Часопис из области економије менаџмента и информатике
Година 2017, волумен 8, број 1, стр. 41-53

Journal of Economics, Management and Informatics
Year 2017, Volume 8, Number 1, pp. 41-53

Стручни рад/ Professional paper

УДК/UDC: 343.533::004(497.11)

DOI: 10.5937/bizinfo1701041P

КРИВИЧНОПРАВНА ЗАШТИТА БЕЗБЕДНОСТИ РАЧУНАРСКИХ ПОДАТАКА

PROTECTION OF SECURITY OF COMPUTER DATA IN CRIMINAL LAW

Мирјана Павловић[1]
Висока школа струковних студија за криминалистику и безбедност, Ниш

Данијела Тошић[2]
Предшколска установа „Лане“ Дољевац

Резиме: *Компјутер је једна од најзначајнијих тековина технолошког развоја на крају 20. века. Не постоји област људског деловања у којој рачунари нису нашли своју примену. Али, поред предности које рачунар носи са собом, убрзо је постао и средство злоупотребе. Тако настаје рачунарски криминалитет као посебан и специфичан облик криминалитета. Постоји више начина заштите безбедности рачунарских података. У раду аутори приказују један од видова заштите безбедности рачунарских података. У питању је кривичноправна заштита, која представља део казненоправне заштите. Аутори анализирају законска решења и примену тих решења у пракси.*

Кључне речи: *рачунарски подаци, заштита, кривично дело, компјутерски криминалитет*

Abstract: *Computer is one of the most significant achievements of technological development at the end of the 20th century. There isn't part of*

[1]mirjana_985@yahoo.com
[2]nela985@yahoo.com

human life in which computers have found not their application. But, despite the fact that the computer has great advantages, it has quickly become a means of abuse. This is the beginning of computer crime as a special and specific form of crime. There are a several ways to protect the security of computer data. The authors describe only one system to protect the security of computer data in this paper. It is criminal protection. The authors analyze the legal solution and implement those solutions into practice.
Key words: *computer data, protection, criminal act, syber crime*

1. УВОД

Први рачунар настао је као резултат вишевековне човекове тежње да олакша процес рачунања и учини га тачнијим. То су заправо биле машине, које представљају претече рачунара и служиле су искључиво за рачунање. Алан Тјуринг, енглески математичар, логичар и криптоаналитичар сматра се оцем модерног рачунарства. Први рачунар, назван ENIAC, пуштен је у експериментални погон фебруара 1944. године, да би коначно био завршен тек 1946. године. Његова је основна функција била да у ратне сврхе израчунава путање артиљеријских граната, а његова израда је коштала око 400.000 тадашњих долара, што је у то време била значајна сума, међутим он је оправдао ту цену, јер је могао да израчуна путању гранате, пет секунди пре него што погоди мету (Алексић, Шкулић, 2004). Временом се рачунари усавршавају па данас постоје различити модели рачунара. Користи их огроман број људи, а познавање рада на рачунару представља општу писменост. Према томе, рачунар је једно од најзначајнијих открића у историји човечанства.

Појава рачунара и његов развој довели су до изузетног напретка људског друштва. Готово да нема области у којој рачунари нису нашли своју примену у савременом друштву. Међутим, данас скоро да не постоји техничко и технолошко достигнуће које није наишло на неких вид злоупотребе. Нажалост, свакодневно се злоупотребљавају и рачунари што је изазвало и одговарајућу реакцију државе. Држава, односно друштво на злоупотребу рачунара реагују различитим превентивним и репресивним мерама. Превентивне мере усмерене су на отклањање узрока криминалитета, док су репресивне мере кривичноправне мере које се јављају као одговор друштва на вршење забрањених дела. Држава унапред одређује кажњива понашања и кривичноправне мере које се изричу учиниоцима таквих понашања. Један начин заштите од злоупотребе рачунара је кривичноправна заштита. Кривичноправна заштита рачунарских података подразумева предвиђање кривичних дела против безбедности рачунарских података у Кривичном законику Републике Србије. Правни оквир државних

органа надлежних за борбу против високотехнолошког криминала уређен је Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала. Овим Законом уређено је образовање, организација, надлежност и овлашћења појединих организационих јединица државних органа ради откривања, кривичног гоњења и суђења за кривична дела високотехнолошког криминала.

