УНИВЕРЗИТЕТ У НИШУ

ПРАВНИ ФАКУЛТЕТ

Криминолошки аспект компјутерског криминалитета

(Мастер рад)

Ментор

Проф. др Миомира Костић

Студент

Драган Мирковић

Број индекса: М 008/16- О

Ниш, 2017. године

САДРЖАЈ

УВОДНА РАЗМАТРАЊА

Енормна експанзија саме употребе компјутера тако и све веће злоупотребе истог последње деценије, привукла је моју пажњу за потпунијим разумевањем овог типа криминалитета са многобројним модалитетима испољавања. У данашњим условима живота готово је незамисливо непознавање основа рада на компјутеру, који је постао суверен владар најважнијих сфера како друштвеног тако и економског живота. С обзиром на чињеницу да је начин коришћења компјутера прилагођен знању просечног човека, повећана је опасност од извршења кривичних дела која припадају компутерском криминалитету. Опште је познато да готово сваки вид техничко-технолошког достигнућа пре или касније постаје предмет многобројних злоупотреба.

Оно што нарочито забрињава када је реч о компјутерском криминалитету јесте постојање изузетно велике „тамне бројке" криминалитета што је у неоспорној корелацији са непријављивањима истог од стране жртве уколико је у нанета незнатна материјална штета, недовољном обученошћу одговорних лица за сузбијање веома разноликих облика овог типа криминалитета и изузетно скупом технонологијом као и високом ценом самих уређаја потребних за остваривање ове радње

Интернет као најзначајнији светски медиј омогућује пренос информација брзином којој се не може у већини случајева ефикасно ући у траг. Иако се у јавност интернет најчешће јавља као „убојито" средство у рукама организованих криминалних група за измењене методе и технике вршења кривичног дела тероризма, активност на интернету од стране просечног грађанина може указати на повећану опрезност приликом разних видова интеракције на „мрежи" што се не сме занемарити имајући у виду знатну како материјалну тако и нематеријалну штету која том приликом може настати.

Мастер рад „Криминолошки аспект компјутерског криминалитета" подељен је у две веће и једну мању целину: 1) криминолошки и кривичноправни концепт компјутерског криминалитета 2) студија о компјутерском криминалитету у периоду 2009-2015. године 3) превенција, заштита и сузбијање компјутерског криминалитета.

Прва целина полази од појмовно одређења компјутерског криминалитета као и од његовог историјског развоја почев од првих испољавања. Затим следе основне карактеристике наведеног типа криминалитета које доприносе његовом потпунијем одређењу. Кроз приказ институционалог оквира и правне регулативе за борбу против

компјутерског криминалитета како на међународном тако и на националном нивоу успостављају се чврсти темељи за превенцију, заштиту и сузбијање истог. Феноменолошке и етиолошке карактеристике које су обрађене у овом раду представљају саставни део криминолошког концепта наведеног типа криминалитета. Док су код феноменолошких карактеристика посебно издвојени појавни облици, код етиолошких карактеристика су приказани ендогени и егзогени фактори компјутерског криминалитета уз осврт на најзначајније теорије узрочности. Код поделе и основних карактеристика извршиоца дела компјутерског криминалитета посебна је пажња посвећена хакерима као најбројнијој групи извршиоца.

Друга целина рада је у потпуности посвећена студији о компјутерском криминалитету за период од 2009. до 2015. године. Студијом је обухваћена територија Републике Србије и Републике Хрватске уз примену различитих научних метода приликом анализе добијених резултата. Највише су примењени статистички и упоредно-правни научни метод. Анализом добијених резултата проверене су постављене хипотезе чије потврђивање односно непотврђивање омогућава детаљније сагледавање феноменолошких и етиолошких карактеристика компјутерског кирминалитета.

Трећа и последња целина овог рада намењена је облицима формалне и неформалне друштвене контроле компјутерског криминалитета. Од нарочитог значаја за појединачног корисника компјутера и компјурских мрежа су низ практичних савета наведених у оквиру облика неформалне друштвене контроле.

У закључним разматрањима изложена је критичка анализа постојеће правне регулативе уз приказ могућих решења за брже и ефикасније сузбијање овог изузетно динамичног и стварности споро прилагодљивог типа криминалитета.

I КРИМИНОЛОШКИ И КРИВИЧНОПРАВНИ КОНЦЕПТ КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА

1.Појмовно одређење компјутерског криминалитета

Готово неограничена моћ компјутера (рачунара) у меморисању и брзој обради података довели су до напретка неслућених размера у обиму, брзини и квалитету производње, тровине, науке, уметности, безбедности, саобраћаја и финансијског пословања са тенденцијом сталног усавршавања. Савремено пословање, свет науке, уметности, забаве и комуникације уопште постали су готово незамисливи без компјутера. Рачунар представља једну од најзначајнијих и најреволуционарнијих тековина развоја техничко-технолошке цивилизације. Поред свих предности које са собом носи тако и огромне користи човечанству, рачунар је брзо постао и средство злоупотребе несвесних појединаца, група чак и организација. Тако настаје рачунарски криминалитет као посебан и специфичан облик савременог криминалитета по структури, обиму и особеностима. [1] Све учесталији видови и начини злоупотребе компјутера утицали су на стручну и научну јавност да се дубље позабави сложеним питањем дефинисања овог облика криминалног понашања .

Компјутерски криминалитет је немогуће дефинисати јединственим и прецизним појмовним одређењем. То је „ општа форма кроз коју се испољавају различити облици криминалне активности , форма која ће у будућности бити доминантна “. [2] Наиме, тешкоће у дефинисању компјутерског криминалитета произлазе због тога што се ради о релативно новом облику криминалног понашања, недовољно препознатљивом у односу на друге облике криминалитета, присуство велике феноменолошке разноврсности која се тешко може обухватити једном дефиницијом као и проблем недовољно динамичне, стварности споро прилагодљиве позитивне кривичноправне легислативе што науци додатно отежава дефинисање овог појма. Упркос свим проблемима дефинисања у наставку ће бити изложене неке од дефиниција при чему свака са свог аспекта додатно појашњава сам појам компјутерског криминалитета.

Прва дефиниција компјутерског криминалитета потиче из 1979. године, и садржана је у Приручнику Кривичног правосуђа обухваћеног овом врстом криминалитета.

[1] Д. Јовашевић, *Кривично право-посебан део*, Ниш, 2014, Номос стр. 111
[2] D.Parker, *Fighting computer crime*, New York, 1983, p.120

Према овој дефиницији : „ рачунарски криминалитет представља сваки нелегални акт за чије је успешно кривично гоњење неопходно добро познавање рачунарске технологије “. [3] Неколико година касније ово гледиште је унето у Студију о међународним правним аспектима рачунарског криминала 1983. године. [4] На основу Препоруке Савета Европе из 1989. године предвиђен је функционалан приступ, и компјутерски криминалитет упрошћено дефинисан обухватајући сва дела која су набројана и дефинисана у предложеним смерницама или препорукама упућеним националним законодавствима. [5] У Препоруци Савета Европе из 1995. године први пут је употребљен термин кривична дела везана за информационе технологије која обухватају свака кривична дела за које се у истрази, истражни органи морају добити приступ информацијама које се обрађују или преносе у оквиру рачунарских система или електронским системима за обраду података.[6]

Истакнути судија Вебстер (енгл.Webster H. W.) је 1985. године на конференцији о заштити компјутера изложио следећи поглед Федералног истражног бироа на тему ове проблематике : „ За злоупотребу компјутера користе се разни називи, али сви они указују на исту ствар и ми у Федералном истражном бироу користимо израз криминал повезан компјутером. Пошто не постоји општеприхваћена дефиница, ми дефинишемо такве злоупотребе као повреду кривичног закона који укључује компјутер или њихове периферне уређаје као инструменте или жртве криминала. У пракси смо уочили да је највећи део овог криминала у основи „ традиционални “ криминал : проневере, изнуде или уништавање добара. Разлика је у томе што је компјутер много префињенији инструмент “.[7] На десетом Конгресу Уједињених Нација за превенцију криминалитета и третман делинквената, узета је у обзир и ова проблематика : „ Компјутерски криминалитет је општи појам који обухвата кривична дела која се врше посредством компјутерског система или мреже, у компјутерском систему или мрежи, или против компјутерског система или

[3] The Criminal Justice Resource Manual on Computer crime припремљен је од стране SRI International, Menlo Park, California, USA, за Министарство правде Сједињених Америчких Држава у 1979. години

[4] В. Више: Schjolberg, S,,*Computers and Penal Legislation – A Study of the Legal Politics of a new Technology*”, 1986,

[5] Recommendation No. R (89) 9, adopted by the Committee of Ministers of the Council of Europe on September 13, 1989 and Report by the European Committee on Crime Problems: Computer-realted crime, Види : https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&Secmode=1&DocId=702280&Usage=2 п ретражено 08.08.2017

[6] Recommendation No. R (95) 13, approved bz the European Committee on Crime Problems (CDPC) at its 44th plenary session May 29- june 2, 1995: Concerning problems of criminal procedural law connected with information technology, Види : http://www.justice.gov/criminal/cybercrime/crycoe.htm претражено 08.08.2017

[7] M.Tenhuen, *Combating computer crime*, 1989, p. 2

мреже. У принципу он укључује било које кривично дело које се врши у електронском амбијенту “. [8]

Појмовно одређење компјутерског криминалитета од стране аутора који на свеобухватан начин настоје да прецизирају сложеност појма је садржано најпре код Пол Тејлора (енгл.Paul Taylor) према коме компјутерски криминалитет представља криминалну активност која користи инфраструктуру везану за информационе технологије и укључује неовлашћен приступ, неовлашћено пресретање података (техничким средствима, из или унутар компјутерског система), интервенција на подацима (неовлашћено оштећење, брисање, мењање), системско мешање (неовлашћене интервенције у погледу функционисања компјутерског система, убацивањем, преношењем, оштећењем или мењањем компјутеских података) злоупотребу уређаја, кривотворење и електронску превару.[9] Аутор који ставља нарочит нагласак на мотиве извршиоца при самој злоупотреби компјутерске технике је Дон Паркер (Donn Parker) према коме : „ Злоупотреба рачунара је сваки догађај у вези са употребом рачунарске технологије у коме жртва трпи или би могла да трпи губитак, а учинилац делује у намери да себи прибави или би могао да прибави корист “.[10] Према мишљењу аутора овог рада најпотпунију дефиницију компјутерског криминалитета као облика имовинског криминалитета је дао Улрих Зибер (Ulrich Sieber) : „ Рачунарски кримииналитет обухвата противправне повреде имовине, код којих се рачунарски подаци са умишљајем мењају (компјутерска манилупација), уништавају (компјутерска саботажа), неовлашћено захватајају и искоришћавају (компјутерска шпијунажа) или се користе заједно са хардвером (крађа времена) “. [11] Увидевши неопходност модификације дефинисања појма наведени аутор је дао одговарајућу ширину појму и нагласак ставио на значај самог појма : „ Рачунарски криминалитет, или криминалитет повезан са рачунарима јесте противзаконито, неморално и неовлашћено понашање које укључује мешање у аутоматску обраду података и / или у комуникацију подацима “. [12]

---

[8] Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders,2000, Background paper for the workshop on crimes related to the computer network: Crime-fighting on the Net, преузето 15.05.2017. http://www.un.org/events/10thcongress/2088h.html

[9] P.Taylor, *Hackers: Crime in the Digital Sublime*, Routledge,1 edition, p.200

[10] D. Parker, *Computer Abuse*, 1973, Springfild p. 14

[11] U. Sieber, *Computer Crime and Criminal Justice*, Köln,1977, p.188, цит. према Б. Бановић,*Обезбеђење доказа у криминалистичкој обради кривичних дела привредног криминалитета*, Београд, 2002, ПП. 132-133

[12] U. Sieber, The international Emergence of Criminal Infromation Law, Köln, 1992, p. 5

Када је реч о напорима дефинисања овог појма у домаћој научној и стручној литератури, још увек није присутан знатан број дефиниција с обзиром на недовољан број откривених и процесуираних случајева компјутерског криминалитета. На простору Републике Србије, једна од првих дефиниција из ове области је : „ Компјутерски криминал обухвата кривична дела код којих се компјутер појављује као средство, предмет или објект напада, за чије је извршење или покушај неопходно извесно знање из рачунарства или информатике “.[13] Према једној дефиницији под компјутерским криминалитетом се подразумевају сва делинквентна понашања у којима се уређаји за електронску обраду података користе као средство за постизање кажњивих радњи или као директан циљ кажњиве радње.[14] У том смислу прецизнија (и потпунија) дефиниција би гласила : „ Компјутерски криминалитет представља облик криминалног понашања код кога се коришћење компјутерске технологије и информатичких система испољава као начин извршења кривичних дела, или се компјутер употребљава као средство или циљ извршења, чиме се остварује нека у кривичноправном смислу релевантна последица “.[15] Аутори наведене дефиниције износе и аргументацију исте, указујући на карактеристике саме појаве које произилазе из њеног појмовног одређења : „ Одређивање појма компјутерског криминалитета се не може заснивати на утврђивању у оквиру његове дефиниције, елемената, који нису карактеристични за све облике овог вида делинквенције, као што су нпр. профил учинилаца, конкретна врста кривичног дела, врста штетне последице, мотив за криминално понашање, итд. Зато је приликом дефинисања компјутерског криминалитета неопходно имати широк приступ. Тако се једна свеобухватна и широка дефиниција компјутерског криминалитета мора заснивати на три основна елемента: 1. начину извршења, 2. средству извршења, и 3. последици криминалног деловања. Бавећи се анализом актуелних питања из области рачунарског криминалитета, професор Спасић истиче : „ Cyber (компјутерски) криминал представља криминал који се одвија у дигиталном(електронском) окружењу. То је такав облик противправнох понашања код кога је сајбер простор окружење у коме се компјутерске (и друге телекомуникационе мреже) појављују као средство, циљ доказ и / или симбол или окружење извршења кривичних дела. За разлику од тзв. класичног криминала који је видљив, cyber криминал је

[13] B. Brvar , *Pojavne oblike zlorabe računalnika*, Ljubljana, 1982, p. 22
[14] М. Бошковић, *Криминилогија и социјална патологија*, Нови Сад, 1995, стр. 164
[15] Ж. Алексић , М. Шкулић, *Криминалистика,* Београд, 2007, стр. 87

невидљив и увек се дешава на дистанци, употребом било које телекомуникационе технологије.[16] Дефиниција која омогућава сагледавања појединих карактеристика компјутерског криминалитета је следећа : Под појмом рачунарског криминалитета подразумева се свеукупност различитих облика, видова и форми испољавања противправних понашања управљених против безбедности рачунарских, информационих и компјутерских система у целини или њихових појединих делова на различите начине и различитим средствима у намери да се себи или другом прибави корист (имовинске или неимовинске природе) или да се другоме нанесе штета.[17] Из овако одређеног појма рачунарског криминалитета произлазе његове основне карактеристике [18]: објект заштите је безбедност рачунарских података или информационог система у целини или његовог појединог дела (сегмента) 2) посебан, специфичан карактер и природа противправних делатности појединца, 3) посебна знања и специјализација на страни учиниоца ових кривичних дела која искључују могућност да се свако, било које лице нађе у овој улози, 4) посебан начин и средство предузимања радње извршења – уз помоћ или употребом (злоупотребом) рачунара и 5) намера учиниоца као субјективни елеменат у време предузимања радње која се огледа у намери прибављања за себе или другог користи или наношење штете другом физичком или правном лицу.

Значај што прецизнијег одређења појма компјутерског криминалитета огледа се пре свега у ефикаснијем препознавању истог од стране овлашћених лица јер само свеобухватна дефиниција овог типа криминалитета може омогућити надлежним органима брзо и ефикасно деловање. Због ове је чињенице неопходно да научна и стручна јавност увек буде корак испред тренутног стања у законодавству и да константно указује на постојеће позитивноправне пропусте у регулисању како би се благовремено препознали могући нови облици и начини (технике) извршења компјутерског криминалитета.

