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, 44/14 и 30/18 – др. закон),

Влада доноси

СТРАТЕГИЈУ

за борбу против високотехнолошког криминала за период 2019–2023. године

"Службени гласник РС", број 71 од 25. септембра 2018.

1. УВОДНИ ДЕО

Република Србија је у обавези да донесе и спроводи стратегију и акциони план за ефективно решавање високотехнолошког криминала у складу са стратешким и оперативним приступом Европској унији (ЕУ) у погледу високотехнолошког криминала. Наведена обавеза превасходно произилази из Преговарачких мерила за Поглавље 24 – Правда, слобода, безбедност. Европска Унија је констатовала да је Република Србија ратификовала Конвенцију о високотехнолошком криминалу (сачињена у Будимпешти, енгл. *Budapest Convention*) 2009. године и позвала Републику Србију да додатно усклади своје законодавство са Директивом *2013/40/ЕУ* о нападима на информационе системе.

Министарство унутрашњих послова је, у складу са Законом о министарствима („Службени гласник РС”, бр. 44/14, 14/15, 96/15 – др. закон и 62/17) носилац израде наведеног стратешког документа у сарадњи са осталим државним институцијама, тј. заинтересованим странама.

У плану за подршку трансформације Западног Балкана у оквиру Стратегије за веродостојну перспективу проширења и појачану сарадњу са државама са подручја Западног Балкана истакнута је потреба за повећаном подршком у изградњи капацитета у области високотехнолошког криминала, укључујући сарадњу са Европском групом за тренинг и едукацију о високотехнолошком криминалу и будуће учешће у оквиру Агенције за европску мрежу и информациону безбедност.

У оквиру Акционог плана за Поглавље 24 – Правда, слобода и безбедност, где је носилац активности **Министарство унутрашњих послова**, налазе се три препоруке са осам дефинисаних активности, које Република Србија треба да испуни у оквиру приступног процеса у ЕУ, са фокусом на унапређење организационих, кадровских и техничких капацитета, анализирања тренутног нормативног и организационог оквира и предузимања радњи у циљу усаглашавања са правним тековинама ЕУ у области високотехнолошког криминала и ојачавање сарадње између државних органа и институција. Имајући у виду да је једна од главних

карактеристика дела високотехнолошког криминала њихова транснационална природа, од процеса европских интеграција се очекује повећање експедитивности рада у предметима високотехнолошког криминала, у смислу бржег протока информација потребних за откривање и гоњење учинилаца кривичних дела, те бржег одговарања по међусобним захтевима за пружање међународне правне помоћи, а све кроз јачање капацитета државних органа Републике Србије, а нарочито Посебног тужилаштва за борбу против високотехнолошког криминала.

Поред наведених препорука, Република Србија је након отварања Поглавља 24 – Правда, слобода и безбедност добила прелазно мерило које има за циљ израду Стратегије за борбу против високотехнолошког криминала и које гласи: „Србија припрема, доноси и спроводи стратегију и акциони план за ефективну борбу против високотехнолошког криминала у складу са стратешким и оперативним приступом ЕУ у погледу високотехнолошког криминала. Србија ојачава своје оперативне капацитете (у погледу особља и опреме у Јединици за високотехнолошки криминал) како би решила проблем високотехнолошког криминала и усклађује своје законодавство са релевантним правним тековинама ЕУ, укључујући у погледу сексуалног злостављања деце на интернету, обезбеђује специјализоване обуке и подиже ниво свести јавности и међу државним службеницима по питању високотехнолошког криминала".

На основу наведених међународних и националних докумената из ове области Република Србија је донела прву Стратегију за борбу против високотехнолошког криминала са пратећим Акционим планом за њено спровођење.

Стратегија представља наставак и проширење активности којима је циљ јачање ефикасности свих субјеката у области сузбијања високотехнолошког криминала у Републици Србији. Посебно је усмерена на наставак усклађивања законодавства с међународним стандардима, даље унапређење капацитета носилаца борбе против високотехнолошког криминала, унапређење превентивног и проактивног приступа друштва у сузбијању свих облика криминала у тој области, унапређење интерресорне сарадње у друштву, као и сарадње Републике Србије на регионалном и међународном нивоу у области високотехнолошког криминала.

Испуњењем стратешких циљева и даљим развојем међународне и регионалне сарадње у овој области, Република Србија ће допринети не само сигурности у земљи него и у региону. Стратегија за борбу против високотехнолошког криминала представља документ којим Влада утврђује институционални одговор на појавне облике високотехнолошког криминала, дефинише улоге и надлежности државних органа, идентификује циљеве и утврђује основне правце деловања на сузбијању свих видова високотехнолошког криминала.

У овој стратегији одређене именице наведене су у мушком роду, а користе се као неутралне за мушки и женски род.

Стратегија се доноси на период од 2019. до 2023. године.

Акциони план 2019–2020. за спровођење Стратегије за борбу против високотехнолошког криминала за период 2019–2023. године чини њен саставни део.

2. ОСНОВНИ ПОЈМОВИ

Законодавни оквир Републике Србије дефинише високотехнолошки („сајбер") криминал у члану 2. Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала („Службени гласник РС", бр. 61/05 и 104/09), наводећи да високотехнолошки криминал у смислу тог закона представља вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику. Под производима у електронском облику посебно се подразумевају рачунарски програми и ауторска дела која се могу употребити у електронском облику.

Међународни слободно доступни извори наводе да високотехнолошки, тј. „сајбер" криминал представља облик криминалног понашања код кога се коришћење рачунарске технологије и информационих система испољава као начин извршења кривичног дела, где се рачунар или рачунарска мрежа употребљавају као средство или циљ извршења.

Рачунари и рачунарска технологија се могу злоупотребљавати на разне начине, а сам криминалитет који се реализује помоћу рачунара може имати облик било ког од традиционалних видова криминалитета, као што су крађе, утаје, проневере, док се подаци који се неовлашћено прибављају злоупотребом информационих система могу на разне начине користити за стицање противправне користи.

Може се констатовати да је високотехнолошки криминал такав облик криминалног понашања код кога је високотехнолошко окружење у коме се рачунарске мреже појављују као средство, циљ, доказ или окружење извршења кривчног дела. При томе се под „сајбер простором" подразумева или врста „заједнице" сачињене од мреже рачунара у којој се елементи традиционалног друштва налазе у облику бајтова и битова или „простор који креирају компјутерске мреже".

Законом о потврђивању Конвенције о високотехнолошком криминалу („Службени гласник РС – Међународни уговори", број 19/09), у члану 1. прописане су следеће дефиниције од значаја за високотехнолошки криминал:

– „рачунарски систем” означава сваки уређај или групу међусобно повезаних или зависних уређаја, од којих један или више њих, на основу програма, врши аутоматску обраду података;

– „рачунарски податак” означава свако представљање чињеница, информација или концепата у облику који је подесан за њихову обраду у рачунарском систему, укључујући и одговарајући програм на основу кога рачунарски систем обавља своју функцију;

– „давалац услуге” означава сваки јавни или приватни субјект који корисницима своје услуге пружа могућност комуницирања преко рачунарског система и сваки други субјект који обрађује или чува рачунарске податке у име такве комуникационе услуге или корисника такве услуге;

– „податак о саобраћају” означава сваки рачунарски податак који се односи на комуникацију преко рачунарског система, произведену од рачунарског система који је део ланца комуникације, а у којој су садржани подаци о пореклу, одредишту, путањи, времену, датуму, величини, трајању или врсти предметне услуге.

Кривичним закоником („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), у члану 112. прописане су следеће дефиниције од значаја за високотехнолошки криминал:

– „покретном ствари” се сматра и свака произведена или сакупљена енергија за давање светлости, топлоте или кретања, телефонски импулс, као и рачунарски податак и рачунарски програм;

– „рачунарски податак” је свако представљање чињеница, информација или концепта у облику који је подесан за њихову обраду у рачунарском систему, укључујући и одговарајући програм на основу кога рачунарски систем обавља своју функцију;

– „рачунарском мрежом” сматра се скуп међусобно повезаних рачунара, односно рачунарских система који комуницирају размењујући податке;

– „рачунарским програмом” сматра се уређени скуп наредби који служе за управљање радом рачунара, као и за решавање одређеног задатка помоћу рачунара;

– „рачунарски вирус” је злонамерни рачунарски програм или неки други скуп наредби унет у рачунар или рачунарску мрежу који је направљен да сам себе умножава и делује на друге програме или податке у рачунару или рачунарској мрежи додавањем тог програма или скупа наредби једном или више рачунарских програма или података;

– „исправом” се сматра сваки предмет који је подобан или одређен да служи као доказ какве чињенице која има значај за правне односе, као и рачунарски податак;

– спис, писмо, пошиљка и документ могу бити и у електронском облику;

– „рачунар” је сваки електронски уређај који на основу програма аутоматски обрађује и размењује податке;

– „рачунарски систем” је сваки уређај или група међусобно повезаних или зависних уређаја од којих један или више њих, на основу програма, врши аутоматску обраду података.

Законником о кривичном поступку („Службени гласник РС”, бр. 72/11, 101/11, 121/12, 32/13, 45/13 и 55/14), у члану 2. су прописане следеће дефиниције од значаја за високотехнолошки криминал:

– „електронски запис” је звучни, видео или графички податак добијен у електронском (дигиталном) облику;

– „електронска адреса” је низ знакова, слова, цифара и сигнала који је намењен за одређивање одредишта везе;

– „електронски документ” је скуп података који је одређен као електронски документ у складу са законом који уређује електронски документ;

– „електронски потпис” је скуп података који је одређен као електронски потпис, у складу са законом који уређује електронски потпис.

3. АНАЛИЗА СТАЊА СА ПРЕПОРУКАМА

3.1. Међународно-правни и међународни стратешки оквир

Уставом Републике Србије је прописано да су општеприхваћена правила међународног права и потврђени међународни уговори саставни део правног поретка Републике Србије и непосредно се примењују, с тим да потврђени међународни уговори морају бити у складу с Уставом.

1. Конвенција о високотехнолошком криминалу (Будимпешта 2001)

Конвенција тренутно представља једини међународно-правно признат и континентално раширени правни инструмент у области високотехнолошког криминала, који у свом тексту обједињује прецизно одређене, и што је још битније, употребљиве и савремене методе поступања надлежних државних органа, али не само њих, већ и других институција и организација у овој области, све у циљу успостављања делотворног међународног механизма, који је састављен од више органских целина на нивоу појединих земаља које су потписале или ратификовале ову Конвенцију.[1] Конвенција за свој циљ има, на првом месту, хармонизацију домаћих материјално кривично правних одредби у области високотехнолошког криминала, омогућавање домаћем кривичном процесно-правном оквиру да надлежним државним органима пружи овлашћења која су неопходна за откривање и гоњење

извршилаца ових кривичних дела, као и успостављање брзог и ефективног оквира међународне сарадње у овој области.[2]

Конвенција о високотехнолошком криминалу је осмишљена у циљу спречавања дела која су усмерена против интегритета, поверљивости и доступности компјутерских система, мрежа и података, а самим тим и спречавања злоупотребе тих система, мрежа и података тако што ће се покренути казнене мере за такво деловање као што је описано у Конвенцији и при чему ће се применити казне за ефикасну борбу против кривичних дела, и на тај начин ће се на унутрашњем и међународном нивоу олакшати откривање, истрага и гоњење за извршена кривична дела и омогућити да се обезбеде услови за брзу и поуздану међународну сарадњу.

У складу са Конвенцијом, Република Србија одредила је две контакт тачке мреже 24/7 које омогућавају хитно реаговање и размену података у предметима високотехнолошког криминала међу свим државама потписницама. Једна контакт тачка је Посебни тужилац за високотехнолошки криминал, док је друга контакт тачка Одељење за сузбијање високотехнолошког криминала, при Министарству унутрашњих послова.

2. Додатни протокол уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система (2003)

Основни циљ овог протокола јесте да допуни одредбе Конвенције о високотехнолошком криминалу у погледу дела расистичке и ксенофобичне природе извршених преко рачунарских система.[3] Он дефинише појам расистичког и ксенофобичног материјала и прописује мере које државе чланице треба да предузму на националном нивоу.

3. Конвенција Савета Европе о заштити деце од сексуалног искоришћавања и сексуалног злостављања (тзв. Ланзарот конвенција – Савет Европе 2007. године, ступила на снагу 2010. године и ратификована исте године од стране Републике Србије)

Овом конвенцијом су, између осталог, посебно дефинисана кривична дела у вези са дечијом порнографијом, као посебним обликом сексуалне експлоатације и злоупотребе деце. Поред тога, ова конвенција препоручује да свака страна потписница усваја мере које могу бити неопходне да би се осигурало да лица, јединице или службе задужене за истрагу буду специјализоване у области борбе против сексуалног искоришћавања и сексуалног злостављања деце или да та лица буду обучена у те сврхе (тзв. принцип специјалности). Она, такође, прописује да ће свака земља потписница предузети све неопходне законодавне или друге мере како би омогућила јединицама истражних служби да идентификују жртве кривичних дела, посебно помоћу анализе порнографског материјала као што су

фотографије и аудио-визуелни записи емитовани или стављени на располагање помоћу информационе и комуникационе технологије.

––––––––––––––

1ВТК водич, стр. 21.

2ВТК водич, стр. 23.

3 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28.I.2003, Art.1.

4. Одлука Савета Европске уније о сузбијању дечије порнографије на интернету 2000/375/ЈНА

Овом одлуком је препоручено да, ако је потребно, а узимајући у обзир управну структуру сваке државе чланице, мере за промовисање ефикасне истраге и кривичног прогона за кривична дела на том подручју, могу бити и установљавање посебних јединица при органима надлежним за извршавање закона која имају потребна стручна знања и средства како би ефикасно поступали на темељу информација о могућој производњи, обради, дистрибуцији и поседовању дечије порнографије. Овом одлуком је препоручено да државе чланице установе властити систем надзора сузбијања производње обраде, поседовања и дистрибуције материјала с дечијом порнографијом.

5. Директива Европског парламента о борби против сексуалне злоупотребе, сексуалне експлоатације и дечије порнографије 2011/92ЕУ

Овом директивом се препоручује државама чланицама да предузму неопходне мере да омогуће истражним јединицама или службама да идентификују жртве кривичних дела (сексуална злоупотреба, сексуална експлоатација, дечија порнографија и тзв. „grooming”), посебно анализом материјала дечије порнографије, као што су фотографије и аудио-видео записи емитовани или стављени на располагање помоћу информационе и комуникационе технологије.

6. Директива 2013/40/ЕУ Европског парламента и Савета ЕУ о нападима на информационе системе и замени Оквирне одлуке Савета 2005/222/ЈНА

Ова директива се односи на нападе усмерене против информационих система. Њен циљ је да приближи кривичним законодавствима земаља чланица ЕУ област напада на информационе системе, успостављањем минималних правила који се односе на дефиницију кривичних дела и одговарајућих кривичноправних санкција, као и унапређење сарадње између надлежних органа који укључују припаднике полиције и других специјализованих агенција за спровођење закона чланица ЕУ, као и надлежних специјализованих агенција и тела саме Европске Уније, као што су EUROJUST, EUROPOL или његов Европски центар за борбу против сајбер

криминала (ЕС 3), као и укључивање у рад Европска агенција за безбедност мрежа и података (ENISA).[4]

7. Безбедносна агенда Европске уније за период од 2015. до 2020. године

Безбедносна агенда препознаје тероризам, организовани криминал и борбу против високотехнолошког криминала као три најозбиљније претње по безбедност ЕУ и кључне приоритете којима се треба бавити. Она има за циљ да искористи постојеће инструменте за сарадњу националних полиција и ЕУ агенција, да те инструменте унапреди и обезбеди њихово пуно спровођење кроз систематску координацију свих релевантних актера у борби против тероризма. ЕУ је установила Иницијативу за борбу против тероризма на Западном Балкану (енг. Western Balkan Counter-Terrorism initiative), која има за циљ да помогне земљама Западног Балкана у борби против претњи џихадиста и екстремизма, да онемогући онлајн комуникацију терориста и њихово финансирање, као и да побољша безбедност на државним границама.[5]

8. Стратегија сајбер безбедности Европске уније из 2013. године – „Отворен, безбедан и заштићен сајбер простор"

Представља први свеобухватни документ који је ЕУ израдила у овој области. Она представља свеобухватну визију ЕУ како на најбољи начин спречити и одговорити на сајбер сметње и нападе, а са друге стране омогућити развој информационих технологија. Она промовише поштовање основних ЕУ вредности, дефинише недозвољено понашање, заговара примену постојећих међународних прописа у области високотехнолошког криминала, помаже другим државама изван ЕУ у изградњи капацитета за борбу против високотехнолошког криминала и промовише сарадњу у овој области.

_____

4ВТК водич, стр. 39.

5Нова безбедносна агенда, стр. 2.

9. IOCTA (Internet organised crime threat assessment 2017) – Процена претње од Интернет организованог криминала

Представља четврти по реду, годишњи извештај, Европоловог центра за високотехнолошки криминал који пружа податке о тренутном стању, трендовима и настанку нових претњи у области високотехнолошког криминала. У извештају су препознате следеће претње у области високотехнолошког криминала и дате препоруке:

Криминал који зависи од напредних технологија – Органи за спровођење закона морају да наставе да се фокусирају на актере који развијају и пружају средства и услуге сајбер криминала, а у односу на кључне претње идентификоване у овом извештају: програмере ransomware-а, банкарске „тројанаце" и друге „малвере" и добављаче средстава за DDoS[6]

напад, услуге усмерене против антивирусна и „ботнете". Органи за спровођење закона и приватни сектор морају наставити да раде заједно на анализи претњи и иницијативама превенције, као што је то случај са пројектом No More Ransom, како би се подигла свест, дао савет и бесплатна средства за дешифровање жртвама ransomware. Запослени у секторима критичне инфраструктуре морају бити боље образовани, припремљени и опремљени за спречавање сајбер напада, користећи ЕУ и националне напоре и ресурсе, нарочито NIS директиву и Општу уредбу о заштити података (GDPR).

„Онлајн" сексуална експлоатација деце – Земље чланице ЕУ треба да обезбеде да је било које истраживачко средство или мера која се користи за борбу против озбиљног и/или организованог криминала доступно и користи се у потпуности у истраживању „онлајн" сексуалне експлоатација деце (CSE). Системи за евидентирање и анализу криминала у земљама чланицама ЕУ треба да се надограде, како би боље одражавали и бележили различите врсте „онлајн" сексуалних кривичних дела, која су пријављена од стране деце или су повезана са децом, као жртвама. Од суштинског је значаја одржавати заједничке, висококвалитетне и вишејезичне активности превенције и подизања свести на нивоу целе ЕУ, како би јаке и ефикасне поруке стигле до оних којима су потребне. Интеграција у едукацију, као и едукација родитеља такође су неопходни.

Преваре везане за плаћање – Органи за спровођење закона и приватни сектор треба да наставе да развијају иницијативе засноване на међусобној сарадњи и размени информација у борби против превара везаних за плаћање, укључујући преваре у којима картице нису присутне, градећи успешне моделе као што су Global Airline Action Days и e-Commerce Action weeks.

„Онлајн" криминална тржишта – Органи за спровођење закона треба да развију глобално координисан стратешки преглед претње „Даркнета", прате и разумеју нове претње и релевантна дешавања. Таква анализа би омогућила будућу координацију глобалне акције за дестабилизацију и затварање криминалних тржишта.

Преплитање сајбер криминала и тероризма – Снажан одговор на џихадистичке сајбер и „онлајн" претње захтева координирану акцију међу мноштвом заинтересованих страна, органима за спровођење закона, обавештајним агенцијама, као и приватном сектору и академској заједници, одређујући џихадистичка дела у контексту сајбер криминала.

Унакрсни фактори криминала – Иновације, у смислу проактивних и адаптивних приступа, стратегије за борбу против криминала, као и сарадња у смислу учешћа свих релевантних партнера, треба да буду језгро било ког одговора на сајбер криминал. Постоји потреба да се настави развијати координисана акција на нивоу ЕУ и шире, како би се одговорило на сајбер криминал, учећи из успешних операција.

„Онлајн" трговина фалсификованом робом – Повреда права интелектуалне својине је широко распрострањена и представља феномен који је у сталном порасту. Европол и Завод за интелектуалну својину Европске уније (*EUIPO*) су, у јулу 2016. године, заједнички основали Коалицију за координацију криминала у области интелектуалне својине (IPC3) у циљу јачања борбе против фалсификовања и пиратерије.

_____

*6**DoS** (енг. Denial of Service) напад је напад на рачунарски сервис којим се корисницима онемогући његово коришћење.*

3.2. Усклађивање политике Републике Србије у области високотехнолошког криминала са политиком ЕУ

Република Србија је 2009. године ратификовала Конвенцију за високотехнолошки криминал из Будимпеште из 2001. године и Додатни протокол, која представљају основ ЕУ Acquis у области борбе против високотехнолошког криминала.

Стратегијом за веродостојну перспективу проширења и појачану сарадњу са државама са подручја Западног Балкана исказана је подршка региону у изградњи и развоју институционалних и стручних капацитета у области високотехнолошког криминала.