2. КОМПЈУТЕРСКИ КРИМИНАЛИТЕТ

2.1. ПОЈАМ КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА

Велики напредак технологије условио је стварање нових начина за вршење традиционалних кривичних дела. Компјутерска техника је најсавршенији начин чувања, преношења и сортирања података. Истовремено, то је и најдалекосежнији начин који отвара пут многим злоупотребама. Према томе, ради се о области у којој постоји повећана могућност злоупотребе у случајевима све веће примене компјутеризованих информационих система с једне стране, а с друге стране у неадекватности односно недовољности постојећих законских прописа на новонастале ситуације (Здравковић, 2012). Врло брзо компјутери су постали средство и начин које користе појединци, групе, али и организације за вршење различитих кривичних дела.

У литератури се користе различити синоними за појам компјутерски криминалитет, и то: рачунарски криминалитет, cyber криминалитет, информатички криминалитет, злоупотреба компјутера. За овај појам криминалитета на даље ћемо се служити термином компјутерски криминалитет. У борби против компјутерског криминалитета најпре, је било потребно дефинисати овај појам. Литература не познаје једну јединствену дефиницију појма компјутерски криминалитет. Према једном схватању компјутерски криминалитет дефинише се у: ужем и ширем смислу. Компјутерски криминалитет у ужем смислу представља свако незаконито понашање усмерено на електронске операције, сигурност компјутерских система и података који се у њима обрађују, док компјутерски криминалитет у ширем смислу јесте свако незаконито понашање везано за или у односу на компјутерски систем и мрежу, укључујући и такав криминал какво је назаконито поседовање, нуђење и дистрибуција информација преко компјутерских система и мрежа (Зорнић, 2010). У криминолошкој литератури постоји схватање да је компјутерски криминалитет део привредног криминалитета, али и схватање да се ради о имовинском криминалитету. Компјутерски криминалитет обухвата криминалитет везан за компјутерске мреже (Internet или syber криминалитет) где се компјутерске мреже користе као циљ напада (нападају се сервиси, функције и садржаји који се налазе на

мрежи); средство или алат (online продаја сексуалних услуга, људских органа, жена и деце за проституцију, производња и дистрибуција недозвољених штетних садржаја, као што су дечја порнографија, верске секте, расистичке, нацистичке и сличне идеје) и као окружење у коме се напади реализују (коришћење мреже за прикривање криминалних радњи) (Константиновић и др., 2009).

Компјутерски криминалитет обухвата злоупотребе које се односе на угрожавање интегритета, доступности или поверљивости рачунарских мрежа и телекомуникационих система и са њима повезаних података или се односе на употребу таквих мрежа и система за извршавање традиционалних кривичних дела (Писарић, 2011). То је свеукупност различитих облика, видова и форми испољавања противправних понашања управљених против безбедности рачунарских података, информационих и компјутерских система у целини или њихових појединих делова на различите начине и различитим средствима у намери да се себи или другом прибави каква корист (имовинске или неимовинске природе) или да се другоме нанесе каква штета (Ђурђић, Јовашевић, 2006, стр. 204). Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала под појмом високотехнолошки криминал подразумева се вршење кривичних дела код којих се као објект или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци као и њихови производи у материјалном или електронском облику. Иако постоји много различитих дефиниција компјутерског криминалитета, најважније је указати на три основна елемента дефиниције овог појма, а то су: средства извршења (рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци) начин извршења (злоупотреба рачунара и других средстава) и последица деловања (имовинска, неимовинска или комбинована).

2.2. КАРАКТЕРИСТИКЕ КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА

Компјутерски криминалитет по својим карактеристикама издваја се од осталих облика испољавања криминалитета. Као основне карактеристике компјутерског криминалитета наводе се: велика динамичност, константно ширење на нове области, тежина последица које наступају вршењем компјутерских кривичних дела, велика тамна бројка, отежано откривање и доказивање, специфичан профил учиниоца, велике могућности за прикривање извршеног кривичног дела (Матијашевић, Игњатовић, 2010, стр. 853).

Тежња ка модернизацији, усавршавању постојеће технологије и све већој примени електронског банкарства ствара погодно тло и за већу злоупотребу личних података. Штета која настаје извршењем ових кривичних дела најчешће је материјална, али је могуће и да се услед приказивања нечијих личних података наруши лични углед. Такође, злоупотреба података фирми представља лошу рекламу за саму фирму која није у могућности да заштити своје податке, али и податке својих клијената. Због тога фирме избегавају пријављивање дела што доприноси повећању тамне бројке криминалитета.

