На основу члана 45. став 1. Закона о Влади („Службени гласник РС”, бр. 55/05, 71/05 – исправка, 101/07, 65/08, 16/11, 68/12 – УС, 72/12, 7/14 – УС и 44/14),

Влада доноси

СТРАТЕГИЈУ РАЗВОЈА ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ У РЕПУБЛИЦИ СРБИЈИ ЗА ПЕРИОД ОД 2017. ДО 2020. ГОДИНЕ

1. УВОД

1.1. Информациона безбедност у Републици Србији

Информациона безбедност је аспект безбедности који се односи на безбедносне ризике повезане са употребом информационо-комуникационих технологија, укључујући безбедност података, уређаја, информационих система, мрежа, организација и појединаца.

Развој нових технологија доноси несумњиве користи за друштво, али паралелно са технолошким развојем долазе и нови безбедносни изазови. Према наводима из Стратегије информационе безбедности Европске уније (Cybersecurity Strategy of the European Union), високотехнолошки криминал је врста криминала која је у највећем порасту, а милион људи, укључујући децу, свакодневно буде жртва напада. Хакерски напади на информационе системе могу битно да угрозе пословање предузећа, функционисање државне инфраструктуре и националну безбедност, док су појединци, а пре свега деца, све више изложени ризику од превара, уцена и злостављања путем интернета.

Употреба информационо-комуникационих технологија (ИКТ) од стране државе, привреде и грађана је у порасту и све више послова и активности се заснива на њиховом коришћењу. Државни органи се у великој мери ослањају на информационе системе, који омогућавају лакше и ефикасније обављање послова из њихових надлежности. Када је у питању општење органа и странака, треба истаћи да се електронска управа развија, да је број електронских услуга органа јавне власти у порасту, чиме се грађанима омогућује олакшано прибављање различитих докумената који су им потребни. Јавна предузећа која обављају делатности од општег интереса, као и привредна друштва, употребљавају информационе системе у великој мери, а у појединим делатностима, као што је, на пример, делатност производње, дистрибуције и снабдевања електричном енергијом, послови се у знатној мери ослањају на ИКТ системе. Бројне установе, као, на пример, установе у области здравствене заштите, воде евиденције у оквиру својих информационих система. Употреба Интернета је у порасту на свим нивоима. Према подацима Републичког завода за статистику, објављеним у оквиру документа „Употреба информационо-комуникационих технологија у Републици Србији, 2016”, утврђено је да 99.8% предузећа на територији Републике Србије користи рачунар у свом пословању, да 99,8% предузећа има интернет прикључак, а 99,1% има широкопојасну (broadband) интернет конекцију. Према истом извору, 98,6% предузећа користи електронске сервисе јавне управе. Са друге стране, 65,8% домаћинстава поседује рачунар, 64,7% домаћинстава поседује интернет прикључак, а 57,8%

домаћинстава у Републици Србији има широкопојасну (broadband) интернет конекцију. Такође, преко 1.510.000 лица користи електронске сервисе јавне управе, а преко 1.450.000 лица куповало је или поручивало робу/услуге путем интернета у последњих годину дана.

Напади на информационе системе могу да битно угрозе функционисање државе, као што је био случај у Естонији 2007. године, када је извршен сајбер напад на ИКТ системе државних органа и финансијских институција, и када је дошло до блокаде услуга електронске управе, које се масовно користе у тој држави, као и платног промета. Познат је и случај уношења рачунарског вируса „Стакснет" у нуклеарну електрану у Ирану 2010. године, са намером да се изврши саботажа индустријских система. У фебруару 2016. године хакери су успели да украду 81 милион долара Централној банци Бангладеша тако што су провалили у њихову рачунарску мрежу, открили кључеве за приступ SWIFT систему и неовлашћено издали налоге за пренос средстава са рачуна у Банци федералних резерви у Њујорку. Поред тога, постоје претње по националну безбедност које се по међународном праву не могу сврстати у облике оружане агресије, али су присутне у међународним односима.

Према подацима Министарства унутрашњих послова, број пријављених кривичних дела из области високотехнолошког криминала расте 50% годишње. Напади на сервере државних органа све су учесталији и напреднији.

Република Србија је препознала информациону безбедност као једну од шест приоритетних области развоја информационог друштва и предузела кораке у циљу успостављања свеобухватног оквира информационе безбедности. У складу са тим, Стратегија развоја информационог друштва у Републици Србији до 2020. године („Службени гласник РС", број 51/10) предвиђа да развој и унапређење информационе безбедности треба постићи кроз унапређење правног и институционалног оквира, заштиту критичне информационе инфраструктуре, борбу против високотехнолошког криминала и научно–истраживачки рад.

Закон о информационој безбедности („Службени гласник РС", број 6/16 – у даљем тексту: Закон) створио је основ за успостављање и примену свеобухватног оквира у области информационе безбедности. Законом се уређују мере заштите од безбедносних ризика у ИКТ системима од посебног значаја, одговорности оператора ИКТ система од посебног значаја приликом управљања и коришћења ИКТ система и одређују се надлежни органи за спровођење мера заштите, координацију између чинилаца заштите и праћење правилне примене прописаних мера заштите.

У смислу успостављања свеобухватног оквира, Закон такође оставља простор и за укључивање других актера, попут приватног сектора, академске заједнице и цивилног друштва, тако што предвиђа формирање посебних радних група у оквиру Тела за координацију послова информационе безбедности.

