Дарко Димовски, асистент
Правни факултет Универзитета у Нишу

UDK: 343.4:004

КОМПЈУТЕРСКИ КРИМИНАЛИТЕТ

Апстракт: *Аутор је у чланку одредио дефиницију компјутерског криминалитета. Предмет ширег интересовања аутора је међународноправни аспект борбе против компјутерског криминалитета, са посебним освртом на одредбе Конвенције о високотехнолошком криминалу. Како је компјутерски криминалитет појава од које није имуна ниједна држава, обрађене су одредбе домаћег законодавства које се односе на борбу против компјутерског криминала. У даљем тексту аутор је посветио посебну пажњу на појавне облике компјутерског криминалитета. Такође, дата су својства компјутерског криминалитета и компјутерских криминалаца..*

Кључне речи*: компјутерски криминалитет, карактеристике компјутерског криминалитета, појавни облици.*

Увод

Несумњиво је да је XX век био период великих открића у математици, физици, хемији, медицини, али и у области стварања и коришћења компјутера. Још је мање сумњиво да ће XXI век бити век велике експанзије употребе компјутера у свим областима људског друштва. Развој једне државе се мери, између осталог, и степеном компјутеризације државне управе и локалне самоуправе. Историја је показала да свако епохално откриће има, поред своје добре стране, и страну коју карактерише злоупотреба и вршење разних кривичних дела. Таква је ситуација и са компјутером и његовом применом. Процењује се да је годишња штета од компјутерског криминала у Републици Србији око 50 милиона долара[1] а у свету штета се процењује на 40 милијарди долара.[2]

Као година настанка првог компјутера узима се 1944. када је у експериментални рад пуштен компјутер под именом ENIAC.[3] Функција овог компјутера је била да у ратне сврхе израчунава путању артиљеријских граната. Са тадашњом ценом од невероватних 400.000 $, он је оправдао сврху свог постојања јер је успевао да израчуна балистичку путању артиљеријске гранате за двадесет пет секунди, пет секунди брже него што је њој требало да погоди мету.[4]

Развој компјутера и његових компоненти, као и њихов константан пад цена, довели су до тога да се компјутери данас доступни не само владама најмоћнијих држава у свету, већ да се они налазе у скоро сваком дому у свету. Данас није потребно посебно знање за употребу компјутера, јер је начин њиховог коришћења сведен на ниво просечног човека. На тај начин, повећан је број потенцијалних делинквената у области компјутерских технологија. Због тога су потребни велики

1 Видети: http://www.elitesecurity.org, приступ 15.2.2009. године

2 Видети: http://news.bbc.co.uk/hi/english/static/in_depth/uk/2001/life_of_crime/cybercrime.stm, приступ 22.2.2009. године

3 ''Он је могао да помножи 14 десетоцифрених бројева за једну секунду, док су данашњи квалитетнији компјутери у стању да у том времену помноже чак 1800 милијарди итих таквих бројева.'' Цитат према: Алексић, Ж., Шкулић, М., Криминалистика, Досије, Београд, 2004. година, страна 384

4 Цетинић, М., ''Компјутерска кривична дела и њихови појавни облици'', Правни живот, Удружење правника Србије, Београд, 1998. година, страна 259

финансијски, технолошки и људски ресурси који би заштитили компјутер као средство и циљ напада.

Појам компјутерског криминалитета

До једне јединствене и прихватљиве дефиниције компјутерског криминалитета тешко је доћи из неколико разлога. Врсте извршених кривичних дела која спадају у компјутерски криминалитет је изузетно велик, тако да их је немогуће обухватити једном јединственом дефиницијом. Како је реч о новом облику криминалног понашања, компјутерски криминалитет се још увек није искристалисао у односу на друге врсте криминалног понашања. Иако је у последње време повећан број држава које су донеле законе о борби против компјутерског криминалитета, кривичноправна наука и криминологија се не могу у одређивању компјутерског криминалитета ослањати на законску дефиницију. Једна од дефиниција компјутерског криминалитета би била да компјутерски криминалитет представља друштвеноопасну појаву за чије се остварење учинилац користи знањима компјутерске технологије, тако што се компјутерски систем схваћен у најширем смислу (хардвер, софтвер, њихово јединство; један компјутер или мрежа компјутера), користи као средство или као објекат криминалног напада или једно и друго.[5] Неки теоретичари употребљавају израз ‘’cyber crime’’ за означавање компјутерског криминалитета.[6]

Из дефиниције компјутерског криминалитета могу се уочити три елемента, која разликују компјутерски криминалитет од других облика криминалитета, а то су: 1. начин извршења, 2. средство извршења, 3.