Компјутерски криминалитет карактерише и специфичан профил учиниоца. Као извршиоци дела јављају се лица која поседују одговарајућа знања из области информационих технологија. Што су знања која извршилац поседује већа, то је мања могућност откривања дела.

Једна од карактеристика компјутерског криминалитета јесте и чињеница да извршилац и жртва уопште не морају да буду на истом месту у време извршења дела, чак не морају да буду ни у истој држави. Најпознатији облик компјутерског криминалитета јесте и тзв. „нигеријска превара“ или „превара 419“. Назив је добила по држави у којој се и појавила 80-их година двадесетог века. Овај вид преваре извршен је и у нашој земљи и то 2008. и 2009. године када је пријављено девет случајева „нигеријске преваре“. Као оштећени појавила су се физичка лица, али и фирме, а штета се процењује на преко 60.000 еура. (Урошевић, 2009, стр. 8). „Нигеријска превара“ започиње слањем тзв. спам поруке (нежељена порука). Порука се шаље већем броју лица. Написана је тако да лице које је прими има утисак да се односи на њега лично. У порукама се жртва обавештава да је наследила неки новац из иностранства и да је потребно оставити број рачуна како би жртви новац био пребачен. На ове поруке не одговарају сви, али они који одговоре потенцијалне су жртве ових превараната. Први облик „нигеријске преваре“ био је обавештење да је неко лице зарадило огромну своту новца, али да због ситуације у земљи није у могућности да тај новац изнесе из земље, због чега тражи помоћ жртве да користи њен рачун, а за узврат ће жртви дати 20% зарађеног новца.

За извршење ове преваре учиниоцима осим знања нису потребна готово никаква средства. Интернет адресе потенцијалних жртава лако се могу набавити (пријављивањем жртве на бесплатне интернет новине, вести и сл.), спам поруке шаљу се углавном из кафеа у којима је доступан бесплатан интернет, што је и један од разлога зашто се теже проналазе извршиоци ових дела. Показало се да ни један систем заштите није савршен, јер је, према неким проценама у САД просечна штета од

компјутерског криминалитета од сто до триста милиона долара годишње (Константиновић, и др. 2003, стр. 161).

3. КРИВИЧНА ДЕЛА ПРОТИВ БЕЗБЕДНОСТИ РАЧУНАРСКИХ ПОДАТАКА

Кривична дела против безбедности рачунарских података су нова кривична дела која улазе у тзв. високотехнолошки или компјутерски криминалитет, или syber криминалитет. (Чејовић, Кулић, 2014, стр. 504.). Ова дела по први пут у домаће кривично законодавство уведена су 2003. године у циљу заштите и обезбеђивања рачунарских података. Законом о изменама и допунама Кривичног закона Републике Србије (КЗ РС, 2003) из априла 2003. године у кривично право Државне заједнице Србије и Црне Горе уведено је неколико кривичних дела која припадају компјутерском криминалитету. И то: неовлашћено коришћење рачунара и рачунарске мреже (чл. 186а), рачунарска саботажа (чл. 186б), прављење и уношење рачунарских вируса (чл. 186 в), рачунарска превара (чл. 186г), ометање функционисања електронске обраде и преноса података и рачунарске мреже (чл.186д), неовлашћени приступ заштићеном рачунару или рачунарској мрежи (чл. 186ђ) и спречавање и ограничавање приступа јавној рачунарској мрежи (чл. 186е). На тај начин наша држава се по први пут супротставила овом новом изузетно опасном облику криминалитета.

Важећи Кривични законик Републике Србије у глави 27. прописује кривична дела против безбедности рачунарских података. И то: оштећење рачунарских података и програма (чл. 298), рачунарска саботажа (чл. 299), прављење и уношење рачунарских вируса (чл. 300), рачунарска превара (чл. 301), неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (чл. 302), спречавање и ограничавање приступа јавној рачунарској мрежи (чл. 303), неовлашћено коришћење рачунара и рачунарске мреже (чл. 304) и прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података (чл. 304а). Објект заштите ових кривичних дела је безбедност рачунарских података. Рачунарски податак је свако представљање чињеница, информација или концепта у облику који је подесан за њихову обраду у рачунарском систему, укључујући и одговарајући рачунарски програм на основу кога рачунарски систем обавља своју функцију, док се под рачунарским програмом сматра уређени скуп наредби који служе за управљање радом рачунара, као и за решавање одређеног задатка помоћу рачунара. Радња извршења рачунарских кривичних дела је злоупотреба рачунара на различите начине.