По питању информационе безбедности појединаца, посебно је значајна безбедност деце. Употреба ИКТ и интернета код деце у Републици Србији је веома раширена. Истраживање УНИЦЕФ-а[1] спроведено 2012. године на територији Републике Србије, показало је да више од 90% старијих основаца и средњошколаца

[1] Попадић Д, Кузмановић Д. Коришћење дигиталне технологије, ризици и заступљеност дигиталног насиља међу ученицима у Србији, УНИЦЕФ/Институт за психологију Филозофског факултета Универзитета у Београду, 2012.

имају мобилне телефоне и да око 90% деце користи интернет. Исто истраживање је указало на високе стопе изложености ризицима на интернету и изложености дигиталном насиљу, односно две трећине деце су били изложени некој врсти онлајн ризика. При томе половина испитаних наставника изјављује да не поседује одговарајуће вештине коришћења рачунара и интернета, а скоро половина сматра да је недовољно информисана о дигиталном насиљу. Према истраживању УНИЦЕФ-а из 2016. године, „Истраживање о нивоу свести о потенцијалним интернет ризицима и злоупотребама међу родитељима деце узраста 8 до 17 године", тек нешто више од 50 одсто родитеља сматра себе довољно, али не и потпуно способним да пружи помоћ и подршку свом детету у таквим ситуацијама. У истраживању је истакнуто да 25 одсто родитеља наводи да је њихово дете било изложено ризичној или опасној ситуацији на интернету у последњих 12 месеци од дана испитивања. Поред тога, наведено је да 85% деце у узрасту од 8 до 17 година поседује мобилни телефон, од којих су 63% „паметни телефони", као и да два од три детета у проводе у просеку преко сат времена дневно на интернету.

Општи циљ Стратегије је развој и унапређење информационе безбедности у Републици Србији и њено одржавање на адекватном нивоу, а с обзиром да су доношењем прописа у овој области дефинисани ИКТ системи од посебног значаја, мере заштите, надлежни органи, изазов за остварење циља налази се у стварању предуслова за континуирано унапређење кадрова, како кроз увођење посебних програма на универзитетима из области информационе безбедности, тако и кроз континуирано обучавање и усавршавање запослених у релевантним институцијама који се баве информационом безбедношћу. Узимајући у обзир динамичност ове области, један од кључних предуслова за континуирано одржавање адекватног нивоа информационе безбедности је успостављање центра за развој и истраживање који би имао улогу праћења кретања у овој области и, сходно томе, давање доприноса даљем унапређењу информационе безбедности у складу са најновијим сазнањима и технолошким решењима. Остваривањем циљева Стратегије постиже се стабилно функционисање ИКТ система од посебног значаја, информациона безбедност грађана и Републике Србије, подижу се капацитети за борбу против високотехнолошког криминала, с тим да је за реализацију тога од кључног значаја сарадња између јавног сектора, приватног сектора, невладиних организација, академске заједнице и других релевантних чинилаца.

С обзиром значај и ширину области информационе безбедности, Влада доноси ову стратегију у циљу развоја и унапређења информационе безбедности у Републици Србији.

1.2. Регулаторни оквир информационе безбедности

Област информационе безбедности регулисан је следећим прописима:

- Закон о информационој безбедности („Службени гласник РС", број 6/16);
- Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала („Службени гласник РС", бр. 61/05 и 104/09);
- Кривични законик („Службени гласник РС", бр. 85/05, 88/05 - исправка, 107/05 - исправка, 72/09, 111/09, 121/12, 104/13, 108/14 и 94/16);
- Закон о тајности података („Службени гласник", број 104/09);

- Закон о заштити података о личности („Службени гласник РС”, бр. 97/08, 104/09 – др. закон, 68/12 –УС и 107/12);
- Закон о електронским комуникацијама („Службени гласник РС”, бр. 44/10, 60/13 –УС и 62/14);
- Закон о потврђивању Конвенције о високотехнолошком криминалу („Службени гласник РС”, број 19/09);
- Закон о потврђивању Додатног протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система („Службени гласник РС”, број 19/09);
- Закон о потврђивању Конвенције Савета Европе о заштити деце од сексуалног искоришћавања и сексуалног злостављања („Службени гласник РС – Међународни уговори”, број 1/10);
- Закон о Војнобезбедносној агенцији и Војнообавештајној агенцији („Службени гласник РС”, бр. 88/09, 55/12 - УС и 17/13).

2. ПРИНЦИПИ РАЗВОЈА ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ

Развој информационе безбедности у Републици Србији почива на следећим принципима:

1) Информациона безбедност чини саставни део свеукупне безбедности и у функцији је остваривања и поштовања права, слобода и интереса грађана, привреде и државе;

2) Информациона безбедност је од значаја за све друштвене чиниоце који користе информационо-комуникационе технологије, а који треба да буду свесни ризика повезаних са употребом технологије и да предузимају превентивне и друге потребне мере заштите;

3) Информациона безбедност подразумева благовремено препознавање ризика, предузимање превентивних мера и ефикасну реакцију на инциденте;

4) Потребно је успоставити и унапређивати редовну и ефикасну размену информација о ризицима и инцидентима у области информационе безбедности на националном и међународном нивоу;

5) Наставити континуирани развој система заштите у информационој безбедности на правном, организационом и техничком нивоу, уз прилагодљивост новим околностима и изазовима;

6) Систематски подизати свест и унапређивати знања и вештине код свих категорија грађана по питању информационе безбедности у свакодневном животу и на радном месту;

7) Успоставити сталну сарадњу између јавног и приватног сектора, као основ за развој и унапређење стратешких приоритета.