Акционим планом за Поглавље 24 – Правда, слобода и безбедност, чији је носилац **Министарство унутрашњих послова**, предвиђено је усклађивање са законодавством ЕУ у области високотехнолошког криминала, а акценат је на унапређењу организационих, кадровских и техничких капацитета, анализи тренутног нормативног и организационог оквира и јачању сарадње између државних органа и институција.

Посебни тужилац за високотехнолошки криминал, као представник Републике Србије, учествује у раду T-CY Комитета Конвенције о високотехнолошком криминалу који чине овлашћени представници земаља које су ратификовале наведену конвенцију Савета Европе. Поред тога, Посебни тужилац је учествовао у раду радне групе овог комитета на изради новелираних упутстава за примену Конвенције која су постала саставни део изворног текста, чиме је дат значајан допринос развоју међународног права у овој области. Такође, значајно је учествовање Посебног тужиоца у раду Групе за прекогранични криминал ове конвенције и у активностима које се тичу израде даљих Препорука и Смерница за примену конвенције, а посебно израде Другог додатног протокола уз ову конвенцију на тему међународне сарадње земаља потписница.

Управа за спречавање прања новца активно учествује у следећим преговарачким поглављима о приступању ЕУ:

– Поглавље 4 – Слободно кретање капитала – које се, пре свега, односи на усклађивање прописа из области кретања капитала и текућих плаћања, као

и на борбу против прања новца и финансирања тероризма. У области спречавања прања новца и финансирања тероризма, захтева се од банака и других економских оператера да идентификују клијенте и пријаве одређене трансакције, за које постоји сумња да се ради о прању новца или финансирању тероризма. Новац који је предмет описаних трансакција може проистећи и од кривичних дела која се доводе у везу са високотехнолошким криминалом.

– Поглавље 23 – Правосуђе и основа права – Један од основних делова наведеног поглавља је и борба против корупције у којој Управа активно учествује кроз праћење и анализу трансакција лица, које могу бити повезане са вискоотехнолошким криминалом.

– Поглавље 24 – Правда, слобода и безбедност – Један од делова овог поглавља је и борба против организованог криминала у којој Управа за спречавање прања новца активно учествује. Високотехнолошки криминал и правни прописи који се односе на ову проблематику су, такође, предмет разговора у оквиру овог поглавља.

Привредна комора Србије у овом тренутку има водећу улогу у формирању федерације идентитета у оквиру нових сервиса е Управе, што је један од основа за успостављање стандардизоване размене података у оквиру европских интеграција.

Министарство трговине, туризма и телекомуникација води Преговарачку групу 10 – Информационо друштво и медији. У оквиру усклађивања са правним оквиром ЕУ у овој области, Министарство је задужено за транспоновање одредби из области електронских комуникација и информационог друштва. У годишњем Извештају Европске комисије о напретку Републике Србије за 2016. годину се истиче да је постигнут известан напредак нарочито са усвајањем Закона о информационој безбедности којим се успостављају надлежни органи за информациону безбедност и национални ЦЕРТ (енг. CERT – Computer Emergency Response Team, Тим за хитно реаговање на нападе на ИКТ систем). Потребно је да Република Србија изврши потпуно усклађивање Закона о информационој безбедности са Директивом број 2016/1148 о мерама за висок заједнички ниво безбедности мрежних и информационих система у Европској унији и према до сада утврђеним роковима наведено би требало да се заврши до трећег квартала 2018. године.

3.3. Законски и стратешки оквир високотехнолошког криминала у Републици Србији

3.3.1. Закони, међународни уговори и подзаконски акти

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) прописује следећа кривична дела против безбедности рачунарских података: оштећење рачунарских података и програма (члан 298),

рачунарска саботажа (члан 299), прављење и уношење рачунарских вируса (члан 300), рачунарска превара (члан 301), неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (члан 302), спречавање и органичавање приступа јавној рачунарској мрежи (члан 303), неовлашћено коришћење рачунара или рачунарске мреже (члан 304), прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података (члан 304а). За наведена кривична дела кривично гоњење је у искључивој надлежности Посебног тужилаштва за борбу против високотехнолошког криминала. Такође, у Кривичном законику се дефинише значење појединих израза од важности за област високотехнолошког криминала.

Законик о кривичном поступку („Службени гласник РС”, бр. 72/11, 101/11, 121/12, 32/13, 45/13 и 55/14) прописује низ посебних доказних радњи које се могу применити у кривичним поступцима против учинилаца кривичних дела из стварне надлежности Посебног тужилаштва за борбу против високотехнолошког криминала. И у овом законику се дефинише значење израза од важности за област високотехнолошког криминала.

Конвенцијом о високотехнолошком криминалу („Службени гласник РС – Међународни уговори”, број 19/09) предвиђено је увођење адекватних инструмената када је реч о процесним одредбама, како би се створила основа за истраживање и процесуирање ових кривичних дела, установљавање брзих и ефикасних институција и процедура међународне сарадње. Такође, предвиђено је оснивање контакт тачке или тачки „24/7 мреже” која би служила као подршка полицијским и другим органима земаља које су ратификовале Конвенцију, као контакт за сва обавештења и почетна тачка за све захтеве који се тичу процесуирања и истраживања кривичних дела високотехнолошког криминала.

Додатни протокол уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система („Службени гласник РС – Међународни уговори”, број 19/09) предвиђа инкриминисање аката расистичке и ксенофобичне природе почињених путем рачунарских система. Његова основна сврха је да се инкриминишу понашања која нису обухваћена Конвенцијом, а која се тичу ширења мржње, нетолеранције и нетрпељивости према расним, националним, верским и другим групама и заједницама, коришћењем рачунара као средстава комуникације и ширења пропаганде.

Конвенција Савета Европе о заштити деце од сексуалног искоришћавања и сексуалног злостављања („Службени гласник РС – Међународни уговори”, број 1/10) регулише спречавање и борбу против сексуалног искоришћавања и сексуалног злостављања деце, као и заштиту права деце – жртава сексуалног искоришћавања и сексуалног злостављања,

те унапређење националне и међународне сарадње у борби против сексуалног искоришћавања и сексуалног злостављања деце.

Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала („Службени гласник РС”, бр. 61/05 и 104/09) дефинише оквир за откривање, кривично гоњење и суђење за кривична дела против безбедности рачунарских података, интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство дела јављају рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, као и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 2.000 или настала материјална штета прелази износ од 1.000.000 динара; кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира и уставног уређења и безбедности Републике Србије, која се због начина извршења или употребљених средстава могу подвести под високотехнолошки криминал.

Закон о организацији и надлежности државних органа у сузбијању организованог криминала, тероризма и корупције („Службени гласник РС”, број 94/16) уређује образовање, организацију, надлежност и овлашћења државних органа и посебних организационих јединица државних органа, ради откривања, кривичног гоњења и суђења за кривична дела одређена овим законом. Кривична дела високотехнолошког криминала могу имати елеменат организованости.

Испуњавајући преузете обавезе из Конвенције о заштити деце од сексуалног искоришћавања и сексуалног злостављања, Република Србија је донела **Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима** („Службени гласник РС”, број 32/13), а којим су први пут уведене посебне мере према учиниоцима кривичних дела против полне слободе према малолетним лицима, између осталог, као што су обавезно јављање надлежном органу полиције и Управе за извршење кривичних санкција, односно забрана посећивања места на којима се окупљају малолетна лица (вртићи, школе и сл.), као и да је прописано посебно вођење евиденција осуђених лица.

Закон о електронским комуникацијама („Службени гласник РС”, бр. 44/10, 60/13 – УС и 62/14) уређује услове и начин за обављање делатности у области електронских комуникација, надлежности државних органа у области електронских комуникација, заштиту права корисника и претплатника, безбедност и интегритет електронских комуникационих мрежа и услуга, тајност електронских комуникација, законито пресретање и задржавање података, надзор над применом овог закона, мере за поступање супротно одредбама овог закона, као и друга питања од значаја за функционисање и развој електронских комуникација у Републици Србији.

Законом о информационој безбедности („Службени гласник РС”, бр. 6/16 и 94/17) се уређују мере заштите од безбедносних ризика у

информационо-комуникационим системима, одговорност 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. Законом је одређено да је **Министарство трговине, туризма и телекомуникација** надлежно за послове информационе безбедности. У циљу остваривања сарадње и усклађеног обављања послова у функцији унапређења информационе безбедности Влада оснива **Тело за координацију послова информационе безбедности**, које у свом раду формира **стручне радне групе** Тела за координацију. Послове превенције и заштите од безбедносних ризика у ИКТ (информационо-комуникационим технолошким) системима у Републици Србији врши **Национални центар за превенцију безбедносних ризика у ИКТ системима** (Национални ЦЕРТ), за чији рад је надлежна **Регулаторна агенција за електронске комуникације и поштанске услуге**.[7] **Посебан центар за превенцију безбедносних ризика у ИКТ системима** (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. **Центар за безбедност ИКТ система у републичким органима** (ЦЕРТ републичких органа) обавља послове који се односе на заштиту од инцидената у ИКТ системима републичких органа, изузев ИКТ система самосталних оператора. Законом о информационој безбедности дефинисани су **ИКТ системи од посебног значаја**, као и **самостални оператори ИКТ система** (Министарство унутрашњих послова, Министарство одбране, Министарство спољних послова, службе безбедности) који су у обавези да у складу са законом донесу акт о безбедности ИКТ система. Министарство унутрашњих послова и Министарство одбране, као самостални оператори ИКТ система израдили су Предлоге акта о безбедности, који још увек нису донети. Актом о безбедности одређују се мере заштите, а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система од посебног значаја.

Закон о одговорности правних лица за кривична дела („Службени гласник РС”, број 97/08) уређује услове одговорности правних лица за кривична дела, кривичне санкције које се могу изрећи правним лицима и правила поступка у којем се одлучује о одговорности правних лица, изрицању кривичних санкција, доношењу одлуке о рехабилитацији, престанку мере безбедности или правне последице осуде и извршењу судских одлука.

Закон о међународној правној помоћи у кривичним стварима („Службени гласник РС”, број 20/09) уређује поступак пружања међународне правне помоћи у кривичним стварима у случајевима када не постоји потврђен међународни уговор или када одређена питања њиме нису уређена.

Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине („Службени гласник РС”, бр. 46/06 и 104/09 – др. закони) уређује посебна овлашћења органа државне управе и организација које врше јавна овлашћења ради ефикасне заштите права интелектуалне својине у складу са прописима којима се уређује право интелектуалне својине.

Закон о спречавању прања новца и финансирања тероризма („Службени гласник РС”, број 113/17) прописује мере и радње које Управа за спречавање прања новца предузима уколико постоји сумња да ће новац који је проистекао из неког кривичног дела из којег проистиче имовинска корист (између осталих и кривична дела која се доводе у везу са високотехнолошким криминалом) бити интегрисан у легалне новчане токове.

Закон о ограничавању располагања имовином у циљу спречавања тероризма и ширења оружја за масовно уништење („Службени гласник РС”, бр. 29/15, 113/17 и 41/18), у члану 9. прописује да Управа за спречавање прања новца може да захтева податке о означеном лицу и његовој имовини од државних органа, организација и лица којима су поверена јавна овлашћења, који су дужни да податке доставе. Управа без одлагања о наведеном лицу сачињава извештај који доставља министру надлежном за послове финансија, који ако утврди да се ради о означеном лицу и имовини која подлеже ограничавању располагања, решењем налаже ограничавање располагања имовином тог лица. Ово се односи и на случајеве када се извршење кривичног дела означених лица доводи у везу са високотехнолошким криминалом.

Закон о полицији („Службени гласник РС”, бр. 6/16 и 24/18) у члану 34а прописује платформу за безбедну електронску комуникацију, размену података и информација у циљу спречавања организованог криминала и других облика тешког криминала. Врши се евидентирање приступа, као и размена података о кривичним делима у складу са законом којим се уређује сузбијање организованог криминала, корупције и других посебно тешких кривичних дела, уз примену мера информационе безбедности.

Закон о Безбедносно-информативној агенцији („Службени гласник РС”, бр. 42/02, 111/09, 65/14 – УС, 66/14 и 36/18) прописује послове који се односе на: заштиту безбедности Републике Србије и откривање и спречавање делатности усмерених на подривање или рушење Уставом утврђеног поретка Републике Србије; истраживање, прикупљање, обраду и процену безбедносно-обавештајних података и сазнања од значаја за безбедност Републике Србије и информисање надлежних државних органа о тим подацима, као и друге послове одређене законом. Поред тога, кад посебни разлози безбедности Републике Србије то захтевају, Агенција може да преузме и непосредно обави послове који су у надлежности министарства надлежног за унутрашње послове, о чему одлуку споразумно доносе директор Агенције и министар надлежан за унутрашње послове. У случају

сукоба надлежности одлучује Влада, у складу са законом и другим прописима. Преузете послове припадници Агенције обављају под условима и на начин, као и применом овлашћења, утврђених законом и другим прописима које примењују овлашћена службена лица и радници на одређеним дужностима министарства надлежног за унутрашње послове, у складу са прописима о унутрашњим пословима.

Закон о Војсци Србије („Службени гласник РС”, бр. 116/07, 88/09 и 101/10 – др. закон, 10/15, 88715 – УС и 36/18) у члану 53. уређује надлежност Војне полиције за обављање послова сузбијања криминалитета у Министарству одбране и Војсци Србије, односно да овлашћена службена лица Војне полиције спроводе оперативну и криминалистичку обраду према запосленом у Министарству одбране и припадницима Војске Србије за кога постоје основи сумње да је у служби или у вези са службом извршио кривично дело за које се гони по службеној дужности, при чему у поступању имају обавезе и овлашћења у складу са законом којим се уређује кривични поступак, Законом о полицији и прописима донетим на основу тог закона. Војна полиција може применити службена овлашћења и према цивилима у случају када постоје основи сумње да су учинили кривично дело на штету Министарства одбране или Војске Србије за које се гони по службеној дужности. Полазећи од цитираних одредби, борбу против, пре свега, све већег броја напада сајбер криминалаца на информационо-комуникационе системе у Министарству одбране и Војсци Србије, односно процесуирање кривичних дела високотехнолошког криминала, у складу са Закоником о кривичном поступку, Кривичним закоником и Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала, предузимају овлашћена службена лица Војне полиције.

Закон о Војнобезбедносној агенцији и Војнообавештајној агенцији („Службени гласник РС”, бр. 88/09, 55/12 – УС и 17/13) у члану 5. уређује надлежност Војнобезбедносне агенције за обављање безбедносне и контраобавештајне заштите Министарства одбране и Војске Србије у оквиру које обавља безбедносне, контраобавештајне и остале послове и задатке од значаја за одбрану Републике Србије, у складу са законом и прописима донетим на основу закона. У одредби члана 6. став 2. тачка 4. утврђено је да је Војнобезбедносна агенција овлашћена да открива, истражује и прикупља доказе за кривична дела против безбедности рачунарских података, прописана Кривичним закоником, као и другим законима када су наведена кривична дела усмерена против Министарства одбране и Војске Србије.

Закон о тајности података („Службени гласник РС”, број 104/09) уређује јединствен систем одређивања и заштите тајних података који су од интереса за националну и јавну безбедност, одбрану, унутрашње и спољне послове Републике Србије, заштите страних тајних података, приступ тајним подацима и престанак њихове тајности, надлежност органа и надзор над спровођењем овог закона, као и одговорност за неизвршавање обавеза из овог закона и друга питања од значаја за заштиту тајности података.

Законом о заштити података о личности („Службени гласник РС”, бр. 97/08, 104/09 – др. закон, 68/12 – УС и 107/12) уређују се услови за прикупљање и обраду података о личности, права лица и заштита права лица чији се подаци прикупљају и обрађују, ограничења заштите података о личности, поступак пред надлежним органом за заштиту података о личности, обезбеђење података, евиденција, изношење података из Републике Србије и надзор над извршавањем овог закона.

Закони из области права интелектуалне својине уређују за сваку врсту права интелектуалне својине посебно предмет и услове за стицање заштите, поступак заштите, садржину, стицање и обим права, престанак права и грађанскоправну заштиту. Законодавни оквир у области интелектуалне својине чине следећи закони: Закон о ауторском и сродним правима („Службени гласник РС”, бр. 104/09, 99/11, 119/12 и 29/16 – УС), Закон о патентима („Службени гласник РС”, бр. 99/11 и 113/17), Закон о жиговима („Службени гласник РС”, бр. 104/09, 10/13 и 44/18 – др. закон), Закон о правној заштити индустријског дизајна („Службени гласник РС”, бр. 104/09, 45/15 и 44/18 – др. закон), Закон о заштити топографија полупроводничких производа („Службени гласник РС”, број 55/13), Закон о ознакама географског порекла („Службени гласник РС”, бр. 18/10 и 44/18 – др. закон), Закон о оптичким дисковима („Службени гласник РС”, број 52/11), Закон о заштити пословне тајне („Службени гласник РС”, број 72/11).

У вези са Законом о информационој безбедности значајне су следеће четири уредбе: Уредба о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја; Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја; Уредба о утврђивању Листе послова у областима у којима се обављају делатности од општег интереса и у којима се користе информационо-комуникациони системи од посебног значаја; Уредба о поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, као и Правилник о ближим условима за упис у Евиденцију посебних центара за превенцију безбедносних ризика у информационо-комуникационим системима.

Поред наведних уредби донета је и Уредба о безбедности и заштити деце при коришћењу информационо-комуникационих технологија, којом су предвиђене превентивне мере за безбедност и заштиту деце при коришћењу информационо-комуникационих технологија, односно безбедност и заштиту деце на интернету и поступање у случају нарушавања или угрожавања њихове безбедности на интернету.

На основу **Закона о електронским комуникацијама,** Регулаторна агенција за електронске комуникације и поштанске услуге је донела

Правилник о општим условима за обављање делатности електронских комуникација по режиму општег овлашћења. Овим правилником ближе су прописани општи услови за обављање делатности и одређени услови који важе за обављање свих или појединих делатности електронских комуникација по режиму општег овлашћења и прописан образац обавештења о обављању делатности електронских комуникација. Такође, у члану 127. став 5. Закона о електронским комуникацијама прописано је да министарство надлежно за послове телекомуникација, по прибављеном мишљењу министарства надлежног за послове правосуђа, министарства надлежног за унутрашње послове, министарства надлежног за послове одбране, Безбедносно-информативне агенције и органа надлежног за заштиту података о личности, ближе прописује захтеве за уређаје и програмску подршку за законито пресретање електронских комуникација. На основу наведене одредбе Министарство трговине, туризма и телекомуникација је донело Правилник о захтевима за уређаје и програмску подршку за законито пресретање електронских комуникација и техничким захтевима за испуњење обавезе задржавања података о електронским комуникацијама, који је у примени од 31. октобра 2015. године.

Поред тога, донети су и следећи правилници: Правилник о ближим условима за упис у Евиденцију посебних центара за превенцију безбедносних ризика у информационо-комуникационим системима, након уредби које су донете на основу Закона о информационој безбедности („Службени гласник РС”, бр. 6/16 и 94/17), Правилник о методологији за извршавање послова у складу са Законом о спречавању прања новца и финансирања тероризма, Правилник о начину обавештавања физичких и правних лица о промени на листи означених лица донетој од стране Савета безбедности Уједињених нација и других међународних организација у којима је Република Србија члан.

––––––––––––––

7 Закон о информационој безбедности, члан 14.

3.3.2. Актуелне промене у правном оквиру

Ради усклађивања одређених законских прописа са правом ЕУ, израђени су нацрти закона чије се усвајање очекује у току 2018. године или у првом делу 2019. године. У току 2018. године, очекује се усвајање измена и допуна Закона о ауторском и сродним правима, Закона о патентима, Закона о жиговима, Закона о заштити топографија полупроводничких производа, затим, увајање новог Закона о ознакама географског порекла и Закона о електронским комуникацијама, а у првом кварталу 2019. године и усвајање новог Закона о заштити пословне тајне. Поред наведеног, урађен је Нацрт закона о изменама и допунама Закона о посебним овлашћењима ради ефикасне заштите права интелектуалне својине.

Такође, Министарство правде је основало радне групе за измене и допуне Кривичног законика и Законика о кривичном поступку ради даљег усклађивања домаћег кривичног законодавства са позитивним прописима Европске Уније. Усвајање измена и допуна Кривичног законика и Законика о кривичном поступку очекује се до 2020. године.

Тренутно су у изради подзаконска акта на основу Закона о електронском документу, електронском идентитету и услугама од поверења у електронском пословању, а очекују се и измене Закона о информационој безбедности.

У Нацрту о критичној инфраструктури по коме се успоставља нормативни оквир за идентификацију, означавање и заштиту критичне инфраструктуре у Републици Србији, сходно Акционом плану за Поглавље 24, где је носилац задатка Сектор за ванредне ситуације у Министарству унутрашњих послова, у члану 2. дефинисан је појам критичне инфраструктуре.