Оштећење рачунарских података и програма (чл. 298 КЗ РС) је кривично дело које има један основни и два тежа облика. Основни облик дела састоји се у неовлашћеном брисању, измени, оштети, прикривању или на други начин чињењу неупотребљивим рачунарског податка или програма. Објект заштите је безбедност рачунарског податка, а објект напада рачунарски податак или програм. Радња извршења овог кривичног дела је брисање, измена, оштета, прикривање или на други начин чињење неупотребљивим рачунарског податка или програма. Извршилац овог дела може бити свако лице. Први тежи облик дела постоји ако је предузетом радњом проузрокована штета која прелази 45.000 динара, а други тежи облик постоји ако је извршењем радње наступила штета која прелази 1.500.000 динара. За ово кривично дело Законик прописује новчану казну или казну затвора и обавезно изрицање мере безбедности одузимања предмета.

Рачунарска саботажа (чл. 299 КЗ РС) је кривично дело које чини лице које унесе, уништи, избрише, измени, оштети, прикрије или на други начин учини неупотребљивим рачунарски податак или програм или уништи или оштети рачунар или други уређај за електронску обраду података и пренос података са намером да онемогући или знатно омете поступак електронске обраде и пренос података који су од значаја за државне органе, јавне службе, установе, предузећа или друге субјекте. Код овог кривичног дела важно је да уређаји и средства који су објект заштите припадају државном органу, установи, предузећу или другом субјекту. За ово кривично дело прописана је казна затвора од шест месеци до пет година.

Прављење и уношење рачунарских вируса (чл. 300 КЗ РС) је дело које се састоји у прављењу рачунарског вируса у намери његовог уношења у туђ рачунар или рачунарску мрежу. Рачунарски вирус је 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. Тежи облик овог дела постоји ако је уношењем вируса причињена штета. Кривични законик за ово дело прописује новчану казну или казну затвора и меру одузимања предмета.

Рачунарска превара (чл. 301 КЗ РС) је дело које се састоји у уношењу нетачног податка, пропуштању уношења тачног податка или на други начин прикривању или лажном приказивању података чиме се утиче на резултат електронске обраде података и пренос података у намери да се себи или другом прибави противправна имовинска корист и тиме проузрокује штета другом лицу. Тежи облици овог дела постоје ако је

прибављена противправна имовинска корист која прелази износ од 45.000 динара, односно ако прелази износ од 1.500.000 динара. Законодавац предвиђа и један привилеговани облик овог дела, који постоји ако је радња извршења учињена само да се други оштети.

Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (чл. 302 КЗ РС) је дело које се врши неовлашћеним укључивањем у рачунар или рачунарску мрежу или неовлашћеном приступу електронској бази података кршењем мера заштите. Извршилац овог дела може бити свако лице које има одговарајућа знања из области заштите рачунара. Тежи облици постоје у случају снимања или употребе података који су добијени радњом извршења основног облика, односно проузроковањем застоја или озбиљног поремећаја функционисања електронске обраде података или наступањем других тешких последица. Појам тешке последице не дефинише КЗ РС па је то питање које ће у поступку решавати надлежни суд.

Чланом 303. КЗ РС предвиђено је кривично дело спречавања и ограничавања приступа јавној рачунарској мрежи. Ради се о делу које врши лице које неовлашћено спречава или омета приступ јавној рачунарској мрежи. Тежи облик дела постоји ако радњу основног облика врши службено лице у вршењу службе. Прописана је новчана казна или казна затвора.

Неовлашћено коришћење рачунара и рачунарске мреже (чл. 304. КЗ РС) је дело које се састоји у неовлашћеном коришћењу рачунарске услуге или рачунарске мреже у намери да се себи или другом прибави противправна имовинска корист. Извршилац овог дела може бити свако лице. За разлику од осталих кривичних дела против безбедности рачунарских података за која се поступак покреће и води по службеној дужности, за ово кривично дело поступак се покреће приватном тужбом.

И на крају, прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података је дело које врши лице које поседује, прави, набавља, продаје или даје другом на употребу рачунаре, рачунарске системе, рачунарске податке и програме ради извршења појединих кривичних дела против безбедности рачунарских података.