3. ПРИОРИТЕТНЕ ОБЛАСТИ И СТРАТЕШКИ ЦИЉЕВИ

У циљу развоја и унапређења информационе безбедности у Републици Србији утврђују се следеће приоритетне области:

1) безбедност информационо-комуникационих система, што се односи на ризике нарушавања функционисања органа власти, привреде и организација као последица инцидената у информационо-комуникационим системима;

2) информациона безбедност грађана, што се односи на ризике нарушавања безбедности грађана злоупотребом информационо-комуникационих технологија;

3) борба против високотехнолошког криминала, што се односи на превенцију и санкционисање кривичних дела која се заснивају на злоупотреби информационо-комуникационих технологија;

4) информациона безбедност Републике Србије, што се односи на ризике нарушавања националне безбедности путем информационо-комуникационих система;

5) међународна сарадња, што подразумева сарадњу са страним државним органима, међународним организацијама и другим партнерима у области информационе безбедности.

У оквиру приоритетних области одређују се следећи стратешки циљеви:

1) у области безбедности информационо-комуникационих система:

(1) превенција и заштита путем размене информација, праћења актуелних ризика и подизање свести,

(2) безбедност ИКТ система у привредним субјектима и безбедност електронског пословања,

(3) безбедност ИКТ система од посебног значаја,

(4) безбедност тајних података у ИКТ системима,

(5) сарадња јавног и приватног сектора у области информационе безбедности;

2) у области безбедности грађана при коришћењу технологије:

(1) безбедност деце на интернету,

(2) заштита приватности и заштита од злоупотреба при коришћењу ИКТ,

(3) информациона безбедност у образовном систему;

3) у области борбе против високотехнолошког криминала:

(1) унапређење механизама за откривање високотехнолошког криминала и кривично гоњење учинилаца,

(2) подизање свести о опасностима од високотехнолошког криминала,

(3) унапређење међународне сарадње у борби против високотехнолошког криминала;

4) у области информационе безбедности Републике Србије:

(1) систем информационе безбедности од значаја за националну безбедност,

(2) развој научних, технолошких и индустријских капацитета неопходних за заштиту информационе безбедности Републике Србије,

(3) изградња војних капацитета система одбране за одбрану од високотехнолошких напада,

(4) Изградња безбедносно-обавештајних капацитета у области информационе безбедности;

5) међународна сарадња.

3.1. Безбедност информационо-комуникационих система

Инциденти у области информационе безбедности су обично повезани са нарушеном безбедношћу информационо-комуникационих система, што може бити провала у систем, приступ подацима који није требало да буде омогућен, изазивање проблема у раду система и слично. Крајње последице таквих инцидената најчешће излазе из оквира самог ИКТ система и односе се на послове, организације и људе који се непосредно или посредно ослањају на ИКТ систем. На пример, прекид рада информационог система у банци може онемогућити банку да опслужује своје клијенте, а клијента банке може довести у ситуацију да не може да плати рачун својом кредитном картицом. Такви инциденти ширих размера могу угрозити функционисање државе, привреде и друштва, због чега се одређују ИКТ системи од посебног значаја за које постоји законска обавеза старања о информационој безбедности у складу са Законом.

3.1.1. Размена информација, праћење актуелних ризика и подизање свести

У свим сферама безбедности се континуирано појављују нове технике и средства угрожавања безбедности и нове мере заштите, али ни у једној области се то не дешава толико динамично као у информационој безбедности.

Због тога је правовремено информисање, подизање свести, кориговање навика и пружање релевантних информација о безбедносним ризицима и начинима отклањање последица инцидената од изузетне важности.

Брза, поуздана и ефикасна размена информација може да утиче да органи јавне власти, привредни субјекти и грађани предузму благовремене и адекватне мере заштите својих система и уређаја, и тако спрече да се деси инцидент, односно ублаже последице инцидента који се остварио.

Због тога, Законом је установљен Национални центар за превенцију безбедносних ризика у ИКТ системима (Национални ЦЕРТ) у оквиру Регулаторне агенције за електронске комуникације и поштанске услуге (РАТЕЛ), а чији је задатак да 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.

Национални ЦЕРТ треба да сарађује са сличним организацијама других земаља, с обзиром на глобални карактер изазова у области информационе безбедности.

Национални ЦЕРТ треба да сарађује са релевантним међународним институцијама на пољу информационе безбедности и учествује као члан у њиховом раду.

Од изузетног је значаја ефикасно успостављање и стално унапређивање рада Националног ЦЕРТ-а, како би у што већој мери одговорио на улогу која му је дата.

У оквиру републичких органа законом је установљен Центар за безбедност ИКТ система у републичким органима (у даљем тексту: ЦЕРТ републичких органа) у оквиру Управе за заједничке послове републичких органа, а обавља послове који се односе на

заштиту од инцидената у ИКТ системима републичких органа, изузев ИКТ система самосталних оператора.