3.4. Програми и стратегије

3.4.1. Програми и пројекти у фази програмирања

1. Програм „Изградња капацитета за представнике полиције и правосуђа укључене у борбу против сајбер криминала”

Програм је намењен представницима полиције и правосуђа из региона Западног Балкана, Источне Европе и Централне Азије. Предвиђено је да пројекат траје од 1. маја 2017. године до 30. априла 2019. године, а вредност је 648.433,80 евра и да се у првој години организује пет обука за представнике полиције и правосуђа држава Западног Балкана.

2. Пројекат за борбу против високотехнолошког криминала у оквиру Фонда за унутрашњу безбедност – Полиција (ISPF)

Пројекат има за циљ борбу против сајбер криминала и планира се учешће: форензичких експерата, истражитеља, оперативних аналитичара и тужилаца из земаља чланица EUSDR. Предложени буџет пројекта је оквирно 1,2 милиона евра. Тренутно водећи партнери пројекта чекају отварање одговарајућег позива од стране Европске комисије у оквиру ISFP фонда ради подношења предлога пројекта. Такође, водећи партнери су отворени за додатне предлоге и идеје будућих партнера. Ради једноставније комуникације замолили су да се заинтересоване државе чланице EUSDR изјасне о заинтересованости за партнерство у пројекту и определе контакт особу одговорну за предвиђено партнерство и одговарајућу комуникацију.

3. Твининг пројекат на тему борбе против сајбер криминала

У оквиру програмирања ИПА 2017 у припреми је Твининг пројекат, који предвиђа следеће обуке: Истраживање „малвера” (злонамерних софтвера); Аутоматизована претрага података на Интернету за прикупљање података о извршеним кривичним делима у „Online” простору; Коришћење бесплатних алата и техника у сврхе спречавања високотехнолошког криминала (Open

sorce inteligence – OSINT); Обука за прикупљање података са рачунара (енг. „first responder") и форензика рачунара у online режиму рада (енг. „live forensic"); Обука типа „тренинг тренера" у области високотехнолошког криминала. Осим обука предвиђена је и конференција о сарадњи полиције са приватним компанијама, академским институцијама, невладиним сектором и истакнутим стручњацима у области информационих технологија. Одељење за сузбијање високотехнолошког криминала има изражену потребу за сарадњом са партнерима из области државног и јавног сектора, приватног сектора и истакнутих стручњака у овој области. Потреба за оваквим видом сарадње настаје због природе високотехнолошког криминала. Знања, вешине и подаци која поседују банке, приватне компаније, па и стручњаци који се баве информационом безбедношћу понекад су далеко испред вештина и техничких могућности држава које се супротстављају високотехнолошком криминалу. То се посебно односи на мултинационалне компаније. Пројектом су предвиђене и студијске посете које би требале да омогуће увид у најбољу праксу везану за истраживање злонамерних софтвера, аутоматизовану претрагу података на интернету и за прикупљање података са рачунара (енг. „first responder") и форензика рачунара у online режиму рада (енг. „live forensic"). У оквиру програмирања ИПА 2017 у припреми је и Уговор о набавци опреме који предвиђа набавку ИТ опреме и софтвера намењених борби против сајбер криминала.

3.4.2. Пројекти у фази спровођења

1. Пројекат „Сарадња у борби против криминала у сајбер простору: циљање имовине стечене криминалом на интернету у Југоисточној Европи и Турској":

Корисник овог пројекта је Управа криминалистичке полиције, Служба за борбу против организованог криминала (вишекорисничка ИПА 2014). Укупна вредност пројекта је 5.560.000 евра (од чега 5.000.000 евра је допринос ЕУ, а 560.000 евра је кофинансирање Савета Европе). Имплементатор пројекта је Савет Европе, Канцеларија за борбу против криминала у сајбер простору у Букурешту, Румунија. Остале земље које учествују у пројекту су: Република Албанија, Босна и Херцеговина, Црна Гора, Република Србија, Република Македонија, Република Турска и Косово*. Пројекат ће трајати 42 месеца (од јануара 2016. до јуна 2019. године). Општи циљ пројекта је ојачати законодавство у погледу тражења, заплене и одузимања прихода сајбер-криминала и спречавање прања новца на интернету у складу са захтевима за заштиту података.

Резултати овог пројекта су: допринос јачању владавине права кроз борбу против корупције и организованог криминала; јачање капацитета институција за истраге, заплене и одузимање имовине проистекле из криминала у сајбер простору и превенција прања новца на интернету; успостављање јавног система пријављивања превара; унапређење законског оквира; сарадња полицијских јединица; израда приручника за

финансијски сектор; механизми размене информација приватног и јавног сектора; правосудни тренинг и међународна сарадња.

У оквиру пројекта, у току 2016. и 2017. године реализован је велики број активности од којих су најзначајније: конференција у Охриду, регионална студија случаја о компјутерском криминалу и финансијским истрагама „Regional case simulation exercise on cybercrime and financial investigations" у Тбилисију, међународна радионица на тему сајбер криминала у Бриселу, радионице о ризицима прања новца у вези са технологијама, као и о онлајн финансијским преварама и преварама у вези са платним и кредитним картицама, семинар у Букурешту на тему „Истраге у вези са Даркнетом и виртуелним валутама", обука о истрази „Даркнета" и виртуелних валута и курс у Загребу под називом: „Training on WMD Cyber Crimes Investigations".

_____

** Овај назив је без прејудицирања статуса и у складу је са Резолуцијом Савета безбедности Уједињених нација 1244 и мишљењем Међународног суда правде о декларацији о независности Косова.*

2. Научно-истраживачки пројекат Advanced Tools for fighting online illegal trafficking – АНИТА (787061) у склопу Horizon 2020

Криминалистичко-полицијски универзитет учествује у реализацији овог пројеката, који је усмерен на развој и усавршавање софтверских решења и обуке припадника полиције, тужилаштва и других органа и организација чија је основна делатност у сузбијању кривичних дела и превенције вискотехнолошког криминала. Пројекат је почео 15. маја 2018. године и има за циљ да, преко радних сценарија, развије и усаврши, већ постојећа, као и нова, софтверска решења којима би се пратиле незаконите активности у Darknet и Deep Web[9]. Предвиђено је да се пројекат реализује до 15. маја 2020. године.

3. Пројекат Европске уније и Савета Европе iPROCEEDS@IPA

У пројекат су укључене земље југоисточне Европе и Република Турска. Он има за циљ оспособљавање и јачање капацитета државних органа надлежних за борбу против високотехнолошког криминала у Републици Србији и земљама у региону у поступцима одузимања имовине у предметима високотехнолошког криминала. У оквиру пројекта спроведене су две експертске мисије, када је одржан састанак о сарадњи државних органа и приватног сектора у сузбијању високотехнолошког криминала и одузимању имовине проистекле из кривичних дела из ове области, док је друга мисија, одржана у јуну 2017. године, у циљу израде водича за превенцију и откривање имовине проистекле из кривичних дела учињених путем Интернета. У оквиру пројекта одржан је низ радионица и стручних скупова у којима су учествовали представници јавног тужилаштва.

Такође, представник Посебног тужилаштва наставио је учешће у изради логичке матрице за сектор унутрашњих послова ИПА 2017 пројекта, којим се планира јачање административних и техничких капацитета Посебног тужилаштва, кроз спровођење опремања тужилаштва и организовање специјализованих обука.

У оквиру овог пројекта, од 12. до 13. октобра 2017. године, представници ЦЕРТ, Регулаторне агенције за електронске комуникације и поштанске услуге и Министарства унутрашњих послова учествовали су у студијској посети ЦЕРТ Румуније[10], која је имала за циљ јачање капацитета новооснованих ЦЕРТ кроз размену знања, искуства и најбољих пракси везаних за оперативно окружење ЦЕРТ. Поред тога, 20. децембра 2017. године у Скопљу је одржана Регионална радионица о размени добрих пракси о механизмима извештавања у Југоисточној Европи и Турској[11]. Радионица је послужила као форум за расправу за тужиоце, истраживаче у области сајбер криминала, представнике Министарства правде, Министарства унутрашњих послова и ЦЕРТ тимове у вези са функционисањем и коришћењем механизма извештавања о сајбер криминалу. Утврђена је структура и методе за прикупљање информација за извештај и допринос извештаја кроз дељење информација, као и истраживање кривичних предмета и статистичких разлога. Договорена је и размена добрих пракси у региону на онлине платформама за пријављивање сајбер криминала.

––––––––––––––

9Deep weeb (срп. „Дубока мрежа") – позната и као невидљива или скривена мрежа, означава претрагу која се односи на садржај на светској мрежи, која није индексирана од стране стандардних претраживача.

10 https://www.coe.int/en/web/cybercrime/-/iproceeds-study-visit-on-csirt-cert-regulations-and-operational-environment

11 https://www.coe.int/en/web/cybercrime/-/iproceeds-regional-workshop-on-sharing-good-practices-on-reporting-mechanisms-in-south-eastern-europe-and-turkey

3.4.3. Реализовани пројекти

1. Пројекат „Подршка владавини закона кроз јачање капацитета за информациону безбедност Министарства унутрашњих послова"

Пројекат финансира Влада Уједињеног Краљевства Велике Британије и Северне Ирске (из Good Governance Fund-a), док је DCAF био имплементациони партнер. Корисник пројекта је Сектор за аналитику, телекомуникационе и информационе технологије, Центар за реаговање на нападе на информациони систем (ЦЕРТ). Поред ЦЕРТ-а и Одељења за информациону безбедност, у одређеним фазама у пројекат су били укључени и други државни органи од значаја за информациону безбедност у Републици Србији, од којих су највише ангажовања имали Регулаторна

агенција за електронске комуникације и поштанске услуге – РАТЕЛ (као институција која треба да формира Национални ЦЕРТ), УЗЗПРО[12] (као институција која треба да формира ЦЕРТ републичких органа) и Министарство трговине, туризма и телекомуникација (Министарство надлежно за информациону безбедност). Сврха пројекта је подршка Министарству унутрашњих послова у развијању одрживе структуре отпорне на претње из сајбер простора МУП-овим системима и сервисима, која је оспособљена да сарађује са свим релевантним националним и међународним заинтересованим странама и која доприноси националној и међународној сајбер безбедности, а вредност пројекта је 143.720 фунти. Пројекат је реализован у периоду од 1. марта 2017. до 31. августа 2017. године.

Један од важнијих резултата прве фазе пројекта био је оквир за обуку кадрова који је планирано да се конкретизује и спроведе у другој фази пројекта током 2018. године, за чији наставак су заинтересовани и имплементатор и донатор.

2. Пројекат Савета Европе и Европске Уније Global Action on Cyber Crime + (GLACY+)

Посебно тужилаштво за високотехнолошки криминал је укључено у овај пројекат, чији је циљ свеобухватна, планетарна примена Конвенције о високотехнолошком криминалу и пружање директне административне и техничке помоћи земљама које су обухваћене овим пројектом, у оквиру ког је Посебни тужилац ангажован на изради међународних стандарда и обука за поступање у овој области јавних тужилаштва и судова, као и израде процедура за поступање са електронским доказима припадника надлежних служби за откривање кривичних дела и анализу дигиталних доказа.

Поред наведених активности, Републичко јавно тужилаштво и Посебно тужилаштво за високотехнолошки криминал учествују и у следећим пројектима:

3. Пројекат „Унапређење обуке за кадрове правосудних органа у области заштите деце од насиља на интернету”

Овом пројекту финансијску подршку пружа међународна организација цивилног друштва Save the children. Његов циљ била је израда плана и програма обуке за судије и јавне тужиоце у области високотехнолошког криминала и заштитите малолетних лица на интернету. Посебни тужилац је био члан радне групе за израду плана и програма обуке. Такође, у оквиру пројекта израђен је приручник – Водич за судије и јавне тужиоце на тему високотехнолошког криминала и заштите малолетних лица у Републици Србији. У склопу сарадње са међународном организацијом цивилног друштва Save the children, а у складу са Акционим планом за Поглавље 24 и активношћу 6.2.9.3.1. – Сачинити и потписати споразуме о сарадњи између државних органа и организација цивилног друштва у борби против

високотехнолошког криминала, разматра се закључење Споразума о сарадњи.

_____

12 Тренутно надлежна Канцеларија за информационе технологије и електронску управу.

3.4.4. Стратешка документа

1. Стратешка процена јавне безбедности за период од 2017. до 2021. године и Стратешки план полиције 2018–2019. година

У Стратешкој процени јавне безбедности одређени су приоритети у раду полиције за период 2017–2021. године, на основу анализе стања и кретања криминала. Стратешка процена је као један од осам приоритета одредило и борбу против злоупотреба информационо-комуникационих технологија на територији Републике Србије. У оквиру Стратешког плана полиције конкретизован је наведени приоритет кроз дефинисане активности, носиоце, рокове и ресурсе за период 2018–2019. године.

2. Процена претњи од тешког и организованог криминала у Србији (енг. Serious and Organised Crime Threat Assessment – SOCTA) из 2015. године

Ова процена је стратешки документ који има за циљ стварање објективне основе за доношење релевантних стратешких и оперативних одлука којима ће се унапредити правни и институционални капацитети Министарства унутрашњих послова и других органа за спровођење закона и постићи већи степен заштите основних права и слобода грађана Србије.[13] Процена као безбедносне претње идентификује различите облике тешког и организованог криминала, укључујући и високотехнолошки криминал, а на којима полиција заснива свој оперативни рад у складу са постојећим трендовима.

3. Регионална процена претњи од тешког и организованог криминала из 2016. године

У питању је документ, израђен по методологији EUROPOL, који омогућава свеобухватно сагледавање актуелног стања и кретања, као и последица које проузрокују организовани и тешки криминал укључујући и високотехнолошки криминал, као и рано упозоравање на нове трендове и претње по регион како би се олакшала превенција и супротстављање наведеним облицима криминала. Конкретни циљеви овог документа су да се изврши приказ актуелног стања на територији Републике Србије, Црне Горе и Републике Македоније, укаже на области које представљају највећу претњу у овом делу региона (међу којима су и различити видови високотехнолошког криминала), да се одреде фактори који утичу на ове појаве, идентификују заједничке карактеристике деловања криминалних група, као и да се дају претпоставке о развоју будућих претњи које могу

послужити као основ за доношење одлука о заједничком супротстављању на регионалном нивоу.

4. Стратегија развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године

Министарство трговине, туризма и телекомуникација је било носилац активности у изради наведене стратегије, која је усвојена 29. маја 2017. године. У њој је као посебна целина обрађена борба против високотехнолошког криминала у Републици Србији, где су именовани најважнији субјекти у Републици Србији у овој области. Основни циљ је побољшање размене информација, праћење актуелних ризика и подизање свести у овој области.

У циљу развоја и унапређења информационе безбедности у Републици Србији утврђена је, између осталог, приоритетна област борба против високотехнолошког криминала, што се односи на превенцију и санкционисање кривичних дела која се заснивају на злоупотреби информационо-комуникационих технологија;

У области борбе против високотехнолошког криминала одређени су следећи стратешки циљеви:

– унапређење механизама за откривање високотехнолошког криминала и кривично гоњење учинилаца;

– подизање свести о опасностима од високотехнолошког криминала;

– унапређење међународне сарадње у борби против високотехнолошког криминала.

Влада је донела Акциони план за 2018. и 2019. годину, за спровођење Стратегије развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године.

_____

13SOCTA, стр. 1.

5. Стратегија развоја информационог друштва у Републици Србији до 2020. године

Ова стратегија је акт којим се на целовит начин дефинишу основни циљеви, начела и приоритети развоја информационог друштва и утврђују активности које треба предузети у периоду који обухвата ова стратегија.[14] Министарство трговине, туризма и телекомуникација је било носилац реализације у изради ове стратегије, у којој је борба против високотехнолошког криминала препозната као један од стратешких приоритета у области информационе безбедности.

6. Национална стратегија за борбу против прања новца и финансирања тероризма

У формулисању циљева Националне стратегије у обзир је узета и хијерарија циљева делотворног система за борбу против прања новца и финансирања тероризма која је дата у методологији ФАТФ. Отуда је и општи циљ и сврха Националне стратегије да у потпуности заштити финансијски систем и привреду државе од опасности које узрокују прање новца и финансирање тероризма и ширење оружја за масовно уништење, чиме се јача интегритет финансијског сектора и доприноси безбедности и сигурности.[15] Ова стратегија је од важности када је у питању прање новца стеченог извршењем кривичних дела високотехнолошког криминала.

7. Национална стратегија за спречавање и борбу против тероризма за период 2017–2021. година

Ова стратегија има за сврху заштиту Републике Србије од терористичке претње по њене грађане, вредности и интересе, уз истовремено подржавање међународних напора у борби против тероризма. Између осталог, наведена сврха биће остварена спровођењем циљних и осмишљених мера на доктринарном плану, кроз развијање и подизање безбедносне културе друштва и промовисање одређених вредности, као и на нормативном и институционалном плану, кроз унапређење капацитета за превенцију и борбу против тероризма, посебно капацитета за супротстављање насилном екстремизму и радикализацији која води у тероризам, као све израженијем феномену.[16] Препознајући доступност савремених информационих технологија, где су информациони ресурси објекат напада, Република Србија је у поступку израде Стратегије за борбу против високотехнолошког криминала обухватила све области које нису предвиђене овим стратешким документом.

У оквиру Стратегије је као Приоритетна област 1 одређена превенција тероризма, насилног екстремизма и радикализације који воде у тероризам, док је стратегијски циљ 1.4 – Високотехнолошки системи комуникације и дигиталних мрежа отпорни на ширење радикализације и насилног екстремизма.

Развој модерних друштава, оличен у снажном високотехнолошком, убрзаном напретку информатичког друштва, учинио је неопходним пажљиво дефинисање политике супротстављања стављању ових система у службу тероризма, јер појединац може подлећи утицају пропаганде и стећи знања за извршење терористичког акта без непосредног контакта са окружењем.

Остварење овог циља биће постигнуто кроз настојања да се ојача свест у друштву о опасностима коришћења високотехнолошких система комуникације за ширење говора мржње и на националном нивоу изградe и имплементирају најбоље политике, законска решења и пракса супротстављању коришћења ових средстава комуницирања за ширење насилног екстремизма и радикализације који воде у тероризам, укључујући пажљиво дефинисање и промовисање ставова који представљају противтежу.[17]

_____

14 Стратегија развоја информационог друштва у Републици Србији до 2020. године, стр 2.

15 Национална стратегија за борбу против прања новца и финансирања тероризма, стр. 1.

16 Национална стратегија за спречавање и борбу против тероризма за период 2017–2021. година, стр. 1.

17 Национална стратегија за спречавање и борбу против тероризма за период 2017–2021. година

8. Стратегија развоја образовања у Србији до 2020. године

Један део ове стратегије односи се и на развој знања у вези са информационо-комуникационим технологијама. Нова Стратегија за чију се израду формира радна група, треба да обухвати и сегменте превентивне заштите неопходне у борби против високотехнолошког криминала.

9. Стратегија превенције и сузбијања трговине људима, посебно женама и децом и заштите жртава 2017–2022.

Ова стратегија предвиђа посебне активности и задатке који ће обезбедити да деца у Републици Србији, одрастају у окружењу безбедном од трговине људима, искоришћавања у порнографији и проституцији. Откривање и процесуирање случајева трговине децом и искоришћавања у порнографији и проституцији ће бити у складу са проактивним приступом, чији је циљ да се олакша положај деце као жртава и оштећених у поступку. Ово је веома значајно, с обзиром да се зна да се за овај вид искоришћавања злоупотребљавају савремене технологије, мобилни интернет и социјалне мреже.

10. Стратегија националне безбедности Републике Србије

У оквиру политике унутрашње безбедности дефинише „Деловање државних и осталих органа и институција Републике Србије у области унутрашње безбедности усмерено је на заштиту уставног поретка, живота и имовине грађана, спречавање и сузбијање свих облика тероризма, организованог, финансијског, економског и високотехнолошког криминала, корупције, прања новца, трговине људима, наркоманије, пролиферације конвенционалног наоружања и оружја за масовно уништење, обавештајних и субверзивних делатности, као и других изазова, ризика и претњи безбедности".

11. Национална стратегија за борбу против организованог криминала

Ова стратегија одређује да су „појавни облици организованог криминала заступљени у Републици Србији трговина наркотицима, изнуде, отмице, уцене, трговина људима, кријумчарење људи, корупција, прање новца, злоупотреба службеног положаја, фалсификовање новца и других средстава

плаћања, проституција, трговина оружјем и експлозивним материјама, међународно кријумчарење возила, кријумчарење акцизне робе и високотехнолошки криминал”.

12. Концепт сајбер одбране Војске Србије

Војска Србије израдила је Нацрт концепта сајбер одбране Војске Србије, који још увек није усвојен. Документ представља поглед на питање како се процењује одбрамбени, безбедносни, технолошки и друштвени утицај који ће у наредном петогодишњем периоду развоја и употребе Војске Србије остварити развој информационо-комуникационих технологија, активности и дејстава у сајбер простору и употреба офанзивних сајбер способности могућих противника на одбрану Републике Србије. При томе се посебан значај посвећује структури и међусобним односима организационих целина и носилаца оперативних и функционалних способности Војске Србије, као и однос и утицај који се остварује у њиховој интеракцији са спољним актерима, системима, процедурама и ресурсима.

