ЗВЕЗДАН Љ. РАДОЈКОВИЋ*
Министарство унутрашњих послова Р. Србије
Београд
ЗДРАВКО О. СКАКАВАЦ**
Факултет за правне и пословне студије
др Лазар Вркатић
Нови Сад

УДК 004.7:343.3/.7(487.11)
Прегледни рад
Примљен: 11.01.2019
Одобрен: 25.04.2019
Страна: 217-231

АКТУЕЛНИ ТРЕНДОВИ У ОБЛАСТИ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА У РЕПУБЛИЦИ СРБИЈИ

Сажетак: Високотехнолошки криминал (у даљем тексту: ВТК) све више долази до изражаја, и то не само на глобалном нивоу. Број деликата из ове области континуирано расте из године у годину скоро свуда у свету. Република Србија није изузета из ове проблематике ни по ком основу и мора пратити светске трендове, како у погледу појавних облика ВТК, тако и у погледу примене адекватних мера супротстављања. Када су приоритети борбе против ВТК у питању, на првом месту је адекватна законска регулатива, у потпуности усклађена са савременим међународним стандардима. Република Србија је у обавези да донесе националну стратегију за борбу против високотехнолошког криминала и у складу са њом и акциони план за њено спровођење.. Та обавеза произилази из Преговарачких мерила за Поглавље 24 Правда, слобода, безбедност. На ту обавезу упозорила је Европска унија (у даљем тексту: ЕУ), јер је Република Србија ратификовала Конвенцију о високотехнолошком криминалу (сачињена у Будимпешти, енгл. Budapest Convention) 2009. године и позвала је Србију да додатно усклади своје законодавство са Директивом 2013/40/ЕУ о нападима на информационе системе. У циљу сагледавања ове проблематике у Републици Србији, у овом раду ће се указати на актуелне трндове ВТК у периоду 2013-2017. године.

Кључне речи: високотехнолошки криминал, Европска унија, интернет, рачунарски подаци, хакери, компјутерске преваре, Facebook

Увод

21 столеће је револуционарно обележила и нова информацијона технологија, и средства која су својом применом осигурала до тада незабележен индустријски напредак, нагли развој у свим сферама савременог друштва, како у економском тако и у свим другим сферама. Изузетан и посебан напредак остварен је на пољу информатизације која данас незаустављиво расте (Бабић,

* zvezdan.radojkovic@mup.gov.rs
** zskakavac@useens.net

2015: 7-8). ВТК, други назив за комјутерски криминалитет; кривична дела код којих се као објекат или средство извршења јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику; злоупотреба информационих технологија ради чињења кривичних дела при чијем се извршењу појављују елементи незаконитог коришћења интернета (Бошковић, 2015:64). У облати борбе против ВТК у Србији је најзначајнији помак учињен оснивањем специјализованих органа на нивоу тужилаштва, суда и полиције (Карин,&Ануцојић, 2016:188).

Високотехнолошки криминал све више долази до изражаја свуда у свету и захтева масимално ангажовање безбедносних служби на његовом идентификовању, спречавању и сузбијању. Уосталом, на то указује број деликата из ове области који из године у годину континуирано расте скоро свуда у свету. Из актуелних статистичких података очигледно је да је слична ситуација и у Републици Србији.

Пре него што се ближе прикажу актуелни трендови из ове области, није на одмет указати и на нека савремена кретања у погледу коришћења савремених информационих технологија у свакодневном животу. Тако на пример, број корисника интернета како на глобалном нивоу, тако и у Републици Србији је у константном порасту. Доступни регистровани статистички подаци1 говоре да је у 2007. години 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 ИКТ 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 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 16-24 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 Србији, наспрам просечних 3,3 сата у Западној Европи. Истраживања показују и да се 62% старијих основаца и 84% средњошколаца бар једном се током го-

1 Доступни статистички подаци којима располаже МУП Републике Србије.

дину 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 при чему је најпопуларнији „Facebook". Тако на пример, у јуну 2016. године, у Србији је било укупно 4.758.861. корисника Интернета 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 (близу 2 милијарде) него WhatsUp (900.000.000), Twitter (328.000.000) и Instagram (400.000.000) заједно.

Статистичке базе података

У Републици Србији статистику ВТК прате бројне службе и институције и о томе су установиле одговарајуће 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* подаци о кривичним делима, укључујући и кривична дела високотехнолошког криминала, евидентирају се 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.

Управа за спречавање прања новца, која је организациона везана за *Министарство финансија*, располаже базама готовинских и сумњивих трансакција 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 ком-

пјутеризовани транзитни 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 тренутно води Регистар сертификационих тела за издавање квалификованих електронских сертификата и Регистар издавалаца временског жига у Републици Србији. Ступањем на снагу подзаконских аката.