Поред тога Законом је остављена могућност формирања независних посебних ЦЕРТ-ова који обављају послове превенције и заштите од безбедносних ризика у ИКТ системима у оквиру одређеног правног лица, групе правних лица, области пословања и слично. Посебни ЦЕРТ-ови се евидентирају код Националног ЦЕРТ-а. На тај начин треба да се успостави мрежа ЦЕРТ-ова између којих ће се ефикасно и брзо размењивати информације и искуства.

3.1.2. Безбедност ИКТ система у привредним субјектима и безбедност електронског пословања

Развојем електронског пословања привредни субјекти су све више изложени безбедносним ризицима везаним за технологију коју користе.

Пре свега је у привредним субјектима потребно успостављати и унапређивати системе управљања информационом безбедношћу у складу са међународним стандардима и добрим праксама из других земља.

Поред активности ЦЕРТ-а које су усмерене на подизање свести, између осталог, привредних субјеката, потребно је као посебан приоритет поставити унапређивање безбедности ИКТ система у привреди. Сходно томе, значај Националног ЦЕРТ-а се огледа и у подизању свести привредних субјеката о потреби примена мера заштите, у складу са националним и међународним стандардима, као и о користима успостављања посебних ЦЕРТ-ова (у оквиру одређеног привредног субјекта, групе привредних субјеката или области пословања) који треба да имају важну улогу у превенцији и заштити ИКТ система и размени информација са другим релевантним чиниоцима система информационе безбедности у Републици Србији. У циљу подизања свести о безбедносним ризицима и значају примена мера заштите, од великог значаја је учешће и невладиног сектора, академске заједнице и других субјеката у овој области.

3.1.3. Безбедност ИКТ система од посебног значаја

Када нарушавање безбедности појединог ИКТ система или неколико ИКТ система из исте области може да доведе до значајног нарушавања функционисања јавних институција, привреде и свакодневног живота грађана, тада одговорност за безбедност таквог ИКТ система излази из оквира штете нанете предузећу, организацији или институцији којој ИКТ систем припада. То су ИКТ системи од којих зависи критична инфраструктура или системима који сами по себи представљају критичну инфраструктуру. С обзиром да у правном систему још увек није формално уведен појам критичне инфраструктуре, у Закону се такви системи означавају као ИКТ системи од посебног значаја.

Оператори ИКТ система од посебног значаја имају Законом утврђене обавезе старања о информационој безбедности и по том питању су под надзором надлежних државних органа.

Такође је прописано да ИКТ системи од посебног значаја обавештавају надлежни орган увек када се деси инцидент у ИКТ системима који може да има значајан утицај на нарушавање информационе безбедности. Оператори ИКТ система од посебног значаја морају да буду свесни значаја пријаве инцидената, као и њихових последица на националном и међународном нивоу.

Надлежни орган успоставља и унапређује међународну сарадњу у области безбедности ИКТ система, која ће се додатно формализовати приступањем Републике Србије Европској унији, а на основу Директиве о мрежној и информационој безбедности Европске уније.

Надлежни орган континуирано прати стање информационе безбедности путем инспекцијског надзора, пријема и обраде пријава обавештења о инцидентима у ИКТ системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности, као и на основу анализе ризика и инцидената коју израђује Национални ЦЕРТ, и у складу са тим унапређује област информационе безбедности уз сарадњу свих релевантних институција, а посебно оних чији представници учествују у раду Тела за координацију послова информационе безбедности. Сходно томе, од изузетног је значаја изградња капацитета надлежног органа, то јест Министарства трговине, туризма и телекомуникација, по питању инспекције за информациону безбедност и пријема и обраде пријава о инцидентима, као и капацитета других институција надлежних у области информационе безбедности.

Са друге стране предстоји успостављање система управљања информационом безбедношћу у складу за прописаним условима у великом броју оператора ИКТ система од посебног значаја, што је крајња сврха законских мера и од кључне је важности за безбедност критичне инфраструктуре у Републици Србији.

3.1.4. Безбедност тајних података у ИКТ системима

Тајни податак у ИКТ системима је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности.

Заштита тајних података у ИКТ системима представља посебни безбедносни изазов, имајући у виду да најсофистицираније облици високотехнолошких напада (укључујући шпијунажу) представљају управо напад на садржаје тајних података.

Неовлашћени приступ тајним подацима и њихова крађа из ИКТ система државних институција, јавних и приватних предузећа, као и напади на ИКТ инфраструктуру од виталног значаја за функционисање државе могу се посматрати као један од најтежих облика напада на ИКТ систем.

Законом о тајности података, и на основу тог закона донетим подзаконским актима, успостављен је основ нормативног оквира за рад са тајним подацима, укључујући и питања тајних података који се обрађују у информационо-комуникационим системима, као и надлежности Канцеларије Савета за националну безбедност и заштиту тајних података у овој области. У наредном периоду треба извршити надоградњу националне регулативе и надлежности Канцеларије Савета за националну безбедност и заштиту тајних података у подручју заштите тајних података у ИКТ системима, у складу са одговарајућим директивама Европске уније, са посебним

тежиштем на одређивање надлежности и прописивање процеса акредитације ИКТ система за рад са тајним подацима.