Процена је заснована на резултатима предвиђања релевантних међународних субјеката о очекиваном развоју информационо-комуникационих технологија и њиховом комплексном утицају на одбрану и безбедност Републике Србије, на идентификованим претњама и ризицима на националну безбедности и одбрану, и достигнутом и очекиваном степену развоја капацитета и способности других државних и недржавних субјеката за дејства и активности у сајбер простору или из њега, која могу бити од утицаја на мисије и задатке Војске Србије.

Концепт сајбер одбране Војске Србије представља основни водич који служи доносиоцима одлука на стратегијском националном нивоу за развој одговарајућих, делотворних, оптималних и одрживих војних капацитета и способности Републике Србије у саставу оружаних снага за извођење свеобухватних активности и дејстава у сајбер простору у обављању своје уставне функције одбране.

13. Стратегија развоја интелектуалне својине за период 2018–2022. године

Израђен је Предлог стратегије, чије се усвајање очекује. У Предлогу ове стратегије, за реализацију одређених планираних активности као носилац реализације је одређен Завод за интелектуалну својину, а за реализацију других активности задужен је Завод у партнерству са осталим органима одговорним за спровођење заштите права интелектуалне својине, а за остале је задужено Координационо тело за ефикасну заштиту права интелектуалне својине у Републици Србији. Посебно тужилаштво за високотехнолошки криминал има значајну улогу у погледу заштите права интелектуалне својине, односно надлежно је за гоњење учинилаца кривичних дела у области интелектуалне својине, код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци, као и њихови производи у

материјалном или електронском облику. Под производима у електронском облику посебно се подразумевају рачунарски програми и ауторска дела која се могу употребити у електронском облику.

4. ИНСТИТУЦИОНАЛНИ ОКВИР ЗА БОРБУ ПРОТИВ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА У РЕПУБЛИЦИ СРБИЈИ

4.1. Институционални оквир – тренутно стање

Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала из 2005. године, основано је **Посебно одељење за борбу против високотехнолошког криминала (Посебно тужилаштво**), у оквиру Вишег јавног тужилаштва у Београду. Ово одељење надлежно је за кривично гоњење учинилаца кривичних дела високотехнолошког криминала и надлежно је да поступа на целој територији Републике Србије. Сходно одредбама наведеног закона, за поступање у предметима високотехнолошког криминала надлежан је Виши суд у Београду за територију Републике Србије, а за одлучивање у другом степену надлежан је Апелациони суд у Београду. Тренутно у Посебном тужилаштву, којим руководи Посебни тужилац, распоређена су четири заменика јавног тужиоца, два виша тужилачка сарадника, један тужилачки сарадник и два административна радника. Обученост је на завидном нивоу са тенденцијом констатног усавршавања, које се огледа у континуираним похађањима специјалистичких програма обука заменика јавног тужиоца и тужилачких помоћника.

Такође, одредбом Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала, у оквиру **Министарства унутрашњих послова** (МУП), предвиђено је формирање службе за борбу против високотехнолошког криминала која поступа по налозима Посебног тужиоца за високотехношки криминал. У Министарству унутрашњих послова је формирано Одељење за борбу против високотехнолошког криминала која је постала једина специјализована јединица МУП задужена за кривична дела високотехнолошког криминала. Ово одељење поступа по захтевима надлежног Одељења за борбу против високотехнолошког криминала Вишег јавног тужилаштва у Београду, које руководи предистражним поступком у овим предметима, али због природе посла, ово одељење поступа и по захтевима других тужилаштава у Републици Србији, посебно Тужилаштва за организовани криминал, те активно пружа оперативно-техничку подршку другим полицијским јединицама, пре свега одељењима у саставу СБПОК. Одељење се бави спречавањем свих облика кривичних дела из области безбедности рачунарских података, сексуалне експлоатације деце на интернету (дечија порнографија), кршења права интелектуалне својине на интернету (софтверска пиратерија, филмска и музичка пиратерија), трговине на интернету, интернет банкарства, превара и злоупотреба платних картица на интернету, ширења штетних и недозвољених садржаја (расне, верске и националне мржње, пропагирање тероризма и ксенофобије),

угрожавање сигурности путем Интернета и др. Одељење за борбу против високотехнолошког криминала, од формирања 2007. године до средине јуна 2018. године, у свом саставу имало је два одсека: Одсек за сузбијање електронског криминала и Одсек за сузбијање криминала у области интелектуалне својине**.** Актом о систематизацији предвиђено је формирање поред наведених још два одсека и то Одсек за сузбијање недозвољених и штетних садржаја на интернету и Одсек за сузбијање злоупотреба у области електронске трговине, електронског банкарства и платних картица на интернету. Уједно је промењен назив одељења у Одељење за сузбијање високотехнолошког криминала у коме је систематизовано 22 радна места

У оквиру Министарства унутрашњих послова, Сектора за аналитику, телекомуникационе и информационе технологије формиран је Центар за реаговање на нападе на информациони систем (ЦЕРТ) који, између осталог, обавља следеће послове: стално прикупљање информација о новим безбедносним проблемима и мерама заштите, идентификација критичне информационе инфраструктуре у Министарству, предлагање мера за заштиту критичне информационе инфраструктуре, анализа захтева које треба да испуни информациони систем Министарства унутрашњих послова за повезивање на информационе системе ЕУ, сарадња и размена информација са националним ЦЕРТ, ЦЕРТ тимовима других државних институција и међународним ЦЕРТ тимовима, превентивно реаговање у случају потенцијалне опасности по информациони систем Министарства унутрашњих послова, помоћ у санирању последица напада на информациони систем Министарства унутрашњих послова. ЦЕРТ предузима све мере и поступке против починиоца напада са Интернета кроз сарадњу са Одељењем за сузбијање високотехнолошког криминала, Управе криминалистичке полиције, у циљу прикупљања документације и обезбеђења доказа за покретање поступка против починиоца напада који су неопходни Посебном јавном тужилаштву за високотехнолошки криминал, ради подношења кривичних пријава и покретања поступка пред судом да би се законски испоштовао тзв. ланац надређености постојања кривичних дела учињених у сајбер простору – CHAIN OF CUSTODY, тј. ланац кретања доказа, односно непрекинут ланац који омогућава праћење кретања доказног материјала од тренутка када је пронађен, и то кроз образац-формулар који садржи хронолошке податке о датуму, лицу које је руковало доказом и евентуалним променама или радњама које су наступиле у вези са истим током доказног поступка (нпр. пренос, место чувања, анализа и др.), а у сврху употребе доказа у судском поступку.

У циљу иновирања система полицијског образовања, Криминалистичко-полицијски универзитет је у оквиру департмана Рачунарства и информатике, у сарадњи са Министарством унутрашњих послова, акредитовао студијске програме на сва три нивоа студија који стварају услове за образовање у областима супротстављања високо-технолошком криминалу и информатичке безбедности, као и за научна истраживања у тим областима.

Значајну улогу у овој области имају Народна банка Србије и Министарство трговине, туризма и телекомуникација (МТТТ). Народна банка Србије надлежна је за контролу, односно надзор информационо-комуникационих система финансијских институција које су под њеним надзором. Министарство трговине, туризма и телекомуникација је надлежни орган за информациону безбедност, односно безбедност ИКТ система од посебног значаја у Републици Србији. У вршењу ове надлежности МТТТ обавља следеће послове: израда прописа и стратегија у области информационе безбедности; инспекцијски надзор над радом ИКТ система од посебног значаја; прима обавештења о инцидентима који значајно угрожавају безбедност ИКТ система од посебног значаја и предузима мере у складу са законом, у сарадњи са Министарством унутрашњих послова и тужилаштвом; спроводи међународну сарадњу у области информационе безбедности. Фебруара 2017. године МТТТ је, у складу са Уредбом о безбедности и заштити деце при коришћењу информационо-комуникационих технологија („Службени гласник РС”, број 61/16), основало Национални контакт центар за безбедност деце на интернету 19833[18]. Путем Националног контакт центра врши се саветовање и омогућава се пријем пријава штетног, непримереног и нелегалног садржаја и понашања на интернету, односно угрожености интереса и права деце, телефонским путем и путем електронског обрасца на веб сајту. У складу са чланом 11. став 6. Закона о информационој безбедности, у случају да је инцидент у ИКТ систему од посебног значаја повезан са извршењем кривичних дела која се гоне по службеној дужности, Министарство о томе обавештава надлежно јавно тужилаштво, односно министарство надлежно за унутрашње послове.

Имајући у виду потребу за појачаном контролом робе која се наручује, односно продаје путем интернета, Управа царина, у оквиру Министарства финансија, ради на успостављању услова за формирање јединице Сајбер царина, која би се активно борила против високотехнолошког криминала, са циљем идентификације дела која су у супротности са царинским прописима на интернету. У склопу Плана развоја царинске службе, као и одговарајућег Акционог плана, наводи се обавеза формирања одговарајуће организационе јединице у оквиру Сектора за контролу примене царинских прописа која би се искључиво бавила питањем тзв. „илегалне интернет трговине”, што је и наведено у Плану развоја царинске службе за период 2017–2020. године и Акционог плана за спровођење наведеног Плана развоја. Такође, Управа за спречавање прања новца је орган управе у саставу министарства надлежног за послове финансија. Управа обавља финансијско-информационе послове: прикупља, обрађује, анализира и прослеђује надлежним органима информације, податке и документацију коју прибавља у складу са овим законом и врши друге послове који се односе на спречавање и откривање прања новца и финансирања тероризма у складу са законом. Ако у вези са одређеним трансакцијама или лицима постоје основи сумње да се ради о прању новца, финансирању тероризма или претходном кривичном делу, Управа за спречавање прања новца може започети поступак прикупљања

података, информација и документације у складу са овим законом, као и извршити друге радње и мере из своје надлежности и на основу писмене и образложене иницијативе надлежног суда и тужилаштва, Министарства унутрашњих послова, Безбедносно-информативне агенције, Војнобезбедносне агенције, Пореске управе, Управе царина, Народне банке Србије, Комисије за хартије од вредности, надлежних инспекција и државних органа надлежних за државну ревизију и борбу против корупције. Ако у вези са одређеним трансакцијама постоје основи сумње да се ради о прању новца, финансирању тероризма или претходном кривичном делу, државни органи могу да траже од Управе податке и информације потребне за доказивање тих кривичних дела.

У Министарству просвете, науке и технолошког развоја, последњом систематизацијом радних места формиран је Сектор за дигитализацију у просвети и науци. Овај сектор чине три ниже организационе јединице: Група за е-просвету, Група за е-науку и Група за дигитализацију у образовању (од по три државна службеника). Поред овог сектора, у Секретаријату Министарства постоји Група за одржавање квалитета у интерној мрежи рачунара (три државна службеника), као и радна места за информатичке послове у неким школским управама. Када је у питању спречавање насиља (па и злоупотреба информационо-комуникационих технологија), три особе су задужене за заштиту од насиља у образовно васпитним систему, односно у Министарству и у оквиру тога се такође баве овом облашћу. Подршку пружају и просветни саветници из школских управа.

Безбедносно-информативна агенција (БИА) у складу са Законом о Безбедносно-информативној агенцији обавља послове који се односе на: заштиту безбедности Републике Србије и откривање и спречавање делатности усмерених на подривање или рушење Уставом утврђеног поретка Републике Србије; истраживање, прикупљање, обраду и процену безбедносно-обавештајних података и сазнања од значаја за безбедност Републике Србије и информисање надлежних државних органа о тим подацима. Тероризам и организовани криминал представљају значајну претњу по националну безбедност, посебно ако се као објект или средство извршења јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском смислу. Осим тероризма и организованог криминала, БИА је надлежна за супротстављање и свим другим врстама високотехнолошког криминала, ако су његове последице такве природе да могу дестабилизовати националну безбедност нпр. кроз угрожавање уставног, економског или монетарног система.

Супротстављање наведеним безбедносним претњама врше оперативни радници који су распоређени у организационе јединице за супротстављање свим видовима тероризма, организованог криминала и криминала који угрожава националну безбедност, тако да није могуће одредити број,

структуру и обученост запослених у БИА само за ову област. Потребно је истаћи да Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала није препознао Безбедносно-информативну агенцију као једну од институција која се бави супростављањем овој врсти криминала, иако је за то надлежна по Закону о Безбедносно- информативној агенцији.

Војнобезбедносна агенција у складу са законом обавља послове безбедносне и контраобавештајне заштите Министарства одбране и Војске Србије и у оквиру исте, послове откривања, спречавања и доказивања кривичних дела против безбедности рачунарских података. Војнобезбедносна агенција је овлашћена да спроводи безбедносну заштиту ИКТ система. Поред наведеног, Војнобезбедносна агенција је овлашћена за откривање, праћење и онемогућавање унутрашњег и међународног тероризма, екстремизма и других облика организованог насиља усмерених против Министарства одбране и Војске Србије; односно открива, истражује и прикупља доказе за кривична дела против уставног уређења и безбедности Републике Србије, кривична дела против човечности и других добара заштићених међународним правом, кривична дела организованог криминала, кривично дело прање новца као и кривична дела корупције (злоупотреба службеног положаја, трговина утицајем, примање мита и давање мита) и ако нису резултат деловања организоване криминалне групе, унутар Министарства одбране и Војске Србије. Ове послове, конкретно, врше овлашћена службена лица распоређена у организационим јединицама Војнобезбедносне агенције, према акту о формацији.

Регулаторна агенција за електронске комуникације и поштанске услуге (РАТЕЛ), основана Законом о електронским комуникацијама, је регулаторно тело у области електронских комуникација и поштанских услуга, надлежна је, између осталог, за сарадњу са регулаторним и стручним телима држава чланица Европске уније и других држава ради усаглашавања праксе, примене прописа из области електронских комуникација и подстицања развоја прекограничних електронских комуникационих мрежа и услуга. Такође, учествује у раду међународних организација и институција у области електронских комуникација у својству националног регулаторног тела у области електронских комуникација. Ступањем на снагу и почетком примене Закона о информационој безбедности утврђено је да је РАТЕЛ надлежан за координацију и извршавање послова Националног центра за превенцију безбедносних ризика у ИКТ системима (Национални ЦЕРТ).

Одредбом члана 31. Закона о министарствима прописано је да Завод за интелектуалну својину (ЗИС) обавља стручне послове и послове државне управе који се односе на: патент и мали патент, жиг, дизајн, ознаку географског порекла, топографију интегрисаног кола, ауторско право и сродна права; примену међународних уговора из области заштите интелектуалне својине и представљање и заступање интереса Републике Србије у специјализованим међународним организацијама за заштиту

интелектуалне својине; надзор над радом организација за колективно остваривање ауторског права и сродних права; развој у области заштите интелектуалне својине; информационо-образовне послове у области заштите интелектуалне својине, као и друге послове одређене законом. Предлагање прописа из области заштите и промета интелектуалне својине у делокругу је Министарства просвете, науке и технолошког развоја, као и вршење надзора над радом Завода за интелектуалну својину. Завод сарађује са различитим државним органима надлежним за ефикасно спровођење права интелектуалне својине кроз рад Координационог тела за ефикасну заштиту права интелектуалне својине у Републици Србији, које је основано Одлуком Владе („Службени гласник РС”, број 121/14), као и кроз рад три радне групе које је оформило ово тело. Задатак Координационог тела за ефикасну заштиту права интелектуалне својине у Републици Србији је да, на пољу оперативне заштите права интелектуалне својине, прати и усмерава поједине послове из делокруга више органа државне управе ради обезбеђивања ефикасне заштите права интелектуалне својине.

Улога Привредне коморе Србије (ПКС) у борби против високотехнолошког криминала своди се на едукацију привредника, као и на повремено прикупљање информација о инцидентима, као и њихова анализа и утицај на пословање. Разматра се увођење тима који би се перманентно бавио овом проблематиком.

Удружење банака Србије (УБС) окупља све банке које послују на територији Републике Србије, банке у Удружењу формирају стучне одборе преко којих се баве различитим областима из свог пословања. Одбор за безбедност који функционише при Удружењу банка Србије окупља представнике већине банка који се баве пословима безбедности (информационе, физичко техничке, превенцијом превара и др.). Међусобном сарадњом као и успостављањем сарадње са државним органима из области високотехнолошког криминала Одбор делује превентивно и реактивно у борби против високотехнолошког криминала.

_____

18 http://www.pametnoibezbedno.gov.rs/rs-lat/kontakt-centar

4.2. Сарадња државних органа у оквиру борбе против високотехнолошког криминала

Сходно Законику о кривичном поступку, сви органи који учествују у предистражном поступку дужни су да о свакој радњи предузетој у циљу откривања кривичног дела или проналажења осумњиченог обавесте надлежног јавног тужиоца. Полиција и други државни органи надлежни за откривање кривичних дела дужни су да поступе по сваком захтеву надлежног јавног тужиоца.

У вези предузимања кривичног гоњења учинилаца кривичних дела високотехнолошког криминала, Посебно тужилаштво за високотехнолошки

криминал највећи део сарадње остварује са Министарством унутрашњих послова, Службом за борбу против организованог криминала, Одељењем за сузбијање високотехнолошког криминала, са Службом за специјалне истражне методе која се огледа у проналажењу доказа везаних за извршење кривичних дела високотехнолошког криминала, а изузетна сарадња је остварена и са Одељењем за јавни ред и мир, Полицијске управе за град Београд. Републичко јавно тужилаштво и Посебно тужилаштво за високотехнолошки криминал остварују сарадњу са Министарством трговине, туризма и телекомуникација у вези са применом Уредбе о безбедности и заштити деце при коришћењу информационо-комуникационих технологија која је донета у јуну 2016. године и Националним контакт центром за безбедност деце на интернету.

Одељење за сузбијање високотехнолошког криминала значајан део својих активности спроводи у сарадњи са Тужилаштвом за организовани криминал. У периоду од 2008. године до данас, ово одељење је спровело укупно осам самосталних оперативних обрада. У оквиру једне од оперативних обрада, по први пут у Републици Србији је потписан Уговор о оснивању заједничког истражног тима између Републике Србије и Краљевине Холандије. Одељење је у истом периоду поступало по већем броју замолница за међународну правну помоћ Тужилаштва за организовани криминал и то у међународним операцијама „Rico" и „Bug Byte" са америчким ФБИ, по замолници ФБИ у вези међународног кријумчарења оружја, те у операцији „Атлантис" (нелегално
„on-line" клађење) код које је предистражни поступак започело Тужилаштво за организовани криминал, али је судски поступак вођен пред Вишим судом у Београду, а оптужницу је заступало Посебно тужилаштво за високотехнолошки криминал.

Поред ових самосталних активности, Одељење је учествовало у већем броју оперативних обрада Службе за борбу против организованог криминала, пружајући оперативну и техничку подршку другим одељењима. Спроведено је преко 25 оперативних обрада, међу којима су и неке од највећих оперативних обрада Службе.

Ради ефикасне координације и сарадње државних органа у области информационе безбедности, Влада је образовала Тело за координацију послова информационе безбедности, којим председава представник Министарства трговине, туризма и телекомуникација, а у његовом раду учествују представници министарстава надлежних за послове одбране, унутрашњих послова, спољних послова, правде, представници служби безбедности, Канцеларије Савета за националну безбедност и заштиту тајних података, Генералног секретаријата Владе, Канцеларије за информационе технологије и електронску управу и Националног ЦЕРТ.

Сходно Одлуци о образовању Тела за координацију послова информационе безбедности („Службени гласник РС", бр. 24/16, 53/17, 79/17 и 112/17)

задатак Тела је да остварује сарадњу између органа и усклађује обављање послова у функцији унапређења информационе безбедности, иницира и прати превентивне и друге активности у области информационе безбедности, предлаже мере за унапређење информационе безбедности у Републици Србији, даје сугестије и предлоге који се односе на припрему стратешких докумената, подзаконских аката и политика информационе безбедности у Републици Србији и утврђује међусобну сарадњу у случају инцидената који могу да имају знатан утицај на нарушавање информационе безбедности у Републици Србији.

У области безбедности деце на интернету, ово министарство сарађује са органима надлежним за борбу против високотехнолошког криминала. Наиме, Национални контакт центар за безбедност деце на интернету 19833 (веб сајт: www.pametnoibezbedno.gov.rs) врши саветовање и омогућава пријем пријава штетног, непримереног и нелегалног садржаја и понашања на интернету, односно угрожености интереса и права деце, телефонским путем и путем електронског обрасца на веб сајту. У случају да наводи из пријаве указују на постојање кривичног дела, Министарство прослеђује пријаву ради даљег поступања Републичком јавном тужилаштву и, ради информисања, Министарству унутрашњих послова.