[16] В. Спасић, *Актуелна питања у области сајбер криминала*,Београд, 2006, стр.107
[17] Н. Китаровић, *Компјутерски криминалитет*, Београд, 1998, стр.52-56
[18] Б. Петровић , Д. Јовашевић, *Кривично/Казнено право Босне и Херцеговине –Општи дио,* Сарајево, 2005, стр. 211-241

2. Кратак осврт на историјски развој компјутерског криминалитета

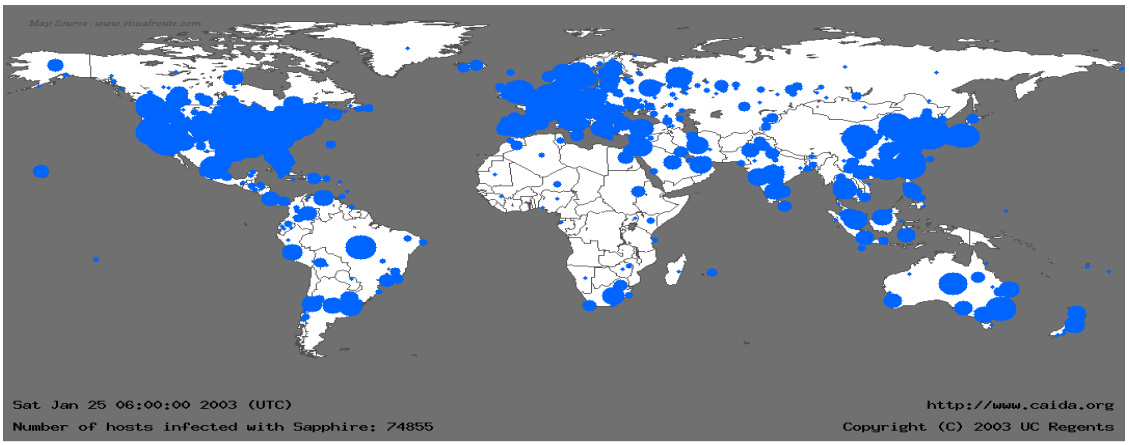
Идеја о компјутерском криминалитету као посебном типу криминалитета настаје шездесетих година двадесетог века са повећаном производњном и дистрибуцијом компјутера. Први познати инцидент са упадом у системе савремене технологије догодио се 1878. године када је оператер компаније Бел Телефон намерно погрешио при повезивању телефонских позива у централи, прислушкивао и осмишљавао различите шале са људима на телефонској линији. Још давне 1939. године британски крипограф Алан Туринг је створио први уређај за дешифровање компјутерских кодова. Први евидентирани случај компјутерског криминалитета појавио се 1958. године, док је први случај кривичног гоњења на федералном нивоу Сједињених Америчких Држава била измена банкарских записа у Минеаполису 1966. године.[19]Највероватније први забележен случај компјутерског криминалитета у Европи представља једна софтверска крађа која се десила у Финској фебруара 1968. године. Шездесетих година двадесетог века полако почињу да се појављују први извештаји о компјутерским манипулацијама, компјутерским саботажама, шпијунажама и нелегалним коришћењима рачунарских система. Први забележени случај хаковања као дела компјутерског криминалитета односи се на студенте приватног универзитета у Кембрицу који су неовлашћено модификовали тада популарне играчке возове, како би убрзали њихово кретање. Захваљујући повезивању на главни компјутер универзитета омогућено им је и даљунско управљање тим возовима. За разлику од каснијих извршиоца овог дела компјутерског дела којима је једини циљ постало стицање материјане користи, ранији су настојали суштински разоткрију начин рада одређеног компјутерског система. Њихов је рад у велики мери допринео побољшању функционисања самих система.

Први озбиљнији третмани компјутерског криминала везују се за седамдесете године при чему је релативно ограничена улога рачунара у свакодневном животу утицала да се ови прекршаји усмере на крађе и преваре везане за телекомуникационе услуге и пренос електронских средстава. Јан Марфи (енгл. Ian Murphy) је прва особа која је процесуирана за дело компјутерског криминалитета 1981. године у Сједињеним Америчким Државама. Први напад великих размера на компјутерске системе и мреже догодио се 1989. године када је украдено око 70 милиона долара Првој Националној Банци

[19] И. Ревјако, *Computer terrorists: The latest technologies as a tool of committing crimes*, 1997, p.34.

града Чикага. Проблеми неовлашћеног приступа приватним информацијама којима располажу банке и корпорација скренули су пажњу на могућност коришћења рачунара у сврхе привредног криминала. На простору бивше СФРЈ први случај компјутерског криминала забележен је 1983. године када су радници СУП-а у Пули ухапсили раднике Истарске банке у Пули и П.Р. радника филијале Загребачке банке у Пули, због основане сумње да су прва двојица радећи као оператери на систему уз помоћ трећег, бившег руководиоца, извели финансијску малверзацију уз помоћ рачунара покушавши тако да извођењем низа програма на рачунару, незаконито изврше беспремни упис камата на који начин су намеравали себи прибавити противправну имовинску корист и оштетити банку за 10 000 000 тадашњих динара. Нарочито је значајно указати и на пример Кевина Митника из САД, који је ухапшен и осуђен 1995. године за фалсификовање 20.000 бројева кредитних картица.

Са повећаном употребом персоналних рачунара повећала се и брига за заштитом од неовлашћеног приступа рачунарским подацима. Захваљујући компјутерским мрежама, које су служиле за војне намене и намене различитих владиних институција у Сједињеним Америчким Државама, временом настају приватне мреже појединих универзитета. Наведене мреже ће коначно бити потиснуте развојем глобалне компјутерске мреже-интернета. Све већа умрежености је довела до нових проблема, попут напада на удаљене рачунаре и мреже, и дала живот делима као што су повреде ауторских права, дистрибуција дечије порнографије и др. Присутност на интернету излаже компјутере опасностима од преноса илегалних садржаја, ДоС (енгл. Denial of Service) напада и ширење малвера. Један од најмасовнијих напада на интернет се догодио 1998. године када је убачен програм способан за самоумножавање са могућношћу да уништава компјутерске податке наношећи том приликом велику штету. Укупна штета коју је овај програм нанео довела је до уништења готово трећине садржаја на интернету у Сједињеним Америчким Државама. Најраспрострањени облик компјутерског програма са најдестуктивнијим капацитетом је био тзв. „сафирни црв" који је 2003. године напао око 90 % сервера на интернету са неадекватном заштитом за мање од 10 минута.



Извор преузет са: https://www.caida.org/publications/papers/2003/sapphire/sapphire.html

Географска распрострањеност црва у року од 30 минута након започетог напада

Сафирни црв је укупно захватио око 75 000 регистованих сервера, иако се претпоставља да је број захваћених сервера далеко већи. Довео је до отказивање изузетно великог броја летова у том периоду и проузроковао поремећаје у раду банкомата. Штета коју је проузроковао се процењује на милијарду америчких долара.[20]

Проценат захваћених жртава по земљама

Country	% Victims
United States	42.87
South Korea	11.82
UNKNOWN	6.96
China	6.29
Taiwan	3.98
Canada	2.88
Australia	2.38
United Kingdom	2.02
Japan	1.72

[20] Више на : ://www.caida.org/publications/papers/2003/sapphire/sapphire.html

Netherlands	1.53

Извор преузет са: https://www.caida.org/publications/papers/2003/sapphire/sapphire.html

Почетак двадесет и првог века довео је до снижења доњег прага потребног знања и стручности за коришћење компјутера и компјутерске технике као и ширења компјутерске писмености почев од основних школа. Велики број младих, лишених етике, почео је да представља огроман потенцијал за све већи број дела компјутерског криминалитета. Џонатан Џејмс (енгл.Jonathan James) је 2000. године постао први малолетник осуђен због хаковања као дела компјутерског криминалитета. Драстично повећање броја мобилних „смарт“ телефона, преносивих рачунара почев од 2010. године омогућило је великом броју појединаца укључење у компјутерске мреже без обзира на време или место, што је додатно повећало број потенцијалних извршиоца и значајно отежало откривање и процесирање истих. Све је веће укључивање организованих криминалних група у компјутерски криминалитет, нарочито када је реч о дистрибуцији и продаји дроге, проституцији, рекетирању, сексуалној злоупотреби деце, трговини људима и интернет клађењу. Последњих година у порасту је и број употребе интернета и компјутерских мреже од стране терористичких организације за међусобну комуникацију, регрутовање својих присталица, прикупљање обавештајних података, илегално добијање пасоша и виза као и за дистрибуцију пропаганде. Почетком 2016. године администрација друштвене мреже „Твитер“ је угасила преко 150 000 једне од најопаснијих терористичких организација данашњице Исламске државе Ирака и Леванта.

3.Основне карактеристике компјутерског криминалитета

Корелација између појмовно одређења компјутерског криминалитета и карактеристика које из њега произилазе указује на присуство мањег или већег броја основних карактеристика у зависности од ужег или ширег приступа при одређењу самог појма. Док поједини аутори истичу само просторну и временску димензију криминалног деловања уз осврт на специфичан профил извршилаца дела компјутерског криминалитета, други настоје да прецизирају начине извршења и последице које настају захваљујући компјутерском криминалитету. У наставку ће бити изложене карактеристике захваљујући којима је могуће лакше пропознати овај тип криминалитета.

- **Просторни оквир деловања** - Корисници компјутерске технологије без надзора улазе у такозвани кибернетички или сајбер (енгл.cyber) простор превазилажећи контролу националних држава. Ово указује на промену дефиниције места, а самим тим и изграђивање нове, томе прилагодљиве тактике криминалистичких мера и радњи које се на њему предузимају, па и проблеме важења кривичних закона и полицијске и судске надлежности. [21] Могућност да се са истог места истовремено покрене више различитих акција, ка различитим местима и са различитим циљевима, представља за криминалца изузетну погодност, јер паралелно са легалним, које му служе као „ димна завеса “ може да активира и једну или више илегалних активности, чиме значајно умањује ризик сопственог откривања. [22] Транснационални карактер овог типа криминалитета указује на неопходност сарадње између држава на највишем нивоу и усклађивање прописа ради ефикасног откривања и сузбијања.

- **Временски оквир деловања** - Сталан развој компјутерске технике омогућава проток информација између уређаја брзином којој се у највећем броју случајева тешко можеући у траг. Велики проблем представља чињеница да су међународним комуникационим системима, који повезују велики број рачунарских центара широм света, омогућили извршиоцима дела компјутерског криминалитета слободу у избору времена када ће одлучити да предузму криминалну активност с обзиром да је временски период потребан за извршење дела изузетно кратак. Дела компјутерског криминалитета се могу извршити и за три хиљадити део секунде. Неопходно је стално усавршавање постојећих

[21] Б. Бановић, *Обезбеђење доказа у криминалистичкој обради кривичних дела привредног криминалитета*, Београд, 2002 , стр. 135
[22] С. Петровић, *Компјутерски криминал*, Београд, 2000, стр. 95-96

знања о о овом типу криминалитета од стране надлежних органа како би се благовремено препознала нова средства која омогућавају све бржу размену података а самим тим отварају простор и новим начинима извршења дела компјутерског криминалитета. [23]

- **Начин извршења дела** - Од првих телекомуникационих уређаја чија је сврха била олакшати свакодневни живот људи па све до најсавремених уређаја за извршење најсложенијих математичких операција увек је одређени број лица настојао да их злоупотреби ради остваривања сопствених циљева. Временом се развијају све сложеније технике прикупљања и злоупотребе великог броја личних података. Суптилне технике и методи које се извршавају истим механизмима као и легалне, не остављају трагове, нити ометају редован рад система, па је самим тим, могућност откривања сведена на најмању меру, а у појединим случајевима ограничена само на откривање у тренутку извршења дела.[24] Као једна од техника извршења издваја се социјални инжињеринг који представља нетехнички напад који зависи од људских ресурса, и превару, као и довођење људи у заблуду, када је у питању одавање неких безбедносно релевантних информација или процедура. [25]

- **Динамичност развоја** - Захваљујући динамичном развоју компјутерске технологије представљеном кроз компјутерску опрему све мањих димензија , сталном повећању брзине и капацитета протока информација, снижењу цене и поједностављивање коришћења технологије дошло је до повећања броја корисника невероватном брзином. Све већа продаја персоналних компјутера из године у годину као и увођење информатике у обавезне школске програме представља показатељ лакоће приступа и елементарне обучености довољне за извршење најосновнијих дела компјутерског криминалитета. Ограничене су могућности за непосредно надгледање и контролу и мала вероватноћа откривања компјутерског криминалитета с обзиром на чињеницу његовог константног ширења на нове области друштвеног живота. Процес аутоматизације у пословању који је довео до експанзије производње такође је створио могућност злоупотребе технологије ради прибављања материјалне користи. Узимајући у обзир да инфраструктуре једне државе, попут брана ,електричних мрежа, финансијских трансакција ,транспортног

[23] Више о томе: М.Будимлић, П.Пухарић, *Компјутерски криминалитет – криминолошки, кривичноправни и сигурносни аспект*, Сарајево, 2009, стр. 9
[24] Б. Бановић, оп.цит., стр. 135
[25] Више на: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html претражено 07.05.2017.

саобраћаја, војних одбрамбених система, све више ослањају свој рад на компјутерске системе, постоји оправдан страх да би у будућности компјутерски напад могао озбиљно да пореметио функционисање нападнутог система, довео до оштећења и угрожавање живота.

- **Велика тамна бројка** – Приликом различитих злоупотреба компоненти рачунарске технологије, оштећено лице често није ни свесно да је у конкретном случају жртва кривичног дела, па самим тим изостаје подношење кривичне пријаве, а ако дође до откривања извршеног дела, често је већ касно да би се могла предузети ефикасна мера.[26] Карактеристично је да и у случајевима када је оштећени открио да је жртва кривичног дела често не подноси пријаву, због страха од губитка поверења од стране пословних партнера , што лако може довести до банкротирања. Тако нпр. ако је дошло до неовлашћеног продора у информациони систем неке банке, и ако се ова чињеница обзнани, странке с правом могу страховати да подаци о њима нису у добрим рукама, па ће потражити другог пословног партнера. Због тога у великом броју случајева руководиоци оштећених субјеката настоје заташкати овакво кривично дело и радије трпе насталу штету него ли да подношењем пријаве рискирају несагледиве последице пољуљаног поверења. [27] Велики део онога што се дешава унутар ове технологије није видљиво и никада се не појављује на хартији, а и сам рачунар може бити програмиран тако да „ обрише “ сопствене трагове, отежавајући на тај начин било какво откривање илегалних активности. [28] Једна новија америчка студија из ове области указује на чињеницу да се информатички криминалитет дешава чак 40 пута чешће од класичног, општег, традиционалног криминалитета, а да 90% информатичких злочина остаје практично неоткривено(у зони тамне бројке криминалитета).[29]

- **Личност извршиоца дела** - Све једноставније могућности употребе компјутерске технологије од стране све већег броја корисника, којима више није нужно ни потребно техничко образовање, шири круг потенцијалних извршилаца дела компјутерског криминалитета, тако да је све теже утврдити њихову типологију и карактеристике с обзиром на брзину обраде података и разноврсне могућности њиховог укрштања,

[26] Ј. Матијашевић, *Кривичноправна регулатива рачунарског криминалитета*, Нови Сад, 2013 стр. 21
[27] И. Фејеш, *Компјутерски криминалитет- криминалитет будућности, изазов садашњости*, 2000, стр. 378
[28] С. Петровић, оп.цит. стр. 86
[29] Д. Јовашевић, Т. Хашимбеговић, *Кривичноправна заштита безбедности рачунарских података*, Тара, 2004 стр. 3

повезивања, селекције и сл., могућности криминалног деловања појединца расту, чак толико драстично да се може рећи да замењују на десетине класичних криминалаца. [30] У погледу старосне структуре извршилаца дела није могуће прецизно одредити границу с обзиром на чињеницу веома широке категорије лица који се могу јавити као извршиоци. У великом је порасту број младих лица као извршиоца дела компјутерског криминалитета чиме изражавају лични бунт према државним структурама. Њих не одликује намера стицања материјалне користи што је карактеристично за већину извршилаца дела компјутерског криминалитета. Извришиоци ових дела су у већини случајева високо интелигентни, истрајни у свом раду, радознали, арогантни, неспособни да испоље емоционалну повезаност према људима итд. [31]

- **Тежина последица и настала штета**- Материјалне последице у већини случајева за собом повлаче и последице нематеријалне природе које могу бити и далеко значајније од материјалних ако се има у виду да нарушавање пословног угледа привредних и ванпривредних субјеката кроз најчешће неовлашћено откривање тајни може довести до потпуне обуставе сарадње између некадашњих пословних партнера. Поједине нематеријалне последице могу довести до оправданог страха и анксиозности за безбедност личних података у случају опасности злоупотребе истих. Висину штету проузроковану компјутерским криминалитетом је у појединим случајевима веома тешко прецизно одредити због могућности појаве нематеријално-финансијске штете. Она постоји када се откривањем одређене тајне, или нпр. повредом ауторског права злоупотребом компјутера, или информатичких мрежа наруши или повреди нечије морално право и тиме истовремено проузрокује и конкретна финансијска штета. [32]

[30] С. Петровић, оп.цит. стр. 18-19

[31] Детаљна анализа појма извршиоца дела компјутерског криминалитета и њихова подела биће представљена у одговарајућем поглављу.