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), ажурирање се врши на годишњем нивоу.

Актуелни статистички трендови у области ВТК2

Ради сагледавања актуелне проблематике ВТК у Републици Србији, неопходно је осврнути се на званичне статистичке податке надлежних државних органа и служби у претходном периоду.

Према подацима *Посебног одељења за борбу против високотехнолошког криминала Вишег јавног тужилаштва у Београду* 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 31.12.2017. године приказан је у Табели 1.

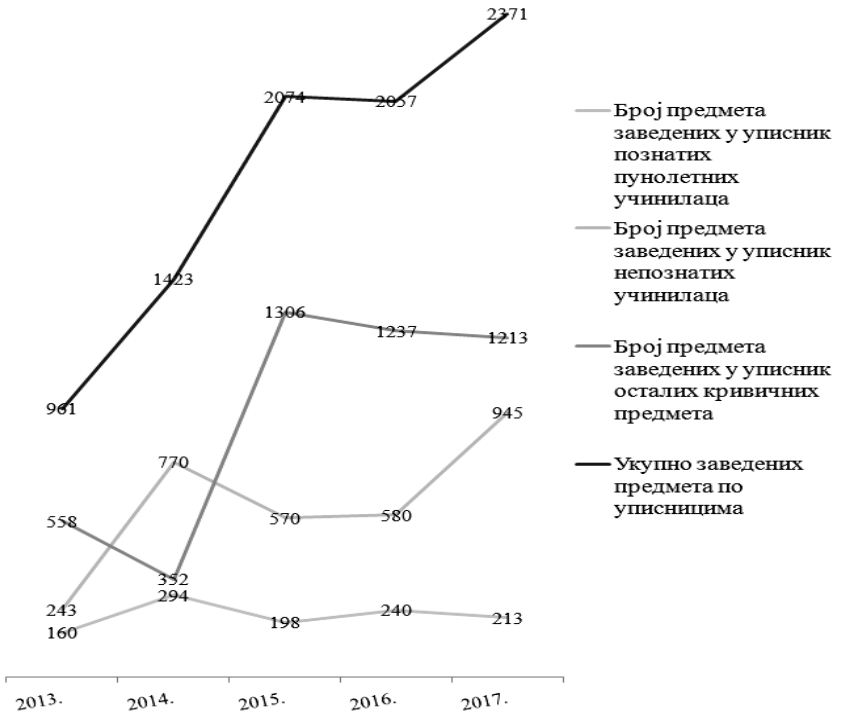
2 Стратешка процена јавне безбедности

Табела 1. *Преглед броја предмета Посебног тужилаштва за високотехнолошки криминал за период 2013-2017. 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%

Кретање ВТК у Републици Србији у задњих пет година (2013-2017.) приказано је на Графикону 1.

Графикон 1. *Кретање броја предмета из области БТК за период 2013-2017. године*



Из наведеног прегледа Посебног тужилаштва за високотехнолошки криминал (Табела 1. и Графикон 1.) видљиво је да је број предмета заведених у уписник како познатих пунолетних учинилаца, тако и непознатих учинилаца, у периоду 2006 – 2017. године , у сталном порасту, што указује на сву озбиљност ове појаве. У периоду од 01.01.2013. до 31.12.2017. 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.3 У питању су следећа кривична дела:

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

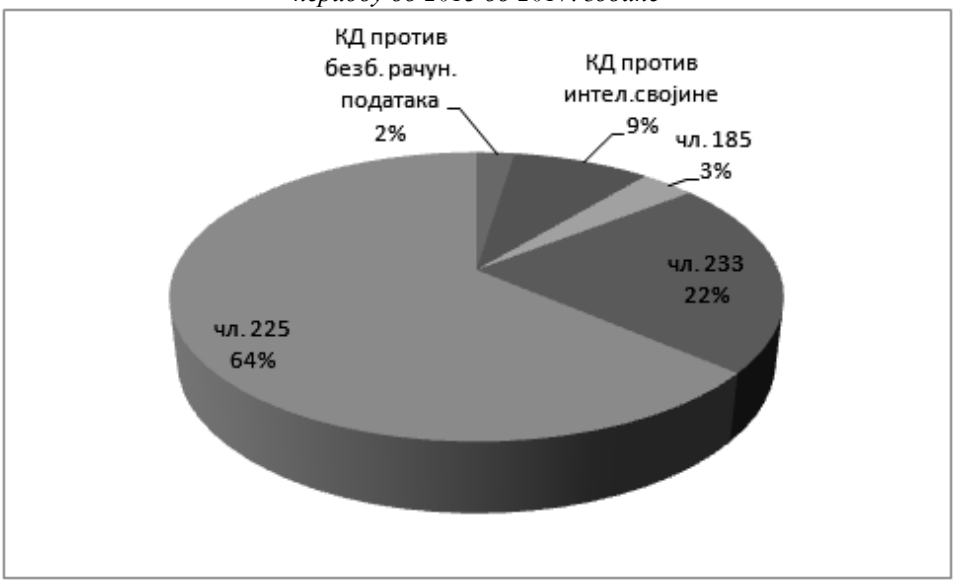
Кривична дела против интелектуалне својине - укупно 328 кривичних дела и то: повреда моралних права аутора и интерпретатора из чл. 198 КЗ (1 или 0,3%), неовлашћено искоришћавање ауторског дела или предмета сродног права из чл. 199 КЗ (316 или 96,3%), повреда проналазачевог права из чл. 201 КЗ (1 или 0,3%) и неовлашћено коришћење туђег дизајна из чл. 202 КЗ (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 чл. 185 ст. 4 КЗ (128 или 3,8%), искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу из чл. 185б КЗ (14 или 0,4%), фалсификовање и злоупотреба платних картица из чл. 225 КЗ (2.412 или 70,8%), прављење, набављање и давање другом средстава за фалсификовање из чл. 227 ст. 2 КЗ (18 или 0,5), неовлашћена употреба туђег пословног имена и друге посебне ознаке робе или услуга из чл. 233 КЗ (827 или 24,3%), одавање пословне тајне из чл. 240 КЗ (6 или 0,2%).