Од приоритетног значаја за унапређивање безбедности тајних података у ИКТ системима је брзо и ефикасно окончање успостављања јединственог система и поступка акредитације ИКТ система за рад са тајним подацима, дефинисање мера заштите ИКТ система за рад са тајним подацима, доношење националног програма за подизање свести при коришћењу ИКТ система за рад са тајним подацима, као и доношење националне методологије за процену ризика за ИКТ системе за рад са тајним подацима. У том циљу, потребно је додатно ојачати капацитете Канцеларије Савета за националну безбедност и заштиту тајних података и других надлежних државних органа.

3.1.5. Сарадња јавног и приватног сектора у области информационе безбедности

За одржавање адекватног нивоа информационе безбедности у Републици Србији, потребно је, поред државе, учешће и других – привреде, грађана, невладиног сектора, академске заједнице и осталих релевантних чинилаца. Сарадња између јавног и приватног сектора може да буде веома значајна за индустријска истраживања и иновације у области информационе безбедности, а веома битан сегмент сарадње је размена информација у циљу адекватне припремљености и одговора на безбедносне ризике и инциденте.

Законом је остављен простор за укључивање актера из приватног, академског и цивилног сектора у напоре усмерене на јачање информационе безбедности у Републици Србији путем формирања посебних радних група у оквиру Тела за координацију послова информационе безбедности. У том смислу, успостављање сарадње јавног и приватног сектора која ће омогућити ефикасну комуникацију и оптимизацију планираних будућих активности, односно благовремену размену информација и дељење ресурса такође је један од полазних приоритета за унапређивање области информационе безбедности у Републици Србији.

Све ове активности треба да воде ка успостављању трајног поверења у оквирима информационе безбедности између свих актера: јавног сектора односно представника државних институција, приватног сектора, односно привреде и грађана организованих у цивилно друштво.

3.2. Безбедност грађана при коришћењу технологије

Поред изложености предузећа, организација и органа власти ризицима информационе безбедности, тим ризицима је изложен и сваки појединац. Појединци могу доживети финансијске преваре, нарушавање угледа због откривања интимних садржаја, уцене, штету због губитка података, а посебно угрожена категорија су деца, која су поред свега тога често жртве злостављања.

3.2.1. Безбедност деце на интернету

Деца у све већој мери и све раније почињу да користе информационо-комуникационе технологије и приступ интернету. Ширењем употребе мобилних уређаја деца у сваком тренутку, без надзора одраслих могу да остваре приступ интернету, да успостављају контакте са непознатим особама преко друштвених мрежа, да превише излажу личне податке о себи и својој породици, да једни према другима испољавају индивидуалну и организовану вербалну агресију, да снимају и размењују фотографије и видео записе који њима или другим особама могу нанети штету. Сви ови ризици дешавају се у околностима сложених социјалних односа међу децом, укључујући нарастајуће вршњачко насиље.

Доношењем Закона о ратификацији Конвенције Уједињених нација о правима детета („Службени лист СФРЈ – Међународни уговори", број 15/90 и „Службени лист СРЈ – Међународни уговори", бр. 4/96 и 2/97) држава се обавезала да предузме мере за спречавање и да обезбеди заштиту детета од свих облика насиља у породици, институцијама и широј друштвеној средини. Одредбама Конвенције предвиђено је да државе предузимају мере које се односе на заштиту детета од: физичког и менталног насиља, злоупотребе и занемаривања и свих других облика искоришћавања (експлоатације) штетних по било који вид дететове добробити. Такође, Конвенцијом је одређена обавеза државе да обезбеди мере подршке за физички и психички опоравак детета – жртве насиља и његову социјалну реинтеграцију.

Општи протокол за заштиту деце од злостављања и занемаривања, који је Влада усвојила Закључком 05 Број: 011-5196/2005 од 25. августа 2005. године, предвиђа да у процесу заштите детета од злостављања и занемаривања треба да учествују установе и појединци из различитих система (здравство, образовање, социјална заштита, полиција, правосуђе и др), сваки од њих у оквиру својих надлежности.

Стратегијом Европске уније за бољи интернет за децу, донетој 2012. године, предвиђено је да деца, родитељи, старатељи и наставници морају да буду свесни ризика који постоје на интернету, као и да је потребно да деца буду саветована и информисана о безбедним начинима коришћења интернета. Наведено је да је потребно да се успоставе механизми који ће омогућити једноставно и лако доступно пријављивање штетног и непримереног садржаја за децу.

Влада је у јулу 2016. године донела Уредбу о безбедности и заштити деце при коришћењу информационо-комуникационих технологија („Службени гласник РС", број 61/16). На основу ове уредбе, Министарство трговине, туризма и телекомуникација предузима превентивне мере за безбедност и заштиту деце на интернету путем информисања и едукације, и успоставило је Национални контакт центар за безбедност деце на интернету као јединствено место за пружање савета и пријем пријава у вези са безбедношћу деце на интернету.

За адекватну заштиту деце на интернету потребно је подизање свести и родитеља и деце, као и јачање улоге школе кроз одговарајуће школске програме и подизање капацитета наставника. Јавне институције које са различитих позиција реагују када дође до одређених последица, као што су Министарство унутрашњих

послова, центри за социјални рад и здравствене установе такође треба да подижу своје капацитете у овој области.

Већу пажњу заштити деце на интернету, кроз одговарајуће програмске садржаје, потребно је посветити и у медијима и тиме допринети подизању свести родитеља и деце, а што се посебно односи на јавне сервисе.