На предлог Министарства трговине, туризма и телекомуникација Влада је донела Одлуку о образовању Координационог тела у области безбедности и заштите деце при коришћењу информационо-комуникационих технологија („Службени гласник РС”, број 9/18) у чијем саставу су представници Министарства трговине, туризма и телекомуникација, Министарства за рад, запошљавање, борачка и социјална питања, Министарства здравља, Министарства унутрашњих послова, Министарства културе и информисања и Министарства просвете, науке и технолошког развоја. Задатак Координационог тела је да остварује сарадњу између органа и усклађује обављање послова у функцији унапређења безбедности и заштите деце при коришћењу информационо-комуникационих технологија, иницира и прати превентивне и друге активности у области безбедности и заштите деце на интернету, предлаже мере за унапређење безбедности и заштити деце на интернету и утврђује међусобну сарадњу.

Управа царина у овој области сарађује са Посебним тужилаштвом у погледу размене података. Такође, развијена је сарадња са царинском администрацијом Француске и Аустрије, кроз чије је обуке на тему „Cyber customs” у два наврата већ прошао део царинских службеника. Поред тога, Управа царина свакодневно размењује податке са другим царинским администрацијама, на основу потписаних међународних споразума.

У оквиру потписаног Протокола између Министарства унутрашњих послова и Министарства просвете, науке и технолошког развоја реализује се пројекат „Основи безбедности деце”. У оквиру овог пројекта обучени полицијски службеници реализују наставу у свим четвртим и шестим разредима

основних школа, а између осталог посебно се обрађују теме Безбедност деце на интернету. Одређене теме из области високотехнолошког криминала прилагођене су узрасту деце, а деца се едукују у областима коришћења интернета у којима су најрањивија.

Имајући у виду надлежност Безбедносно-информативна агенција у овој области, остварује сарадњу са Посебним одељењем за борбу против високотехнолошког криминала, Вишег јавног тужилаштва у Београду и Службом за борбу против организованог криминала – Одељењем за сузбијање високотехнолошког криминала.

Војнобезбедносна агенција у остваривању својих надлежности сарађује са свим релевантним државним органима. Ради се о законској обавези, коју установљава одредба члана 3. став 4. Закона о Војнобезбедносној агенцији и Војнообавештајној агенцији према којој Војнобезбедносна агенција сарађује и размењује податке са надлежним органима, организацијама, службама и телима Републике Србије, у складу са Уставом, законом, другим прописима и општим актима, односно утврђеном безбедносно-обавештајном политиком Републике Србије.

Одбор за безбедност који функционише при Удружењу банака Србије сарађује са Народном банком Србије као регулатором. Финансијске институције, које су ИКТ системи од посебног значаја у складу са Законом о информационој безбедности, у обавези су да о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности обавесте Народну банку Србије. Поред редовних канала комуникације ка државним органима, Одбор је успоставио и ради на унапређењу сарадње са Одељењем за сузбијање високотехнолошког криминала и Посебним тужилаштвом за високотехнолошки криминал у циљу ефикасне и правовремене реакције на различите облике високотехнолошког криминала.

4.3. Сарадња са субјектима цивилног друштва, стручном јавношћу, медијима и привредом

Облици сарадње са субјектима цивилног друштва и привредом су на задовољавајућем нивоу и остварују се кроз потписивање одговарајућих уговора и протокола о сарадњи између заинтересованих страна, организовањем јавних расправа о нацртима прописа, као и одржавањем конференција, семинара, обука, радионица.

Посебно тужилаштво приликом сузбијања кривичних дела високотехнолошког криминала има добру сарадњу са цивилним друштвом и привредом, а поготово са банкарским сектором, интернет сервис провајдерима, мобилним операторима, Привредном комором Србије и Београда, медијским кућама, удружењима која заступају носиоце ауторских права, Националним ЦЕРТ, а која се огледа у размени информација, учествовањем у радним групама и округлим столовима и другим облицима

сарадње, а све у циљу успешне борбе против високотехнолошког криминала.

Потребно је истаћи и да је Републичко јавно тужилаштво закључило 2013. године Меморандум о сарадњи са Фондом Б92 у циљу реализације пројекта „Кликни безбедно" Центар за безбедни интернет Србија на сузбијању и решавању проблема незаконитог, непримереног и штетног садржаја и непримереног понашања на интернету, као и на ширењу информација о начинима безбедног коришћења интернета.

У оквиру пројекта формирана је online платформа под називом Нет партола у циљу анонимног пријављивања незаконитог садржаја на интернету, посебно искоришћавања малолетних лица у порнографске сврхе, као и извршење других кривичних дела путем интернета (нпр. малтретирање у виртуелном свету тзв. cyberbullying). Нет патрола члан је међународне организације INHOPE – Internation Association of Internet Hotlines, која координише и помаже рад мреже оваквих сервиса за пријаву нелегалног садржаја на интернету широм света.

Поред наведене сарадње, Републичко јавно тужилаштво и Посебно тужилаштво за високотехнолошки криминал успоставили су сарадњу са међународном организацијом цивилног друштва „Save the children", у оквиру програма Правосудне академије за израду плана и програма обуке за судије и јавне тужиоце у области високотехнолошког криминала и заштите малолетних лица на интернету. У складу са успостављеном сарадњом, од јануара 2017. године почеле су основне и напредне обуке на тему високотехнолошког криминала и безбедности деце на Интернету. У оквиру пројекта израђен је Приручник за судије и јавне тужиоце на тему заштите деце од насиља на интернету и разматра се потписивање споразума о сарадњи са организацијом „Save the children".

Организација „Save the children" је у сарадњи са Министарством трговине, туризма и телекомуникација израдила Мапу пута превенције онлајн и других облика насиља над децом на интернету у Републици Србији[19], која пружа приказ добрих пракси и примера других земаља. Наведени документ такође даје смернице на путу којим би Република Србија требало да се креће у односу на сопствене капацитете у овом пољу.

Такође, 26. децембра 2016. године Републичко јавно тужилаштво, Министарство унутрашњих послова, Удружење новинара Србије, Независно удружење новинара Србије, Удружење новинара Војводине, Независно друштво новинара Војводине, Асоцијација независних електронских медија, Асоцијација медија и Асоцијација онлајн медија закључили су Споразум о сарадњи и мерама за подизање нивоа безбедности новинара. Овим споразумом предвиђене су обуке новинара и власника медија о основама информационе безбедности информативних интернет портала, укључујући и обуку у погледу примене основних мера заштите од напада коришћењем информационих технологија.

Наступи у медијима кроз проактиван приступ су веома значајни за превентивне активности за све субјекте на пољу борбе против високотехнолошког криминала. Наступи у медијима упознају грађане и подижу свест о опасностима које доноси континуирани развој дигиталног друштва, те се на тај начин грађани едукују како би самостално могли да идентификују опасности и превентивно делују и тиме не постану жртве неког кривичног дела путем интернета, односно минимализују штетне последице.

Удружење банака Србије информише грађане о безбедносним ризицима посредством јавног веб сајта Удружења и активностима које организује у самом Удружењу (Центар за банкарску обуку, рад Одбора за безбедност и др.). Банке чланице информишу банкарске клијенте различитим каналима информисања.

Министарство трговине, туризма и телекомуникација спроводи информисање деце, родитеља и наставника о опасностима на интернету и мерама превенције путем веб сајта „Паметно и безбедно" (www.pametnoibezbedno.gov.rs), као и путем телевизијских видео програма. Наиме, Министарство трговине, туризма и телекомуникација у оквиру наведеног пројекта спроводи на годишњем нивоу кампању „ИТ караван". Први „ИТ караван" спроведен је од 20. априла до 3. јуна 2016. године. Школским презентацијама присуствовало је 5.000 ученика старијих разреда основних школа у 15 школа, док је на градским трговима промоцију овог пројекта видело више хиљада грађана. У 2017. години у оквиру „ИТ каравана" презентацијама о заштити од дигиталног насиља и других облика злоупотребе деце на Интернету присуствовало је више од 5.500 ученика и око 90 наставника из 17 основних школа из Србије. И у 2018. години, трећу годину за редом, спроведена је кампања „ИТ караван" за ученике основних школа у Србији, њихове родитеље и наставнике, са циљем подстицања паметног и безбедног коришћења нових технологија. Главни програм који чине едукативна презентација о безбедности деце на интернету и радионице за ученике и родитеље, представљен је за укупно 26 школа, у регионалним центрима у Републици Србији. Програм из Ниша и Новог Пазара пратило је још око 800 школа путем директног интернет преноса, а на мапи пута ИТ каравана 03 били су и Београд, Суботица и Нови Сад. У оквиру кампање реализоване су и отворене промоције за грађане, као и додатне радионице за родитеље у још шест градова: Сечњу, Зрењанину, Лесковцу, Чачку, Краљеву и Ужицу. Стални партнери Министарства у реализацији ове кампање су и Министарство просвете, науке и технолошког развоја и Компанија Мајкрософт, а у прве две године један од партнера је било и Министарство унутрашњих послова, док су се у 2018. години кампањи придружили Национална асоцијација родитеља и наставника Србије и Фондација Петља.

Превентивне активности Министарства финансија, Управе за спречавање прања новца огледају се кроз континуиране обуке обвезника и упознавање

истих са новим трендовима и типологијама, у вези са прањем новца и финансирањем тероризма. Успостављена је одговарајућа сарадња са релевантим државним и међународним институцијама кроз велики број стручних скупова, семинара, обука, као и трибина у смислу заједничке едукације свих заинтересованих субјеката у циљу подизања свести о значају сузбијања ове врсте криминалитета.

На Криминалистичко-полицијском универзитету у Земуну, за студенте четврте године на смеру криминалистике у оквиру предмета Економски криминал, предавање на тему „Систем заштите интелектуалне својине", већ трећу годину заредом одржавају представници Завода за интелектуалну својину. У 2017. години, за представнике Управе царина одржана је радионица о претраживању база података индустријске својине, пре свега жигова и индустријског дизајна.

_____

19 https://nwb.savethechildren.net/sites/nwb.savethechildren.net/files/library/Mapa%20puta-Srbija.pdf.

4.4. Међународна сарадња у области високотехнолошког криминала

Међународна сарадња се спроводи кроз различите видове: међународне сајбер вежбе, drill, радионице са циљем повећања разумевања и изградње капацитета са тежиштем на транснационалним сајбер безбедоносним изазовима и претњама, колективном приступу њиховом решавању како би се побољшала регионална и глобална размена информација за развој сајбер стратегија и политика сајбер безбедности у циљу брзог одговора на сајбер претње.

Посебно тужилаштво за високотехнолошки криминал од 2010. године у оквиру Европске уније, Савета Европе и ОЕБС и других међународних организација учествује у пројектима који имају за циљ олакшавање међународне сарадње, њено убрзавање и правовремено реаговање приликом извршења кривичних дела високотехнолошког криминала. Поред тога, Посебни тужилац за високотехнолошки криминал одређен је за контакт тачку мреже 24/7 прописане Будимпештанском конвенцијом. На тај начин, успостављена је директна сарадња са осталим контакт тачкама из земаља потписница Конвенције, у циљу ефикаснијег поступања у предметима са елементом иностраности.

Одељење за сузбијање високотехнолошког криминала је једна од најактивнијих организационих јединица Министарства унутрашњих послова у области међународне сарадње. Сарадња се остварује на дневној бази кроз све стандардне канале међународне полицијске сарадње, посредством Интерпола и Европола, преко официра за везу деташираних у амбасадама у Београду (пре свега САД и Велике Британије), посредством регионалних организација (нпр. SECI Center, SELEC,), али врло често и у директној

полицијској сарадњи у заједничким међународним акцијама. У Одељењу је успостављена међународна контактна тачка 24/7 за високотехнолошки криминал у оквиру Савета Европе, као и контактне тачке у оквиру Еуропол и то „Twins" (дечија порнографија) и „Cyborg" (сајбер криминал).

Такође, 2016. године полицијски службеници Службе за борбу против организованог криминала спроводећи вишегодишњу међународну полицијску акцију „BUGBYTE" на сузбијању кривичних дела против сајбер криминала, фалсификовања и злоупотреба платних картица коју спроводи Федерални истражни биро (ФБИ) из САД-а, сарађивали су са полицијским службама из: Републике Србије, Републике Српске, Канаде, Аустралије, Републике Индије, Савезне Републике Бразила, Државе Израела, Уједињеног Краљевства Велике Британије и Северне Ирске, Румуније, Републике Хрватске, Републике Македоније, Краљевине Данске, Краљевине Шведске, Републике Летонске Републике, Републике Костарике, Кипарске Републике, Републике Колумбије и Савезне Републике Нигерије. Поред тога, 2016. године, одобрено је повезивање Министарства унутрашњих послова на Интерполову базу „ICSE" (база фото и видео материјала сексуалне експлоатације деце).

У просторијама Одељења за сузбијање високотехнолошког криминала инсталирана је комуникациона опрема која је донирана од стране Генералног Секретаријата Интерпола, те је приступ бази података „ICSE" омогућен. Када говоримо о резултатима, ово је база која служи за идентификацију жртава као и информацији са којих места се дистрибуирају илегални снимци. У нашој земљи ово још није тип криминала који је у озбиљној мери заживео по питању производње илегалних снимака и продаје те се код нас неће проналазити жртве путем ове базе у тој мери као што је то пример у неким другим државама. Допринос ће углавном бити што ће остале државе које имају приступ овој бази евентуално добити материјал са новим жртвама који је пронађен током претреса у Републици Србији. Предстоји реализација обуке намењена коришћењу ове базе података коју ће изводити инструктори из Генералног Секретаријата Интерпола.

Министарство финансија, Управа за спречавање прања новца је члан Егмонт групе, групе која окупља финансијско-обавештајне службе из 156 држава. То јој даје могућност да веома брзо дође до веома битних финансијско-обавештајних података од других држава, ако у вези са одређеном трансакцијом или лицем постоје основи сумње да се ради о прању новца или финансирању тероризма. Управа активно учествује у раду Комитета Манивал, стручног комитета Савета Европе који ради по систему узајамних процена држава чланица. Још један веома значајан аспект међународне сарадње Управе за спречавање прања новца је могућност за закључивање споразума о сарадњи са страним партнерима. Управа за спречавање прања новца је до сада потписала споразуме о сарадњи са 44 државе.

Управа царина у складу са постојећим законским овлашћењима, Протоколом 6 Споразума о стабилизацији и придруживању, у међусобној административној сарадњи у царинским питањима између Републике Србије и ЕУ и постојећим потписаним билатералним споразумима, размењује податке са другим царинским администрацијама.

Безбедносно-информативна агенција остварује регионалну и ширу међународну сарадњу, првенствено са другим сигурносним или сигурносно-обавештајним службама и агенцијама.

Војнобезбедносна агенција остварује међународну сарадњу у складу са одредбом члана 36. став 1. Закона о Војнобезбедносној агенцији и Војнообавештајној агенцији према којој, Војнобезбедносна агенција, сходно утврђеној безбедносно-обавештајној политици Републике Србије, размењује податке са органима и службама безбедности страних држава и међународних организација, у складу са Уставом, законом, другим прописима и општим актима и потврђеним међународним уговорима.

Завод за интелектуалну својину има развијену сарадњу са Светском организацијом за интелектуалну својину (WIPO), Европском патентном организацијом (ЕПО) и Заводом за интелектуалну својину Европске Уније (EUIPO). Представници Завода за интелектуалну својину присуствују састанцима Саветодавног коминтета WIPO за примену права интелектуалне својине који пружа техничку помоћ и координира у области примене права интелектуалне својине. На овим састанцима се редовно разматра и „онлајн" повреда права интелектуалне својине. *EUIPO* организује семинаре за представнике органа надлежних за примену права интелектуалне својине (судије, тужиоце, царинске службенике и представнике националних завода за интелектуалну својину). Теме које се обрађују у оквиру ових обука обухватају понекад и питања повреде права интелектуалне својине посматране са аспекта кривичног права. Представници Завода за интелектуалну својину су до сада два пута посетили и Опсерваторију *EUIPO* која прати повреде права интелектуалне својине и која пружа потребно знање и информације својим члановима. Сарадња са Европском организацијом за патенте одвија се кроз активности уговорене Билатералним планом сарадње за период 2016. до 2018. године, које се односе на обуку стручњака, сарадњу у развоју усаглашених европских информационо-технолошких сервиса и алата и сарадњу у подизању свести о значају заштите интелектуалне својине. Међународни уговори из области интелектуалне својине које је ратификовала Република Србија, а који су значајни за уређење дигиталног окружење су WIPO Уговор о ауторском праву и WIPO Уговор о интерпретацијама и фонограмима, који су закључени 20. децембра 1996. године у Женеви („Службени лист СРЈ – Међународни уговори", број 13/02). Ови уговори су познати под називом „Интернет уговори" и садрже норме које имају за циљ спречавање неовлашћеног приступа креативним делима и спречавање њиховог коришћења на интернету или другој дигиталној мрежи.

5. КРАТАК ПРЕГЛЕД ТРЕНДОВА У ОБЛАСТИ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

5.1. Општи показатељи

Посебно је потребно нагласити да је број корисника интернета како на глобалном нивоу, тако и у Републици Србији у константном порасту. Јавно доступни статистички подаци говоре о томе да је у 2007. години регистровано да је Интернет користило укупно 1.365.000.000 корисника. Дана 31. марта 2017. године укупан број корисника у целом свету износио је 3.731.973.423. У Републици Србији је у току 2007. године регистровано 1.270.000 корисника. Дана 31. марта 2017. године број интернет корисника у нашој држави износио је укупно 4.705.141. Од 2007. године до 31. марта 2017. године на глобалном нивоу број корисника се повећао за укупно 273,40%. У Републици Србији се број корисника у наведеном временском периоду повећао за 370%.

Истраживање Републичког завода за статистику о употреби информационо-комуникационих технологија у домаћинствима које је спроведено на узорку од 2.800 домаћинстава у Републици Србији говори о томе да 68,1% домаћинстава у Републици Србији поседује рачунар, док је 2007. године 34% домаћинстава имало рачунар. У истом истраживању које је спроведено утврђено је да 68,0% домаћинстава поседује интернет прикључак. Број интернет прикључака у домаћинствима 2007. године износио је укупно 26,3%. У 2017. години 61,9% домаћинстава имало је широкопојасну интернет конекцију. Тај број је 2007. године износио 7,3%. У 2017. години у Републици Србији у четвртом кварталу било је 1,49 милиона активних претплатника широкопојасног приступа Интернету.

Веома је интересантан податак да су мобилни телефони у Републици Србији 2017. године били као уређаји заступљени са 90,5%. Заступљеност употребе 3G мреже (интернет преко мобилне телефоније) је код 53,6% корисника. Млади узраста од 16 до 24 године старости користе мобилне телефоне за приступ Интернету у проценту који се креће и до 92,6%. Просечно коришћење паметних телефона износи пет сати дневно у Републици Србији, наспрам просечних 3,3 сата у Западној Европи.

Истраживања показују и да се 62% старијих основаца и 84% средњошколаца бар једном током годину дана изложило неком ризику на Интернету.

Спроведена истраживања Републичког завода за статистику указују и на то да 99,7% анкетираник предузећа (репрезентативни узорак је био 1655 предузећа) користи рачунаре, као и да 99,7% тих предузећа има интернет конекцију.

Интересантно је да је од 2007. године приступ широкопојасном интернету имало 55% предузећа, док је тај број 2017. године износио чак 98,6%, дакле број се готово удвостручио.

Социјалне мреже су, такође, јако заступљене. Најпопуларнији је „Facebook". У јуну 2016. године, у Републици Србији је било укупно 4.758.861. корисника Интернета (према подацима Internet live stats; у 2017. години према подацима Hootsuite – We are social, је 5,74 милиона) од којих је укупно 3.500.000 користило „Facebook". И на глобалном нивоу број корисника социјалне мреже Фејсбук је у константном порасту од 2008. године. Ова друштвена мрежа је једна од најомиљенијих и за њу је дат приказ имајући у виду да крајем 2017. године има већи број корисника (преко 2,1 милијарде) него WhatsUp (900.000.000), Twitter (328.000.000) и Instagram (400.000.000) заједно.

5.2. Статистика и базе података

Посебно тужилаштво води евиденцију свих предмета и поступања по истим, кроз јединствени информациони систем јавних тужилаштава, а база података се ажурира на дневном нивоу.

У Министарству унутрашњих послова се подаци о кривичним делима, укључујући и кривична дела високотехнолошког криминала, евидентирају на месечном нивоу у програмском систему под називом „Кривична дела и учиниоци". Ради се о јединственој електронској евиденцији података о кривичним делима која се гоне по службеној дужности. Ова обимна база података обухвата, поред наведеног и податке о учиниоцима кривичних дела и оштећеним лицима, као и о њиховој старосној, полној и другој структури, затим о начину извршења (време, место, средство извршења кривичних дела), расветљеним и нерасветљеним кривичним делима, предметима кривичних дела, примењеним мерама према учиниоцима итд. Подаци се у овој бази евидентирају на основу поднетих кривичних пријава од стране подносиоца, односно полицијских службеника организационих јединица надлежних за послове сузбијања криминала. Подаци се уносе на основу прописане методологије и редовно се ажурирају.