[32] M. Boer, *Cooperation contre le piratage enregistrements sonores*, Lyon, 1996 цитирано према: М. Шкулић, *Компјутерски криминалитет- како одговорити на изазов*, Копаоник, 1998 стр. 1226

4. Институционални оквир и правна регулатива за борбу против компјутерског криминалитета

4.1 Међународноправне институције и инструменти супротстављања компјутерском криминалитету

Информационе и комуникационе технологије довеле су до напретка у многим областима друштвеног живота, незаменљиво олакшавајући функционисање друштва у целини. Међутим, експанзија кривичних дела компјутерског криминалитета је указала на потребу да се на глобалном нивоу предвиде одговарајуће, пре свега правне мере и механизми ради сузбијања овог типа криминалитета. Ефикасна борба против компјутерског криминалитета је незамислива без укључивања међународне заједнице кроз адекватну правну регулативу и без ангажовања међународних институција. Усвајањем правних стандарда донетих на међународном нивоу настаје одговарајући амбијент и правни оквир за сузбијање компјутерског криминалитета у националним оквирима. Најзначајнији правни нструменти у борби против компјутерског криминалитета настали су под окриљем Савета Европе, Европске Уније и Организације уједињених нација и они ће, због свог значаја, у раду бити детаљније објашњени.

4.1.1 **Активност Савета Европе у сузбијању компјутерског криминалитета**

Прва иницијатива ради правног регулисања и санкционисања компјутерског криминалитета на међународном нивоу покренута је од стране Савета Европе за време одржавања Европске конференције о криминолошким аспектима привредног криминалитета у Стразбуру.[33] Савет министара (енгл.Committee of Ministers), састављен од министара иностраних послова држава чланица Савета Европе, 1989. године је усвојио Препоруку о криминалним активностима везаним за употребу рачунара 89 (9) [34], којом су државе чланице позване да размотре увођење нових прописа који се односе на сузбијање и санкционисање компјутерског криминалитета. Препоруку за кривично процесно право у

[33] A Paper for the 12th Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime, Strasbourg, 15-18 November 1976, стр. 225 - 229, https://openlibrary.org/works/OL11001385W/Criminological_aspects_of_economic_crime, претражено 08. 06. 2017. године

[34] Препорука Савета Европе о криминалитету везаном за рачунаре бр. 89 (9), (Council of Europe Computer-related crime Recommendation No. R (89) 9, 1989) http://www.oas.o rg/juridico/english/89-9&final%20Report.pdf, претражено 07. 08. 2017. године

вези са информационим технологијама R (95)13 бр. 95,[35] усвојио је Савет Европе 11. септембра 1995. године. У Препоруци се користи термин „ злочини повезани са информационом технологијом “ (енгл. Offences connected with Information Tehnology – IT offences IT crimes) и наводи се да, у фази истраге за било које кривично дело повезано са информационом технологијом, овлашћени органи морају добити приступ свим информацијама које се обрађују или преносе комјутерским системима. Препорука садржи осамнаест основних принципа борбе против компјутерског криминалитета и представља први покушај међународног дефинисања процедура проналажења и заплене, надгледања, прикупљања и оцене електронских доказа, шифровање података и установљавања принципа међународне правне помоћи у области кривичних дела компјутерског криминалитета путем сарадње држава на међународном плану. [36] Упознат са опасношћу развоја информационе и комуникацине технологије, Европски комитет за проблеме кривичног права Савета Европе је током друге половине деведесетих година основао експертску групу, Комитет експерата за кривична дела почињена у сајбер простору [37] са задатком да сачини текст прве међународне конвенције чија би материја обухватила превенцију, хватање и кажњавање учинилаца кривичних дела из области високотехнолошког криминала.[38] Конвенција Савета Европе о високотехнолошком криминалу усвојена је 23. новембра 2001. године у Будимпешти,[39] ступила на снагу 1. јула 2004. године, и отворена за потписивање и према држава које нису чланице Савета Европе што указује на огроман значај овог међународног документа за ефикасно сузбијање високотехнолошког криминалитета. Разлози за доношење Конвенције су многобројни: постојање ризика да се због дигитализације, конвергенције и сталне глобализације рачунарске мреже и електронске информације могу користити и за извршење кривичних дела и да докази који се односе на таква дела могу бити сачувани и пренесени преко тих

[35] Recommendation No. R (95) 13 of the Committee of Ministers to Member States concering problems of Criminal Procedural Law connected with Information Technology, www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(1995)013_EN.asp, претражено 07.08. 2017. године

[36] В. Вилић, *Повреда права на приватност злоупотребом друштвених мрежа као облик компјутерског криминалитета (докторска дисертација)* Ниш, 2016 стр. 263

[37] Committee of Experts on Crime in Cyberspace (PC-CY)

[38] Одлука GDPC/103/211196 од 21. новембра 1993. Године; цитирано према: Л. Комплен- Николић,Р. Гвозденовић, С. Радуловић, А. Милосављевић, Р. Јерков, В. Живковић, С. Живановић, М. Рељановић, И. Алексић, Сузбијање високотехнолошког криминала,Београд, 2010 стр. 41

[39] Council of Europe, Convention on Cybercrime, European Treaty Series (ETS)- No. 185, Budapest, 23, XI 2001., http://conventions.coe.int/Treaty/en/Treaties/Word/185. doc претражено 07.09.2017. године

мрежа; потреба међународне сарадње између држава због транснационалног карактера високотехнолошког криминалитета; потреба заштите легитимних интереса у коришћењу и развоју информационе технологије; олакшавање откривања, истраге и гоњења кривичних дела компјутерског криминалитета на националном и међународном нивоу јер је тамна бројка веома велика; као и потреба поштовања и заштите права на приватност, личних података, сопственог мишљења и слободе изражавања.[40] Материјалне и процесне кривично правне одредбе Конвенције о високотехнолошком криминалу би својом имплементацијом у национална законодавства држава чланица требало да постигну висок степен хармонизације националних законодовстава, изградњу адекватних инструмената у циљу стварања неопходних основа за истрагу и кривично гоњење извршиоца кривичних дела компјутерског криминалитета и и да омогуће убзан квалитативан напредак међународне сарадње на пољу борбе против компјутерског криминалитета.

Додатни протокол уз Конвенцију о високотехнолошком криминалу донет је 28. јануара 2003. године , ступио на снагу 01. марта 2006. године.[41] Протокол се односи на инкриминацију следећих дела расистичке и ксенофобичне природе извршених преко рачунарских система: ширење расистичког и ксенофобичног материјала преко рачунарских система, претња мотивисна расизмом и ксенофобијом извршена преко рачунарског система, увреда мотивисана расизмом и ксенофобијом пласирана преко рачунарског система (јавно вређање преко рачунарског система лица или групе лица који се разликују по раси, боји коже, наследном, националном или етничком пореклу или вери), порицање, значајно умањивање, одобравање или оправдавање геноцида или злочина против човечности учињено уз помоћ рачунарског система. Наведена кривична дела морају бити извршена намерно или противправно. Основна сврха доношења Протокола јесте инкриминација понашања која нису обухваћена Конвенцијом, а која се тичу ширења мржње, нетолеранције и нетрпељивости према расним, националним, верским и другим групама и заједницама, коришћењем рачунара као средства комуникације и ширења

[40] В. Вилић, оп.цит. стр. 265

[41] Закон о потврђивању Додатног протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система(„Службени гласник РС”, бр. 19/2009) и Додатни протокол уз Конвенцију Савета Европе о високотехнолошком криминалитету бр .185 који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених путем компјутерских система (Additional Protocol on the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems), 2005, http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm, претражено 09. 07. 2017. године

пропаганде. [42] Конвенција о заштити права појединца у вези са аутоматском обрадом личних података [43] је отворена за потписивање државама чланицама 28. јануара 1981. године, ступла на правну снагу 01. октобра 1985. године. Усвојена је са циљем јачања правне регулативе на пољу заштите података о личности и поштовања приватности с обзиром на све интензивнији прекогранични промет личних података који су предмет аутоматске обраде.[44] Уочено је да национална законодавства држава чланица не пружају потребан ниво заштите грађанима у погледу заштите приватности посебно када се прикупљају лични подаци аутоматском обрадом за потребе државних органа и других правних лица. [45] Неопходне је да се лицима која имају приступ информација и подацима који су похрањени у рачунарима и рачунарским системима, ускрати и онемогући злоупотреба или било каква незаконита употреба ових података .[46] Најважнији део Конвенције чине одредбе материјалне природе које се односе на основне принципе као што су : квалитет прикупљања и аутоматске обраде личних података, посебне категорије података, безбедност података, додатне мере заштите субјекта података итд. Конвенција регулише и прекограничан промет аутоматски прикупљених података о личности као и међусобну сарадњу држава уговорница.

Конвенција о заштити деце од сексуалне експлоатације и сексуалног злостављања тзв. Ланзарот конвенција [47] је отворана за потписивање државама чланицама 25. октобра. 2007. године а на правну снагу је ступила 01. јула 2010. године. Са аспекта борбе против високотехнолошког криминала, Конвенција представља окосницу хармонизације националних законодавстава у погледу материјалног кривичног права у свим оним случајевима, у којима се елементи рачунарске технике користе у циљу дистрибуције, размене и складиштења недозвољеног садржаја.[48]Правно регулисање овог питања на међународном нивоу настало је због забрињавајуће великог пораста сексуалне

[42] Л.Комплен-Николић,Р. Гвозденовић, С. Радуловић, А. Милосављевић, Р. Јерков, В. Живковић, С. Живановић, М. Рељановић, И. Алексић, оп.цит. стр. 52
[43] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, the 28 January 1981(Entry into force: 01.10.1985);
http://conventions.coe.int/treaty/en/treaties/html/108.htm претражено 07.09. 2017. године
[44] В. Вилић, оп.цит. стр 274
[45] Ibid.
[46] Ј. Матијашевић, оп. цит. стр. 227
[47] Council of Europe, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No. : 201, Lanzarote, the 23 October 2007. (Entry into force 01.07. 2010);
http://conventions.coe.int/Treaty/EN/Treaties/Word/201.doc претражено 07.10.2017 . године
[48] Ј. Матијашевић, оп. цит. стр. 228

експолоатације и злоупотребе деце коришћењем информационих, рачунарских технологија и друштвених мрежа. Други разлог је неједнако правно регулисање у националним законодавствима до ког узраста се нека особа сматра дететом, због чега се кривична дела извршена према деци нису могла квалификовати као дела сексуалне експлоатације и злоупотребе деце. Због тога се у Конвенцији одређује да се под дететом подразумева свака особа млађа од 18 година.[49]Посебно се истиче значај сагледавања потребе припреме свеобухватног међународног инструмента за превенцију, заштиту и кривичноправни аспект борбе против свих форми сексуалног искоришћавања и сексуалне злоупотребе деце, при чему се посебна важност ставља на успостављање специјалног механизма за надзор спровођења Конвенције.[50] Основне поставке Конвенције обухватају: превентивну заштиту од насиља (енгл.„ prevention ”), заштиту детета жртве („ protection ”), кривично гоњење учиниоца („ prosecution ”) и учешће деце („ participation ”).

Савет Европе је 1977. године усвојио Конвенцију о сузбијању тероризма,[51] која је допуњена Конвенцијом о спречавању тероризма 2005. године. Конвенција је ступила на снагу 01. децембра 2009. године . Терористи и њихове организације, захваљујући употреби компјутера и интернета све чешће организују и остварују своје терористичке нападе. Уколико је циљ напада приступ информацијама од значаја за нормално функционисање државе и њених становника, напад може довести до масовне панике и страха становништва. Значајни чланови Конвенције су чл. 5-7, који се односе на одређене припремне радње које су таквог квалитета и значаја да имају потенцијал да изазову или помогну акте тероризма (јавно позивање, регрутовање на вршење терористичких аката, тренинг, обука будућих терориста).[52]

Препорука Савета Министара државама чланицама која се односи на заштиту људских права на друштвеним мрежама [53] усвојена 4. априла 2012. године под окриљем Савета Европе, друштвене мреже препознаје као„средство за реализацију људских права и

[49] В. Вилић, оп.цит. стр 276
[50] Ј. Матијашевић, оп. цит. стр. 228
[51] Закон о потврђивању Европске конвенције о сузбијању тероризма(“Службени лист СРЈ– Међународни уговори“ бр 10/2001 од 09. 11. 2001. године
[52] Ibid. 229
[53] Препорука Савета Министара Савета Европе CM/Rec(2012)4 државама чланицама која се односи на заштиту људских права на друштвеним мрежама(Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services), 2012, https://wcd.coe.int/ViewDoc.jsp?id=1929453, претражено 07. 07. 2017. године

катализатор за демократију".[54]Како друштвене мреже представљају средство за изражавање и комуникацију између појединаца али и директну групну комуникацију милиона људи, оне су својеврстан потенцијал за унапређење и остваривање људских права и основних људских слобода, а посебно за изражавање слободе говора, размене идеја и садржаја и слободу окупљања.[55] Препорука указује на могућност које друштвене мреже могу имати у повећању учешћа појединаца у политичком, друштвеном и културном животу, али такође могу представљати и потенцијално место за непоштовање и кршење људских права. Веома је важно предвидети одговарајуће материјалне и процесне одредбе како би се ефикасно уочили први видови злоупотребе на друштвеним мрежама и како би се извршиоцима дела компјутерског криминалитета онемогућио даљи приступ мрежама. На овај начин се обезбеђује делотворно санкционисање извршилаца без могућности даљег криминалног деловања на друштвеним мрежама. Препорука предвиђа као ефикасан начин да се спречи излагање непријатностима и опасностима деце на друштвеним мрежама, неопходност едукације о начинима безбедног коришћења мрежа од стране родитеља и наставника. Препорука је указала и на обавезу држава да свако сакупљање података о личности мора да буде транспарентно, да се тачно нагласи сврха сакупљања и складиштења података, начини сврха обраде ових података као и крајњи корисника сакупљене збирке података .[56]

4.1.2 **Активност Европске уније у сузбијању компјутерског криминалитета**

Поред упућивања препорука земаљама чланицама да потписују и усвајају конвенције и закључке Савета Европе, Европска унија доноси одговарајуће акте чији је циљ ефикаснија борба против компјутерског криминалитета. Комисија Европске заједнице објављује 1990. године одлуку која се тиче информатичке сигурности и заштите личних података. У оквиру Европске уније 2000. године усвојена је Директива о електронској тговини [57] и Одлука Европског савета о превенцији дечије порнографије на интернету.