5 Симоновић, Б., Криминалистика, Правни факултет у Крагујевцу, Крагујевац, 2004. година, страна 665

6 Неки писци дефинишу компјутерски криминалитет на следећи начин: ‘’Према једној дефиницији под компјутерским криминалитетом се подразумевају сва делинквентна понашања у којима се уређају за електронску обраду података користе као средство за постизање кажњивих радњи или као директан циљ кажњиве радње.’’ Цитат према: Константиновић Вилић, С., Николић Ристановић, В., Костић, М., Криминологија, ПЕЛИКАНТ ПРИНТ, Ниш, 2009. година, страна 181; ‘’Компјутерски криминалитет је сваки догађај везан за рачунарску технологију, који је проузроковао или могао проузроковати губитак за оштећеног, а учиниоцу донео или могао донети корист.’’ Цитат према: Алексић, Ж., Миловановић, З., Криминалистика, Партенон, Београд, 1994. година,страна 328

последици. Компјутер се као начин извршења кривичног дела може употребити као целовит *modus operandi* или се може употребити као сегмент извршеног кривичног дела. Компјутер као средство криминалног напада значи да се уз помоћ компјутера реализује криминална радња.[7] Компјутер може, поред тога што је основно средство за извршење компјутерског криминалитета, и помоћно средство за извршење разних других кривичних дела. Последица компјутерског криминалитета може се манифестовати и на самим компјутерима и интернет мрежи.

Међународноправни аспект компјутерског криминалитета

Како је компјутерски криминалитет област који заврређује пажњу не само једне државе, већ целе међународне заједнице, дошло је доношења међународних правила која су регулусала ову област. Уједињене нације су на Осмом конгресу за спречавање криминала, одржаном у Хавани 1990. године, донеле посебну Резолуцију у којој је константована потреба за инкриминисањем различитих злоупотреба. Њоме је државама чланицама дата обавеза да успоставе систем мера за спречавање различитих злоупотреба. Ова Резолуција је прихваћена и од Генералне скупштине УН.

Године 1985. ОЕБС је препоручио државама чланицама да инкриминишу различите злоупотребе везане за уношење мењање или брисање података или програма ради остваривања криминалних циљева.[8]

Исто тако, Савет Европе је 1989. године донео Препоруку Р(89)9 којом се захтева од држава чланица да инкриминишу дела која се налазе на посебној тзв. ‘’минималној листи’’. Препоруком је дата могућност државама чланицама да уведу у своја законодавства кривична дела и са тзв. ‘’опционе листе’’. Најзначајнији документ у овој области донет је 2001. године од стране Савета Европе и носи назив Конвенција о високотехнолошком криминалу.[9]

7 Симоновић, Б., op. cit., страна 666

8 Камбовски, В., Организиран криминал, 2-ри Август, Скопље, 2005. година, страна 309

9 ‘’Конвенција о високотехнолошком криминалу је била доступна за потписивање на церемонији у Будимпешти 23. новембра 2001. године, на којој је 30 држава потписало Конвенцију (од којих је 26 чланица Савета Европе и четири државе са

Такође, током 2002. године донет је Допунски протокол о криминализацији аката расизма и ксенофобије извршених преко компјутерских система. Конвенција о високотехнолошком криминалу представља први и једини мултилатерални уговор који регулише сарадњу и истрази и оптужењу у вези кривичних дела високотехнолошког криминала. Први део Конвенције носи назив ''Мере које ће се спровести на националном нивоу''. У овом делу се регулишу кривична дела која државе-потписнице треба да уведу у своје законодавство.[10] Кривична дела су у Конвенцији[11] одређена на такав начин да дају места државама-потписницама да ближе одреде биће кривичног дела. Други део Конвенције регулише процесна овлашћења државних органа приликом процесуирања кривичних дела компјутерског криминалитета, и сходно томе носи назив ''Процесно право''. На основу Конвенције државни органи имају право да заплене и прегледају сваки компјутер или носач података на коме се налазе, или сумњају да се могу налазити инкриминишући материјал. Такође, Конвенцијом је дато овлашћење државним органима да од провајдера траже да им достави податке који се односе на употребу кредитних картица и интернета да би се дошло до IP адресе. Оно што изазива велику расправу јесте и овлашћење државних органа да врше прислушкивање електронских комуникација. Како компјутерски криминал превазилази границе једне државе, нужно је постојање сарадње између држава ради његовог сузбијања. Због тога трећи део Конвенције регулише сарадњи држава на размени информација које се тичу извршења кривичног дела које регулише Конвенција. Конвенцијом је предвиђена могућност екстрадиције извршилаца овог кривичног дела између држава-потписница.