Министарство финансија, Управа за спречавање прања новца располаже базама података о готовинским и сумњивим трансакцијама које пријављују обвезници по Закону о спречавању прања новца и финансирања тероризма. Наведене базе се ажурирају на дневном нивоу. Управа царина користи: Информациони систем царинске службе, Обавештајну база података, право приступа Пореској бази података (ЈРПО). Поред наведених, од почетка 2015. године у функционалној употреби је и Нови компјутеризовани транзинти систем (НЦТС). Такође, треба поменути и базу података Светске царинске организације (CEN) у коју се уносе искључиво подаци (неноминални) о царинским прекршајима. Подаци у свим базама ажурирају се на дневном нивоу. Одељење за обавештајне послове води статистику на: дневном, недељном, месечном, кварталном и годишњем нивоу. Подаци које Одељење за обавештајне послове редовно прикупља су: наркотици, цигарете, дуван лекови, оружје и муниција (све врсте и количине), злато, нафтни деривати (у количини од најмање 100 литара), девизни прекршаји (износи од 10.000

EUR/USD/CHF па навише), прекршаји против животне средине, културна добра, илегални мигранти, сва друга царинска роба вредности преко 3.000 евра.

Министарство трговине, туризма и телекомуникација води Регистар пружалаца квалификованих услуга од поверења и Регистар квалификованих средстава за креирање електронских потписа и електронских печата.

Регулаторна агенција за електронске комуникације и поштанске услуге води евиденцију о посебним ЦЕРТ, која се ажурира редовно.

На сајту Завода за интелектуалну својину приступачне су следеће националне базе података: База података жигова и индустријског дизајна и База података за патенте MIMOSA RS. Такође, налази се линк ка некомерцијалној светској бази података патентне документације – Espacenet, која је доступна свима преко интернета и која садржи податке од преко 70 милиона објављених патентних пријава и одобрених патената из преко 90 различитих земаља (и наших) и региона из целог света, од 1836. године до данас.

Привредна комора Србије поседује Базу података о спољнотрговинској робној размени Србије и спољнотрговинској робној размени земаља (ажурирање се врши на месечнм нивоу) и Базу COMTRADE (преузимање преко веб сервиса), где се ажурирање врши на годишњем нивоу.

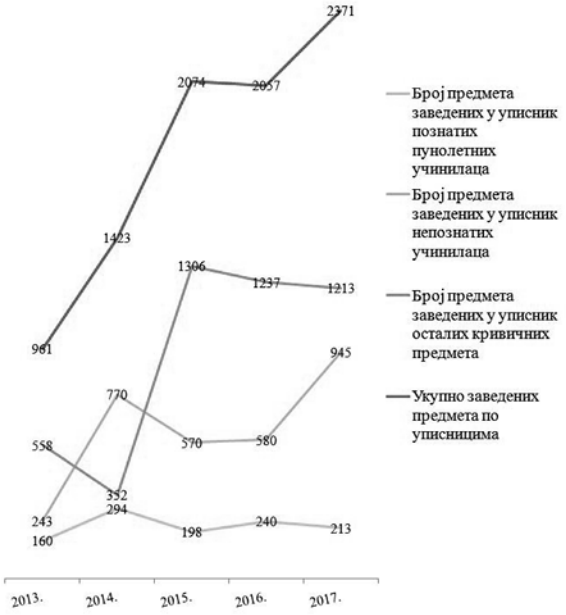
5.3. Статистички трендови у области високотехнолошког криминала[20]

Према подацима Посебног одељења за борбу против високотехнолошког криминала у протеклих пет година на територији Републике Србије (период 2013–2017. година) стопа криминала је у порасту.

Преглед броја предмета Посебног тужилаштва за високотехнолошки криминал закључно са 31. децембром 2017. године.

	Број предмета заведених у уписник познатих пунолетних учинилаца	**Број предмета заведених у уписник непознатих учинилаца**	**Број предмета заведених у уписник осталих кривичних предмета**	**Укупно заведених предмета по уписницима**	**Проценат повећања/смањења броја предмета у односу на претходну годину**
2006.	19	0	0	19	

2007.	75	11	68	154	+710.53%
2008.	110	14	60	184	+19.48%
2009.	91	42	114	247	+34.24%
2010.	116	13	443	572	+131.58%
2011.	130	28	502	660	+15.38%
2012.	114	65	609	788	+19.39%
2013.	160	243	558	961	+21.95%
2014.	294	770	352	1423	+48,07%
2015.	198	570	1306	2074	+45,74%
2016.	240	580	1237	2057	-0,82%
2017.	213	945	1213	2371	+15,26%



У периоду од 1. јануара 2013. године до 31. децембра 2017. године, Посебном тужилаштву за високотехнолошки криминал поднете су кривичне пријаве против укупно 1.318 познатих пунолетних лица, док је оптужни акт поднет против укупно 280 познатих пунолетних лица.

Министарство унутрашњих послова је у периоду од 2013. до 2017. године, поднео кривичне пријаве због извршења укупно 3.824 кривичних дела високотехнолошког криминала. У питању су следећа кривична дела:

– Кривична дела против безбедности рачунарских података – укупно 91 кривично дело и то: оштећење рачунарских података и програма из члана 298. Кривичног законика (5 кривичних дела или 5,5% од укупног броја), рачунарска саботажа из члана 299. Кривичног законика (7 или 7,7%), прављење и уношење рачунарских вируса из члана 300. Кривичног законика (4 или 4,4%), рачунарска превара из члана 301. Кривичног законика (40 или 43,9%), неовлашћен приступ заштићеном рачунару, рачунарској мрежи и електронској обради података из члана 302. Кривичног законика (34 или 37,4%) и спречавање и ограничавање приступа јавној рачунарској мрежи из члана 303. Кривичног законика (1 или 1,1%).

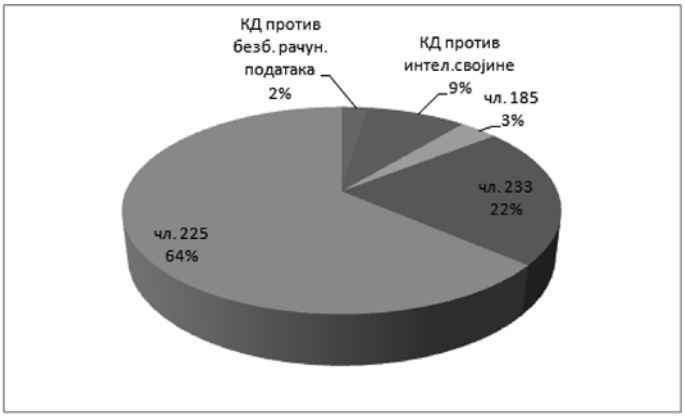
– Кривична дела против интелектуалне својине – укупно 328 кривичних дела и то: повреда моралних права аутора и интерпретатора из члана 198. Кривичног законика (1 или 0,3%), неовлашћено искоришћавање ауторског дела или предмета сродног права из члана 199. Кривичног законика (316 или 96,3%), повреда проналазачевог права из члана 201. Кривичног законика (1 или 0,3%) и неовлашћено коришћење туђег дизајна из члана 202. Кривичног законика (10 или 3,1%).

– Остала кривична дела – укупно 3.405 кривичних дела и то: приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију из члана 185. став 4. Кривичног законика (128 или 3,8%), искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу из члана 185б Кривичног законика (14 или 0,4%), фалсификовање и злоупотреба платних картица из члана 225. Кривичног законика (2.412 или 70,8%), прављење, набављање и давање другом средстава за фалсификовање из члана 227. став 2. Кривичног законика (18 или 0,5), неовлашћена употреба туђег пословног имена и друге посебне ознаке робе или услуга из члана 233. Кривичног законика (827 или 24,3%), одавање пословне тајне из члана 240. Кривичног законика (6 или 0,2%).

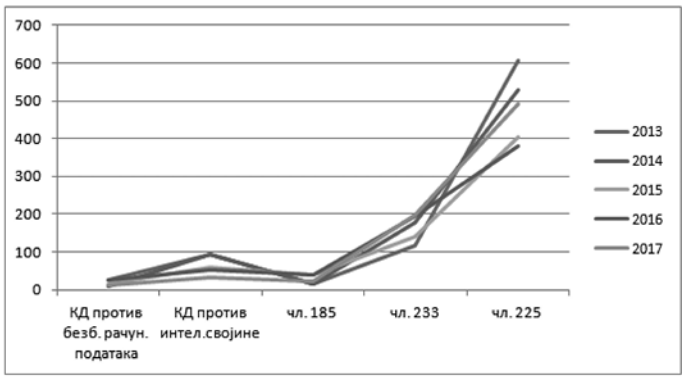
_____

20 Стратешка процена јавне безбедности, МУП.

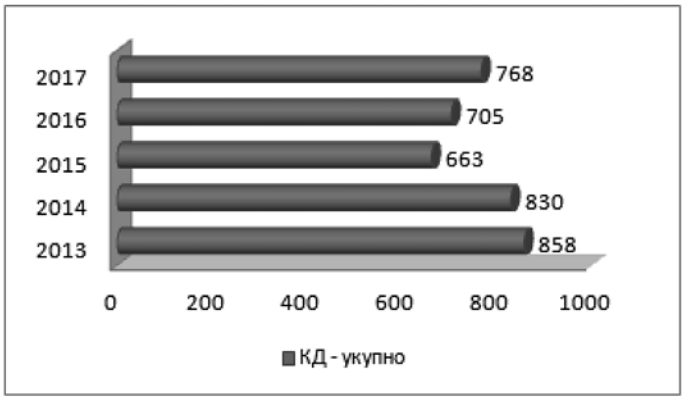
Структура извршених кривичних дела у периоду од 2013. до 2017. године



Тренд извршења кривичних дела у периоду од 2013. до 2017. године

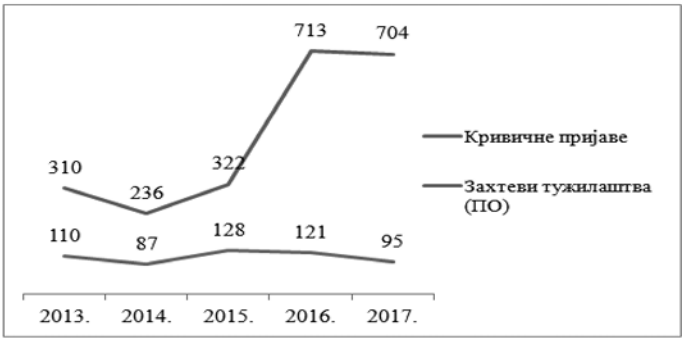


Укупан број извршених кривичних дела високотехнолошког криминала у периоду од 2013. до 2017. године



Одељење за сузбијање високотехнолошког криминала је у периоду од 2015. до 2017. године, поднело кривичне пријаве против 379 осумњичених лица за 496 кривичних дела. Лишена су слободе 164 лица, извршена су 683 претреса стамбених и других просторија и привремено је одузето 6.058 предмета.

Преглед броја предмета Одељења за сузбијање високотехнолошког криминала у периоду од 2008. до 2017. године



Према подацима Министарства трговине, туризма и телекомуникација у оквиру којег функционише Национални контакт центар за безбедност деце на интернету, од фебруара 2017. године закључно са 15. мајом 2018. године, укупна регистрована комуникација која је остварена путем телефонских позива, електронске поште, пријава путем сајта и друштвених мрежа, износи 4.750. Ради унапређења сарадње и размене идеја, оператери/едукатори Националног контакт центра одржали су презентације на тему безбедности деце на интернету и то: за 150 запослених у домовима здравља (директорима, педијатрима школских диспанзера и психолозима) и за 4.730 ученика и око 2.500 родитеља у 73 основне школе.

5.4. Појавни облици високотехнолошког криминала

Министарство унутрашњих послова је 2017. године у складу са чланом 24. Закона о полицији, израдило прву Стратешку процену јавне безбедности и Стратешки план полиције. Након обимне стратешке анализе стања у области безбедности, дефинисано је осам безбедносних приоритета у раду полиције, од којих се један односи на борбу против високотехнолошког криминала „Борба против злоупотреба информационо-комуникационих технологија на територији Републике Србије". Анализом је утврђено да се кривична дела у којима се злоупотребљавају информационо-комуникационе технологије повећавају, као последица брзог развоја ИКТ и то она која се односе на безбедност рачунарских података, сексуалну злоупотребу малолетних лица и деце у порнографске сврхе на Интернету, преваре путем Интернета, неовлашћено коришћење ауторског и сродног права, угрожавање сигурности, тероризам и насилни екстремизам који води ка тероризму.

Преваре путем Интернета најчешће се дешавају на различитим аукцијским сајтовима као и сајтовима на којима се врши оглашавање. Извршиоци кривичних дела објављују лажне електронске огласе на којима оглашавају продају различите робе (аутомобили, пољопривредне машине, мобилни телефони, сатови и др.). Када жртва наручи робу и уплати одређени новчани износ на име куповине, извршилац кривичног дела који је објавио потпуно лажан оглас, задржава новац код себе и одржава жртву у заблуди да ће добити робу.

Јављају се и преваре са „емотивним односима" на Интернету где се жртве од стране извршилаца кривичних дела контактирају и започиње комуникација

и развијање емоционалног и партнерског односа. Након што се жртве доведу у заблуду нуди им се нпр. склапање брака. За наведено, жртве требају да уплате одређени новчани износ за административне трошкове (таксе, судски и адвокатски трошкови и слично). Слична је ситуација и у кривичним делима, где се за одређени износ новца који се креће од 10% до 20%, жртвама нуди да на име трансфера новца на свој рачун уплате одређене таксе на напред описани начин. Жртве се доводе најчешће у заблуду да су новац наследили од далеких рођака који су преминули у иностранству. Врло често долази и до комбинације прва два случаја када се прво жртва емоционално доводи у везу са лажним партнером, а затим се тражи од ње да отвори рачун и да за извршиоца који стоји иза „емотивног односа" подигне новац који наводно у држави где се партнер налази није могуће подићи из одређених разлога. Уплате се најчешће врше преко Western Union-а i MoneyGram-а. Дестинације где се новац упућује најчешће су државе са подручја Африке, али и Велике Британије, Шпаније и др.

На територији наше државе све су чешћа и кривична дела на штету правних лица која се називају „Bussiness Compromised Email", и „Ransomware". Појавиле су се и „CEO Frauds" преваре. Наведена превара се врши путем електронских порука у којима се извршиоци представљају лажно као надређени (шефови, руководиоци или директори) и доводе у заблуду жртве (запослена лица) у привредним субјектима да изврше уплату на њихов рачун. Број оштећених привредних субјеката преваром типа „Bussiness Compromised Email" све је већи. Злоупотребом комуникације извршиоци кривичних дела лажно се представљају у име стране компаније са којом правни субјекат из наше земље већ има пословну сарадњу и након уговореног посла у преварним порукама одмах након легитимно прослеђене поруке од стране легитимне компаније у којој се налазе инструкције за уплату, шаљу нове поруке са измењеним диспозицијама за плаћање (ИБАН број). Имајући у виду да се ради о електронском трансферу новца извршиоци кривичног дела новац подижу у иностранству веома брзо, понекад и у року од 24 часа. За то време оштећено предузеће је у убеђењу да је уплатило новац страној компанији, а страна компанија чека уплату за нпр. одређену робу. Да су преварени оштећени сазнају тек након што контактирају страну компанију. Наведеним радњама извршилаца кривичног дела преваре највише су угрожена мала и средња предузећа са територије Републике Србије.

Извршиоци кривичних дела на рачунаре оштећених привредних лица, али и грађана Републике Србије, шаљу злонамерне рачунарске програме – вирусе познатије као *ransomware* који енкриптују електронске податке на рачунарима оштећених лица, а потом служе за уцењивање оштећених лица како би им се изнудио одређени новчани износ за враћање важних података тј. њихову декрипцију.

У Републици Србији врше се злоупотребе електронских података о платним картицама на Интернету *(card not present).* Извршиоци су електронске

податке са платних картица користили за набављање скупоцене робе путем Интернет сајтова. Податке о платним картицама прибаљали су путем кардерских форума. Углавном се радило о платним картицама страних држављана које су злоупотребљаване од стране извршилаца са територије Републике Србије. У свету је било случајева злоупотреба електронских новчаника, бесконтактног начина плаћања и др.

Доласком Pay-Pal-a у Републику Србију, вишеструко се повећало наручивање робе путем интернета. Испорука тако наручене робе најчешће се врши поштанским саобраћајем, често и експресним пошиљкама. Међутим, поред робе која је легално на тржишту, путем интернета се продаје и роба (лекови и разна медицинска средства, електронске цигарете, козметика, кондиторски производи итд.) која није испитана и за која се не поседују све прописане дозволе. Посебан проблем представља могућност да се не ради о оригиналним производима у ком случају неће бити само повређена права интелектуалне својине, већ ти производи могу озбиљно угрозити живот и здравље становништва.

Преко интернета се најчешће продаје роба од стране физичких лица која немају регистровано привредно друштво и нису предузетници. При томе, ради се о роби која се нелегално налази на тржишту (не поседују се потребне дозволе и сертификати, нису плаћене дажбине – царина и ПДВ). Уколико постоји константно снабдевање тржишта овом робом, то може изазвати нелојалну конкуренцију и пораст сиве економије.

Управа царина, као и царинске администрације других држава, поред фискалне улоге, има и безбедносну, односно сугурносну тј. заштитну улогу. Имајући у виду потребе за појачаном контролом робе која се наручује, односно продаје путем интернета, царинске администрације ЕУ (Француска Република, Холандија, Република Аустрија и др.) формирале су посебне организационе јединице за борбу против високотехнолошког криминала са циљем идентификације дела која су у супротности са царинским прописима, а која су учињена коришћењем компјутера и информационих система.

С обзиром на напред наведено, Управа царина налази да постоји потреба појачане контроле робе која се продаје преко интернета и у вези с тим, повећање улоге коју тренутно Управа царина има.

Када је реч о кривичним делима против безбедности рачунарских података, може се констатовати да се најчешће врше кривична дела Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података, затим Прављење и уношење рачунарских вируса, као и рачунарске преваре и рачунарске саботаже. Ова кривична дела врше се од стране извршилаца који поседују специфична техничка знања. Појачано је и коришћење специјализованих форума на којима извршиоци кривичних дела размењују своја знања и проналазе саизвршиоце, као и алате за вршење кривичних дела. Присутна је и појава злоупотребе нових технологија за вршење кривичних дела. Један од таквих примера је и злоупотреба

концепта Интернета ствари (*Internet of Things-IoT*) где се уређаји који су мрежно повезани, након што су заражени рачунарским вирусом, појављују као део DDoS мреже, тако да су ови видови напада јачи по свом интензитету.

Нове технологије као што су *IoT*, *Cloud* рачунарство, *BYOD* све су присутније и извршиоци кривичних дела увиђају предност ових технологија широм света. Злоупотреба ових технологија утиче на интензитет напада и њихов обим, као и на насталу штету. Рачунарство у *cloud* окружењу такође представља ризик због широког спектра могућих злоупотреба уколико дође до компромитовања заштите и платформи.

Концепт BYOD (Bring Your Own Device) се односи на могућност да запослени донесу своје мобилне уређаје, као што су лаптопови, таблети и мобилни телефони и користе их на свом радном месту у пословне сврхе. Ризик коришћења овог концепта је у томе што је потребна адекватна примена безбедносних мера у систему у коме запослени доносе своје уређаје и повезују их у корпоративну мрежу. Пропусти могу повећати ризик од утицаја извршилаца кривичних дела на корпоративно окружење у коме се налази уређај и самим тим постоји могућност за вршење кривичних дела на штету пословних субјеката.

Напредне упорне претње (*Advance Persistent Threat*-APT) сваке године у све већој мери погађају привредне субјекте широм света. Очекује се да акценат више неће бити само на упорним претњама, већ да ће извршиоци кривичних дела из ове области креирати и отпорније претње или малвер програме без фајлова, смањујући на тај начин трагове у инфицираном систему и избегавајући детекцију.

Извршиоци кривичних дела везаних за сексуалну злоупотребу малолетних лица у порнографске сврхе, на Интернету користе П2П (Peer to Peer) мреже како би прибављали и/или размењивали незаконите аудио-визуелне материјале настале сексуалном злоупотребом. Незаконити аудио-визуелни материјали прибављају се на такав начин што се користећи Peer to Peer мреже, укуцавањем траженог појма, проналази одређени садржај, а затим се преузима и складишти на меморији својих рачунара. Такви садржаји могу се делити са другим извршиоцима кривичних дела широм света који су у исто време тражили материјал који је преузимао извршилац у нашој земљи и који је допустио дељење у мрежи.

У мањем броју случајева извршиоци кривичних дела користе и различите форуме како би размењивали наведене незаконите материјале и како би пронашли саизвршиоце. За прибављање и размену материјала насталог сексуалном злоупотребом малолетних лица у порнографске сврхе на Интернету, користе се и социјалне мреже. Поред преузимања, поседовања и размене тих садржаја, социјалне мреже се користе и како би се ступило у контакт са малолетним лицима. Углавном се користе лажни профили који се прилагођавају узрасту деце и њиховим интересовањима, покушавајући да

задобију њихову пажњу и поверење. Након што остваре контакт и задобију поверење извршиоци кривичних дела из ове области траже од деце да изврше одређену радњу (снимање одређеног дела тела или показивање интимних делова тела *online* и др.) и након тога материјал који добију користе за даље уцене према жртви како би продужили вршење кривичног дела.

