домаће и стране криптографске производе и решења заштите од КЕМЗ;

5) дефинише процедуре и критеријуме за евалуацију криптографских безбедносних решења;

6) врши функцију националног органа за одобрења криптографских производа и обезбеђује да ти производи буду одобрени у складу са одговарајућим прописима;

7) врши функцију националног органа за заштиту од КЕМЗ;

8) у оквиру акредитације ИКТ система врши проверу са аспекта криптобезбедности и заштите од КЕМЗ;

9) врши функцију националног органа за дистрибуцију криптоматеријала и дефинише управљање, руковање, чување, дистрибуцију и евиденцију криптоматеријала у складу са прописима;

10) планира и координира израду криптопараметара, дистрибуцију криптоматеријала и заштите од компромитујућег електромагнетног зрачења у сарадњи са самосталним руковаоцима ИКТ система;

11) формира и води централни регистар верификованог и дистрибуираног криптоматеријала;

12) формира и води регистар изадатих одобрења за криптографске производе;

13) израђује електронске сертификате за криптографске системе засноване на инфраструктури јавних кључева (Public Key Infrastructure – PKI),

14) предлаже доношење прописа из области криптобезбедности и заштите од КЕМЗ на основу овог закона;

15) врши послове стручног надзора у вези криптобезбедности и заштите од КЕМЗ;

16) пружа стручну помоћ носиоцу инспекцијског надзора информационе безбедности у области криптобезбедности и заштите од КЕМЗ;

17) пружа услуге уз накнаду правним и физичким лицима, изван система јавне власти, у области криптобезбедности и заштите од КЕМЗ према пропису Владе на предлог министра одбране;

18) сарађује са домаћим и међународним органима и организацијама у оквиру надлежности уређених овим законом.

Компромитујуће електромагнетно зрачење

Члан 24.

Уколико је у оквиру ИКТ система предвиђено руковање подацима који су одређени као тајни, у складу са законом, у ИКТ систему се, ради спречавања нарушавања информационе безбедности, примењују мере заштите од компромитујућег електромагнетног зрачења.

Мере заштите од КЕМЗ могу примењивати на сопствену иницијативу и руковаоци ИКТ система којима то није законска обавеза.

За све техничке компоненте система (уређаје, комуникационе канале и просторе) код којих постоји ризик од КЕМЗ, а што би могло довести до нарушавања информационе безбедности из става 1. овог члана, врши се провера заштићености од КЕМЗ и процена ризика за отицање тајних података путем КЕМЗ.

Проверу заштићености од КЕМЗ врши министарство надлежно за послове одбране.

Самостални руковаоци ИКТ система могу вршити проверу КЕМЗ за сопствене потребе.

Ближе услове за проверу КЕМЗ и начин процене ризика од отицања података путем КЕМЗ уређује Влада, на предлог министарства надлежног за послове одбране.

Обавеза примене метода криптозаштите

Члан 25.

Мере криптозаштите примењују се када се тајни подаци преносе средствима електронске комуникације изван безбедносне зоне која је утврђена за чување и поступање са одговарајућим подацима.

Мере криштозаштите се могу применити и за подизање степена заштите тајних података који се чувају, као и за заштиту интегритета, аутентичности и непорецивости података.

Мере криптозаштите се могу применити и приликом преноса и чувања података који нису означени као тајни у складу са законом који уређује тајност података, када је на основу закона или другог правног акта потребно ограничити приступ подацима и ради заштите интегритета, аутентичности и непорецивости података.

Мере криптозаштите које се примењују за заштиту тајности, интегритета, аутентичности и непорецивости података класификују се у складу са законом који регулише тајност података, законом који регулише заштиту података о личности и другим законима који ограничавају или на други начин условљавају приступ подацима.

Влада, на предлог министарства надлежног за послове одбране уређује техничке услове за криптографске алгоритме, параметре, протоколе и информациона добра у области криптозаштите који се у Републици Србији користе у криптографским производима ради заштите тајности, интегритета, аутентичности, односно непорецивости података.

Одобрење за криптографски производ

Члан 26.

Криптографски производи који се користе за заштиту преноса и чувања података који су одређени као тајни, у складу са законом, морају бити верификовани и одобрени за коришћење.

Влада, на предлог министарства надлежног за послове одбране, ближе уређује услове које морају да испуњавају криптографски производи из става 1. овог члана.

Издавање одобрења за криптографски производ

Члан 27.

Одобрење за криптографски производ издаје министарство надлежно за послове одбране, на захтев руковаоца ИКТ система, произвођача криптографског производа или другог заинтересованог лица.

Одобрење за криптографски производ се може односити на појединачни примерак криптографског производа или на одређени модел криптографског производа који се серијски производи.