Једна од главних замерки Конвенцији је непостојање одредбе која би предвиђала обавезу државама-потписницама да оснују посебне органе који би се бавили високотехнолошким криминалом. Међутим, у члану 35 Конвенције се предвиђа оснивање тзв. ''24/7 службе'' у свакој

статусом посматрача). Од тог времена, још држава је потписало Конвенцију.'' Цитат према: www.usdoj.gov/criminal/cybercrime, приступ 10.2.2009. године

10 ''Борба против организованог криминала у Србији'', Досије, Београд, 2008. година, страна 242

11 Република Србија је Конвенцију потписала, али је није ратификовала.

држави-потписници, која би била доступна сваког дана у недељи током целог дана, са циљем асистирања државним органима у току истраге или оптужењу високотехнолошког криминала.[12] ‘’Ратификовањем Конвенције ће се извршити хармонизација високотехнолошког криминалитета, нарочито у мање развијеним земљама које нису донеле одговарајуће законе о високотехнолошком криминалу. Од држава потписница се захтева да инкриминишу различита кривична дела, укључујући неовлашћени упад у мрежу, преваре, ослобађење различитих вируса, дечије порнографије и кршења ауторских права.’’[13]

Такође, органи Европске Уније се донели одговарајуће документе којим се регулише област компјутерског криминалитета. Тако је током Самита ЕУ 1999. године донета одлука којом се тражи од држава чланица да изврше унификацију кривичног права, па између осталог и кривична дела која се односе на компјутерски криминалитет. Године 2002. припремљен је предлог за доношење оквирне одлуке Савета, чији је циљ био заједничка активност у спречавању компјутерског криминала комплементарних са применом мера предвиђених у Конвенцији у високотехнолошком криминалу. На основу ове одлуке требао се донети јединствени национални приступ у државама чланицама у вези појмова ‘’електронска комуникацијска мрежа’’, ‘’компјутер’’, база података’’ и ‘’информациони систем’’.Одлуком је предвиђена одговорност правних лица.[14]

Кривично правни аспект компјутерског криминала

Кривичним закоником Републике Србије из 2006. године уведена су кривична дела против безбедности рачунарских података (глава XXVII). У кривична дела против рачунарских података спадају: оштећење рачунарских податак и програма (члан 298), рачунарска саботажа (члан 299), прављење и уношење рачунарских вируса (члан 300), рачунарска превара (члан 301), неовлашћен приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (члан

12 Видети: http://nventions.coe.int/Treaty/EN/Treaties/Html/185., приступ 10.2.2009. године

13 Видети: http://news.cnet.com/Senate-ratifies-controversial-cybercrime-treaty, приступ 10.2.2009. год.

14 Камбовски, В., op. cit., страна 310-311

302), спречавање и ограничавање приступа јавној рачунарској мрежи (члан 303), неовлашћено коришћење рачунара или рачунарске мреже (члан 304) и прављање, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података (члан 304а).

Како су код рачунарских кривичних дела рачунарски податак, рачунарске мреже, рачунарски програм и рачунарски вирус објекти напада, законодавац је у члану 112 дао дефиницију датих појмова. Рачунарски податак је представљена информација, знање, чињеница, концепт или наредба која се уноси, обрађује или памти или је унет, обрађен или запамћен у рачунару или рачунарској мрежи. Рачунарска мрежа представља скуп међусобно повезаних рачунара који комуницирају размењујући податке. Рачунарски програм је уређени скуп наредби који служи за управљење радом рачунара као и за решавање одређеног задатка помоћу рачунара. Рачунарски вирус је програм или неки други скуп наредби који је унет у рачунар или рачунарску мрежу који је направљен да сам себе умножава и делује на друге програме или подарке у рачунару или рачунарској мрежи додавањем тог програма или скупа наредби једном или више рачунарских програма.