4. НАДЛЕЖНОСТ ДРЖАВНИХ ОРГАНА ЗА БОРБУ ПРОТИВ КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА

Један од показатеља озбиљности овог вида криминалитета који сваког дана поприма све шире размере, али и намере државе да томе стане на пут, јесте и доношење закона којим се оснива посебно тужилаштво за борбу против високотехнолошког криминала. Наиме, 2005. године донет је Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала. Овај закон промењен је 2009. године повећањем примерака ауторских дела са 500 на 2000 и повећањем настале материјалне штете са 850.000 на 1.000.000 динара. Такође, у члану 3 додат је нови став 3 где је одређена примена овог закона и на 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 сматрати кривичним делима високотехнолошког криминала, у складу са чланом 2.став 1.овог закона.

Законом се уређује образовање, организација, надлежност и овлашћења посебних организационих јединица државних органа ради откривања, кривичног гоњења и суђења за кривична дела одређена овим законом, а то су кривична дела против безбедности рачунарских података одређена Кривичним закоником; кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења кривичних 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 2000 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 употребљених средстава могу сматрати кривичним делима високотехнолошког криминала.

Закон дефинише високотехнолошки криминал као 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 материјалног и електронском облику (под којима се подразумевају рачунарски програми и ауторска дела која се могу употребити у електронском облику).

За поступање код наведених кривичних дела, Законом је одређено као надлежно Више јавно тужилаштво у Београду и то за целу територију Републике Србије. У оквиру овог тужилаштва образовано је посебно

одељење за борбу против високотехнолошког криминала. Радом овог тужилаштва руководи и посебан тужилац кога поставља Републички јавни тужилац из реда заменика јавних тужилаца који испуњавају услове за избор за заменика вишег јавног тужиоца, уз писмену сагласност лица које се поставља, при чему предност имају заменици јавних тужилаца који поседују посебна знања из области информатичких технологија. Посебни тужилац се у случају када дође до сазнања да се у једном кривичном предмету ради о делима предвиђеним овим законом, обраћа у писменој форми Републичком јавном тужиоцу захтевајући да му се пренесе или повери надлежност.

Поред посебног тужилаштва овим законом предвиђа се и образовање службе за борбу против високотехнолошког криминала у оквиру министарства надлежног за унутрашње послове, а ради обављања послова органа унутрашњих послова у вези са кривичним делима одређеним овим законом.

Суд надлежан за поступање код ових кривичних дела у првом степену је Виши суд у Београду, а у другом Апелациони суд у Београду. У оквиру Вишег суда у Београду образовано је Одељење за борбу против високотехнолошког криминала. Судије у овом Одељењу распоређују се из реда судија тог суда уз њихову сагласност, а распоређује их председник Вишег суда у Београду. Као и код тужиоца и код судија предност имају судије које поседују посебна знања из области информатичких технологија.

5. СТАТИСТИЧКИ ПОДАЦИ О КРИВИЧНИМ ДЕЛИМА ПРОТИВ БЕЗБЕДНОСТИ РАЧУНАРСКИХ ПОДАТАКА

Убрзани развој рачунара, рачунарских и информационих технологија довео је до огромних предности у свим сферама живота. Упоредо са свим позитивним странама овог убрзаног напретка долази и до многих злоупотреба. Република Србија је на ове изазове реаговала одређеним мерама. Извршене су одговарајуће измене Кривичног законика, Законика о кривичном поступку, донет је Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала. У овом делу рада, бавимо се анализом статистичких података Републичког завода за статистику који се односе на кривична дела против безбедности рачунарских података.

Просторна граница истраживања односи се на територију Републике Србије, док је анализиран временски период од 2006. године до 2015. године. Предмет истраживања је број пријављених и број осуђених учинилаца кривичних дела против безбедности рачунарских података,

као и кривичне санкције које су изрицане осуђеним лицима. Под појмом пријављени учинилац подразумева се лице против кога су поступак по кривичној пријави и претходни поступак завршени одлуком којом је: пријава одбачена, прекинута истрага, обустављена истрага или је подигнута оптужница; односно непознато лице против кога је поднета кривична пријава јавном тужилаштву, али учинилац није откривен. Под појмом осуђено лице подразумева се лице које је проглашено кривим и изречена му је одговарајућа кривична санкција. Предмет истраживања су само пунолетни учиниоци кривичних дела.

Анализом свих података за период од 2006. до 2015. године запажамо изузетно мали број и пријављених и осуђених учинилаца кривичних дела против безбедности рачунарских података. Највећи број пријављених учинилаца забележен је 2009. године, и то 45 учинилаца. Највећи проценат пријављених кривичних дела чине: рачунарска превара, оштећење рачунарских програма и података, рачунарска саботажа и неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података.