[54] Тачка1 Препоруке Савета Министара државама чланицама која се односи на заштиту људских права на друштвеним мрежама
[55] В. Вилић, оп.цит. стр 280
[56] Тачка3 Препоруке Савета Министара државама чланицама која се односи на заштиту људских права на друштвеним мрежама
[57] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market(Directive on electronic commerce), Official Journal of the European Comuunities, L 178,17.07.2000 PP. 1-16; http://europa.eu.nint претражено 20.07.2017 године

Европска унија је 2004. године формирала Европску агенцију за безбедност мрежа и информационих система. Године 2005. ступила је на снагу Оквирна одлука о нападима на информационе системе.[58] Одлука регулише илегални приступ информационим системима, илегално ометање рачунарских система као и илегално ометање преноса података, али такође прописује и санкције за извршиоце кривичних дела компјутерског криминалитета.[59] Почетком 2007. године Европска унија је усвојила Стратегију за безбедно информационо друштво у Европи [60], док је Европска комисија 2009. године усвојила акциони план за заштиту критичне информационе инфраструктуре - „ Заштита Европе од бројних кибернетичких напада и ометања: побољшати спремност, безбедност и отпорност“,[61]постављајући безбедност и отпорност критичне информатичке инфраструктуре као дугорочни циљ у оквиру европске политике развоја безбедности мрежа и информација. [62]

У погледу борбе против компјутерског криминалитета важно је указати на Директиву Савета Европске заједнице о правној заштити компјутерских програма, [63] Директиву 2006/ 24 /ЕУ Европског парламента и Савета о чувању података који су добијени или обрађени приликом пружања јавно доступних услуга електронске комуникације или јавних комуникационих мрежа [64] и Директиву 2013/40/EU.[65] Директива

[58] Овирна одлука о нападима на информационе системе Комисије европских заједница(Framework Decision on attacks against information systems of the Commission of the European Communities), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222&from=EN, претражено12. 08. 2017. године

[59] Чл. 6 длуке предвиђа да је за неовлашћен упад у компјутерски систем и неовлашћено пресретање података прописана казна затвора у трајању од једне до три године, док је чл. 7 Одлуке предвиђено да, ценећи све отежавајуће околности извршеног дела, максимална казна затвора која може да буде пресуђена износи између две и пет година

[60] Стратегија за безбедно информационо друштво у Европи–Strategy for a Secure Information Society in Europe “Dialogue, partnership, and empowerment”, http://ec.europa.eu/information_society/doc/com2006251.pdf , претражено 21.07.2017.године

[61] Акциони план за заштиту критичне информационе инфраструктуре,, Заштита Европе од бројних кибернетичких напада и ометања: побољшати спремност, безбедност и отпорност“ – Communication on Critical Information Infrastructure Protection “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, secuirty and resilience”, 2009, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF, претражено 07. 11. 2017. године

[62] В. Вилић, оп.цит. стр 286

[63] Директива Савета Европске заједнице о правној заштити компјутерских програма (Council Directive of 14.may 1991. On the legal proctection of computer Programs) са обавезном применом у државама чланицама ЕУ почев од1.1.1993. године, објављена је у„Службеном листу Европске заједнице бр. Л122/42“ од1 7.5.1991. године

[64] Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in electronic communications services or of public communications networks and amending Directive

Савета европске заједнице о правној заштити компјутерских програм која је обавезу примењивања у државама чланицама стекла почев од 01. јануара 1993. године . Она предвиђа обавезу правног санкционисања низа понашања у вези са злоупотребом компјутера и компјутерских програма као и заштиту компјутерских програма ауторским правом као књижевна дела , и то у смислу одредаба Бернске конвенције за заштиту књижевних и уметничких дела. Директива 2006 / 24 / ЕУ Европског парламента и Савета о чувању података који су добијени или обрађени приликом пружања јавно доступних услуга електронске комуникације или јавних комуникационих мрежа [66] донета је 15. марта 2006. године са основним циљем да се ускладе одредбе држава чланица које се тичу обавезе даваоца јавно доступних услуга електронске комуникације и јавних комуникационих мрежа да чувају одређене податке које добијају или обрађују како би се осигурало да ти подаци буду доступни у сврху откривања, истраге и гоњења извршилаца тешких кривичних дела. Директива се примењује искључиво на податке о промету и локацији правних и физичких лица и на то повезане податке неопходне за идентификацију претплатника или регистрованог корисника. Директивом је регулисана и правна заштита лица о којима се подаци прикупљају и чувају за одговарајући временски период. Директива 2013/ 40/ EU, коју је донео Европски парламент 20. августа 2013. године обухвата област напада на информационе системе. У циљу приближавања кривичним законодавствима земаља чланица Европске уније, у Директиви се наводе минимална правила која се односе на дефиницију кривичних дела, кривичноправне санкције, унапређење сарадње између надлежних органа, укључујући припаднике полиције и других специјализованих агенција за спровођење закона чланица ЕУ, надлежних специјализованих агенција и тела ЕУ, као што су EUROJUST, EUROPO, Европски центар за сајбер криминиалитет и Европска агенција за безбедност мрежа и информационих система ENISA.[67] Директива, између осталог, уводи кривичне санкције за кривично дело у

2002/58/EC, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32006L0024, претражено17. 08. 2017. године

[65] Directive 2013/40/EU of the European Parliament and of the Council 12. 08. 2013, Offical Journal of the European Union 218/8, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040, претражено19. 08. 2017. године

[66] Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in electronic communications services or of public communications networks and amending Directive 2002/58/EC,

[67] В. Вилић, оп.цит. стр 286

виду прављења и коришћења тзв. „ ботнетова “ [68]и указује да велики напади могу изазвати значајну економску штету, која се огледа у прекидању рада информационих система и комуникација, као и губитак или измену комерцијално битних поверљивих информација и података.[69]

4.1.3 **Активност Уједињених Нација у сузбијању компјутерског криминалитета**

Правно регулисање компјутерског криминалитета у оквиру Уједињених Нација започето је 1990. године усвајањем Резолуције о законодавству у области компјутерског криминалитета.[70] Године 1994. донет је Приручник Организације Уједињених Нација о спречавању и контроли компјутерског криминала [71] да би маја 1988. године била донета Женевска резолуција о злоупотреби интернета у сврху сексуалне експолатације.[72] На 55. заседању Генералне скупштине Организације уједињених нација ревидирана је Резолуција бр. 55/ 63 о борби против злоупотребе информатичких технологија[73] која као своји основни принцип предвиђа потребу за усаглашеним законским решењима на међународном нивоу. У Резолуцији се наводи потреба за координисаном активношћу надлежних органа држава чланица који се баве истрагом и кривичним прогоном у вези са зоупотребом информатичких технологија, упознавањем јавности са опасностима које прете из сајбер простора и указивањем на мере превенције,истиче се и потреба да се адекватним правним механизмима заштити поверљивост и др. Резолуција садржи и

---

[68] Da би се успоставила удаљена контрола над значајним бројем рачунара они се инфицирају кроз инсталацију малициозног софтвера и прецизно усмерене сајбер нападе. Једном када се таква мрежа креира она конституише “ботнет“ који може бити активиран без знања и пристанка корисника рачунара ради отпочињања напада у широком обиму и захвату да може изазвати знатну штету. цит. према група аутора: „Високотехнолошки криминал“, Практични водич кроз савремено кривичноправо и примери из праксе , OSCE, Подгорица, март 2014, www.osce.org/me/montenegro/117630?download=true, претражено 15. 08. 2017. године

[69] В. Вилић, оп.цит. стр 286

[70] РезолуцијаУједињених Нацијао законодавству у области компјутерског криминалитета(UN resolution on computer crime legislation), http://www.unodc.org/documents/congress//Previous_Congresses/8th_Congress_1990/028_ACONF.144.28.Rev.1_Report_Eighth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders.pdf, претражено дана 11. 08. 2017. године

[71] Приручник УН о спречавању и контроли компјутерског криминала (United Nations Manual on the Prevention and Control of Computer-related Crime), 1994,

[72] РезолуцијаУједињених Нација(тзв. Женевска резолуција) о злоупотреби интернета у сврху сексуалне експлоатације(UN Resolution on Missuse of the Internet for the Purpose of Sexual Exploatation), http://www.uri.edu/artsci/wms/hughes/ppr.htm, прежено 05. 07. 2017. године

[73] Ревидирана Резолуција Уједињених Нација A/res/55/63 о борби против злоупотребе информационих технологија(UN resolution A/res/55/63 on combating the criminal misuse of information technologies), 2001, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf, претражено11. 08. 2017. године

упозорење државама да у борби против компјутерског криминалитета мора да се очува баланс између индивидуалних права и слобода гарантованих сваком појединцу, са једне стране, и права држава да кривично гони извршиоце кривичних дела, са друге стране. [74] Резолуција бр. 56/121 о борби против злоупотребе информатичких технологија[75] је усвојена на 88. пленарном заседању Генералне скупштине Организације Уједињених Нација 2002. године. Резолуција представља допуну претходно усвојене резолуције 55/63 указајући на потребу да се приликом усвајања одговарајућих закона, као и приликом утврђивања политике кривичног прогона узму у обзир резултати рада Комисије за превенцију криминала и кривично правосуђе као и других релевантних међународних организација. Резолуција Економско - социјалног савета 2007/ 20 [76] ,усвојена јула 2007. године, подстиче ширу и ефикаснију употребу модерних технологија у превенцији и сузбијању криминалитета. Резолуција позива на разматрање могућности приступања пре свега Конвенцији о високотехнолошком криминалу, ка о и осталим међународно-правним актима који се односе на привредни криминалитет и злоупотребу идентита и података који се истог тичу. Усвајањем Резолуције 65/230 [77] предложено је формирање међувладине експертске групе која би спровела свеобухватну студију о компјутерском криминалитету и о томе како државе реагују на поједине случајеве ове врсте криминалитета. Студија је имала за циљ да сагледа и ојача постојеће механизме реаговања на компјутерски криминалитет, да предложи начине за побољшање постојећих.

Једно од најзначајнијих специјализованих тела ОУН и једна од најактивнијих институција Организације Уједињених Нација у домену борбе против високотехнолошког криминалитета, која има главну улогу у поступку хармонизације националних законодавстава и безбедности у сајбер простору, је Међународна телекомуникациона унија чије је седиште у Женеви у Швајцарској. Ова институција је свој активни рад

[74] М. Ромић , Н. Грбић-Павловић,*Међународноправни документи којима се уређује област високотехнолошког криминала*, , Лакташи 28 - 30. 03. 2012. године, стр. 196, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2017.године

[75] РезолуцијаУједињених НацијаA/res/56/121 о борби против злоупотребе информационих технологија(UN resolution A/res/56/121 on combating the criminal misuse of informationtechnologies), 2002, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf, претражено20. 08. 2017.године

[76] Резолуција2007/20 од 26. 07. 2007. године, www.un.org/.../ecosoc/.../2007 /Resolution%2020, претражено 25. 04. 2017. године

[77] Comprehensive Study on Cybercrime – Draft, United Nations office on drugs and crime, Vienna, February 2013, United Nations, New York 2013, стр. Ix, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, претражено 12. 08. 2017. године

започела маја 2007. године, када је донет Меморандум о глобалној сајбер безбедности[78], у циљу стварања глобалног оквира за дијалог и међународну сарадњу приликом предлагања стратегије за повећање безбедности у сајбер простору. Важно је напоменути и Канцеларију Уједињених нација за контролу наркотика и превенцију криминала која се нарочито бави злоупотребом идентитата, и Канцеларија Уједињених нација за послове разоружања која обухвата у своју делатност информациони рат и сајбер тероризам.

4.2 Националноправни инструменти супротстављања компјутерском криминалитету

Потписивањем Конвенције о високотехнолошком криминалу Савета Европе и Додатног протокола 2005. године а нарочито ратификацијом 2009. године Република Србија је преузела обавезу да створи одговарајући нормативни и институционални оквир за успешну борбу против компјутерског криминалитета. Најзначајнији пропис материјалноправне природе који садржи кривична дела компјутерског криминалитета, Кривични законик Републике Србије,[79] и најзначајнији пропис статусног карактера , Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала,[80] обезбеђују полазни правни оквир за поступање државних органа у кривичноправним стварима које се односе на компјутерски криминалитет. Законик о кривичном поступку[81] успоставља процесноправне оквире којима су предвиђени механизми и овлашћења државних органа у поступцима откривања, прикупљања доказа, кривичног гоњења и суђења учиниоцима кривичних дела високотехнолошког криминала.[82] Међу најзначајнијим законима издвајају се и: Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима,[83] Закон о

[78] Глобална платформа о сајбер сигурности Међународне телекомуникационе уније (Global Cybersecurity Agenda (GCA) of the International Telecommunication Union), www.itu.int/osg/csd/cybersecurity/gca, претражено 11. 08. 2017. године

[79] Кривични законик Републике Србије(„Службени гласникРС" бр.85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012 и104/2013 108/2014 и 94/2016)

[80] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала(„Службени гласник РС" бр.61/2005 и104/2009)

[81] Законик о кривичном поступку („Сл. гласник РС", бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014)

[82] Л.Комплен-Николић,Р. Гвозденовић, С. Радуловић, А. Милосављевић, Р. Јерков, В. Живковић, С. Живановић, М. Рељановић, И. Алексић, оп.цит. стр. 52

[83]Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима(„СлужбенигласникРС" бр.32/2013)

ауторским и сродним правима [84] и Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине. [85] Институционални оквир за примену одредби закона који се односе на компјутерски криминалитет обухвата посебне организационе јединице постојећих државних органа, чије је деловање усмерено на ефикаснију и бржу заштиту од компјутерског криминалитета и спровођењу превентивних и репресивних мера. Специјализација државних органа за борбу против компјутерског криминалитета неопходна је због сложености и посебних карактеристика компјутерског криминалитета, као и због сталног праћења развоја савремених компјутерских технологија.[86] Поред посебних организационих јединица у државним органима, значајну улогу у овој области имају Министарство трговине, туризма и комуникацијама, Републичка агенција за електронске комуникације и Републичка радио дифузна агенција.

Кривична дела компјутерског криминалитета предвиђена Кривичним законом Републике Србије (у даљем тексту КЗ РС) могу се сврстати у три групе према члану 3 Закона о организацији и надлежности државних органа: (1) сва кривична дела која за групни заштитни објекат имају безбедност рачунарских података; (2) кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења јављају рачунари, рачунарске мреже, рачунарски подаци и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 2000 или настала материјална штета прелази износ од милион динара и (3) кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира, уставног уређења и безбедности Републике Србије, која због начина извршења или употребљених средстава несумњиво припадају компјутерском криминалитету.

У члану 112. став 16-20 и 33-34 КЗ РС дефинисани су појмови: рачунар, рачунарски податак, рачунарска мрежа, рачунарски програм, рачунарски вирус и рачунарски систем. Рачунар је сваки електронски уређај који на основу програма аутоматски обрађује и размењује податке. Рачунарски податак је свако представљање чињеница, информација или концепта у облику који је подесан за њихову обраду у рачунарском систему,

[84] Закон о ауторским и сроднимправима („СлужбенигласникРС“ бр. 104/2009, 99/2011 и119/2012 и 29/2016-одлука УС).
[85] Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине(„Службени гласника РС“ бр. 46/2006, 104/2009 – др. закони)
[86] В. Вилић оп.цит. стр 316

укључујући и одговарајући програм на основу кога рачунарски систем обавља своју функцију, Рачунарска мрежа представља скуп међусобних рачунара, односно рачунарских система који комуницирају размењујући податке. Рачунарски програмом сматра се уређени скуп наредби који служе за управљање радом рачунара, као и за решавање одређеног задатка помоћу рачунара. 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. Рачунарски систем је сваки уређај или група међусобно повезаних или зависних уређаја од којих један или више њих, на основу програма, врши аутоматску обраду података.

4.2.1 **Кривични законик**

4.2.1.1 **Прва група кривичних дела компјутерског криминалитета**

Прва групу кривичних дела компјутерског криминалитета према КЗ РС односи се на безбедност рачунарских података. КЗ РС у највећем делу је услађен са одредбама Конвенције о високотехнолошком криминалу предвиђајући дела која су у складу са одредбама чланова 4,5,6,7 и 8 Конвенције : оштећење рачунарских података и програма (чл. 298), рачунарска саботажа (чл. 299), прављење и уношење рачунарских вируса (чл.300), рачунарска превара (чл. 301), неовлашћен приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (чл. 302), спречавање и ограничавање приступа јавној рачунарској мрежи (чл. 303), неовлашћено коришћење рачунара или рачунарске мреже (чл. 304) и прављење, набављање и давање другом средства за извршење кривичних дела против безбедности рачунарских података (чл. 304а).

- **Оштећење рачунарских података и програма** - има један основни и два квалификована облика. Основни облик се састоји у у неовлашћеном брисању, измени, оштећењу, прикривању или чињењу неупотребљивим рачунарског податка или програма. Квалификовани облици постоје када штета предузетом радњом извршења кривичног дела прелази одређени новчани износ. Правилна квалификација дела, која се тиче и других одговарајућих кривичних дела, претпоставља утврђење неколико битних чињеница. Пре свега потребно је утврдити својство учиниоца, односно да ли је извршилац поступао неовлашћено или је пак био овлашћен да предузме одређену радњу, затим тачно време и

место извршења дела, начин на који је дело извршено (интерни ли екстерни напад) и у склопу тога да ли је учинилац користио одређену опрему (и коју) приликом извршења дела, врсту и тежину последице, итд. [87] С обзиром да се ради о кривичном делу из области високотехнолошког криминала, посебан је акценат стављен на правилно и благовремено обезбеђење доказа за даље фазе поступка .[88] С обзиром на радњу извршења овог кривичног дела, често је отежано прикупљање доказа због чега каснији повраћај података не представља околност која елиминише постојање кривичног дела.[89]

- **Рачунарска саботажа** - представља дело уношења, уништавања, брисања, измене, оштећења, прикривања или на други начин чињења неупотребљивим рачунарског податка или програма или уништење или оштећење 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 државне органе, јавне службе, установе, предузећа или друге субјекте. Битно обележје овог дела јесте намера учиниоца да предузимањем радње онемогући или омете поступак електронске обраде или преноса података значајних за поменуте субјекте, те је ову намеру потребно утврдити и доказати, односно наведена последица не може настати као резултат само случаја или непажње. [90] Повећана друштвена опасност овог кривичног дела произилази из чињенице да се њиме оштећују државни органи, јавне службе, установе, предузећа или други субјекти.