Кривично дело оштећење рачунарских података и програма се састоји у неовлашћеном брисању, измени, оштећењу, прикривању или на други начин чињењу неупотребљивим рачунарског податка или програма.

Рачунарска саботажа се састоји у уношењу, уништавању, брисању, оштећивању, прикривању или на други начин чињењем неупотребљивим рачунарски податак или програм или уништавању или оштећивању рачунара или другог уређаја за електронску обраду и пренос података са намером да онемогући или знатно омете поступак електронске обраде и преноса података који су од значаја за државни орган, јавну службу, установу, предузеће или друге субјекте.

Кривично дело прављења и уношења рачунарских вируса се састоји у прављењу рачунарског вируса у намери његовог уношења или његовом уношењу у туђи рачунар или рачунарску мрежу.

Рачунарска превара се односи на уношењу нетачног податка, пропуштању уношења тачног податка или на други начин прикривању

или лажном приказивању податка чиме се утиче на резултат електронске обраде и преноса података у намери да се себи или другом прибави противправна имовинска корист и тиме проузрокује штета другом лицу.

Дело неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података се састоји у неовлашћеном укључивању у рачунар или рачунарску мрежу или у неовлашћеном приступу електронској обради података кршењем мера заштите.

Спречавање и ограничавање приступа јавној рачунарској мрежи се састоји у неовлашћеном спречавању или ометању приступа јавној рачунарској мрежи, док се кривично дело неовлашћено коришћење рачунара или рачунарске мреже састоји од неовлашћеног коришћења рачунарске услуге или рачунарске мреже у намери да се себи или другом лицу прибави противправна имовинска корист.

Биће кривичног дела прављења, набављања и давања другом средстава за извршење кривичних дела против безбедности рачунарских података се састоји у поседовању, прављењу, набављању, продаји или давању другом на употребу рачунара, рачунарске системе, рачунарске системе, рачунарске податке и програме ради извршења кривичних дела предвиђена главом XXVII Кривичног законика, изузев кривичног дела неовлашћено коришћење рачунара или рачунарске мреже.

Током 2005. године донет је Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала којим се регулише Посебно тужилаштво при Вишем јавном тужилиштву у Београду, Одељење за борбу против високотехнолошког криминала и Служба за борбу против високотехнолошког криминала ради откривања, кривиног гоњења и суђења за кривична дела која спадају у високотехнолошки криминал. Кривична дела која спадају у високотехнолошки криминал су кривична дела против безбедности рачунарских података одређена Кривичним закоником, кривична дела против интелектуалне својине, имовине и саобраћаја када се као објекат или средство извршења јављају рачунари, рачунарске мреже или рачунарски подаци, као и њихови производи у материјалном или електронском облику, уколико број примерака ауторског дела прелази 2000 или настала материјална штета прелази износ од 1.000.000 динара и 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.[15]

За поступање за ова кривична дела надлежно је Више тужилаштво у Београду које је надлежно за територију целе државе. У оквиру Вишег тужилаштва оснива се Посебно одељење за борбу против високотехнолошког криминала.[16] Уколико овим Законом није другачије регулисано, ово Посебно одељење ради на основу закона о јавном тужилаштву. На челу Посебног одељења налази се посебни тужилац кога поставља Републички јавни тужилац из редова јавних тужилаца и заменика јавних тужилаца који испуњавају услове за избор за заменике вишег јавног тужилаштва. Посебни тужилац се поставља на период од четири године и при његовом избору предност се даје оним јавним тужиоцима који поседују посебна знања из информатичких технологија. Посебан тужилац располаже истим правима и дужностима као јавни тужилац. Када посебан тужилац дође до сазнања о почињеном кривичном делу предвиђеним овим Законом обраћа се у писменој форми Републичком јавном тужиоцу, захтевајући од њега да пренесе или повери надлежност.