Потребно је даље подизати капацитет и јачати улогу јединственог места за пружање савета и пријем пријава у вези са безбедношћу деце на интернету, укључујући координацију подршке у појединачним случајевима и координацију успостављања нових системских решења за препознате типове проблема.

У сарадњи надлежних министарстава са операторима електронских комуникација и Академском мрежом Републике Србије треба дефинисати мере којима ће на техничком нивоу моћи да се ограничи изложеност деце неодговарајућим садржајима.

3.2.2. Заштита приватности и заштита од злоупотреба при коришћењу ИКТ

Ризици који настају због прекомерне доступности личних података често у довољној мери нису сагледани како од власника података, тако ни од обрађивача, при чему код обрађивача нису ретки случајеви и намерног пренебрегавања потребе заштите података о личности.

Већина инцидената у области информационе безбедности у којима је угрожена безбедност појединца укључују и злонамерно сазнавање личних података, било да су ти подаци добијени на превару (такозвано „пецање" личних података), провалом у рачунар или други лични уређај или отицањем података из збирки података.

Потребно је даље унапређивати законски оквир у области заштите података о личности, а у складу са стандардима Европске уније, као и отклањати препреке за ефикаснију примену закона.

Са друге стране је код грађана потребно значајно подићи свест о значају чувања сопствених личних података и неприхватања несразмерног давања и објављивања личних података, као и о могућим преварама и другим злоупотребама путем интернета и о одговарајућим превентивним мерама.

3.2.3. Информациона безбедност у образовном систему

„Мисија система образовања у Републици Србији у 21. веку је да осигура основни темељ живота и развоја сваког појединца, друштва и државе заснованог на знању." [2] У складу са тако дефинисаном мисијом, Стратегијом развоја образовања до 2020 године, као један од циљева развоја образовања поставља се достизање и одржавање релевантности образовања, у складу са непосредним и развојним потребама појединаца, економског, социјалног, културног, истраживачког, образовног, јавног, административног и других система.

[2] Стратегија развоја образоваања у Србији до 2020. године („Службени гласник РС", број 107/12).

Образовни систем треба да обезбеди развој и стицање општих/међупредметних компетенција ученика основне и средње школе које су релевантне за лични, професионални и социјални развој и функционисање појединца у савременом свету. Овако дефинисане компетенције излазе из оквира традиционалних школских предмета и ангажују школска знања на припреми ученика да буду конкурентни и функционални у садашњем и будућем образовном и професионалном простору и да компетентно и активно реализују своје грађанске улоге. Једна од међупредметних компетенција је и дигитална писменост: „Ученик је способан да користи расположива средства из области информационо-комуникационих технологија (уређаје, софтверске производе, електронске комуникационе услуге и услуге које се користе путем електронских комуникација) на одговоран и критички начин ради ефикасног испуњавања постављених циљева и задатака у свакодневном животу, школовању и будућем послу. Приликом коришћења ИКТ-а свестан је ризика за сопствену и туђу сигурност и добробит и одговорним поступањем себе и друге штити од нежељених последица.”[3]

Мисија образовања за 21. век и усмереност образовног процеса на развој компетенција утицале су на дефинисање стратешких мера за развој дигиталних компетенција и коришћење ИКТ. Ове мере пре свега се односе на унапређење квалитета услова (дефинисање стандарда школског простора и дидактичке, уметничке и информатичке опреме и дефинисање механизама контроле примене тих стандарда) и квалитет процеса наставе и учења, у којима се позива на коришћење предности информационо-комуникационих технологија и различитих облика учења у он-лине окружењу (електронске конференције, предметни блогови, дискусионе трибине, електронска тестирања итд.), и подизање компетенција наставника да користе информационо - комуникационе технологије у настави или њеној припреми кроз иницијално образовање и систем усавршавања наставника.

Због комплексности питања успешне интеграције ИКТ у систем образовања, као и чињенице да до сада нису израђени документи који би помогли формулисању образовне политике у овој области, Национални просветни савет (НПС) је иницирао израду документа Смернице за унапређивање улоге информационо-комуникационих технологија у образовању (Смернице). [4]

Смернице дају приказ свих препорука организованих на основу два критеријума: у односу на ниво општости и према приоритету имплементације (висок-хитна интервенција, средњи почетак у току једне године и низак приоритет у периоду три до пет година). Према критеријуму општости, препоруке су класификоване у односу на ниво: а) Стратегије развоја: дугорочно планирање, примарно доношење закона и праћење савремених тенденција; б) Образовне институције: препоруке које се примењују на институционалном нивоу; и в) Наставне праксе: препоруке које се односе на непосредан рад наставника.

Због вишефункционалности образовно-васпитног система, неопходна је чврста интерресорска сарадња у вези са безбедношћу деце при коришћењу ИКТ (нарочито с областима безбедности, здравства и социјалне политике). Ресори у доменима својих

[3] Стандарди општих међупредметих компетенција за крај средњег образовања, Завод за вредновање квалитета образовања и васпитања, Београд, 2013.

[4] Смернице за унапређивање улоге информационо-комуникационих технологија у образовању, Национални просветни савет Републике Србије, Београд 2013.

надлежности треба да дефинишу и реализују одговарајуће стручне стандарде. Неопходно је на националном нивоу успоставити функционалне механизме координације између различитих система и јасно дефинисати њихове улоге.