Структура извршених кривичних дела у периоду од 2013 до 2017. године приказана је на Графикону 2.

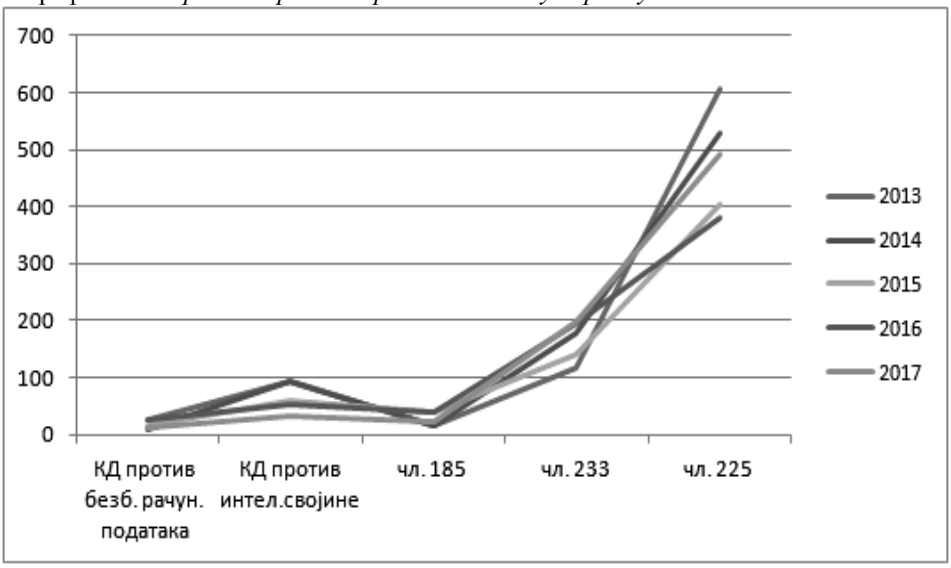
3 Евиденција МУП-а за период 2013-2017. године.

Графикон 2. *Структура извршених кривичних дела у периоду од 2013 до 2017. године*



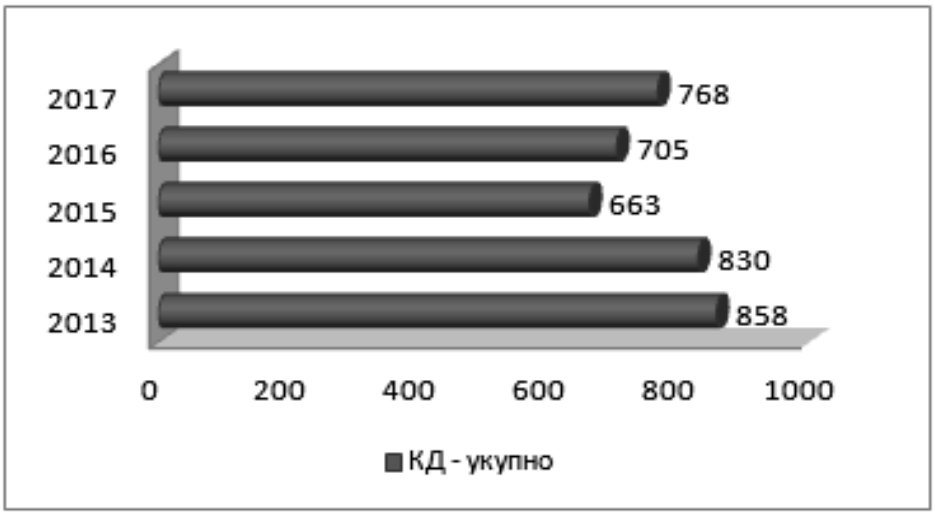
Тренд извршења кривичних дела у периоду од 2013 до 2017. године приказан је на графикону 3.