У оквиру Министарства надлежног за унутрашње послове организује се Служба за борбу против високотехнолошког криминала и њоме руководи старешина кога поставља министар надлежан за унутрашње послове, након прибављеног мишљења Посебног тужиоца. Служба поступа захтевима Посебном тужиоца.[17]

Одељење за борбу против високотехнолошког криминала се образује при Окружном суду у Београду и оно је надлежно за територију целе државе. Судије у Већу се образују одлуком председника Окружног суда у Београду. За њихово именовање потребна је њихова сагласност. Њихов мандат у Већу траје најдуже две године, с тим што постоји могућност продужења за две године уз њихову писмену са-

15 Члан 3 Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала

16 Члан 4 Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала

17 Члан 9 Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала

гласност. Предност имају оне судије које поседују посебна знања из области информатичих технологија.[18]

Чланом 12 Закона предвижена је обавеза Министарства надлежног за послове правосуђа да обезбеди одговарајуће просторије и друге техничке услове потребне за рад Посебног тужилаштва и Већа.

Основна примедба овом Закону је неспецијализованост кадрова који ће радити у Служби за борбу против високотехнолочког криминала, јер у Закону није предвиђена обавеза да кадрови и старешина Службе поседује посебна знања из области информатичких технологија. Законска решења нису добра ни код Посебног тужиоца ни код Одељења, јер Законом је предвиђено да предност имају јавни тужиоци односно судије који поседују посебна знања из области информатичких технологија, тако да се може десити да Посебан тужилац односно судија Одељења за борбу против високотехнолошког криминала не поседује таква посебна знања.

У току 2007. године било је 86 предмета компјутерског криминала, којима су обухваћене 103 особе, а поднето је 11 оптужница.[19] Током 2008. године Посебном тужилаштву за борбу против високотехнолошког криминала поднете су кривичне пријаве против 166 лица, што представља значајан пораст у односу на претходну годину. Захтев за спровођење истраге стављен је против 147 лица, што је такође значајан пораст у односу на претходну годину. Против 75 лица подигнуте су оптужнице.[20]

Појавни облици компјутерског криминалитета

Појавни облици компјутерског криминалитета су: противправно коришћење услуга и неовлашћено прибављење информација, компјутерске крађе, компјутерске преваре, компјутерске саботаже, компјутерски тероризам и криминал везан за компјутерске мреже.[21]

18 Члан 11 Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала

19 Видети: http://www.vesti.rs/exit/Sajber-kriminal-u-Srbiji-piraterija-kartice-i-pedofilija.html, приступ 21.2.2009. године

20 Видети: http://www.beograd.vtk.jt.rs/index.php?option=com_content&view=article&id=83%3Astatistika-rada-tuzilastva-za-2008-godinu&catid=48%3Avesti&Itemid=70&lang=yu, приступ 13.4.2010. године

21 Видети: www.apisgroup.org/sec.html, приступ 7.2.2009.

Противправно коришћење услуга постоји у случају неовлашћене употребе компјутера, или у његовој овлашћеној употреби, али за остваривање потреба неовлашћеног корисника. Уколико се компјутер користи у било које друге сврхе, осим оних које представљају део његове намене у информатичком систему, онда постоји неовлашћена употреба компјутера. Овлашћена употреба компјутера, али за остваривање потреба неовлашћеног корисника постоји уколико неко лице употребљава компјутер за обављање некох својих послова. Ово лице у оквиру свог редовног посла у радно време користи исте програме за друге наручиоце којима приватно наплаћује обављени посао.[22] Неовлашћено прибављање информација постоји уколико неко лице краде податке садржане у компјутерским системима, у циљу прибављања противправне имовинске користи.

Компјутерске крађе имају висок обим појављивања у оквиру компјутерског криминалитета. Од различитих врста компјутерских крађа најопаснијом се сматра крађа идентитета. На овај начин долази до подривања у интегритет комерцијалних трансакција и угрожава индивидуалну приватност. Крадљивци идентитета на овај начин купују разне ствари, добивају кредите од банака, набављају лажне пасоше и личне карте. Процењује се да ће доћи до повећања ове крађе даљом експанзијом електронске трговине.

Компјутерске преваре су врше у циљу прибављања противправне имовинске користи. Оно што компјутерске преваре од обичних превара је што се код њих не доводи или одржава у заблуду неко лице, већ се та заблуда односи на компјутер у који се пропушта уношење тачних података, или се уносе нетачни подаци, или се компјутер користи на било који други начин за остваривање преваре у кривичноправном смислу.[23] Компјутерске преваре привлаче велику пажњу јавности.[24] Међутим, њих је веома тешко доказати.