- Кривично дело прављење и уношење рачунарских вируса - има два облика: прављење рачунарског вируса у намери његовог уношења у туђ рачунар или рачунарску мрежу и уношење рачунарског вируса у туђ рачунар или рачунарску мрежу при чему је настала штета. Рачунарски вируси поседују капацитет угрожавања објеката инфраструктуре, електричних мрежа, финансијских трансакција, транспортног саобраћаја,

[87] Ј. Матијашевић оп. ци.т стр. 103
[88] Ibid.
[89] Најчешћи вид извршења овог кривичног дела је рушење веб сајтова. Хакери нападају најчешће само део сајта , на пример насловну страну која се промени и на њој се остави хакерски,, потпис “ , порука или поздрав. Слаба заштита веб сајтова и недовољна информисаност о опасностима које могу доћи са интернета погодују вршењу ових кривичних дела. Извршиоце је врло тешко открити јер они користе алате за скривање који онемогућавају утврђивање места са кога је напад дошао . Видети више: Л.Комплен-Николић,Р. Гвозденовић, С. Радуловић, А. Милосављевић, Р. Јерков, В. Живковић, С. Живановић, М. Рељановић, И. Алексић,Кратак приказ развоја правне регулативе о високотехнолошком криминалитету на међународном нивоу, Београд, 2010, стр .91
[90] Л. Комплен- Николић,Р. Гвозденовић, С. Радуловић, А. Милосављевић, Р. Јерков, В. Живковић, С. Живановић, М. Рељановић, И. Алексић, Сузбијање високотехнолошког криминала,оп. цит. стр. 93

војних одбрамбених система, и других система који се све више ослањају у свом раду на компјутерску технологију. Ово кривично дело одликује велика присутност тамне бројке што директно имплицира на недовољно развијену свест опште и научне, стручне јавности о начинима ефикасног откривања и процесуирања. Код овог кривичног дела поред казне предвиђено је одузимање уређаја и средстава којима је кривично дело учињено.

- **Кривично дело рачунарска превара** - има основни облик, два тежа и један посебан облик. Основни облик постоји када се уносе нетачан податак, пропусти уношење тачног податка, прикрије или лажно прикаже податак, чиме извршилац утиче на резултат електронске обраде и преноса података у намери да себи или другом прибави противправну имовинску корист и тиме другом проузрокује имовинску штету. Тежи облици овог кривичног дела постоје у два случаја када износ прибављене против правне имовинске користи прелази износ од четири стотине педесет хиљада динара и када износ прелази милион петсто хиљада динара. Ово кривично дело има привилегован облик када је дело извршено само у намери да се другоме причини штета Кривично дело рачунарске преваре треба разликовати од класичног кривичног дела преваре (чл. 208 КЗ РС) које припада групи кривичних дела против имовине. Иако у закону није изричито наглашено, кривично дело преваре може бити извршено коришћењем рачунарских технологија, када извршилац у намери да себи или другоме прибави противправну имовинску корист лажним приказивањем неких чињеница или њиховим прикривањем оштећеног доведе у заблуду или га одржава у заблуди и тиме га наведе да на штету своје или туђе имовине нешто учини или не учини. [91] Правилна квалификација и доказивање кривичног дела претпоставља тачно утврђење предузете радње, начин уношења нетачног података и последица на резултат елекронске обраде и преноса података.

- **Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података** - постоји у случају кршења мера заштите неовлашћеним укључивањем у рачунар или рачунарску мрежу или у случају неовлашћеног приступу електронској обради података, као и услед употребе података добијених на овај начин. Поред наведеног основног облика дела постоје и два тежа облика. Први тежи облик чини лице које сними или употреби податак добијен радњом извршења наведеном у основном облику. Најтежи, други, тежи облик постоји када је услед предузете радње извршења

[91] В. Вилић оп.цит. стр. 320

дошло до застоја или озбиљног померемећаја у функционисању електронске обраде и преноса података или мреже или су наступиле друге тешке последице. Ово кривично дело је према начину извршења слично кривичном делу шпијунаже (члан 315 КЗ РС), које припада групи кривичних дела против уставног уређења и безбедности Републике Србије. Због тога је приликом квалификације кривичног дела неопходно да се са сигурношћу утврди да ли је упадом у рачунарски систем извршилац дошао до војних, економских или службених података или докумената који су законом, другим прописом или одлуком надлежног органа донетом на основу закона, проглашени тајним; да ли је одавање таквих података проузроковало штетне последице за безбедност, одбрану или за политичке, војне или економске интересе земље и какав је умишљај учиниоца.[92]

- **Кривично дело спречавање и ограничавање приступа јавној рачунарској мрежи -**има основни и тежи облик. Основни постоји када се неовлашћено спречава или омета приступ јавној рачунарској мрежи, док тежи постоји уколико је дело извршило службено лице у вршењу службе. За правилну квалификацију дела неопходно је посебно утврдити својство мреже (да ли је реч о јавној рачунарској мрежи или не) и да ли је извршилац поступао неовлашћено или је спречавање, ограничавање приступа јавној рачунарској мрежи извршио уз постојање правног основа. Доказивање овог кривичног дела је веома тешко због немогућности идентификовања идентитета извршилаца напада, великог броја „заражених“ рачунара чији корисници нису ни свесни да им је рачунар злоупотребљен.[93] У пракси, потребно је обратити пажњу на то да ли је наведно кривично дело извршено у функцији неког другог кривичног дела или је праћено још неком радњом која по својим елементима представља биће неког другог кривичног дела, у ком случају се поставља питање њиховог међусобног односа и повезаности.[94]

---

[92] Ibid.

[93] Најчешћи су DDoS (Distributed Denial of Sevice) напади, када се помоћу одређеног малициозног софтвера остварује контрола над великим бројемn рачунара. Пример за ове нападе је напад на интернет сајт Православне цркве и обарање интернет презентације радио емисије„Печшаник“. Видети: : Л.Комплен-Николић,Р. Гвозденовић, С. Радуловић, А. Милосављевић, Р. Јерков, В. Живковић, С. Живановић, М. Рељановић, И. Алексић,Кратак приказ развоја правне регулативе о високотехнолошком криминалитету на међународном нивоу, оп.цит , стр .91 Cyber секција Народноосободилачког фронта преузела је пуну одговорност за напад на хрватски Телеком, који се догодио у току ноћи 21. И 22. 09. 2015. године, тврди да су напад извели јер се боре против капитализма и за успостављање самоуправног социјалистичког друштва. Али и на Twitteru KuNaNeT стоји порука како су они извршили DdoS напад , тако да није познато да ли су те две групе хакера повезане,.Видети : Јутарњи лист , www.jutarnji.hr, претражено 22. 08. 2017. године

[94] Група аутора: „ Приручник за истрагу кривичних дела у области високотехнолошког криминала“, Савет Европе, 2008, стр. 126; цит. према: Л. Комплен- Николић,Р. Гвозденовић, С. Радуловић, А. Милосављевић, Р.

- Неовлашћено коришћење рачунара или рачунарске мреже - постоји када особа неовлашћено користи рачунарске услуге или рачунарску мрежу у намери да себи или другом прибави противправну имовинску корист. Карактеристика овог кривичног дела која га разликује од напред наведених састоји се у кривичном гоњењу које се предузима по приватној тужби. Међутим, и у случају овог кривичног дела овлашћена службена лица су дужна да предузму радње из своје надлежности и да прикупе потребне доказе, уколико постоје основи сумње да је у вези са радњама које спадају у ово кривично дело извршено и неко друго кривично дело за које се гоњење предузима по службеној дужности, у ком случају за то дело важе овлашћења и одредбе које се односе на подношење кривичне пријаве. [95]

- Кривично дело прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података - постоји када извршилац поседује, прави, набавља, продаје или даје другом на употребу рачунаре, рачунарске системе, рачунарске податке и програме ради извршења једног од кривичних дела против безбедности рачунарских података. У складу са овим, нарочито је битно утврдити намеру учиниоца кривичног дела, као и његово својсво и прилике у којима је деловао, затим врсту и садржај рачунарских података, програма и система, разлог његовог поседовања (нарочито уколико су штетни), време и околности прављења, набављања, продавања или давања другом и друге битне податке потребне да би се утврдило који су мотиви предузетих радњи и да ли је у конкретном случају дошло до вршења кривичног дела, односно до кривичне одговорности учиниоца.[96]Предмети коришћени за ивршење кривичног дела (рачунари, рачунарски системи, рачунарски подаци и програми) одузимају се од извршилаца.

4.2.1.2 Друга група кривичних дела компјутерског криминалитета

Друга група обухвата кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења јављају рачунари, рачунарске мреже, рачунарски подаци и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 2000 или настала

Јерков, В. Живковић, С. Живановић, М. Рељановић, И. Алексић, Сузбијање високотехнолошког криминала,оп. цит. стр. 107

[95] Ibid., стр. 110

[96] Ј. Матијашевић оп. цит. стр. 115

материјална штета прелази износ од милион динара. Нека од дела која су наведена у овом раду су : повреда моралних права аутора и интерпретатора (члан 198), неовлашћено искоришћавање ауторског дела или предмета сродног права (члан 199), неовлашћено уклањање или мењање електронске информације о ауторском и сродним правима (члан 200), фалсификовање и злоупотреба платних картица (члан 243), превара (члан 208).

- **Повреда моралних права аутора и интерпретатора -** постоји: (1) када неко лице под својим именом или именом другог лица у целини или делимично објави, стави у промет примерке туђег ауторског дела или интерпретације или на други начин јавно саопшти туђе ауторско дело или интерпретацију; (2) када се без дозволе аутора измени или преради туђе ауторско дело или туђа снимљена интерпретација; (3) када се стави у промет примерак туђег ауторског дела или интерпретације на начин којим се вређа част или углед аутора или извођача. Развој компјутерске технологије, а нарочито компјутерских мрежа, омогућио је настанак нових начина комуникације и размене ифнормација. Упоредо је створена и могућност за најразличитије видове злоупотребе наведене технологије. Многобројни текстови који се објављују на интернету доступни су великом броју корисника, што представља идеалну подлогу за објављивање туђих дела под својим именом и без дозволе аутора.

- Кривично дело неовлашћено искоришћавање ауторског дела или предмета сродног права - има неколико појавних облика. Први облик се састоји у неовлашћеном објављивању, снимању, умножавању или на други начин јавном саопштавању у целини или делимично ауторског дела, интерпретације, фонограма, видеограма, емисије, рачунарског програма или базе података. Други облик обухвата стављање у промет или у намери стављања у промет држање неовлашћено умножених или неовлашћено стављених у промет примерака ауторских дела. Трећи облик је тежи јер се наведене радње предузимају у намери прибављања имовинске користи за себе или другог. Посебан, четврти облик овог кривичног дела постоји када дође до производње, увоза, стављања у промет,продаје, давања у закуп, рекламирања у циљу продаје или давања у закуп или држања у комерцијалне сврхе уређаја или средстава чија је основна или претежна намена уклањање, заобилажење или осујећивање технолошких мера намењенихспречавању повреда ауторских и сродних права, или коришћење таквих уређаја или средстава у циљу повреде ауторског или сродног права. Последњим обликом инкриминисане су припремне

радње за извршење осталих облика кривичног дела. Предмети из претходно наведена три облика вршења овог кривичног дела ће се одузети и уништити. Овим кривичним делом инкриминисана је пиратерија као једна од криминалних активности која гарантује за извршиоце дела велике новчане приходе. Тешкоће приликом откривања и доказивања овог дела произилазе из чињенице да извршиоци могу бити било ког узраста и образовања, да се пиратске копије врло тешко проналазе и веома лако дистрибуирају.

- **Неовлашћено уклањање или мењање електронске информације о ауторском и сродним правима -** постоји када дође до неовлашћеног уклањања или измене електронске информације о ауторском или сродном праву, или стављању у промет, увозу, извозу, емитовању или на други начин јавном саопштавању ауторског дела или предмета сродно правне заштите са којег је електронска информација о правима неовлашћено уклоњена или измењена. Доказивање овог кривичног дела је веома комплексно, треба обратити пажњу на средства којима је дело извршено, напостојање одређене заштите ауторског и сродног права у облику електронске информације, на везу између извршиоца са уклањањем информације, као и на чињеницу да се уклањање врши неовлашћено. [97]

- **Фалсификовање и злоупотреба платних картица -** постоји када лице направи лажну платну картицу или преиначи праву платну картицу у намери да је употреби као праву или такву лажну картицу употреби као праву. Квалификовани облици постоје када је употребом картице прибављена противправна имовинска корист, када је учинилац прибавио противправну имовинску корист у износу који прелази износ од милион и петсто хиљада динара, када лице неовлашћено употреби туђе картице или поверљиве податке који јединствено уређују ту картицу у платном промету . Посебан облик постоји у случају да лице набави лажну платну картицу у намери да је употреби као праву или прибави податке у намери да их искористи за прављење лажне платне картице. Лажне платне картице се одузимају. Последњих година извршење овог кривичног дела је у драстичном порасту захваљујући све савременијим начинима и уређајима за његово извршење. Нарочито је потребно обратити пажњу на могуће радње саучесништва , јер ово кривично дело и његове радње, као и начин његовог извршења, могу обухватати више лица са различитим задужењима у оквиру криминалне групе – набавка бланко картица, набавка

[97] Д.Прља, М. Рељановић, З.Ивановић, *Интернет право*, Београд, 2012, стр. 50

уређаја, набавка кодова, израда лажних платних или преиначење правих платних картица, каснија употреба у промету или дистрибуција ради употребе у промету итд. [98]

- Кривично дело превара - постоји када лице у намери да себи или другом прибави противправну имовинску корист доведе кога лажним приказивањим или прикривањем чињеница у заблуду или га одржава у заблуди и тиме га наведе да овај на штету своје или туђе имовине нешто учини или не учини. Привилегован облик постоји у случају да је извршилац имао само намеру да другог оштети. Превара има два кавилификована облика. Први постоји када је прибављена имовинска корист или нанета штета у износу који прелази четристопедесет хиљада динара. Други постоји ако је прибављена имовинска корист или нанета штета у износу који прелази милион и петсто хиљада данара. Глобална рачунарска мрежа представља нову област деловања извршилаца кривичних дела, који на превараан начин остварују имовинску корист.[99] Извршиоци се служе погодношћу да им интернет пружа скоро потпуну анонимност, као и чињеница да је дигиталне финансијске токове, који обично воде преко више држава, веома тешко пратити и утврдити крајњу дестинацију средстава. [100]

4.2.1.3 Трећа група кривичних дела компјутерског криминалитета

Трећа група обухвата кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира, уставног уређења и безбедности Републике Србије, која због начина извршења или употребљених средстава несумњиво припадају компјутерском криминалитету. Нека од њих су: приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију (члан 185), искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу (члан 185б).

- Кривично дело приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију - има четири облика с обзиром на радње извршења овог кривичног дела : (1) продаја, приказивање, чињење доступним јавним излагањем или на други начин текстова, слика, аудио визуелних или других предмета порнографске садржине или приказивање порнографске представе

[98] Ј. Матијашевић оп. цит. стр. 121
[99] Л. Комплен- Николић,Р. Гвозденовић, С. Радуловић, А. Милосављевић, Р. Јерков, В. Живковић, С. Живановић, М. Рељановић, И. Алексић, оп.цит., стр. 126
[100] Ibid.