Одобрење за криптографски производ може имати рок важења.

Министарство надлежно за послове одбране решава по захтеву за издавање одобрења за криптографски производ у року од 60 дана од дана подношења уредног захтева, који се може продужити у случају посебне сложености провере највише за још 90 дана.

Министарство надлежно за послове одбране води регистар издатих одобрења за криптографски производ.

Министарство надлежно за послове одбране објављује јавну листу одобрених модела криптографских производа за све моделе криптографских производа за које је у захтеву за издавање одобрења наглашено да модел криптографског производа треба да буде на јавној листи и ако је захтев поднео произвођач или лице овлашћено од стране произвођача предметног криптографског производа.

Министарство надлежно за послове одбране претходно издато одобрење за криптографски производ може повући или променити услове из ст. 3. и 4. овог члана из разлога нових сазнања везаних за техничка решења примењена у производу, а која утичу на оцену степена заштите који пружа производ.

Влада, на предлог министарства надлежног за послове одбране, ближе уређује садржај захтева за издавање одобрења за криптографски производ, услове за издавање одобрења за криптографски производ, начин издавања одобрења, накнаду за издавање одобрења и садржај регистра издатих одобрења за криптографски производ.

Опште одобрење за коришћење криптографских производа

Члан 28.

Опште одобрење за коришћење криптографских производа имају самостални руковаоци ИКТ система .

Самостални руковаоци ИКТ система који имају опште одобрење за коришћење криптографских производа самостално оцењују степен заштите који пружа сваки појединачни криптографски производ који се користи у ИКТ систему тог органа, а у складу са прописаним условима и условима из општег одобрења.

Регистри у криптозаштити

Члан 29.

Самостални руковаоци ИКТ система који имају опште одобрење за коришћење криптографских производа устројавају и воде регистре криптографских производа, криптоматеријала, правила и прописа и кадра криптозаштите.

Регистар страних криптоматеријала води Канцеларија Савета за националну безбедност и заштиту тајних података, у складу са ратификованим међународним споразумима.

Влада, на предлог министарства надлежног за послове одбране, ближе уређује вођење регистара из ст. 1. овог члана.

V. УСЛОВИ ЗА УНУТРАШЊУ ОРГАНИЗАЦИЈУ

Члан 30.

Руковаоци ИКТ система за рад са тајним подацима и самостални руковаоци ИКТ система ће формирати организационе јединице за информациону безбедност у чијем је делокругу:

1. израда потребне безбедносне документације;
2. избор, тестирање и имплементација техничких мера заштите, опреме и програма;
3. избор, тестирање и имплементација мера заштите од КЕМЗ;
4. надзор имплементације и примене безбедносних процедура;
5. управљање и коришћење криптографских производа;
6. спровођење безбедносне анализе у циљу процене ризика;
7. безбедносна обука запослених.

VI. ИНСПЕКЦИЈА ЗА ИНФОРМАЦИОНУ БЕЗБЕДНОСТ

Послови инспекције за информациону безбедност

Члан 31.

Инспекција за информациону безбедност врши инспекцијски надзор над применом овог закона и радом руковаоца ИКТ система од посебног значаја, осим самосталних руковаоца ИКТ система и ИКТ система за рад са тајним подацима.

Comment [GZ25]: Инспекција треба да обједини све послове инспекцијског надзора који се односе на Информациону безбедност укључујући и Закон о телекомуникацијама и друге законе у вези… а све оно што је надлежности Министарства.

Comment [GZ26]: Ко онда врши контролу и надзор самосталних ИКТ система и ИКТ системе за рад са тајним подацима ? Дефинисати ко и како контролише контролоре и специфичне ИКТ системе

Послове инспекције за информациону безбедност обавља министарство надлежно за послове информационог друштва преко инспектора за информациону безбедност.

У оквиру инспекцијског надзора рада руковаоца ИКТ система, инспектор за информациону безбедност утврђује да ли су испуњени услови прописани овим законом и прописима донетим на основу овог закона.

Comment [GZ27]: Кориговати у складу са коментаром број 29

Члан 32.

Самостални руковаоци ИКТ система одредиће посебна лица за инспекцијски надзор сопствених ИКТ система.

Лица за инспекцијски надзор самосталних руковаоца ИКТ система извештај о нађеном стању подносе руководиоцу самосталног руковаоца ИКТ система.

Овлашћења инспектора за информациону безбедност

Члан 33.