---

22 Константиновић Вилић, С., Николић Ристановић, В., Костић, М., op. cit., страна 182-183

23 Алексић, Ж., Шкулић, М., op. cit., страна 389

24 ‘’Веома је илустративан и пример програмера у једној великој лондонској банци, који је успео да дође до потребне шифре и изврши трансфер износа од 4 милиона фунти на свој тајни рачун у Швајцарској. Након напуштања земље, он се јавио својој банци после неколико месеци и објаснио да је успео да, вештим пословањем на берзи, увећа почетни износ за још два милиона фунти и да је сада

Компјутерска саботажа се може поделити на два дела: физичка саботажа и логичка саботажа. Физичка саботажа се састоји у физичком оштећењу или уништењу компјутера и других уређаја за за обраду података, док се логичка саботажа састоји у брисању, модификацији и спречавању коришћења информација садржаних у меморији информатичких уређаја.

Компјутерски тероризам се дефинише као акт уништавања или ометања компјутерског система са циљем дестабилизације једне земље или вршење притиска на њену владу.[25] Компјутерски тероризам обухвата три категорије радњи које се предузимају према компјутерском систему. Први је физички напад који се састоји од оштећивања компјутерског система на традиционалан начин употребом бомби. Синтатички напад се састоји од модификовања логике у систему са циљем да доводе да одлагања или да учини систем непредвидљивим. Овај напад обухвата напад вирусима. Семантички напад се ослања на поверењу које имају корисници компјутерског система. Он се састоји у мењању информација које улазе или излазе из система у циљу изазивања грешака у компјутерском систему, без знања корисника.

Како је интернет глобална међукомпјутерска веза, он омогућује лакшу приватну и пословну кореспонденцију, али се интернет уједно може користити и у криминалне сврхе. Интернет је дао нови облико класичном криминалитету, али је уједно допринео стварању нових облика криминалитета, као што су: ширење дечје порнографије, разни облици угрожавања личне сигурности, ширење разних облика организованог криминалитета.[26]

Карактеристике компјутерског криминалитета

Карактеристика компјутерског криминалитета је велика динамичност базирана на брзом развоју компјутерске технологије и

спреман да врати оних 4 милиона, које је првобитно присвојио, али под условом да се банка обавеже да га неће гонити. Сасвим разумљиво, банка је, руководиће се првенствено пословним разлозима, прихватила ову понуду.'' Цитат према: Алексић, Ж., Миловановић, З., op. cit., страна 330

25 Видети: /www.iwar.org.uk/cyberterror/index.htm, приступ 7.2.2009.

26 Симоновић, Б., op. cit., страна 673-674

њеном свакодневном применом. Употреба компјутера доводи до тога да класична кривична дела постају далеко опаснија, а уједно доводи до појаве сасвим нових кривичних дела.

Друга карактеристика компјутерског криминалитета је мањи значај просторних и временских оквира у појавним облицима компјутерског криминалитета. Могућност приступа компјутеру ради вршења кривичних дела, са било ког места у било које време, мењају значај просторних и временских оквира. Извршилац компјутерских кривичних дела може са било ког места, уз помоћ компјутера, да изврши напад на компјутерски систем, који се налази на било којем месту у свету, с тим што се пружа могућност да се код компјутерског криминалитета изврши напад на компјутерске системе који се налазе на различитим местима. Брзина рада компјутера омогућава да се она искористи приликом вршења кривичних дела. У просеку дужина трајања компјутерског криминалитета је око милионитог дела секунде, што знатно смањује могућност његовог откривања. Према извештају, који је дао амерички Национални институт за статистичко праћење криминала, незаконита активност која траје мање од два минута има 10% мање шанси да буде откривена, док незаконита активност која траје више од шест минута има 80% више шанси да буде откривена.[27] На основу тога долазимо до тога да је шанса да компјутерски криминалитет буде откривен веома мали.

На основу предходно реченог долазимо до наредне карактеристике комјутерског криминалитета, а то је постојање велике тамне бројке компјутерског криминалитета. Не може се са сигурношћу тврдити колика је тамна бројка компјутерског криминалитета. Према неким проценама тамна бројка се креће од 90% до 99% .