У структури осуђених учинилаца кривичних дела за анализирани период број учинилаца кривичних дела против безбедности рачунарских података је незнатан. По годинама овај број не прелази 10 осуђених лица. У највећем броју случајева учиниоцима ових кривичних дела изрицана је условна осуда, осим за неколико осуђених лица којима је изречена казна затвора. Једина новчана казна изречена је 2011. године за кривично дело оштећење рачунарских података и програма. Овако мали проценат пријављених и осуђених учинилаца кривичних дела против безбедности рачунарских података не сме нас заварати, јер не указује на мали број извршених кривичних дела, већ на тешко откривање ових кривичних дела и њихових учинилаца. Због тога је потребно посебну пажњу усмерити на ове чињенице у циљу унапређења и побољшавања услова за откривање дела и учинилаца.

6. ЗАКЉУЧАК

Иако држава улаже напоре у циљу пружања одговарајуће заштите у борби против компјутерског криминалитета, још увек та заштита није задовољавајућа. Висока „тамна бројка“ требало би да забрињава не само законодавце, већ и медије који би овом виду криминалитета морали да пруже одговарајући медијски простор у циљу упознавања грађана са могућностима, начинима извршења, али и начинима на које грађани могу да се заштите. Поред имовинске штете, треба имати у виду и чињеницу да извршењем дела наступају и друге последице, као и чињеницу да је сваким даном све већи број дела која се могу извршити

употребом компјутера. Коришћење кафеа ради бесплатног интернета, непријављивање дела од стране жртве, посебна знања потребна како за извршење тако и за откривање дела, отежавају борбу против све присутнијег компјутерског криминалитета. И управо из тог разлога држава не треба да се задовољи само доношењем закона, већ свакодневно морају бити предузимане активности у борби против овог вида криминалитета, али и заштите грађана.

РЕФЕРЕНЦЕ

1. Алексић, Ж., Шкулић, М., 2004. *Криминалистика,* Београд: Досије
2. *Закон о изменама и допунама Кривичног закона Републике Србије* 2003. (Службени гласник Републике Србије, бр. 39/03). Београд: Службени гласник Републике Србије
3. *Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала* 2005. (Службени гласник РС, бр. 61/05, 104/09). Београд: Службени гласник Републике Србије
4. Здравковић, Љ., 2012, *Криминологија,* Ниш: Висока школа струковних студија за криминалистику и безбедност.
5. Zornić, Dž., 2010. Kompjuterski kriminal, [online] *Naučno stručno savetovanje Ziteh 2010.* Доступно на:<https://singipedia.singidunum.ac.rs/izdanje/40128-kompjuterski-kriminal> [Приступ 10 март 2017]
6. Ђурђић, В., Јовашевић, Д., 2006. *Кривично право, посебни део,* Београд: Номос
7. Константиновић, Вилић, С., Ристановић, Николић, В. 2003. *Криминологија,* Ниш: Правни факултет у Нишу, Центар за публикације
8. Константиновић, Вилић, С., Ристановић, Николић, В., Костић, М, 2009. *Криминологија,* Ниш: Пеликан принт
9. *Кривични законик Републике Србије* 2005. (Службени гласник РС, бр. 85/05, 88/05, 107/05, 72/09, 111/09, 121/12, 104/13 и 108/14). Београд: Службени гласник Републике Србије
10. Матијашевић, Ј., Игњатијевић, С., 2010. *Компјутерски криминалитет у правној теорији, појам, карактеристике, последице,* Јахорина: Инфотех
11. Писарић, М., 2011. Стање и тенденције у супротстављању компјутерском криминалу на Европском нивоу. *Зборник радова Правног факултета, Нови Сад* 45 (1) стр. 487-505.
12. Републички завод за статистику, 2017. [online] Доступно на: <http://stat.gov.rs/WebSite/Default.aspx> [Приступ 17 март 2017]

13. Урошевић, В., 2009. „Нигеријска превара“ у Републици Србији. *Безбедност, Београд* 3/2009 стр. 1-12
14. Чејовић, Б., Кулић, М., 2014. *Кривично право,* Нови Сад: Универзитет Привредна академија, Правни факултет за привреду и правосуђе

Рад је примљен: 31.03.2017.
Прихваћен за објављивање: 07.04.2017.
Received: 31 March, 2017
Accepted: 09 April, 2017