малолетнику; (2) искоришћавање малолетника за производњу слика, аудио-визуелних или других предмета порнографске садржине или за порнографску представу; (3) извршење оба облика кривичних дела према детету представља тежи облик кривичног дела; (4) прибављање за себе или другог, поседовање, продаја, приказивање, јавно излагање или електронски или на други начин чињење доступним слике, аудио визуелног или другог предмета порнографске садржине настале искоришћавањем малолетног лица. Код последњег облика овог кривичног дела, које може бити извршено само према пунолетном лицу (ако је извршено према малолетнику, дело се квалификује према ст.1 овог члана) изричито се наводи као радња извршења чињење доступним слике, аудио визуелног или другог предмета порнографске садржине настале искоришћавањем малолетног лица електронским путем, што значи, поред осталог, искоришћењем компјутера и интернета. Предмети којима се врши ово дело се одузимају.Према члану 112. ст. 8 КЗ РС дететом се сматра лице које није навршило четрнаест година. Малолетником се сматра лице које није навршило осамнаест година(ст.9). С обзиром да Законик не дефинише појам порнографског материјала, ово питање се мора утврђивати у сваком конкретном случају. Сузбијање дечије порнографије на интернету представља велики изазов за полицију и правосудне органе, посебно у транзиционим земљама попут Србије, јер криминалци стално усавршавају начине извршења кривичног дела како би даље развили тржиште, осигурањем бржег и лакшег приступа педофилским садржајима, уз што је могуће већу анонимност клијената.[101] Веома је важно истаћи чињеницу да је у случају овог кривичног дела реч о малолетним лицима, што захтева посебну пажњу у поступању, имајући у виду њихове године, специфично психофизичко стање и процес развоја и сазревања, било да је у питању малолетно лице као извршилац кривичног дела или такво лице као оштећени или сведок. [102]

- Кривичним делом искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу - (чл.185б КЗ РС) санкционисано је коришћење рачунарске

[101] С. Кораћ, Сузбијање дечије порнограгије на Интернету: ЕУ стандарди, Београд, 2008, стр. 47
[102] Група аутора: „ Приручник за истрагу кривичних дела у области високотехнолошког криминала“, Савет Европе, 2008, стр. 148; цит. према: Л. Комплен- Николић,Р. Гвозденовић, С. Радуловић, А. Милосављевић, Р. Јерков, В. Живковић, С. Живановић, М. Рељановић, И. Алексић, Сузбијање високотехнолошког криминала,оп. цит. стр. 112

мреже или комуникације другим техничким средствима у намери извршења кривичних дела против полне слободе према малолетном лицу или детету договарањем састанка и појављивањем на договореном месту ради састанка. Први облик овог кривичног дела састоји се у коришћењу рачунарске мреже или комуникације другим техничким средствима за договарање састанка и појављивање на договореном месту ради састанка у намери извршења кривичног дела силовања(чл. 178 ст. 4), обљубе над немоћним лицем (чл. 180 ст. 1 и2), обљубе са дететом(чл. 180 ст. 1 и2), обљубе злоупотребом положаја (чл. 181 ст. 2 и 3), недозвољене полне радње(чл. 182 ст. 1), подвођење и омогућавање вршењаполног односа (чл. 183 ст. 2), посредовање у вршењу проституције (чл. 184 ст. 2), коришћење малолетниказа производњу слика, аудио-визуелних или других предмета порнографске садржинеили за порнографску представу (чл. 185 ст. 2.) и навођење малолетног лица на присуствовање полним радњама (чл. 185а). Тежи облик овог кривичног дела постоји када је кривично дело учињено према детету.

4.2.2 **Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала**

Ступањем на снагу Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала 25. јула 2005. године и његових измена и допуна 11. децембра 2009. године,успостављена је организација и одређена надлежност државних органа у борби против високотехнолошког криминала. Закон уређује образовање, организацију, надлежност и овлашћења посебних организационих јединица државних органа ради откривања , кривичног гоњења и суђења за кривична дела високотехнолошког криминала (чл.1). Високотехнолошки криминал у смислу овог закона представља вршење кривичних дела код којих се као објект или средство извршења јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику – рачунарски програми и ауторска дела која се могу употребити у електронском облику (чл.2). У члану 3 закона прецизирано је да се његове одредбе примењују ради откривања, кривичног гоњења и суђења за (1) сва кривична дела против безбедности рачунарских података одређена Кривичним закоником; (2) кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења јављају рачунари, рачунарске мреже,

рачунарски подаци и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 2000 или настала материјална штета прелази износ од милион динара и (3) кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира, уставног уређења и безбедности Републике Србије, која због начина извршења или употребљених средстава несумњиво припадају компјутерском криминалитету . За поступање по кривичним делима високотехнолошког криминалитета надлежно је Више јавно тужилаштво у Београду за територију Републике Србије. У оквиру Вишег јавног тужилаштва у Београду образовано је Посебно тужилаштво за борбу против високотехнолошког криминала 20. фебруара 2007. године као посебно одељење Окружног јавног тужилаштва у Београду. Посебног тужиоца поставља на четири године Републички јавни тужилац, при чему предност у избору имају јавни тужиоци и заменици јавних тужиоца који поседују знање из области информатичких технологија. Посебни тужилац се поставља на четири године са могућношћу реизбора. У оквиру Министарства надлжног за унутрашње послове формирана је Служба за борбу против високотехнолошког криминала ради поступања по захтевима Посебног тужиоца за високотехнолошки криминал. Службом руководи старешина кога поставља и разрешава министар надлежан за унутрашње послове, по прибављеном мишљењу Посебног тужиоца. Министар надлежан за унутрашње послове у складу са овим законом ближе уређује рад Службе. У оквиру Вишег суда у Београду за поступање по кривичним делима високотехнолошког криминалитета образовано је Одељење за борбу против високотехнолошког криминала. Судије у одељењу, на период од две године уз могућност продужења, распоређује председник Вишег суда у Београду из реда судија наведеног и других судова, уз њихову сагласност. Предност имају судије које поседују посебна знања из области информатичких технологија. Наведени органи имају територијалну надлежност на целој територији Републике Србије. Оваквим законским решењем успостављен је адекватан правно институционални оквир за поступање правосудних и полицијских органа у овој области, који пружа добар основ за успешну борбу против високотехнолошког криминалитета. [103] Пре измена Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала, до којих је дошло 2009. године, био је спорна начин

[103] В. Вилић оп.цит. стр.334

формулисања стварне надлежности поменутих органа.[104] Због тога је предложено проширивање стварне надлежности ових органа за сва кривична дела која по начину, средствима и објекту извршења представљају дела из области високотехнолошког криминалитета.[105]

4.2.3 **Законик о кривичном поступку Републике Србије**

Законик о кривичном поступку Републике Србије (у даљем тексту ЗКП) садржи одребе процесноправног карактера које се односе на процесне механизме и овлашћења учесника у кривичном поступку, откривање учинилаца кривичих дела, прикупљање доказа, процесуирање и суђење. С обзиром да се у поступцима за дела компјутерског криминалитета не мења процесна структура (процесна фаза и стадијуми), већ само поједине одредбе о процесним субјектима или процесним радњама, не може се радити о посебној кривичнопроцесној форми, него искључиво о процесном варијабилитету.[106] Један од недостатака важећег ЗКП јесте што не дефинише електронски доказ који има посебан значај за компјутерски криминалитет. ЗКП не садржи посебне одредбе које се односе на прикупљање и обезбеђивање доказа за кривична дела која припадају компјутерском криминалитету нити издваја посебно и не препознаје значај електронских доказа у процесу доказивања кривичних дела компјутерског криминалитета. Наведени докази имају исту вредност као и сви други материјални докази и за њих важе иста процесна правила као и за остале доказе. Електронски докази се могу врло лако изменити, обрисати или на било који други начин уништити. Такође, електронски докази могу бити смештени на појединачном рачунару, рачунарској мрежи или удаљеном серверу ван територијалне надлежности органа који их прикупљају, могу бити видљиви или невидљиви, што, поред поменуте могућности њихове лаке измене или уништења, како намерно, тако и услед нестручног руковања, намеће и низ специфичности у њиховом

---

[104] У чл. 3 Закона наведена су кривична дела за које је установљена надлежност посебних органа. Међутим, овако формулисана стварна надлежност не обухвата сва кривична дела која припадају компјутерском криминалитету. Тако, на пример, нису обухваћена следећа кривична дела.: приказивање, прибављање, и поседовање порнографског материјала, искоришћавање малолетног лица за порнографију– чл.185 КЗ РС и кривично дело фалсификовање и злоупотреба платних картица – чл. 225 КЗ. цит према С.Бејатовић, *Високотехнолошки криминал и кривичноправни инструменти супротстављања,* Лакташи 28-30.03.2012, стр.24 с. 17-30 , http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2017. године

[105] Л. Комплен- Николић,Р. Гвозденовић, С. Радуловић, А. Милосављевић, Р. Јерков, В. Живковић, С. Живановић, М. Рељановић, И. Алексић, Сузбијање високотехнолошког криминала,оп. цит. стр. 278

[106] Ј. Матијашевић, оп. цит. стр.131

прибављању.[107]Основни принципи прибављања електронских доказа подразумева да ниједном радњом овлашћених лица не сме бити измењен садржај података који се прегледају . Наведене принципе неопходно је доследно примењивати у сваком конкретном случају како би се сачувао интегритет доказа који се прибављају, документовао процес њиховог прибављања који омогућава понављање процеса уколико се за тим укаже потреба у каснијем току поступка, чиме се обезбеђује њихова доказна снага пред законом. [108]

ЗКП садржи неколико релевантних одредби за остваривање приступа и увида у садржај ускладиштених компјутерских података. Према чл. 152 ст. 3 ЗКП предмет претресања (претресање стана и других просторија или лица) могу да буду и уређаји за аутоматску обраду података и опреме на којој се чувају или се могу чувати електронски записи. За разлику од претресања стана и других просторија или лица, који се могу извршити у одређеним случајевима и без одлуке суда, за претресање уређаја и опреме то није могуће, те се може закључити да је у сваком случају неопходна судска наредба.[109] То значи да орган поступка када пронађе рачунар са подацима у вези са извршењем кривичног дела компјутерског криминалитета, може само да предузме мере обезбеђења, односно да уз помоћ стручног лица предузима и проналази, обезбеђује или описује трагове, али не и да изврши претресање рачунара док не добије одлуку суда.[110]Друге одредбе ЗКП-а односе се на привремено одузимање предмета (чл. 147). У предмете који се могу привремено одузети и послужити као доказ у кривичном поступку спадају и уређаји за аутоматску обраду података и уређаји и опрема на којој нсе чувају или се могу чувати електронски записи.[111] Законик није предвидео сходну примену ових правила на рачунарске податке, али, с обзиром на то да се рачунарски подаци сматрају исправом уколико су подобни или одређени да служе као доказ чињенице која се утврђује у поступку, они би се такође могли привремено одузети. [112]

ЗКП предвиђа у члану 162. одређивање посебне доказне радње тајног надзора комуникације под условима из члана 161. за следећа кривична дела: неовлашћено

[107] С. Радуловић, *Специфичност прибављања електронских доказа о извршењу кривичних дела високотехнолошког криминала*, Београд, 2008, стр. 17-18
[108] Ibid.
[109] В. Вилић оп. цит. стр. 330
[110] Видети више : М.Писарић, Претресање рачунара ради проналажења електронских доказа, Зборник радова Правног факултета у Новом Саду, 1/2015, стр. 233
[111] С. Кнежевић, Кривично процесно право: општи део, Ниш, 2015, стр. 318
[112] В. Вилић оп. цит. стр. 331

искоришћавање ауторског дела или предмета сродног права (чл. 199 КЗ РС), оштећење рачунарских података и програма (чл. 298 ст. 3 КЗ РС), рачунарска саботажа (чл. 299 КЗ РС), рачунарска превара (чл. 301 ст. 3 КЗ РС) и неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (чл. 302 КЗ РС) .Тајни надзор коминикације одређује се на образложени предлог јавног тужиоца према лицу за које постоје основи сумње да је учинило неко од наведених кривична дела или да припрема извршење неког од наведених кривичних дела, може се, уколико се на други начин не могу прикупити докази за кривично гоњење или би њихово прикупљање било знатно отежано. Изузетно, ова посебна доказна радња се може одредити и у случају постојања основа сумње да се припрема неко од наведених кривичних дела, а околности указују да се на други начин кривично дело не би могло открити, спречити или доказати или би то изазвало несразмерне тешкоће или велику опасност.

Посебне доказне радње се могу одредити под условима који су предвиђени у ЗКП за следећа кривична дела која припадају компјутерском криминалитету: приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетних лица за порнографију (чл. 185 ст. 2 и 3 КЗ), изазивање националне, расне и верске мржње и нетрпељивости (чл . 317 КЗ), трговина људима (чл . 388 КЗ) и кривично дело из чл . 98 ст. 3 до 5. Закона о тајности података.[113] Приликом прикупљања доказа уз употребу компјутерске технологије важно је указати на рачунарско претраживање података (чл . 178 - 180 ЗКП), као посебну доказну радњу. Рачунарско претраживање већ обрађених личних и других података и њихово поређење са подацима који се односе на осумњиченог и кривично дело може одредити суд под условима предвиђеним ЗКП на образложени предлог јавног тужиоца. Наредбу о спровођењу рачунарског претраживања података извршава полиција, Безбедносно-информативна агенција, Војно-безбедносна агенција, царинске, пореске или друге службе или други државни органи, односно правно лице које на основу закона врши јавна овлашћења.

[113] У чл. 98 Закона о тајности података(“ Службени гласник РС “ бр. 104/2009) предвиђено је кажњавање казном затвора за кривично дело неовлашћеног саопштавања, предаје или чињење доступним података или докумената који су поверени и представљају тајне податке са ознаком„државна тајна“ непознатом лицу, затим ако је део учињено из користољубља или ради објављивање или коришћење тајних података или је извршено за време ратног или ванредног стања или је дело учињено из нехата
.

4.2.4 **Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима**

Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима (тзв. „ Маријин закон ”) прописује посебне мере које се спроводе према учиниоцима кривичних дела против полне слободе извршених према малолетним лицима одређених законом и уређује вођење посебне евиденције лица осуђених за та кривична дела. Сврха закона је спречавање сексуалне делинквенције према малолетним лицима. Подручје примене закона обухвата тачно одређена кривична дела извршена према малолетним лицима, међу којима су кривична дела компјутерског криминалитета и то приказивање , прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију (чл. 185 КЗ РС) и искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу (чл. 185б КЗ РС). Посебне мере предвиђене законом примењују се према учиниоцу наведених кривичних дела после издржане казне затвора и оне се састоје у обавезном јављању надлежном органу полиције и Управе за извршење кривичних санкција; забрани посећивања места на којима се окупљају малолетна лица (вртићи , школе и сл .); обавезном посећивању професионалних саветовалишта и установа; обавезном обавештавању о промени пребивалишта, боравишта или радног места; обавезном обавештавању о путу у иностранство. Нарочито је значајна одредба чл. 5 ст. 3 Закона којом је предвиђено да кривично гоњење и извршење казне не застаревају за кривична дела против полне слободе извршена према малолетним лицима. На основу наведених одредби, као и одредби Кривичног законика, може се закључити да су у нашем законодавству усвојене законодавне и друге мере предвиђене у чл. 9 Конвенције о високотехнолошком криминалу у погледу кривичних дела у вези са дечијом порнографијом .[114]

4.2.5 **Закон о ауторском и сродним правима**

Закон о ауторском и сродним правима регулише права аутора књижевних, научних, стручних и уметничких дела (ауторско право), као и право интерпретатора, право првог издавача слободног дела, права произвођача фонограма, видеограма, емисија, база

[114] В. Вилић оп. цит. стр. 336

података и право издавача штампаних издања (сродна права), начине остваривања ових права и њихову судску заштиту. Закон садржи казнене одредбе којима се одређује прекршајна одговорност и одговорност за привредне преступе у вези са ауторским правима, као и грађанско - правне односе у области права интелектуалне својине. У чл. 2 Закона се одређује као ауторско дело, у оквиру писаних дела, рачунарски програми у било којем облику њиховог изражавања, укључујући и припремни материјал за њихову израду. Иако у Закону не постоје посебне одредбе које се односе само на рачунарске програме, у чл. 47 предвиђен да лице које је на законити начин прибавило примерак рачунарског програма,може,ради сопственог уобичајеног наменског коришћења програма, без дозволе аутора и без плаћања ауторске накнаде, поред осталог да: смешта програм у меморију рачунара и пушта програм у рад; отклања грешке у програму, као и да врши друге неопходне измене у њему које су у складу са његовом сврхом , ако уговором није друкчије предвиђено; начини један разервни примерак програма на трајном телесном носачу и изврши декомпилацију програма искључиво ради прибављања неопходних података за постизање интероперабилности тог програма са другим независно створеним програмом или одређеном рачунарском опремом, под условом да тај податак није био на други начин доступан и да је декомпилација ограничена само на онај део програма који је неопходан за постизање интероперабилности. Уколико је податак добијен последњом описаном радњом постоји забрана да се тај податак саопштава другоме или користи за друге сврхе, посебно за пласман другог рачунарског програма којим би се повредило ауторско право на првом. Радњу из става 1. тачка 4. овог члана може извршити непосредно лице које је на законит начин прибавило примерак рачунарског програма или друго стручно лице које ради по његовом налогу. У Закону су установљени основни елементи општег режима заштите ауторских дела од недозвољеног емитовања, који се односе и на писана дела, односно рачунарске програме (чл. 28 - 30). Такође, Закон је аутору дао право да другоме забрани или дозволи да његово дело, које је забележено на носачу звука, односо носачу слике (компакт диск, аудио касета, видео касета, филмска трака, оптички диск, дијапозитив) јавно саопштава уз помоћ техничких уређаја за репродуковање звука односно слике (чл. 33). Иако није изричито наведено, свакако да се ово право аутора односи и на електронско емитовање. [115] У члану 215. Закона, поред осталог, предвиђа

[115] Ibid., стр. 331

кажњавање привредног друштва или другог правног лица новчаном казном за привредни преступ уколико произведе, увезе, стави у промет, прода, да у закуп, рекламира у циљу продаје или давања у закуп или држи у комерцијалне сврхе уређаје, производе, саставне делове, рачунарске програме, који су превасходно конструисани, произведени или прилагођени да омогуће или олакшају заобилажење било које ефикасне технолошке мере, или који немају другу значајнију сврху осим наведене.