Поред тога, у оперативној акцији на сузбијању сексуалне експлоатације малолетних лица у порнографке сврхе путем интернета „Армагедон", од 2010. до 2018. године поднете су кривичне пријаве против 181 осумњиченог лица за 189 кривичних дела, док је 163 лица лишено слободе. Информације на којима се заснива акција „Армагедон" прикупљају се оперативним полицијским радом, пријавама грађана, као и на информацијама добијеним путем међународне оперативне полицијске сарадње (Интерпол, Европол, ФБИ, НЦА и др.). Одељење за сузбијање високотехнолошког криминала и поред ових значајних резултата уопште нема систематизована радна места за истраге сексуалне експлоатације деце на Интернету.

Напредак информационих технологија доводи до константног пораста броја кривичних дела у области ауторског и другог сродног права. Предмет „пиратерисања" нису само дела страних већ и домаћих аутора. Велики проблем у овом смислу представљају најновији филмови, као и серије или филмови домаће производње чија је производња често субвенционисана од стране државе. Предузете су конкретне активности у договору са појединим аукцијским сајтовима који огласе на којима се нуде различита ауторска права (филмови, музика, игре, софтвери), који немају атрибуте оригиналности не постављају на своје веб стране, већ да омогућавају продају оригиналних производа у електронској форми (на ЦД-у). У области индустријске својине на територији Републике Србије најчешће се путем Интернет сајтова продају фалсификована фармацеутска средства, као и гардероба различитих робних марки и др.

Угрожавање сигурности претњом да ће се напасти на живот или тело жртве или њој блиског лица извршиоци су вршили како према грађанима тако и према носиоцима јавних функција. Кривична дела врше се свим средствима комуникације на Интернету, а најчешћи облици се односе на коришћење бесплатних сервиса за електронску пошту, социјалних мрежа, форума, коментара испод одређених текстова објављених у електронским медијима.

Злоупотреба информационо-комуникационих технологија везана за тероризам и насилни екстремизам који води ка тероризму одвија се за вербовање нових следбеника, давање упутстава о начину вршења кривичних дела, а помоћу Интернет сајтова, форума, социјалних мрежа и других форми намењених размени мултимедијалних садржаја врши се и пропаганда идеологије повезане са тероризмом. Сервиси се користе и за међусобну комуникацију, прикривање идентитета и анонимност. Најчешће је коришћење *VoIP* сервиса и заштићених форума. Са тероризмом и насилним

екстремизмом који води ка тероризму повезано је вршење кривичних дела Неовлашћен приступ заштићеним рачунарима, рачунарским мрежама и електронској обради података (пример: *defacement* циљаних Интернет сајтова), али и спречавања и ограничавања приступа и електронске обраде рачунарских података (пример: *DDoS* напади уз употребу *CaaS* сервиса). Присутно је и коришћење виртуелних валута као што је *Bitcoin* за прибављање противправне имовинске користи која се може употребити за финансирање терористичких активности.

6. ИДЕНТИФИКОВАЊЕ ПРОБЛЕМА, УЗРОКА И ПОСЛЕДИЦА

Свеобухватна стратешка анализа базирана на примарним и секундарним изворима информација у области борбе против високотехнолошког криминала, коришћењем савремених метода и техника стратешке анализе, идентификовала је већи број проблема које је неопходно отклонити у циљу ефикаснијег супростављања овом виду криминала. Имајући у виду повећања броја кривичних дела у којима се информационо-комуникационе технологије злоупотребљавају, у контексту тенденције брзог развоја и коришћења информационо-комуникационих технологија неопходно је, у државним органима који су препознати као носиоци борбе против високотехнолошког криминала, унапредити нормативни и институционални оквир, побољшати услове за рад у погледу повећања броја запослених, техничке опремљености и оперативних капацитета и омогућити успостављања ефикасније сарадње како на националном тако и на међународном нивоу:

– Анализа домаћег и међународног нормативног оквира (пре свега прелазног мерила у оквиру Поглавља 24, затим директива, конвенција и стратегија) је показала да је неопходно усаглашавање Кривичног законика и Законика о кривичном поступку са правним тековинама ЕУ. Такође је потребно допунити и изменити постојеће законе који дефинишу надлежности државних органа у делу који се односи на област високотехнолошког криминала. Поред тога, подзаконским актима је неопходно ближе уредити ову област;

– У оквиру успостављања капацитета полиције и тужилаштва која су дефинисана у прелазном мерилу у оквиру Поглавља 24 неопходно је применити одредбе Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала. Поред тога, потребно је извршити измену и допуну наведеног закона, у циљу повећања институционалних капацитета тужилаштва и полиције, али и других државних органа који су носиоци борбе против високотехнолошког криминала. С тим у вези неопходно је изменити акте о унутрашњем уређењу и ситематизацији радних места у органима државне управе;

– У оквиру побољшања оперативних процедура за рад неопходно је обезбедити уједначено поступање носилаца борбе против високотехнолошког криминала, улагати у специјалистичке обуке кадрова, техничку опремљеност, нове софтверске алате, успоставити дефиницију

критичне инфраструктуре, увести могућности спровођења једноставније дигиталне форензике итд.;

– Веома је значајно унапредити сарадњу у овој области, како између органа државне управе, тако и са приватним сектором и организацијама цивилног друштва. Посебно је важно унапредити регионалну и међународну сарадњу, пре свега са Интерполом;

– Од пресудног је значаја спроводити превентивне активности које се односе на јачање свести грађана и грађанки, као и органа власти о могућностима злоупотребе информационо-комуникационих технологија, мобилних телефона, Интернета и друштвених мрежа. С тим у вези, неопходно је унапредити проактивни приступ у којем ће учествовати сви актери препознати као носиоци борбе против високотехнолошког криминала, пре свега Посебно тужилаштво и Министарство унутрашњих послова, Одељење за сузбијање високотехнолошког криминала;

– Потребно је припремити се за успостављање јединственог централизованог кривичног обавештајног система и сигурне платформе за комуникацију међу органима за спровођење закона. Обезбедити бољу повезаност релевантних база података (укључујући анализу трошкова, административних ресурса, буџета и потреба за обуком) и побољшати прикупљање обједињених статистичких података о кривичним делима (Препорука 6.2.2.из АП 24).

С обзиром на обим анализиране проблематике и тенденцију пораста кривичних дела у области високотехнолошког криминала, ради отклањања проблема, а у циљу јачања капацитета Министарства унутрашњих послова планирано је, доношењем новог Правилника о унутрашњем уређењу и систематизацији радних места у Министарству унутрашњих послова, који је ступио на снагу 15. јуна 2018. године, попуњавање специјализованог Одсека за сузбијање и злоупотребу у области електронске трговине, електронског банкарства и платних картица на Интернету и Одсека за сузбијање недозвољених и штетних садржаја на Интернету.

У погледу институционалног оквира за борбу против високотехнолошког криминала, када је реч о Јавном тужилаштву, потребно је истаћи да Посебно тужилаштво за високотехнолошки криминал, према важећим нормама, функционише као део – одељење Вишег јавног тужилаштва у Београду. За разлику од Вишег јавног тужилаштва, које прати стварну и месну надлежност Вишег суда у Београду, Посебно тужилаштво надлежно је за поступање на читавој територији Републике Србије. Овакво решење у пракси доводи до отежаног рада, јер је Више јавно тужилаштво Београду организационо, функционално и месно прилагођено искључиво за поступање, односно, кривично гоњење учинилаца кривичних дела и њихово процесуирање пред Вишим судом у Београду. Специфичност високотехнолошког криминала огледа се, између осталог, и у чињеници да се најчешће место извршења кривичног дела из области високотехнолошког

криминала и место наступања штетне последице не поклапају, због чега је и сам законодавац дао републичку надлежност тужилаштву за високотехнолошки криминал.

У погледу нормативног оквира, ради ефикасног поступања државних органа у борби против високотехнолошког криминала неопходно је допунити и изменити сет закона из ове области, у циљу усклађивања са законодавством ЕУ и то:

– Кривични законик потребно је ускладити са међународним стандардима, детаљније и прецизније описати кривична дела и прописати строжије кривичне санкције. Поред тога, у појмовима дефинисати шта представљају подаци о претплатнику, подаци о саобраћају и подаци о садржини саобраћаја;

– када је реч о измени Законика о кривичном поступку, потребно је прописати следеће посебне доказне радње:

– хитно чување похрањених рачунарских података – односи се на омогућавање издавање наредбе од стране надлежног органа, пожељно јавног тужилаштва, којим ће већ похрањени подаци, укључујући и податке о саобраћају, бити додатно сачувани од стране држаоца у обавезном року од 90 дана који може бити продужен за још 90,

– хитно чување и делимично откривање података о саобраћају – односи се на хитно чување података о сабраћају, без обзира на то да ли је у преносу тих података укључено више субјеката (ИСП) и откривање ограничене, али довољне количине података које могу да послуже надлежном органу за идентификацију субјекта преноса података, као и путање којом су подаци емитовани,

– наредба о достављању података – односи се на издавање наредбе физичком или правном лицу да достави/преда надлежном органу рачунарске податке који се налазе у поседу или под контролом тог лица, а који подаци су похрањени у рачунару или на рачунарском медијуму, као и наредбу ИСП да достави/преда надлежном органу податке о претплатнику одређене услуге које поседује или се налазе под његовом контролом,

– наредба о претрази и одузимању података – обухвата модификацију постојећих наредби о претресу ствари и посебне доказне радње аутоматске обраде података,

– наредба о прикупљању података о саобраћају у реалном времену – односи се на доношење наредбе којом би се употребом техничких метода наведени подаци прикупљали у реалном времену, као и наредбу ИСП да у оквиру постојећих техничких могућности спроведе ову наредбу сам или да сарађује са надлежним органом,

– наредба о пресретању података о садржини саобраћаја – односи се на исту материју као претходна наредба, само је предмет наредбе садржина саобраћаја, уместо података о саобраћају,

– у оквиру међународне кривично-правне помоћи и сарадње потребно је омогућити размену спонтаних информација, као и примену наредби у вези хитног чувања похрањених података, хитног чувања и делимичног откривања података о саобраћају, приступ похрањеним подацима, прекогранични приступ похрањеним подацима уз сагласност или када су јавно доступни, међународну правну помоћ која се односи на прикупљање података о саобраћају у реалном времену, те пресретању података о садржини саобраћаја, као и законски конкретизовано успостављање тачака 24/7 за хитну полицијску сарадњу, као и друге тачке за 24/7 пружање међународне правне помоћи, која би у овом контексту морала бити при Републичком јавном тужилаштву, имајући у виду надлежности.

Боља повезаност релевантних база података и побољшано прикупљање обједињених статистичких података о кривичним делима ће бити предвиђена ревизијом Акционог плана за Поглавље 24.

7. ВИЗИЈА

Визија ове стратегије је:

Створено безбедно друштвено окружење кроз адекватан одговор Републике Србије на све појавне облике високотехнолошког криминала.

8. ОПШТИ ЦИЉ СТРАТЕГИЈЕ

Република Србија поседује ефикасан и одржив систем заједничког деловања свих субјеката у борби против високотехнолошког криминала.

Овакав општи циљ Стратегије би требало да доведе до бољег повезивања свих субјеката Стратегије, у борби против високотехнолошког криминала, као и до боље искоришћености ресурса у решавању проблема.

9. СПЕЦИФИЧНИ ЦИЉЕВИ СТРАТЕГИЈЕ

Специфични циљеви су усмерени у правцу решавања препознатих проблема у супротстављању високотехнолошком криминалу.

Кроз Анализу су препозната четири специфична циља и дефинисане мере у окиру њих:

1. Унапређено и усаглашено законодавство Републике Србије са правним тековинама и стандардима Европске уније у области борбе против високотехнолошког криминала

1.1. Израдити предлоге измена и допуна правних прописа Републике Србије са правним тековинама Европске уније

2. Унапређени организациони, кадровски, технички и оперативни капацитети носилаца борбе против високотехнолошког криминала

2.1. Реорганизовати Одељење за сузбијање високотехнолошког криминала

2.2. Формирати посебне организационе јединице у органима и организацијама у складу са њиховим надлежностима и потребама

2.3. Унапређење кадровских, стручних, техничких и организационих капацитета надлежних институција за размену података о инцидентима и реаговање на инциденте

2.4. Реализовати потребне обуке различитих нивоа

2.5. Набавити савремену електронску опрему и софтверске алате

2.6. Усаглашавање стандардних оперативних процедура носилаца борбе против високотехнолошког криминала

3. Унапређен превентивни и проактивни приступ друштву у борби против високотехнолошког криминала

3.1. Подизање нивоа свести јавности по питању високотехнолошког криминала

3.2. Подизање нивоа свести међу органима јавне власти по питању високотехнолошког криминала

4. Унапређена сарадња на националном, регионалном и међународном нивоу

4.1. Унапредити сарадњу између приватног, јавног сектора и цивилног друштва

4.2. Унапредити сарадњу на спречавању сексуалне експлоатације деце и малолетних лица

4.3. Унапредити међународну и регионалну полицијску сарадњу

10. СПРОВОЂЕЊЕ, ПРАЋЕЊЕ, ОЦЕЊИВАЊЕ И ИЗВЕШТАВАЊЕ

10.1. Органи надлежни за спровођење Стратегије

Стратегију за борбу против високотехнолошког криминала спроводе министарства и други државни органи, у оквиру својих надлежности. Активности могу бити у надлежности само једног или више министарстава, односно државних органа. Ако је за неку активност потребна сарадња више министарстава или државних органа, вођење активности преузима министарство или државни орган у чијој је претежној надлежности активност, а на нивоу Савета за борбу против високотехнолошког криминала обезбеђује се сарадња и координисано деловање са другим министарствима и државним органима.

Савет за борбу против високотехнолошког криминала ће предложити формирање Стручног тима за имплементацију Стратегије за спровођење конкретних активности, који би био састављен од запослених чије су организационе јединице носиоци активности у Акционом плану.

Стручни тим за имплементацију Стратегије је одговоран за праћење успешности примене ове стратегије и пратећег акционог плана. Овај стручни тим ће успоставити механизам континуираног прикупљања података за извештај од свих одговорних органа јавне власти. Институције одговорне за примену стратегије и акционог плана достављаће Стручном тиму за имплементацију извештаје о спроведеним активностима. По потреби и по захтеву Стручног тима одговорне институције ће достављати и додатне извештаје и податке. Континуирано ће се прикупљати и други релевантни подаци, као што су јавно доступне стручне анализе о овој области. Конкретне активности које ће министарства, односно други државни органи спроводити, одредиће се Акционим планом.

10.2. Савет за борбу против високотехнолошког криминала

Савет за борбу против високотехнолошког криминала је радно тело које образује Влада и надлежан је за анализирање спровођења свих планираних активности и у ту сврху подноси периодичне извештаје Влади о напретку у спровођењу Стратегије и Акционог плана. Савет за борбу против високотехнолошког криминала може иницирати усклађивање, измену или допуну Стратегије и Акционог плана, усаглашавање законодавних и нормативних аката са међународним прописима и стандардима који су од значаја за Републику Србију.

10.3. Национални координатор за борбу против високотехнолошког криминала

Национални координатор за борбу високотехнолошког криминала информише Савет о свим аспектима спровођења Стратегије и Акционог плана и координира радом Стручног тима за имплементацију Стратегије. Успоставља сарадњу са међународним организацијама и сектором цивилног друштва ради успешног спровођења Стратегије и Акционог плана.

Националном координатору, чланови Стручног тима за имплементацију Стратегије достављају информације и податаке у вези са високотехнолошким криминалом ради ефикасније реализације циљева Стратегије.

Националног координатора за борбу против високотехнолошког криминала именује Влада на предлог Савета.

Национални координатор за борбу против високотехнолошког криминала и Стручни тим за имплементацију Стратегије су одговорни за праћење успешности примене ове стратегије и пратећег акционог плана. Они ће

успоставити механизам континуираног прикупљања појединачних извештаја свих одговорних органа јавне власти у циљу израде заједничког извештаја.

Национални координатор за борбу против високотехнолошког криминала и Стручни тим за имплементацију Стратегије ће се састајати тромесечно, а према потреби и чешће. Национални координатор ће са овим тимом припремати шестомесечне извештаје са оценом успешности примене Стратегије и достављати их Савету, а Савет Влади.

Да би се оценили ефекти примене стратегије и у складу са тим кориговала њена примена, биће урађене две евалуације: једна на крају друге године спровођења и једна крајем 2023. године. Национални координатор са Стручним тимом за имплементацију стратегије припремиће коначни извештај са оценом успешности примене ове стратегије и доставити га Влади најкасније до почетка 2024. године.

11. ФИНАНСИЈСКИ ЕФЕКТИ СТРАТЕГИЈЕ И АКЦИОНОГ ПЛАНА

Средства неопходна за спровођење активности планираних овом стратегијом, које ће се извршавати у наредном периоду, биће обухваћена финансијским плановима носилаца активности и обезбеђиваће се у буџету Републике Србије у складу са билансним могућностима, а у складу са потребама додатна средства ће се обезбедити из донација, пројеката, помоћи, као и из других извора.

12. ЗАВРШНА ОДРЕДБА

Ову стратегију објавити у „Службеном гласнику Републике Србије”.

05 број 23-8630/2018

У Београду, 14. септембра 2018. године

Влада

Председник,

Ана Брнабић, с.р.

АКЦИОНИ ПЛАН 2019–2020. ЗА СПРОВОЂЕЊЕ СТРАТЕГИЈЕ ЗА БОРБУ ПРТОИВ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА ЗА ПЕРИОД 2019–2023. ГОДИНЕ

ОПШТИ ЦИЉ	**Република Србија поседује ефикасан и одржив систем заједничког деловања свих субјеката за борбу против високотехнолошког криминала**	**показатељ ефекта**
		Проценат повећања евидентираних и процесуираних кривичних дела ВТК који се гоне по службеној дужности
1. ЦИ	**Унапређено и усаглашено законодавство Републике**	**показатељ исхода**
		Степен усклађености националног

Љ	**Србије са правним тековинама и стандардима Европске уније у области борбе против високотехнолошког криминала**			законодавства са правним тековинама Европске уније		
1.1. Мера	**Израдити предлоге измена и допуна правних прописа Републике Србије са правним тековинама Европске уније**			**показатељ резултата**		
				Израђени предлози измена и допуна		
				полазна вредност	циљна вредност	
				0%	100%	
Активност		извор верификације	рок реализације	потребна средства	извор финансирања	носиоци активности
1.1.1.	Израдити Нацрт законика о изменама и допунама Законика о кривичном поступку и Кривичног Законика ради усаглашавања са Директивом 2013\40	Израђен Нацрт законика и достављен Влади	IV квартал 2020.	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Министарство правде**, Републичко јавно тужилаштво, Министарство унутрашњих послова
1.1.2.	Израдити Нацрт	Израђен Нацрт	IV кварта	**Нема додатних**	**Нема додатних**	**Министарство**

	законика о изменама и допунама Законика о кривичном поступку и Кривичног Законика ради усаглашавања са Директивом 2011\93	законика и достављен Влади	л 2020.	**трошкова –** запослени раде у оквиру редовних радних активности	**трошкова –** запослени раде у оквиру редовних радних активности	**правде**, Републичко јавно тужилаштво, Министарство унутрашњих послова
2. ЦИЉ	**Унапређени организациони, кадровски, технички и оперативни капацитети носилаца борбе против високотехнолошког криминала**			**показатељ исхода**		
				Повећан степен институционалних капацитета носилаца борбе против високотехнолошког криминала		
2.1. Мера	**Реорганизовати Одељење за сузбијање високотехнолошког криминала**			**показатељ резултата**		
				Повећан број запослених у Одељењу за сузбијање високотехнолошког криминала попуњавањем два нова одсека у оквиру Одељења високотехнолошког криминала		
				полазна вредност	циљна вредност	
				16 запослених	22 запослена	
Активност		извор верификације	рок реализације	потребна средства	извор финансирања	носиоци активности

2.1.1.	Изменити акт о унутрашњем уређењу у складу са кадровским планом Министарства унутрашњих послова и финансијским могућностима	Закључак Владе	I квартал 2019. године	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Министарство унутрашњих послова**
2.1.2.	Попунити Одсек за сузбијање злоупотреба у области електронске трговине, електронског банкарства и платних картица на Интернету	Акт о унутрашњем уређењу и систематизацији радних места у Министарству унутрашњих послова	I квартал 2019. године	**Нема додатних трошкова –** распоређивање у оквиру новоформираног Одсека спроводиће се кроз распоређивање постојећих запослених	**Нема додатних трошкова –** распоређивање у оквиру новоформираног Одсека спроводиће се кроз распоређивање постојећих запослених	**Министарство унутрашњих послова**
2.1.3.	Попунити Одсек за сузбијање недозвољених и штетних садржаја на	Акт о унутрашњем уређењу и систематизацији радних места у	I квартал 2019. године	**Нема додатних трошкова –** распоређивање у оквиру новоформираног	**Нема додатних трошкова –** распоређивање у оквиру новоформираног	**Министарство унутрашњих послова**