За вршење компјутерског криминалитета потребна је велика компјутерска писменост. Међутим, у последње време долази до процеса ширења компјутерске писмености, тако да постоји све већи број потенцијалних извршилаца компјутерског криминалитета.

Овлашћени тужилац се у кривичном поступку суочава се проблемом доказивања кривичних дела компјутерског криминалитета, јер извршиоци ових кривичних дела ретко остављају било какве трагове иза себе. Уколико и постоје докази, трагови компјутерског

27 ibidem

криминалитета могу се налазити у суседним зградама, градовима и државама. Чак и најмања мрежа садржи велики број података и испитивање података, приликом тражења корисних информација, може представљати трагање за иглом у пласту сена. Уколико се и пронађу корисне информације, интернет мрежа обезбеђује висок степен анонимности извршилаца компјутерског криминалитета.[28]

Карактеристике компјутерског криминалца

С обзиром на бројност појавних облика компјутерског криминалитета и мотиве њиховог извршења не може се говорити о јединственом профилу учиниоца компјутерског криминалитета. Међутим, може се говорити о подели извршилаца компјутерског криминалитета на три групе: 1. аматери, 2. професионални криминалци и 3. хакери.

Аматерима припадају криминалци који имају легално занимање, али понекад извршавају компјутерски криминалитет. Ова група није јединствена, већ се у оквиру ње може говорити о трима категоријама: 1. слаби и подложни појединци, 2. фрустрирани појединци и 3. људи са пороком. Слаби и подложни појединци врше дела компјутерског криминалитета зато што су инструменти контроле врло слаби не водећи рачуна о последицама извршеног кривичног дела. Велики број припадника ове категорије остаје неоткривен. Фрустрирани појединци су такви појединци који су незадовољни и разочарани поступцима околине, што им, по њиховом виђењу ствари, даје за право да врше комјутерске крађе и проневере. Социопатолошке појаве, као што су алкохолизам, коцкање и наркоманија, утичу на одређене појединце да се одају вршењу компјутерског криминалитета.[29]

У професионалне криминалце спадају лица чије је једино занимање бављење криминалом. Развој информационе технологије омогућио им је проширење вршења кривичних дела. Професионални криминалци се према степену организације могу поделити на индивидуалне криминалце, организоване групе и криминалне организације. Индивидуални криминалци врше компјутерски криминалитет

28 Видети: http://books.google.com/books, приступ дана 7.2.2009. године

29 Петровић, С., Компјутерски криминал, Министарство унутрашњих послова Републике Србије, Београд, 2000. година, страна 264-265

самостално са циљем остваривања имовинске користи. Њихова карактеристика је мали криминални потенцијал и ограничавање њиховог криминалног понашања на локални карактер. Организоване групе су групе појединаца са заједничким интересима, али су ти интереси пре свега појединачни. Потенцијал за вршење криминалног криминалитета им је већи у односу на индивидуалне криминалце, али су последице њихове криминалне активности и даље локалног карактера. Криминалне организације су највиши организациони облик криминалаца које одликује дисциплина, хијерархија, чврстина и лојалност. Криминалним организацијама се развојем информационих технологија пружа могућност да прошире поље своје криминалне делатности. Настају виртуелне cyber групе чији је задатак укључење у електронско легално и илегално тржиште и дигиталну економију ради вршења различитих врста превара: лажних интернет аукција, превара у играма на срећу, осигурању, коришћењу јавних добара и сервиса, при комуникацијама, инвестиционим улагањима, трансакцијама и слично.[30]

У трећу групу извршилаца компјутерског криминалитета спадају хакери. Они представљају лица, која користећи своја рачунарска знања, уз помоћ модема упадају у туђе компјутерске системе.[31] Хакери имају неодољиву жељу да продру у туђе компјутерске системе. Они врло често немају контакт са реалношћу и проводе за компјутером по 16 сати дневно. Забележени су бројни случајеви продирања у компјутерске системе влада различитих држава и међународних организација.[32] Они

30 Константиновић Вилић, С., Николић Ристановић, В., Костић, М., op. cit., страна 184

31 Алексић, Ж., Шкулић, М., op. cit., страна 387

32 „Европска унија, САД и НАТО су све чешће изложене компјутерским нападима из Кине, а Запад за сада није у стању да се ефикасно одбрани од хакерских упада у компјутерске системе институција и обавештајних служби, објавили су западни медији. НАТО и Европска унија су протеклих дана упозоравале да је потребно хитно заштити поверљиви обавештајни материјал од најновијих напада хакера из Кине, док Пекинг демантује умешаност у хакерске нападе, пише лондонски «Тајмс».