Инспектор за информациону безбедност овлашћен је да у поступку спровођења надзора, поред предузимања радњи на које је овлашћен инспектор у вршењу инспекцијског надзора утврђених законом, предузме и следеће радње:

1) прегледа опрему која је део информационог система, просторије у којима се та опрема користи, као и техничку документацију везану за опрему, софтверске производе, рачунарску мрежу и друге елементе ИКТ система;

2) да узима изјаве и по потреби писана изјашњења од руководиоца руковаоца ИКТ система и запослених лица о чињеницама и подацима значајним за потпуно утврђивање чињеничног стања;

3) да захтева достављање потребних извештаја, података, аката и друге потребне документације и одреди примерен рок за достављање.

Инспектор за информациону безбедност је овлашћен да у поступку спровођења надзора поред налагања мера на које је овлашћен инспектор у поступку вршења инспекцијског надзора утврђених законом, забрани коришћење неадекватних поступака, техничких средстава и услуга и остави рок за отклањање неправилности.

VII. ОСТАЛЕ ОДРЕДБЕ

Казнене одредбе

Члан 34.

Новчаном казном у износу од 50.000,00 до 2.000.000,00 динара казниће се правно лице за прекршај ако:

1) не поступи у складу са налогом инспектора за информациону безбедност;

2) не примени мере одређене Планом мера и интерним правилима;

За прекршај из става 1. овог члана казниће се и одговорно лице новчаном казном у износу од 5.000,00 до 150.000,00 динара.

VIII. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Рокови за доношење подзаконских аката

Comment [GZ28]: Овде треба дефинисати и навести која су то подзаконска акта која треба донети у законском року

Члан 35.

Подзаконска акта предвиђена овим законом донеће се у року од 12 месеци од дана ступања на снагу овог закона.

Ступање на снагу

Члан 36.

Овај закон ступа на снагу осмог дана од дана објављивања у "Службеном гласнику Републике Србије".

Друштво за Информациону безбедност Србије
Примедбе, сугестије и коментари на Нацрт Закона о Инфомационој безбедности
23 Јули 2015 године

Примедбе, сугестије и коментари

1. Податак, у једнини, како се овде користи, је САМО НОСИЛАЦ информације и као такав не захтева било какву заштиту. Заштита се примењује на СКУП података, односно на информације. Из тих разлога би требало за податак користити множину и увек везати за информације. Могућ је и други приступ: користити само термин информације, што би било у складу са називом закона - ***Закон о информационој безбедности***.
2. *Информационо-комуникациони систем* (ИКТ систем) – није коректан назив, јер постоје ***комуникациони системи***, који се баве ***преносом*** података, и ***рачунарски системи***, који се баве обрадом података Њиховом интеграцијом настали су ***информациони системи***.
   Дакле, уколико се желе нагласити појединачни системи заједничким називом онда је реч о ***рачунарско-комуникационом*** систему, или у обједињеним називу: ***информациони систем***.
3. *У члану број два директно у тексту Нацрта унете су примедбе и сугестије пре свега по питању појмова, водећи рачуна на првом месту о потребном минималном академском нивоу документа у рангу Закона*
4. *Термин **РУКОВАОЦ** није одговарајући и прикладан те је боље рећи **РУКОВОДИЛАЦ ИКТ** система*
5. *Од практично 2007 године па све до данас стално смо указивали на припродан редослед стварања услова за доношење Закона, ту пре свега мислимо да је требало прво донети Стратегију па тек онда Закон, да је тако урађено дубоко смо уверени да би сада текст Нацрта Закона био много бољи и пре свега у финкцији стратешких циљева из области Информационе безбедности и Националног Кибер простора.*
6. *У форми КОМЕНТАР , којих је дато укупно 27, дате су најважније, суштинске примедбе и предлози на Нацрт закона.*

Закључак

Познато је са колико труда и енергије Друштво за информациону безбедност Србије готово читаву деценију, од првих дана свог неформалног па затим формалног постојања, чини све како би Србија добила своју Стратегију Инфомационе безбедности, свој Закон о информационој безбедности и своје равноправно место у светској Кибер заједници пре свега кроз оснивање националног ЦЕРТ-а и његово укључивање у светску мрежу. Нажалост, последњих неколико година, на свакој годишњој националној Конференцији Информациона безбедност Србије, имали смо увек исте закључке у делу који се односи на стање у Србији по питању законског оквира и повезаности са међународном зајеницом. Од практично прве Конференције када смо констатовали да смо једна од три земље у Европи које немају Закон о ИБ и једна од 5 које немају ЦЕРТ па све до последње Конференције само се сваке године смањивала цифра