Образовни систем треба да омогући стицање знања у области информационе безбедности, кроз увођење посебних студијских програма на универзитетима, чиме би се допринело повећању броја стручних кадрова у овој области, што је неопходно, имајући у виду брзину развоја ИКТ и повећање ризика од безбедносних инцидената.

3.3. Борба против високотехнолошког криминала

Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, заједно са одредбама Кривичног законика, о кривичним делима високотехнолошког криминала, успостављају институционални и правни основ за санкционисање кривичних дела у овој области. Према подацима Министарства унутрашњих послова, у 2013. години откривено је 961 кривично дело у области високотехнолошког криминала, у 2014. години 1.423 оваквих дела, а у 2015. години тај број је значајно повећан и износи 2.074, што на прави начин илуструје размере и значај спречавања и сузбијања овог облика криминала.

3.3.1. Унапређење механизама за откривање високотехнолошког криминала и кривично гоњење учинилаца

У циљу ефикасне борбе против високотехнолошког криминала неопходно је унапредити постојећи законодавни оквир. Република Србија усвојила је 2009. године Закон о потврђивању Конвенције о високотехнолошком криминалу ЦЕТС 185 (Будимпештанска конвенција) и Закон о потврђивању Додатног протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система, док је 2010. године усвојен Закон о потврђивању Конвенције Савета Европе о заштити деце од сексуалног искоришћавања и сексуалног злостављања.

Међутим, Република Србија још увек није у потпуности ускладила своје законодавство са Директивом 2013/40/ЕУ о нападима на информатичке системе, која је један од механизама за откривање и кривично гоњење извршилаца кривичних дела из ове области.

Еволуција начина извршења високотехнолошког криминала прати развој информационих технологија. Ово је један од видова криминала са највишом стопом раста, имајући у виду да сваког дана више од милион људи широм света постану жртве кривичног дела. Из наведеног разлога, надлежни државни органи – специјализована организациона јединица за високотехнолошки криминал у оквиру Министарства унутрашњих послова и Посебно тужилаштво за високотехнолошки криминал морају унапредити оперативне алате и оперативну способност за сузбијање ове врсте кривичних дела. Такође, неопходно је унапредити координирацију и заједнички приступ органа откривања, органа гоњења, јавног и приватног сектора.

Поред тога, потребно је наставити спровођење обуке судија за поступање у овим предметима, имајући у вида убрзани развој савремених информационих технологија као и нове начине на које се врше кривична дела високотехнолошког криминала.

3.3.2. Подизање свести о опасностима од високотехнолошког криминала

Крајњи корисници играју кључну улогу у обезбеђивању сигурности мрежа и информационих система, те стога морају бити свесни ризика са којима се суочавају на мрежи и спремни да предузму једноставне кораке да спрече настанак ризичних ситуација.

У том смислу, неопходно је да државни органи, јавни и приватни сектор организују јавне кампање о најзаступљенијим облицима високотехнолошког криминала, као што су неовлашћен приступ рачунару или рачунарској мрежи, угрожавање сигурности, преваре путем интернета, злоупотреба платних картица, те кампање и радионице фокусиране на безбедност деце на интернету, пре свега од дигиталног насиља и сексуалне експлоатације.

3.3.3. Унапређење међународне сарадње у борби против високотехнолошког криминала

Имајући у виду да високотехнолошки криминал, услед глобалног домета интернета, не познаје границе, од изузетне је важности додатно унапредити међународну сарадњу са релевантним органима страних земаља. Република Србија, као једна од потписница Будимпештанске конвенције има запажену улогу у раду 24/7 мреже контакт тачака успостављене на основу конвенције, са одређена два представника за сарадњу и хитно поступање у предметима из ове области. Једна контакт тачка је Посебни тужилац за високотехнолошки криминал, а друга представник Јединице за високотехнолошки криминал Министарства унутрашњих послова.

3.4. Информациона безбедност Републике Србије

Информациона безбедност Републике Србије је кључни део свеобухватне националне безбедности која се заснива на информационој безбедности институција, снага, људи, система, процеса, информација и вредности које су од значаја за безбедност и одбрану земље.

Информационо-комуникациона инфраструктура, сервиси и подаци система одбране имају посебан значај за националну безбедност Републике Србије. Самим тим, информациона безбедност система одбране једна је од кључних компоненти информационе безбедности у Републици Србији.

3.4.1. Систем информационе безбедности од значаја за националну безбедност

У Републици Србији је потребно дефинисати систем информационе безбедности од значаја за националну безбедност, у складу са постојећим надлежностима и додатним дефинисаним улогама државних и других тела.

3.4.2. Развој научних, технолошких и индустријских капацитета неопходних за заштиту информационе безбедности Републике Србије

Информациона безбедност у функцији одбране Републике Србије се заснива на организованом управљању знањем у области информационе безбедности и људима, као носиоцима тог знања. Развој система информационе безбедности стога као основни задатак има изградњу, развој и инвестирање у систем образовања, обуке, истраживања и развоја и инвестирање у људе као носиоце знања из области информационе безбедности у подручју одбране. То подразумева заједничко предлагање, усвајање и имплементацију стандарда и пракси које повећавају сигурност и безбедност. Сарадња академске заједнице са надлежним институцијама, уз активно учешће приватног сектора, требало би да буде институционализована како би се заједнички предузимале одређене активности у циљу развоја производа, процеса и сервиса ради превенције и пружања адекватног нивоа информационе безбедности. Академска заједница са једне и приватни сектор са друге стране својом стручношћу и експертизом указаће на примере добре праксе, наглашавајући значај анализе ризика и управљања у организацијама кроз организовање одговарајућих обука, тренинга, семинара, трибина. Образовање стручних кадрова омогућиће успостављање безбедних ИТ решења доступних корисницима.