4.2.6 **Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине**

Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине уређује посебна овлашћења органа државне управе и организација које врше јавна овлашћења, ради ефикасне заштите права интелектуалне својине у складу са прописима којима се уређује право интелектуалне својине (чл. 1). Одредбе закона примењују се на производњу, промет, употребу и држање робе и на пружање услуга којима се повређују права интелектуалне својине. Одредбе овог закона не примењују се када роба није намењена обављању делатности, односно стављању у промет, ни на личне ствари, односно на предмете који су намењени искључиво за личну употребу, осим када се ради о више истоветних примерака исте робе, односно предмета. Закон предвиђа да је роба којом се повређују права интелектуалне својине, поред осталог, нарочито пиратски примерак ауторског дела или предмета сродног права, укључујући и рачунарске програме, који се дефинише као примерак заштићеног ауторског дела или предмета сродног права, односно роба која садржи ауторско дело или предмет сродног права, која је израђена без сагласности носиоца права. У члановима 39. и 40. Закона предвиђена је одговорност за привредне преступе правног лица и одговорног лица у правном лицу за неовлашћену производњу, увоз, извоз, нуђење ради стављања у промет, стављање у промет, складиштење или коришћење у комерцијалне сврхе производа или поступка заштићеног патентом, односно малим патентом. Такође је одређено да ће се предмети извршења привредног преступа и предмета употребљених за извршење привредног преступа бити одузети , а предмети извршења привредног преступа уништени . Радње које представљају кршење права интелектуалне својине извршене у пословању оваквих субјеката привредног промета не могу брзо и ефикасно санкционисати кроз одговорност за привредне преступе,

што оне у суштини јесу, већ се морају посматрати кроз извршење кривичног дела неовлашћеног искоришћавања ауторског дела или предмета сродног права. [116] Ово са једне, стране подразумева ангажовање целокупног механизма кривичноправне заштите који је гломазан и не нарочито брз и ефикасан у смислу остваривања сврхе санкционисања забрањене радње, док, са друге стране, имајући у виду да наше кривично законодавство тек одскора предвиђа одговоност правног лица намеће индивидуално санкционисање појединачне радње једног или више физичких лица, чиме се знатно отежава санкционисање недозвољеног понашања привредног субјекта у привредном и платном промету. [117]

[116] Члан 199. Кривичног законика

[117] Р. Јерковић, *Борба против високотехнолошког криминалитета у Србији,* Телекомуникације- научно-стручни часопис Републичке Агенције за телекомуникације, бр. 3/2009, стр.1, http://www.telekomunikacije.rs/arhiva _brojeva/treci_broj/ranko_jerkovic: _borba_protiv_visokotehnoloskog_kriminaliteta_u_srbiji_.161.html претражено 07.08.2017 године

5.Феноменолошке карактеристике компјутерског криминалитета

За анализу феноменошких карактеристика овог типа криминалитета неопходно је најпре указати на сам појам криминалне феноменологије која као део део криминологије разматра и проучава: обим криминалитета , појавне облике криминалитета и криминалног понашања, структуру и структуралне промене криминалитета и динамику криминалитета.[118] У наставку ће бити изложени појавни облици овог типа криминалитета као једна од најзначајнијих његових карактеристика.

5.1. Појавни облици компјутерског криминалитета

Као што још увек не постоји јединственост у томе шта је компјутерски криминал, тако не постоји сагласност ни која дела и понашања треба третирати као дела у којима постоји овај облик криминалног понашања. У теорији су присутна два начина дефинисања појавних облика компјутерског криминала: прво схватање полази од генералног појма компјутерског (сајбер) криминала и сва дела која имају њему особена својства подразумевају се под сајбер криминалом.

Првој групи припадају схватања која сматрају да се дела компјутерског криминала могу поделити на она у којима компјутери имају „активну" улогу, односно криминал повезан с компјутерима и она у којима се компјутери појављују као периферни објект криминала.[119]Сличан метод се користи приликом класификације компјутерског криминалитета по томе да ли је у питању криминалитет у ужем или ширем смислу при чему је свеобухватна подела дата на десетом конгресу УН :

Компјутерски криминалитет у ужем смислу- као свако незаконито понашање усмерено на електронске операције сигурности компјутерских система и података који се у њима обрађују (прављење и убацивање компјутеских вируса, хакинг, пиратство, компјутерска саботажа, компјутерска шпијунажа, компјутерска превара и крађа компјутерских услуга).

Компјутерски криминалитет у ширем смислу- као свако незаконито понашање везано за или у односу на компјутерски систем и мрежу, укључујући и такав криминал какво је незаконито поседовање, нуђење и дистрибуција информација преко компјутерских система и мрежа (комппјутерски фалсификати, компјутерске крађе,

[118] С. Константиновић-Вилић, В. Николић-Ристановић, М. Костић, Криминологија, Ниш,2012 str. 17
[119] I. Walden, *Information Technology & The Law*, Basingstoke, 1990, Macmillan Publishers p.12

техничке манипулације уређајима или електронским компонентама, злоупотребе система плаћања).

Другој групи припадају схватања која користе метод енумерације,при чему се таксативно наводе дела компјутерског криминалитета. У овом раду биће приказани појавни облици овог типа криминалитета кроз схватање Зиебер-а, који прихвата одређења и поделу Комитета експерата ОЕЦД-а и сматра да се дела компјутерског криминалитета могу сврстати у односу на последице (ако су нападнути економски интерес, приватност, национална сигурност и сл.) у три велике групе:

1),,дела компјутерског криминалитета везана за економски криминал, као што су превара, крађа, компјутерска саботажа, неауторизован приступ системима и хакинг,пиратство софтвера и сл.

2) дела компјутерског криминалитета везана за кршење права приватности, као што су коришћење нетачних података, илегално прикупљање и чување личних података, илегално откривање и злоупотреба података, кршење формалности права приватности и сл.

3) угрожавање осталих правно заштићених интереса, пре свега угрожавање националне сигурности, контрола прекограничног тока података, интегритет процедура везаних за компјутере и мреже података и друга дела".[120]

5.1.1 **Дела компјутерског криминалитета везана за економски криминал**

- **Компјутерске преваре -** Представљају најраширенији облик компјутерског криминалитета обухватајући манипулисање компјутером електронским програмским путем у погледу софтвера или механичким путем у погледу хардвера са циљем прибављања противправне имовинске користи себи или другом или наношења штете. У компјутер се уносе нетачни подаци или се пропушта уношење тачних података или се на било који други начин рачунар користи за остваривање преваре.[121] Најбројније су у области финансијског пословања, осигурања, пореских обавеза, социјалног осигурања, у вези проглашавањем стечаја, прањем новца итд. Компјутерске преваре су по својој природи наближе привредном криминалитету, а и у литератури се, скоро без изузетка, ове

[120] J. Wiley, *The International Handbook of Computer Crime*, Chichester,1991, John Wiley and Sons Publishers pp. 3–27

[121] С.Константиновић-Вилић, В. Николић-Ристановић, М. Костић: оп.цит., стр. 179

појаве третирају као појавни облик привредног криминалитета.[122] Компјутерска превара је инкриминисана кривичним делом рачунарска превара (члан 301 КЗ РС).

Компјутерске преваре могу да се врше на веома разноврсне начине и компјутерски делинквенти у том погледу показују заиста велику инвентивност и висок степен вештина, а сам компјутер за варалице представља неку врсту лаког „ залогаја “, попут људског мозга лишеног моћи разликовања имагинарног од стварног, чиме се испољава као савршена жртва.[123] Као најзначајнији облик компјутерских превара издвајају се интернет преваре које представљају било коју превару при при чијем извршењу лице у намери прибављања противправне имовинске користи за себе или другога искористи један или више сегмената интернета као што су онлајн собе за дописивање , веб странице или електронска пошта да би се створили услови за лажно приказивање или прикривање чињеница којима би се неко лице обмануло и навело на наношење штете својој или туђој имовини.

Специфична врста интернет превара јесте „ Нигеријска превара “ која подразумева уплату одговарајућег новчаног износа превараранту уз његово обећање да ће се остварити знатно већа свота новца након успешно обављеног посла. Када жртва пристане да уплати новац, од ње се накнадно траже нове уплате услед нових трошкова и издатака, а уз стално указивање на то да милиони само што нису пристигли на њен рачун. Ова превара се данас остварује путем електронске поште (енгл. email) док се у прошлости вршила употребом традиционалног писма. За ову превару користи се зависност која се јавља код коцкара. Наивни корисници ризикују мали износ новца зарад могућности да зараде милионе. Увек постоји могућност да се све изгуби. Чак и кад се уплати одређени износ новца, и када преваранти у својству пословних партнера траже нове уплате за новонастале трошкове посла, код жртве преовлада убеђење да ће на крају уследити добитак. Као пошиљалац може да се јаве лица која стварно постоје, али су њихови идентитети украдени без њиховог знања и извршиоци кривичних дела их користе да би прикрили свој прави идентитет, или да би се снагом ауторитета одређених лица улило поверење жртвама преваре и придобило њихово поверење. Електронске поруке насловљене су на било ког примаоца поруке и из њих се не може видети коме се пошиљалац обраћа, а њихов контекст је такав да прималац

[122] Б. Бановић, *Обезбеђење доказа у криминалистичкој обради кривичних дела привредног криминалитета*, Београд, 2002, Виша школа унутрашњих послова стр.140
[123]J. C. Bellour , *Međunarodna prevara,* Zagreb, 1998, Izbor ,br. 1, pp 76-77

поруке лако може помислити да се порука односи управо на њега. Разлози којима се жртва руководи приликом уплате новца су пре свега пословни и похлепни.[124]

Као оруђе за извршење ове преваре користе се : фалсификована документација, бежични трансфери новца за пренос противправно стечених новчаних средстава, техничка средства која им омогућују анонимну комуникацију, веб-базирана електронска пошта, електронски налози предходно преузети од правих корисника, факс-машине за слање факс-порука при размени документације са жртвама преваре, услуге телекомуникационих сервиса за директну комуникацију са жртвом преваре, као и лажне странице на интернету којима се оштећени доводи у заблуду да комуницира и сарађује са представницима легалних и легитимних институција.[125] Ова врста преваре достигла је свој врхунац 2009. године. Према анализираним подацима холандске компаније Ултраскен[126] (енгл. Ultrascan) изгубљено је 2009. године 50% више новца него 2008. године. Као најризичније државе из којих се врше ове врсте превара означене су државе западне Африке: Нигерија, Гана, Бенин, Обала Слоноваче, Того и Буркина Фасо. Ван територије западне Африке као најризичније државе са чијих се територија врше те врсте превара означене су Јужна Африка, Шпанија и Холандија.[127] У домаћој пракси, онлајн купци у Србији као начин плаћања најчешће преферирају плаћање поузећем. Једни то раде у недостатку текућег рачуна и немогућности плаћања робе из фотеље, други због једноставности овог начина плаћања а трећи пак из навике. Одређени купци одлучују се за овај начин плаћања верујући да се на овај начин штите од онлајн превара. С обзиром на чињеницу да плаћање поузећем једино гарантује испоруку одговарајућег пакета уз противнакнаду без у највећем броју случајева, могућности утврђења саме садржине пакета. Овај начин плаћања је све популарнији међу интернет преварантима јер обезбеђује велике шансе за прикривање идентитета. Са једне стране се налази отворен текући рачун са свим подацима о власнику а са друге стране бројне курирске службе које врше доставу пакета и трансфер новца на кућну адресу уз податке за чију валидност нико не може гарантовати. Иако овај начин

[124] Ж. Миладиновић, Кривично дело преваре као модел остваривања сајбер криминала (докторска дисертација), Београд, 2016 стр. 87
[125] M.Dyrud, I *brought You a good news An analysis of Nigerian 419 Letters*, Proceedings of 2005 Annual Association for Business Communication, Convention Association for Business Communication, USA,2005, p. 11.
[126] Више на: Ultrascan Advanced Global Investigations, http://www.ultrascan-agi.com/ претражено 07.07. 2017. Године
[127] Више на: http://www.nigerianspam.com/people-affected-419-scam.htm, претражено 07.07.2017.године

онлајн куповине у пракси може довести до интернет преваре просечног онлајн купца, постоје начини који у великој мери могу допринети заштити од разноликих превара на интернету. Најпре, сви сајтови за електронску трговину имају имплементиран систем оцењивања продаваца и купаца, који иако не идеалан може пружити информације о поузданости особе са којом се врши трговина преко интернета. Далеко значајнији вид заштите обезбеђују сама правила и савети трговине на интернету која се могу разликовати од сајта до сајта с обзиром да су сами администратори сајтова у највећој мери упознати са облицима преваре који су најчешћи као и што ефикаснијим видом заштите од истих.

- **Компјутерске крађе** - Заузимају изузетно значајно место међу облицима компјутерког криминалитета. Под крађом се у компјутерском криминалитету могу подвести крађе рачунара и његових компоненти, крађа разне врсте робе, података, лозинки и злоупотреба платних картица. Крађа компјутерских уређаја и опреме постаје за компјутерску индустрију озбиљна претња у стању да проузрокује штету од више милијарди долара годишње. У Великој Британији је у 2014. години пријављено да је украдено преко 183.523 хиљада компјутерских уређаја (лаптопова, паметних телефона, таблета др.). Огроман проблем представљају осетљиви лични и пословни подаци који се могу наћи на уређајима тако да је Градска управа Глазгова у Шкотској кажњена са 150 000 фунти јер није предузела неопходне мере како би заштитила 74 лаптоп компјутера која су јој украдена. На једном од украдених лаптопова налазили су се подаци о банковним рачунима преко 6.000 хиљада становника Глазгова.[128] С обзиром на чињеницу да је крађа појединих делова компјутера са једне стране једноставна за извршење попут крађе хард дисокова, микропроцесора и меморијских лествица, а са друге изузетно исплатива, у сталном је порасту број овог облика крађе. Према AMA (енгл. American Electronics Association)[129] из Вашингтова само вредност украдених чипова током 1993.године износила је око 40 милиона долара. Као посебан вид крађе издваја се „ Скиминг “ који представља преузимање података са магнетне траке или чипа кредитне картице уз помоћ електронског уређаја, тзв. скимера.[130]

Интернет пружа нове начине крађе туђих личних података што доводи до масовне појаве крађе идентитета на интернету. Нарочито значајно за компјутерске крађе јесте

[128] М. Видојковић, , *Компјутерски криминалитет* (мастер рад),Ниш,2015, стр. 48
[129] B. Violino, high-tech thieves, Information Week, may 29, 1995., no. 529 p. 14(3)
[130] Ј. Матијашевић, оп.цит. стр. 59

стални пораст такозваног „пецања“ или мрежне крађе идентитета који представља покушај крађе података корисника интернета путем фалсификоване веб странице. Подаци добијени мрежном крађом података најчешће се користе за крађу новца са банковног рачуна жртве или за упад у њену електронску пошту (и-мејл). Кориснику који је постао жртва крађе идентитета може помоћи промена лозинке или ПИН кода на рачунима, контактирање банке чије услуге користи те, ако сазна да му је неко приступио подацима, затварање рачуна. Нарочито је забрињавајућа чињеница да је већина жртава потпуно несвесна да су украдени лични подаци и исти злоупотребљени док то не буде прекасно. Из тог разлога се развијају многе врсте заштита против пецања које се на тржишту појављују као самостални програми, или се уграђују у антивирусни софтвер или у саме апликације за интернет пословање. За разлику од пецања, такозвани „ Фарминг “ представља далеко софистицираније систем крађе поверљивих података, бројева рачуна и ПИН кодова користећи се лажним веб сајтовима чак и без потребе да се одговори на приспелу електронску пошту да би „Фармери“ могли доћи до података жртве . Довољно је само отворити неки и-мејл и на компјутер ће се прикачити малвер (Вирус, Тројански коњ) и генератор кључа који ће украсти информације. Улазак у овом случају, рецимо, на сајт банке доводи до преусмеравањана на лажни сајт који изгледа идентично као и сајт банке. Због свега наведеног, од изузетне је важности не отварати електронску пошту од непознатих пошиљалаца као и одлазак само на веб сајтове провереног садржаја.[131]

Процењује се да је крађа идентитета постала деликт који се најбрже развија међу економским деликтима у Сједињеним Америчким Државама, а можда и у поређењу са деликтима било које врсте. [132] Овај облик компјутерског криминалитета детаљније ће бити објашњен у оквиру дела компјутерског кримналитета која се односе на кршење права приватности.