	Интернету	Министарству унутрашњих послова		Одсека спроводиће се кроз распоређивање постојећих запослених	Одсека спроводиће се кроз распоређивање постојећих запослених	
2.2. Мера	**Формирати посебне организационе јединице у органима и организацијама у складу са њиховим надлежностима и потребама**			**показатељ резултата**		
				а) Степен оперативности нових организационих јединица за борбу против ВТК б) Повећање броја запослених у организационим јединицама носилаца борбе против ВТК		
				полазна вредност	циљна вредност	
				а) 0% б) биће одређена на основу података за 2018. годину	а) 100% б) повећање од 20%	
Активност		извор верификације	рок реализације	потребна средства	извор финансирања	носиоци активности
2.2.1.	Формирати организациону јединицу за борбу против високотехнолошког криминала у Управи царина	Правилник о унутрашњем уређењу и систематизацији радних места у Управи царина	I квартал 2020. године	**Нема додатних трошкова –** распоређивање у оквиру новоформиране јединице спроводиће се кроз распоређи	**Нема додатних трошкова –** распоређивање у оквиру новоформиране јединице спроводиће се кроз распоређи	**Министарство финансија-Управа царина**

				вање постојећих запослених	вање постојећих запослених	
2.2.2.	Формирати организациону јединицу за борбу против високотехнолошког криминала у Безбедносно-информативној агенцији	Извештај Безбедносно-информативне агенције	I квартал 2020. године	**Нема додатних трошкова –** распоређивање у оквиру новоформиране јединице спроводиће се кроз распоређивање постојећих запослених	**Нема додатних трошкова –** распоређивање у оквиру новоформиране јединице спроводиће се кроз распоређивање постојећих запослених	**Безбедносно-информативна агенција**
2.2.3.	Формирати посебну организациону јединицу у Војној полицији Војске Србије	Одлука о одранизацијским променама	I квартал 2020. године	**Нема додатних трошкова –** распоређивање у оквиру новоформиране јединице спроводиће се кроз распоређивање постојећих запослених	**Нема додатних трошкова –** распоређивање у оквиру новоформиране јединице спроводиће се кроз распоређивање постојећих запослених	**Министарство одбране**
2.3. Мер	**Унапређење кадровских, стручних, техничких и**			**показатељ резултата**		
				Повећање броја запослених у		

а	**организационих капацитета надлежних институција за размену података о инцидентима и реаговање на инциденте**			организационим јединицама за борбу против високотехнолошког криминала надлежних институција за размену података о инцидентима и реаговање на инциденте		
				полазна вредност	циљна вредност	
				биће одређена на основу података за 2018. годину	20%	
2.3.1.	Спровођење обука за запослене у надлежним органима о поступању у случају инцидената у ИКТ системима	Извештај о раду	IV квартал 2019	**Буџет Министарства трговине, туризма и телекомуникација** 3.000.000 динара у 2019. години	**Буџет Републике Србије** – раздео Министарства трговине, туризма и телекомуникација	**Министарство трговине, туризма и телекомуникација**, Регулаторна агенција за електронске комуникације и поштанске услуге, Народна банка Србије, Канцеларија за информационе технологије и електронску управу, Академска мрежа Републике Србије,

						Министарство унутрашњих послова, Министарство одбране, Криминалистичко-полицијски универзитет
2.3.2.	Подизање дигиталних компетенција запослених у јавном сектору	Извештај о раду	IV квартал 2019	**Буџет Министарства трговине, туризма и телекомуникација** 6.000.000 динара у 2018. години 6.000.000 динара у 2019. години	**Буџет Републике Србије** – раздео Министарства трговине, туризма и телекомуникација	**Министарство трговине, туризма и телекомуникација**, Регулаторна агенција за електронске комуникације и поштанске услуге, Народна банка Србије, Канцеларија за инфомационе технологије и електронску управу, Академска мрежа Републике Србије, Министарство

						унутрашњих послова, Министарство одбране, Криминалистичко-полицијски универзитет
2.4. Мера	**Реализовати потребне обуке различитих нивоа**			**показатељ резултата**		
				Број запослених који су стекли неопходне компетенције		
				полазна вредност	циљна вредност	
				0%	10%	
Активност		извор верификације	рок реализације	потребна средства	извор финансирања	носиоци активности
2.4.1.	Израда анализа образованих потреба основних обука за државне органе носиоце борбе против високотехнолошког криминала	Извештај о спровођењу пројекта	II квартал 2019. год.	Пројекат „Јачање капацитета државних органа у борби против високотехнолошког криминала у Југоисточној Европи” *уз подршку ОЕБС*	Донација	**Министарство унутрашњих послова**, Криминалистичко-полицијски универзитет, Републичко јавно тужилаштво, Министарство правде, Правосудна академија, Државно веће тужилаца

2.4.2.	Израдити програм и план обука у складу са закључцима анализе	Израђен програм и план обука	IV квартал 2019. год.	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Министарство унутрашњих послова**, Криминалистичко-полицијски универзитет, Републичко јавно тужилаштво, Министарство правде, Правосудна академија, Државно веће тужилаца
2.4.3.	Реализовати обуке основног нивоа	Извештаји са обука, Евалуациони формулари учесника	Континуирано у складу са програмом и планом	**Пројекат „**Јачање капацитета државних органа у борби против високотехнолошког криминала у Југоисточној Европи” *уз подршку ОЕБС*	**Пројекат „**Јачање капацитета државних органа у борби против високотехнолошког криминала у Југоисточној Европи” *уз подршку ОЕБС*	**Министарство унутрашњих послова,** Криминалистичко-полицијски универзитет, Републичко јавно тужилаштво, Министарство правде, Правосудна академија
2.4.4.	Реализовати специјали	Извештаји са обука, Евалуаци	Континуирано у	**Нема додатних трошкова**	**Нема додатних трошков**	**Министарство унутрашњ**

	стичке обуке на позив међународних организација које учествују у борби против високотехнолошког криминала	они формулари учесника	складу са програмом и планом	**– запослени раде у оквиру редовних радних активности** Донаторска средства организатора	**а – запослени раде у оквиру редовних радних активности** Донаторска средства организатора	**их послова**
2.5. Мера	**Набавити савремену електронску опрему и софтверске алате**			**показатељ резултата**		
				Проценат испуњења утврђених техничких потреба по спецификацији		
				полазна вредност	циљна вредност	
				биће одређена на основу података за 2018. годину	20%	
Активност		извор верификације	рок реализације	потребна средства	извор финансирања	носиоци активности
2.5. 1.	Набавка рачунарске опреме	1. ИПА 1 2017 пројекат	III квартал 2019. године	**Пројекат ИПА 2017** – предвиђена вредност набавке **1.787.340 евра Донација – Међународни**	1. ИПА 1 2017 2. Буџет Министарства унутрашњих послова 3. Међународни партнери	**Министарство унутрашњих послова**, Републичко јавно тужилаштво

				партнери за Министарство унутрашњих послова 9.055.900 динара за 2019. годину		
2.5.2.	Набавка специјализованог софтвера	ИПА 2017 пројекат	III квартал 2019. године	**Пројекат ИПА 2017** **Буџет Министарства унутрашњих послова 11.900.000 динара,** за 2019. годину, за набавку софтвера и лиценци **2.975.000 динара**, за 2020. годину, одржавање софтвера	Буџет Министарства унутрашњих послова Пројекат ИПА 2017	**Министарство унутрашњих послова,** Републичко јавно тужилаштво
2.5.3.	Обука за примену савремене електронске опреме и софтверских алата	ИПА 2017 пројекат	IV квартал 2019. године	**Веза активност 2.5.2.**	**Веза активност 2.5.2.**	**Министарство унутрашњих послова**
2.6.	**Усаглашавање стандардних**			**показатељ резултата**		

Мера	**оперативних процедура носилаца борбе против високотехнолошког криминала**			а) Обезбеђено уједничано поступање носилаца борбе против високотехнолошког криминала б) Запослени примењују стандардне оперативне процедуре		
				полазна вредност	циљна вредност	
				0%	100%	
Активност		извор верификације	рок реализације	потребна средства	извор финансирања	носиоци активности
2.6.1.	Усвојити оперативне процедуре за прикупљање и обезбеђење електронских доказа	Обавезна инструкција о прикупљању и обезбеђењу електонских доказа	I квартал 2019. године	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Министарство унутрашњих послова**
2.6.2.	Унапредити методологију рада осталих државних органа у складу са усвојеном инструкцијом у поступку прикупљања и обезбеђивања електронских доказа	Појединачне инструкције државних органа усклађене са усвојеном инструкцијом	IV квартал 2020.године	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Министарство унутрашњих послова,** Министарство финансија-Управа царина, Безбедносно-информативна агенција, Министарство одбране

3. ЦИЉ	**Унапређен превентивни и проактивни приступ у друштву у борби против високотехнолошког криминала**			**показатељ исхода**		
				Повећан проценат грађана који препознају опасности од високотехнолошког криминала на основу података за период од 2019–2020. године		
3.1. Мера	**Подизање нивоа свести јавности по питању високотехнолошког криминала**			**показатељ резултата**		
				Број реализованих превентивних и проактивних активности и акција у поступању носилаца борбе против високотехнолошког криминала		
				полазна вредност	циљна вредност	
				биће одређена на основу података за 2018. годину	повећање од 30%	
Активност		извор верификације	рок реализације	потребна средства	извор финансирања	носиоци активности
3.1.1.	Спроводити едукације деце и родитеља, социјалних радника и наставног особља о опасностима од високотехнолошког криминала	Извештај о раду Министарства унутрашњих послова	Континуирано	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Министарство унутрашњих послова,** Министарство трговине, туризма и телекомуникација, Министарство просвете, науке и технолошког развоја, Криминалистичко-

						полицијски универзитет, Министарство за рад, запошљавање, борачка и социјална питања, Народна банка Србије, Удружење банака Србије
3.1.2.	Подизање нивоа свести јавности кроз сарадњу са медијима	Извештај о раду Министарства унутрашњих послова	Континуирано	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Министарство унутрашњих послова,** Министарство трговине, туризма и телекомуникација, Регулаторна агенција за електронске комуникације и поштанске услуге, Народна банка Србије, Удружење банака Србије
3.1.	Информис	Меморанд	Контин	**Нема**	**Нема**	**Министар**

3.	ати банкарске клијенте о опасностима од високотехнолошког криминала	ум о сарадњи, Записници са одржаних састанака	уирано	**додатних трошкова –** запослени раде у оквиру редовних радних активности и	**додатних трошкова –** запослени раде у оквиру редовних радних активности и	**ство унутрашњих послова**, Посебно тужилаштво за високотехнолошки криминал, Народна банка Србије, Удружење банака Србије
3.1.4.	ИТ Караван – едукативна кампања за промоцију корисне, креативне и безбедне употребе информационих технологија *веза са Акционим планом за спровођење Стратегије развоја информационог друштва у Републици Србији	Извештај о раду Министарства трговине, туризма и телекомуникација и Министарства унутрашњих послова	Континуирано	**Буџет Министарства трговине, туризма и телекомуникација –** 3.000.000 динара у 2019. години	Буџет Републике Србије – раздео Министарства трговине, туризма и телекомуникација	**Министарство трговине, туризма и телекомуникација,** Министарство унутрашњих послова

	за период до 2020. године					
3.1.5.	Информисања и едукације деце, родитеља и наставника на тему безбедности деце на интернету кроз организовање обука у школама (веза са Акционим планом за спровођење Стратегије развоја информационог друштва у Републици Србији за период до 2020. године)	Извештај о раду Министарства унутрашњих послова, Министарства трговине, туризма и телекомуникација и Министарства просвете, науке и технолошког развоја	Континуирано	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Министарство унутрашњих послова,** Министарство трговине, туризма и телекомуникација, Министарство просвете, науке и технолошког развоја
3.1.6.	Информисања и едукације деце, родитеља и наставника на тему безбеднос	Извештај о раду Министарства унутрашњих послова, Министарства	Континуирано	**Нема додатних трошкова –** запослени раде у оквиру редовних радних	**Нема додатних трошкова –** запослени раде у оквиру редовних радних	**Министарство трговине, туризма и телекомуникација**, Министарство унутрашњи

	ти деце на интернету кроз рад Националног контакт центра за безбедност деце на интернету – БИТ 19833 (веза са Акционим планом за спровођење Стратегије развоја информационог друштва у Републици Србији за период до 2020. године)	трговине, туризма и телекомуникација и Министарства просвете, науке и технолошког развоја		активности	активности	х послова, Републичко јавно тужилаштво и Министарство просвете, науке и технолошког развоја
3.1.7.	Промотивна кампања Паметно и безбедно (Дан девојка/девојчица у ИКТ, Дан безбедног интернета, Европски сат програми	Извештај о раду Министарства трговине, туризма и телекомуникација и Министарства унутрашњих послова	Континуирано	**Буџет Министарства трговине, туризма и телекомуникација –** 2.000.000 динара у 2019. години	Буџет Републике Србије	**Министарство трговине, туризма и телекомуникација**, Министарство унутрашњих послова

	рања, Дан информационог друштва...) (веза са Акционим планом за спровођење Стратегије развоја информационог друштва у Републици Србији за период до 2020. године)					
3.1.8.	Обуке са циљем подизања капацитета запослених у институцијама система ради примене Уредбе о безбедности и заштити деце при коришћењу информационо-комуникационих технологија (веза	Извештај о раду Министарства трговине, туризма и телекомуникација	IV квартал 2019. године	**Буџет Министарства трговине, туризма и телекомуникација** 7.200.000 динара у 2019. години	Буџет Републике Србије	**Министарство трговине, туризма и телекомуникација,** Министарство унутрашњих послова, Министарство просвете, науке и технолошког развоја

	са Акционим планом за спровођење Стратегије развоја информационог друштва у Републици Србији за период до 2020. године)					
3.2. Мера	**Подизање нивоа свести међу органима јавне власти по питању високотехнолошког криминала**			**показатељ резултата** а) Број полазника, полицијских службеника УКП, који су приступили електронским порталима за обуку (Е-учионица), б)Број полазника у органима јавне власти којима су одржане обуке основног нивоа по питању високотехнолошког криминала		
				полазна вредност 0%	циљна вредност 5%	
Активност		извор верификације	рок реализације	потребна средства	извор финансирања	носиоци активности
3.2.1.	Спроводити обуке основног нивоа органима јавне власти по питању високотехнолошког	Извештај о раду Министарства унутрашњих послова	Континуирано почев од I квартала 2019. год.	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активност	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активност	**Министарство унутрашњих послова,** Министарство трговине, туризма и телекомуни

	криминала			и	и	кација, Републичко јавно тужилаштво, Министарство правде, Регулаторна агенција за електронске комуникације и поштанске услуге, Министарство просвете, науке и технолошког развоја, Министарство одбране, Криминалистичко-полицијски универзитет, Привредна комора Србије, Удружење банака Србије, Управа царина
3.2.2.	Израдити адекватан материјал за е-обуке полицијск	Извештај о раду Министарства унутрашњих	III квартал 2019. год.	**Нема додатних трошкова –** запослени раде у	**Нема додатних трошкова –** запослени раде у	**Министарство унутрашњих послова,** Криминали

	их службеника у области борбе против високотехнолошког криминала	послова		оквиру редовних радних активности	оквиру редовних радних активности	стичко-полицијски универзитет
3.2.3.	Спроводити е-обуке за подизање нивоа свести полицијских службеника у области борбе против високотехнолошког криминала	Извештај о раду Министарства унутрашњих послова	Континуирано почев од IV квартала 2019. год.	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Министарство унутрашњих послова,** Криминалистичко-полицијски универзитет
4. ЦИЉ	**Унапређена сарадња на националном, регионалном и међународном нивоу**			**показатељ исхода**		
				Повећан степен сарадње на националном, регионалном и међународном нивоу		
4.1. Мера	**Унапредити сарадњу између приватног, јавног сектора и цивилног друштва**			**показатељ резултата**		
				Број потписаних меморандума о институционалној сарадњи, број одржаних конференција, оперативних и других састанака		
				полазна вредност	циљна вредност	
				биће одређена	повећање од 20%	

				на основу података за 2018. годину		
Активност		извор верификације	рок реализације	потребна средства	извор финансирања	носиоци активности
4.1.1.	Потписивање заједничког меморандума о сарадњи носилаца борбе против високотехнолошког криминала	Меморандум о сарадњи у борби против високотехнолошког криминала	I квартал 2020. године	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Републичко јавно тужилаштво**, Министарство унутрашњих послова, Министарство трговине, туризма и телекомуникација, Министарство финансија – Управа царина, Пореска управа и Управа за спречавање прања новца, Безбедносно-информативна агенција, Министарство одбране (Војнобезбедносна агенција)
4.1.	Потписив	Меморанд	I	**Нема**	**Нема**	**Министар**

2.	ање меморандума о сарадњи са научним институцијама, Удружењем банака Србије и привредним субјектима	ум о сарадњи у борби против високотехнолошког криминала	кварта л 2020. године	**додатних трошкова –** запослени раде у оквиру редовних радних активност и	**додатних трошкова –** запослени раде у оквиру редовних радних активност и	**ство унутрашњих послова**, Републичк о јавно тужилаштв о, Криминалистичко-полицијски универзитет, Удружење банака Србије, Привредна комора Србије, Безбедносно-информативна агенција, Регулаторна агенција за електронске комуникације и поштанске услуге, Министарство трговине, туризма и телекомуникација, Управа царина
4.1.3.	Организовање и учествова	Извештај о раду Министар	Континуирано од I	**Донаторска средства**	**Донаторска средства**	**Министарство унутрашњ**

	ње у заједничким конференцијама	ства унутрашњих послова и извештаји других органа и организација	квартала 2019. године	**организатора конференције**	**организатора конференције**	**их послова,** Републичко јавно тужилаштво, Народна банка Србије, Удружење банака Србије, Привредна комора Србије и Безбедносно-информативна агенција, Криминалистичко-полицијски универзитет, Управа царина
4.2. Мера	**Унапредити сарадњу на спречавању сексуалне експлоатације деце и малолетних лица**			**показатељ резултата**		
				Број спроведених заједничких акција на регионалном и међународном нивоу на спречавању сексуалне експлоатације деце и малолетних лица		
				полазна вредност	циљна вредност	
				0%	повећање од 20%	
Активност		извор верификације	рок реализације	потребна средства	извор финансирања	носиоци активности
4.2.1.	Успоставити директну комуника	Годишњи извештај о раду	I квартал 2019. године	**Нема додатних трошкова –**	**Нема додатних трошкова –**	**Министарство унутрашњих**

	цију Одељења за сузбијање високотехнолошког криминала са Интерполовом базом података видео и фото материјала насталих искоришћавањем малолетних лица у порнографске сврхе на Интернету			запослени раде у оквиру редовних радних активности	запослени раде у оквиру редовних радних активности	**послова**
4.2.2.	Донети обавезну инструкцију / упутство о формирању и коришћењу националне базе садржаја насталих злоупотребом малолетних лица на	Годишњи извештај о раду	III квартал 2020. године	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Министарство унутрашњих послова**, Републичко јавно тужилаштво

	Интернету					
4.2.3.	Успоставити базу података видео и фото материјала насталих искоришћавањем малолетних лица у порнографске сврхе на Интернету	Годишњи извештај о раду	IV квартал 2020. године	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Министарство унутрашњих послова,** Републичко јавно тужилаштво, Министарство правде
4.3. Мера	**Унапредити међународну и регионалну полицијску сарадњу**			**показатељ резултата**		
				Повећан број откривених кривичних дела на основу спроведених заједничких акција на регионалном и међународном нивоу		
				полазна вредност	циљна вредност	
				биће одређена на основу података за 2018. годину	повећање од 20%	
Активност		извор верификације	рок реализације	потребна средства	извор финансирања	носиоци активности
4.3.1.	Интензивирање размене оперативних података и информац	Извештај о раду Министарства унутрашњих послова	Континуирано	**Нема додатних трошкова –** запослени раде у оквиру редовних	**Нема додатних трошкова –** запослени раде у оквиру редовних	**Министарство унутрашњих послова**, Републичко јавно тужилаштв

	ија			радних активности	радних активности	о, Безбедносно-информативна агенција, Министарство финансија-Управа царина,Министарство одбране (Војнобезбедносна агенција)
4.3.2.	Креирати стандардне оперативне процедуре о раду 24/7 контакт тачки	Оперативне процедуре о раду 24/7 контакт тачака	IV квартал 2019. године	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Министарство унутрашњих послова**, Републичко јавно тужилаштво/Посебно тужилаштво за високотехнолошки криминал
4.3.3.	Учешће у заједничким међународним акцијама	Извештај о раду Министарства унутрашњих послова	Континуирано	**Донације – Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Донације – Нема додатних трошкова –** запослени раде у оквиру редовних радних активности	**Министарство унутрашњих послова**