Академска заједница кроз заједничке пројекте са јавним и приватним сектором утицаће на континуирано побољшање метода идентификације и утврђивања безбедносних проблема, примену адекватне контроле, успостављања ефикасне комуникације свих заинтересованих страна и размену информација о најбољим праксама у другим земљама. Подстицање сарадње између научне заједнице и привреде, са јасно дефинисаним потребама у области информационе безбедности допринеће развоју технологија и услуга у складу са прихваћеним међународним стандардима. Предузимањем мера које ће допринети очувању информационе безбедности у Републици Србији од стране свих релевантних субјеката довешће до унапређења стања у овој области. Покретање експерименталних окружења за развој нових технологија и сервиса на универзитетима допринеће развоју нових решења којим ће се одговорити на све бројније изазове у области информационе безбедности.

3.4.3. Изградња војних капацитета система одбране за одбрану од високотехнолошких напада

Министарство одбране и Војска Србије ће развити свеобухватне способности за одбрану у сајбер простору у складу са уставним и законским надлежностима и додељеним мисијама и задацима. Наведене активности обухватају успостављање информационе безбедности и способности за извођење одбране у сајбер простору, у оквиру делотворне употребе снага и функционалних способности Војске Србије, као основног субјекта система одбране.

Министарство одбране и Војска Србије су носиоци одбране од претњи из информационог простора свих система и ресурса у њиховој надлежности на такав начин, који у потпуности омогућава безбедну и поуздану употребу тих система и ресурса у циљу извршавања додељених надлежности, мисија и задатака.

Посебно је значајно предвидети обавезе субјеката система одбране на заштити ИКТ система у ванредном и ратном стању. Такође, значајно је предвидети ангажовање снага Министарства одбране и Војске Србије на пружању помоћи операторима ИКТ система од посебног значаја, у погледу откривања претњи и адекватног одговора са циљем њихове одбране и спречавања угрожавања националне безбедности Републике Србије.

3.4.4. Изградња безбедносно-обавештајних капацитета у области информационе безбедности

Службе безбедности Републике Србије ће развити свеобухватне способности за заштиту информационе безбедности Републике Србије у складу са законским надлежностима, ради заштите ИКТ система од посебног значаја, у погледу благовременог откривања претњи са циљем спречавања угрожавања националне безбедности Републике Србије.

3.5. Међународна сарадња

Широка међусобна повезаност друштвених, организационих, техничких, финансијских, привредних и других врста система преко државних граница, која је заснована на примени ИКТ и система, ствара комплексно међународно окружење у коме се одвија динамична интеракција између разноврсних субјеката. Друштвени и економски просперитет, национална безбедност и одбрана Републике Србије директно и посредно зависе од мрежа ИКТ које се простиру унутар и изван националних граница у сложеном, динамичном и често непредвидљивом окружењу. Интеракција заснована на ИКТ је двосмерна и остварује сложен директан и посредан утицај на националну безбедност. Тај утицај такође мора бити регулисан на комплексан начин, кроз различите облике и садржаје сарадње на националном и међународном нивоу.

Успостављање и развој информационе безбедности на националном нивоу може бити остварено једино кроз реализацију свеобухватног скупа активности које су истовремено остварене и координисане на националном и међународном нивоу. Контакт са међународним партнерима је вишеслојан, активан и оптималан, јер обухвата широк скуп државних, невладиних и наддржавних организација на политичком, техничком и стручном нивоу.

Кључни међународни партнери Републике Србије у том погледу су Организација Уједињених нација (ОУН), Организација за европску безбедност и сарадњу (ОЕБС), Европска унија (ЕУ), Савет Европе (СЕ), политичке, економске безбедносне и одбрамбене организације и савези са којима Република Србија има закључене споразуме о међусобној сарадњи, суседне и традиционални савезници Републике Србије.

За остваривање постављених циљева међународне сарадње Републике Србије неопходно је успоставити и развијати међународну сарадњу на билатералним и мултилатералним основама са циљем унапређења националне и међународне информационе безбедности. Поред тога, потребно је успоставити сарадњу у циљу размене информација, знања и искуства са иностраном мрежом националних,

професионалних и међународних центара за превенцију безбедносних ризика у ИКТ системима. По могућству, Република Србија треба да активно учествује у међународним цивилним и војним вежбама чији је циљ успостављање и развој информационе безбедности на свим нивоима.

4. РЕАЛИЗАЦИЈА СТРАТЕГИЈЕ

Реализацију ове стратегије прати Министарство трговине, туризма и телекомуникација.

Влада ће донети акциони план за спровођење ове стратегије у року од шест месеци од њеног објављивања у „Службеном гласнику Републике Србије”.

5. ЗАВРШНИ ДЕО

Ову стратегију објавити у „Службеном гласнику Републике Србије”.

05 Број: 030-3942/2017-1

У Београду, 29. маја 2017. године

В Л А Д А

ПРЕДСЕДНИК

Александар Вучић,с.р.