Графикон 3. *Тренд извршења кривичних дела у периоду од 2013 до 2017. године*



Укупан број извршених кривичних дела ВТК по годинама од 2013 до 2017. Године приказан је на графикону 4.

Графикон 4. *Укупан број извршених кривичних дела ВТК по годинама од 2013 до 2017. године*



Одељење за сузбијање високотехнолошког криминала, Службе за борбу против организованог криминала, Управа криминалистичке полиције 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 приказан је на графикону 5.

Графикон 5. *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.

Актуелни 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 (ИКТ) 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 шемама 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 емотивне шеме подигне новац који наводно у држави где се партнер налази није могуће подићи из одређених разлога. Уплате се најчешће врше преко Western Union-a i MoneyGram-a. Дестинације где се новац упућује најчешће су државе са подручја Африке, али и Велике Британије, Шпаније и др.

На територији Републике Србије у порасту су 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 прибављали 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.

Наручивање робе путем интернета вишеструко се повећало доласком *Pay-Pal-a* у Србију. У мањем броју случајева. 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, Холандија, 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.

Што се тиче кривичних дела против безбедности рачунарских података, у структури доминирају 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.

У проблематици ВТК све су присутније и нове технологије као што су *IoT*, *Cloud* рачунарство, *BYOD* где извршиоци кривичних дела увиђају њихову предност 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.

Из године у годину, у све већој мери привредне субјекте широм света погађају напредне упорне претње (*Advance Persistent Threat*-APT). 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 материјал 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.

Извршиоци кривичних дела у мањем броју случајева 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 проб-

лем 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.

Последњих година у повећању је и 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 врбовање 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 активости.

Закључак

Имајући у виду актуелну проблематику ВТК како на глобалном нивоу тако и у Републици Србији и тенденцију сталног повећања броја деликата из ове области, неопходно је плански предузети читав низ активности и мера на ниво државе како би се успешно супротставили овој појави. 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 контек-

сту тенденције брзог развоја и коришћења ИКТ 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.

Све досадашње анализедомаћег и међународног нормативног оквира показале су 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 ВТК. С тим у вези неопходно је изменити Правилнике 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. С тим у вези, 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;

Врло је значајно спроводити читав низ превентивних активности са циљем јачања свести грађана, као и органа власти о могућностима злоупотребе информационо-комуникационих технологија, мобилних телефона, Интренета 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 МУП, 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).

Литература:

1. Babić, Vladica (2015). *Sajber terorizam*, Grafid, d.o.o. Banja Luka.
2. Bošković, Milo (2015). *Kriminološki leksikon*, Matica srpska, Novi Sad.
3. Kaurin, Tanja, Anucojić, Dragan (2016). *Pravna informatika*, Fakultet za pravne i poslovne studije dr Lazar Vtkatić, Novi Sad.
4. Krivični zakonik „*Sl. glasnikRS*“, br. 85/2005 – ispr.., 107/2005 – ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 i 94/2016.
5. Statistički podaci MUP-a Republike Srbije o visokotehnološkom kriminalu.
6. Statistički podaci Posebnog tužilaštva Republike Srbije o visokotehnološkom kriminalu.

CURRENT TRENDS IN HIGH TECH CRIME IN THE REPUBLIC OF SERBIA

Summary: High tech crime (hereinafter: HTC) is becoming ever more conspicuous and not only at the global level. The number of offenses has been growing continuously, from one year to the next, in almost all parts of the world. The Republic of Serbia is not exempt from these issues, on any grounds, and must follow global trends both in terms of the manifestation of HTC and the application of adequate countermeasures. When it comes to the priorities in the fight against HTC, the first place belongs to adequate legislation fully compliant with modern international standards. Serbia is required to adopt a national strategy for combating high tech crime and, in compliance with the same, an action plan for its implementation. This commitment stems from the Negotiating Criteria for Chapter 24 of Justice, Freedom, Security. The European Union warned of this obligation (hereinafter: EU), as Serbia ratified the Convention on High Tech Crime (compiled in Budapest, Budapest Convention) in 2009 and invited Serbia to further align its legislation with the 2013/40/EU Directive on attacks against information systems. In order to examine this issue in Serbia, this paper will address current trends in HTC during the 2013-2017 period.

Key words: High tech crime, the European Union, the Internet, computer data, hackers, computer fraud, Facebook