«Свима је стављено до знања да је Кина постала веома активна у компјутерским нападима. Редовно добијамо упозорења од службе унутрашње безбедности,» рекао је «Тајмсу» дипломатски извор из НАТО. Нападима су изложене и владине и војне институције у САД, а тамношњи аналитичари кажу да Запад нема ефикасан начин

нису злонамерни, али и поред тога својим активностима могу начинити велику штету. Они су према свом професионалном опредељењу, најчешће програмери компјутера, оператери, или високо образовани информатичари, а понекад је реч о особама које су своју вештину и знање стекли бавећи се компјутерима из хобија.[33]

Према једном истраживању хакери су у 100% мушкарци, веома су паметни, склони истраживачком и логичком размишљању и увек такмичарски расположени. Они виде себе као афирмисане ауторитете над компјутером и имају веома мало поштовања према људима који не знају ништа о компјутерима.[34]

Закључак

Како не постоји апсолутна заштита и како је сваки информациони систем изложен врло озбиљним ризицима,[35] најбољи начин борбе против компјутерског криминала је у њеној превенцији. Превенција мора бити тако организована да одврати потенцијалне извршиоце компјутерског криминала од извршења кривичног дела на тај начин што би се предузеле адекватне мере за избор људи који би се бавили радом на компјутеру до мера физичке и софтверске заштите. Како највећи број извршилаца компјутерског криминала потиче из служби које су повезане са радом на информационим системима,[36] потребно је посебну пажњу посветити самом избору људи који ће радити на таквим пословима. Физичким мерама потребно је заштити информационе системе од случајних оштећења компјутерске опреме, али и од намерних оштећења и неовлашћених упада у просторије у којима се налазе информациони системи. Софтверске мере заштите треба да су усмерене ка спречавању неовлашћеног упада у информациони систем преко интернета и преко приступних јединица унутар информационог

да се супростави нападима, навео је лондонски дневник.“ Видети: http://www.blic.rs/pretraga, приступ 8.3.2010. године

33 Цетинић, М., Компјутерска кривична дела и њихови појавни облици, Правни живот, број 10, Удружење правника Србије, година 1998., страна 266

34 Истраживање је спровео Smith A. J., Опширније видети: Петровић, С., op. cit., страна 274

35 Петровић, С., op. cit., страна 362

36 Ibidem

система. Што су важнији подаци који су чувају у информационом систему, то мере софтверске заштите морају да буду веће. Стога се уводе степенасти системи заштите.

Међутим, без обзира на превентивни систем, компјутерски криминалитет је у све већој експанзији. Сигурно је да мере заштите неће утицати на смањење стопе извршења овог типа криминалитета, али је такође сигурно да ће ефикасна превенција утицати на успоравање раста стопе компјутерског криминалитета.

Како савремено друштво постаје све више зависно од употребе компјутера, државе широм света ће морати да „науче“ да се боре против компјутерског криминалитета не само превентивним мерама већ њихово кривично правосуђе мора достићи такав степен откривања и процесуирања извршених кривичних дела против безбедности рачунарских података да потенцијални извршиоци ових кривичних дела буду одвраћени стопом осуђених извршиоца овог типа криминалитета.

Darko Dimovski, LL.B.
Teaching Assistant,
Faculty of Law, University of Niš

CYBERCRIME

Summary

This article deals with the concept of computer-related crime. The author is particularly interested in the international law aspect of combating cybercrime, with specific reference to the provisions contained in the Cybercrime Convention (2002). Given the fact that no state is immune to cybercrime, the author explores the legal provisions related to combating computer crime. Further on in the paper, the author focuses on the categories of computer crime, elaborating on the distinctive features of different computer crimes and the general characteristics of their perpetrators.

Key words*: cybercrime, distinctive features, categories*