испред идентичног текста закључка. На последњој одржаној Конференцији закључак је био исти и веома поражавајући – Србија је једина земља у Европи која нема Стратегију и Закон о Информационој безбедности, једина која нема ЦЕРТ. Изгледа да су наше закључке, препоруке и вапаје боље слушале комшије него надлежни у земљи Србији, није лако суочити се са таквим чињеницама, нарочито ако се радило дуго, истрајно, са пуно ентузијазма и енергије, када се окупио заиста импозантан скуп паметних, стручних и добронамерних људи.
У најбољој намери, једино са жељом да коначно Србија почне да води рачуна на одговоран и домаћински начин о једном од најзначајнијих фактора националне, економске и војне безбедности, непрекидно смо користили сва расположива средства и начине, чак директно и поимснце прозивајући одговорне у претходној али нажалост и у новој влади надајући се да ће коначно давно постављени акциони планови почети да се реализују. Углавном су све те наше покушаје да се и директном прозивком коначно покрене толико потребан процес одговорни из Владе доживљавали лично што је пре свега резултовало покушајима изолације Друштва, избегавање да се препозна допринос Друштва и коначно игносрисање реалне вредности и снаге Друштва као и свега урађеног на начин да нико из Друштва није постао члан нити једног радног тима.

У време доношења Акционог плана развоја ИКТ сектора у Републици Србији почетком 2013 године, којим је било предвиђено да се Закон донесе до краја те године, верујући да ће се један од основних циљева друштва коначно остварити, нисмо замерили члановима владе што су закључке наше претходне Конференције директно копирали у текст акционог плана, укључујући и словне и синтаксне грешке, а да нас нити једним словом нису поменули нити укључили ни у једну радну групу.

Нема везе, нисмо то ни имали на уму када смо се окупили и почели са радом. Били смо све време ту, бићемо и даље, радићемо све као и до сада, транспарентно, без трунке политике, на наш рачун и за нашу Србију.

Прошле године смо донели одлуку да не опрганизујемо Конференцију све док се не појави Нацрт Закона јер нисмо више желели да поново доносемо истоветне закључке. У међувремену смо правили округле столове на најактуелније теме из домена ИКТ и ИБ, учествовали на домаћим и интернационални конференцијама, држали предавања директорима, младима на факултетима, гостовали у емисијама на ту тему, писали чланке, стручне радове, организовали семинаре и чекали да се појави Нацрт Закона.

И ево коначно нацрта пред нама. Обиман је, има 36 чланова, делимично меша стратешки, тактички и технички ниво, негде је врло штур и непрецизан, негде детаљан до нивоа упутства и процедуре. Овакакв какав је није добар.
Врло детаљно смо прочитали и анализирали Нацрт и због тога има толико предлога, сугестија и примедби.

Замољени смо од стране ранде групе да подржимо Закон. Радимо то врло посвећено, на начин како то умемо и можемо. Не замерамо што нас нису звали када је почело стварање Нацрта, мишљења смо да су нас позвали да би све било брже, боље и јефтиније. Али добро је и овако. Нико срећнији од нас није што коначно имамо Нацрт и што ће Србија коначно добити Закон. Али не Закон про форме ради и по сваку цену, не

Закон којим ће неко да се закити, добије медаљу, покаже да је нешто радио и зарадио плату. Не Закон попут оних фамозних нереалних Акционих планова чија је сврха била приказати невероватан и херојски рад администрације, оправдати велике плате, удобне фотеље и небројене службене путеве по кугли земаљској. Само не нешто попут тог фамозног Акционог плана са почетка 2013, плана којег би сада било интересантно анализирати по питању обима и постављених рокова.

Србија заслужује да има добар закон, закон који ће да буде у фунцији стратешких циљева Националне Инфомационе безбедности, да буде у фунцији бољег и сигурнијег живота грађана Србије. Ако га није добила све ове године онда може да сачека још пар месеци ,још пар састанака радне групе, још једну јавну расправу. Да се погледају сви коментари, сугестије и примедбе, да се саслуша сручна јавност, да се Нацрт дотера, избруси, умије, утегне па правац у Скупштину. Све то може да се уради до краја године па да коначно кажемо да нисмо једнини у нечемо лошем у Европи када смо у толико других ствари увек међу најбољима. Тај Закон је још једна шанса да се неке ствари доведу у ред, да се направи још један корак ка модерном свету макар се он данас звао Европска Унија.

Надам се да ће радна група имати разумевања, воље и снаге да искористи све што је добила од нас и осталих актера јавне расправе те да у што краћем року изађе се новом верзијом Нацрта за коју се надам да ће бити и последња пре него што крене у скупштинску процедуру.

Данас је крај јула 2015., крај септембра 2015. је много, много ближе него почетак 2013. или 2007. када смо организовали први округли сто на ову тему.

А ми смо ту, зовите и ето нас, помоћићемо све што знамо и умемо а вољу никада не губимо.

У Београду
23.Јули 2015 године

Председник Друштва за информациону безбедност Србије
Мр Зоран Живковић, дипл.инж.