- **Компјутерска саботажа, неауторизован приступ системима и хаковање, пиратерија** - Наведена дела стоје у изузетно чврстој и комплекној вези као дела компјутерског криминалитета која се односе на економски криминал. Кривичноправна заштита од ових облика криминалитета остварена је предвиђањем кривичних дела против

[131] K. Tan, *Phishing and Spamming via IM (SPIM).*, Internet Storm Center, (2006); преузето 08.05.2017.
[132] Identity Theft: Is there Another You?: Joint hearing before the House Subcommc. On Telecommunications, Trade and Consumer Protection, and on Finance and Hazardious Materials, of the Comm. On Commerce, 106th Cong. 16(1999)(testimony of Rep. John B. Shadegg) http://www.usdoj-crm/mis/jam претражено 08.08. 2017. године

безбедности рачунарских података (Глава XXVII КЗ РС): рачунарска саботажа (члан 299), неовлашћени приступ заштићеном рачунару, и рачунарској мрежи и електронској обради података (члан 302) Неовлашћено коришћење рачунара или рачунарске мреже (члан 304) прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података (члан 304а).

Специфично за компјутерску саботажу јесте посебно својство оштећеног с обзиром на чињеницу да објекти напада морају припадати државном органу, јавној служби или другим правним лицима као што су установе, предузећа или друге организације. Најчешћи видови рачунарске саботаже су они који делују деструктивно на оперативно-информативне механизме и корисничке програме, пре свега оне који имају функцију чувања података. Програмер мотивисан осветом, кажњен је на казну затвора од тридесет месеци, јер је почетком 2008. године у америчкој савезној држави Њујорк, у компанији у којој је био запослен покушао да саботира рачунарски систем и да је у томе успео више од седамдесет сервера компаније, би било оборено и неупотребљиво. На серверима које је компанија користила, налазиле су се поверљиве информације о прописаним рецептима и медицинским подацима пацијената, као и важни финансијски извештаји, рачуни и платни спискови свих запослених. Штета причињена компанији износила је између 70 000 и 120 000 хиљада долара.[133] У Србији, случајеви компјутерске саботаже појединачних починилаца нису тако чести при чему је од велике важности истаћи покушај онемогућавања и ометања рада и функционисања интернет презентације министарстава Владе Републике Србије, неких политичких странака и академских институција као једног од највећих остварења у области појединачне саботаже. У погледу компјутерских саботажа организованих група најзначајније су свакако ,светски познате, хакерске онлине заједнице „Анонимус“ која је у Србији проузроковала и нападе на сајтове Републичког јавног тужилаштва и Министарства правде.[134]

Neауторизован приступ системима и хакинг могу се дефинисати узимајући као полазну основу појам хакера који подразумева два конфликтна значења. Једно од њих означава особу која угрожава сигурност компјутерских система, док друго означава

[133] Преузето са http://www.informationweek.com/medco-sys-admin-pleads-guilty-to-computer-sabotage/d/d-id/1059395? 07.08.2017. године

[134] Детаљније о овоме биће изложено у оквиру дела компјутерског криминалитета којима се угрожава национална сигурност.

изврсног познаваоца компјутера који настоји из њих извући најбоље за општу добробит онлајн заједнице и самог друштва кроз истраживање пропуста у програмима или порталима или писању истих. Основно обележје хаковање је нарушавање система заштите и неовлашћени упад у туђе информационе системе, што је у класичном смислу еквивалентно насилном упаду у туђе објекте.[135] Постоје два основна облика реализације овог дела. Први подразумева прибављање разним методама и техникама (претраживање електронске или обичне поште, новина, лажно представљање, прислушкивање, испитивање, подмићивање, изнуђивање, крађе свих информација потребних за успешан упад у туђи информациони систем (интернет адресе, телефонски бројеви, идентификациони параметри, лозинке, оперативни системи, базе података и сл.) Други облик се одвија по принципу: „ покушај, погреши, отклони грешку “, при чему нападач покушава погађањем параметара заштите да продре у циљни информациони систем. Ово погађање се најчешће одвија на основу унапред припремљеног речника који садржи широк скуп појмова који се по оцени ствараоца најчешће користе као лозинке.[136]Основне карактеристике хаковања су : неауторизован брижљиво планиран приступ: насилан приступ, јер је у питању пробијање заштите система, приступ се реализује кроз упад у систем, при чему се термин „ упад “ користи за означавање разних метода и техника проваљивање у систем , упади у систем базирају се на високом професионалном знању, место упада је, по правилу, удаљено од места где се налази нападач, чињењем хакинга нападач, по правилу истовремено чини и друга дела: шпијунажу, превару, проневеру, крађу услуга, саботажу, дистрибуцију вируса и разне друге манипулације, хакинг могу да чине појединци или групе. [137]

С обзиром да су у већини случајева мотиви и циљеви извршилаца овог дела непознати, неовлашћени упад у системе односно хаковање не познаје границе свог деловања, попримајући размере глобалне епидемије. Када се инциденти истражују у њиховом глобалном контексту, могуће је анализирати динамике и узорке међусобно повезаних инцидената, претходно неразумљивих или игнорисаних.[138] Пиратство софтвера подразумева илегално умножавање, дистрибуцију и употребу компјутерских програма и софтвера. Масовна примена компјутерске технологије директно је узроковала повећање

[135] С. Петровић оп.цит. стр. 178
[136] Ibid., стр. 179
[137] М. Дракулић,*Основи компјутерског права*, Београд, 1996, стр. 499
[138] E. K. Anderson, International intrusions: motives and patterns, The proceedings of the 1994 Bellcore/Bell South Security Simposium, May 1994., http://www.aracnet.com/-kea/Papers/paper.html

потражње за рачунарским програмима. У релативно кратком временском периоду злоупотреба софтверске технологије је постала предмет злоупотреба са циљем стицања велике материјалне користи на прилично лак начин. Оваквом врстом злоупотребе оштећени су првенствено аутори, губећи економску добит на коју рачунају дистрибуцијом софтверских програма. Оштећена је такође и држава, јер нелегалном дистрибуцијом софтверских програма држава губи огромне суме нова које јој припадају по основу пореза. У Велика Британија је према једном извору из 1999. године због пиратства софтвера компјутерско тржиште изгубило 7 милијарди фунти.[139] Софтверски пакет у просеку кошта око 400 долара, а класична крађа износи просечно 50 долара или мање.[140] Нови оперативни систем Микрософта (енгл. Microsoft) Windows 10 представља покушај да се стане пиратерији на пут. Нови систем препознаје нелегалне софтвере и то сваки пут када рачунар користи интернет и о томе обавештава регионалне или локалне филијале компаније, које даље обавештавају надлежне органе. Компанија планира да систем заживи у преко 190 земаља где компанија има филијале или представништва. Систем је већ заживео у Сједињеним Америчким Државама и у Великој Британији где се увелико одузимају рачунари и прописују казне у износу од петско фунти.[141] Проценат коришћења пиратских софтвера у свету износи 42% од укупног броја софтвера у употреби, у земљама Европске уније 33%, док у Србији износи 70% са трендом смањења.[142]На основу истраживања које је спровео популарни сајт „ Torrentfreak “ Србија заузима седмо место по заступљености пиратерије, испред које су Грчка, Шпанија, Хрватска, Литванија, Бугарска и Летонија. У Србији се скоро 22 одсто интернет популације сматра пиратима тј. лицима који „конзумирају“ пиратске интернет садржаје.

[139] The Independent, 25 October 199., цит. према : J. Muncie- E. McLaughlin, *The problem of Crime*, London, 2001, p.266

[140] D. L. Carter. Computer crime categories: How techno-criminals operate, FBI law Enforcement Bulletin, http://nsi.org/Library/Compsec/crimecom.html

[141] М. Видојковић, *Компјутерски криминалитет* (мастер рад),Ниш,2015, стр. 66

[142] Преузето са http://www.politika.rs/rubrike/Ekonomija/Piraterija-odnosi-milijarde-dolara.lt.html дана05.07.2017.године

Топ десет пиратеријом највише захваћених земаља

18.38	Sweden
19.07	Romania
19.84	Ireland
21.31	Serbia
21.87	Greece
22.19	Spain
22.70	Croatia
24.54	Lithuania
27.43	Bulgaria
46.33	Latvia

Извор преузет са: http://torrentfreak.com/europe-has-the-highest-online-piracy-rates-by-far-160801/

На листи земаља са најраширенијом онлајн пиратеријом свих 10 места заузеле су земље из Европе. Истраживање је обухватило преко 14 хиљада најзначајнијих и најпопуларнијих сајтова за бесплатно преузимање разноврсних садржаја који су током 2015. године имали више од 141 милијарде јединствених посета.[143]

- **Компјутерско фалсификовање -** Од изузетне је важности издвојити ово дело као посебно дело компјутерског криминалитета које се односи економски криминал. Основно обележје овог дела је стварање лажних или преиначавање правих предмета, помоћу компјутера, а све ради прибављања противправне имовинске користи. Типични облици коришћења информационих технологија ради фалсификовања су: фалсификовање докумената; фалсификовање јавних исправа; фалсификовање знакова за вредност; фалсификовање знакова за обележавање робе; фалсификовање новца; фалсификовање потписа; фалсификовање жигова и фалсификовање хартија од вредности. [144] Компјутерско фалсификовање је инкриминисано кривичним делима : фалсификовање новца(члан 241 КЗ

[143] Наведено према : http://torrentfreak.com/europe-has-the-highest-online-piracy-rates-by-far-160801/ преузето 08.05.2017.
[144] P. J. Toren,*Intellectual Property and Computer Crimes* (Intellectual Property usiness Crimes Series), New York USA, 2003, p.6-41

РС), фалсификовање хартија од вредности (члан 242 КЗ РС), фалсификовање и злоупотреба платних картица (члан 243 КЗ РС), фалсификовање знакова за вредност (члан 244 КЗ РС), фалсификовање знакова, односно државних жигова за обележавање робе, мерила и предмета од драгоцених метала(члан 244а КЗ РС), фалсификовање исправе (члан 355 КЗ РС), посебни случајеви фалсификовања исправе(члан 356 КЗ РС), фалсификовање службене исправе (члан 357 КЗ РС) .

Релативно новији облик компјутерског фалсификовања јесте фалсификовање електронске поште који подразумева да се садржај поште шаље у измењеном облику приказујући најчешће лажан идентитет и локацију пошиљаоца. Штета коју овај облик може проузроковати је новчано непроценљива имајући у виду чињеницу да се као жртва напада могу наћи већи број субјеката истовремено, полазећи од појединаца преко компанија па све до државе и њених органа.

Компјутери се пре свега користе за фалсификовање новца и путних исправа, преко 60% свих фалсификованих новчаница и документа откривених у Сједињеним Америчким Државама је фалсификовано помоћу компјутера. Управа за трезор Сједињених Америчких Држава је због све већег броја фалсификованих новчаница више пута у последњих 20 година морала да уводи нове мере заштите на новчаницама (водене тигрове, холограме, микро штампа, нов папир за новчанице).

Последњих година злоупотребе са фалсификованим платним картицама постају изузетно распрострањене захваљујући великом напретку техничко-технолошког проналазаштва нарочито у сфери електронског банкарства који је поједноставио и убрзао овај вид плаћања , али истовремено и створио нове начине злоупотребе платних картица. Фалсификоване платне картице се израђују уз помоћ података који се добијају са магнетних линија, предњих или задњих страна платних кратица или уз помоћ ПИН- кода платне картице. Један од најефективнијих начина узимања података са магнетне писте подразумева постављање „скиминг“ уређаја на банкомат. Овај уређај се поставља на отвор за убацивање платне картице, чиме је омогућено да се подаци са магнетне писте корисника банкомата сладиште на самом скиминг уређају или да се путем радио везе пошаљу на одређену дестинацију. Поред скиминг уређаја обично се на одговарајућем месту поставља и камера која снима позиције прстију корсника који укуцавају ПИН-код, а накнадно се упаривањем података са магнетне писте и одговарајућег ПИН-кода добијају сви неопходни

подаци за израду „ клониране “ картице којом се касније врши злоупотреба.[145] Прибављање податак са магнетне писте могуће је и помоћу „ wire taping“ методе која подразумева пресретање оригиналне поруке која се шаље са банкомата или ПОС терминала ради преузимања броја картице и осталих података потребних за израду фалсификоване картице и њене злоупотребе.[146] Ово је један од распрострањених и друштвено врло опасних облика криминала, посебно што сада рачунарска технологија, захваљујући, пре свега, појави скенера и ласерских штампача у боји, као и великог броја врло снажних софтверских пакета за графичку обраду, ствара изузетне услове и могућности за реализацију веома успешних фалсификата. [147]

5.1.2 Дела компјутерског криминалитета која се односе на кршење права приватности

Појам приватности потиче од латинске речи „privatus“ која значи лични, неслужбени, тајни, поверљиви, затворени итд. Значење појма приватности изузетно је динамично, подложно промени захваљујући константном развоју технологије у индустрији компјутера и телекомуникација.

У старом Риму, за време владавине цара Августа, тај термин је означавао особу издвојену из јавног живота.[148] Крајем деветнаестог века Луис Брандеис и Самуел Варен (енгл. Louis Brandeis, Samuel Warren) приватност су дефинисали као „ право да будемо остављени на миру “, што је подразумевало заштиту личне аутономије, моралног и физичког интегритета, права на избор начина живота, интеракције са другим људима и сл. Данас, у времену све доминантнијег и фреквентнијег виртуалног живота, само постојање приватности као друштвене вредности доведено је под знаком питања. Глобалне друштвене мреже на интернету као што су Фејсбук, Твитер или Инстаграм понајвише угрожавају људску приватност, а посебно приватност младих од којих је велики број малолетника, чак и млађих од 12 година. Мада изричито заштићено међународним конвенцијама, пре свега Европском конвенцијом о заштити људских права и основних слобода (члан 8) Универзалном декларацијом о људским правима (члан 12) Међународним пактом о грађанским и политичким правима (члан 17) , као једно од

[145] Ј. Матијашевић оп.цит стр. 73
[146] Ibid., стр. 74
[147] С.Петровић, оп.цит. стр. 133
[148] Ј. Дропулић, *Право на приватни живот и друштвени интегритет* , Загреб, 2002, Визура, стр. 45

основних неотуђивих људских права, право на приватност није ни у једној јурисдикцији на свету у потпуности дефинисано. Устав Србије не штити приватност као посебно право, већ поједина права на приватност нпр. право на достојанство и слободан развој личности (члан 23) физички и психички интегритет (члан 25) стан (члан 40) тајност писама и других средстава општења (члан 41) подаци о личности (члан 42) слобода и мисли и савести (члан 43), слобода мишљења и изражавања (члан 46) породица (члан 66). Суштина овог „камелеонског" права произилази из просте потребе људи да самостално одлучују шта ће и коме саопштити о себи и свом животу. Могућност реализације права зависи од супротстављености разнородних интереса сваког појединца и читаве заједнице и нопходности компромиса између њих.

Као најзначајнији део права на приватност издваја се право на заштиту података о личности које се развило седамдесетих година прошлог века у земљама Западне Европе и САД. Заштита података о личности је скуп међусобно повезаних активности, метода, техника и норми којима се обезбеђује приватност, сигурност, поверљивост, расположивост и интегритет података од свих опасности које им прете.[149] Подаци о личности су сви они подаци који се односе на неко одређено или одредиво физичко лице, на основу којих оно може бити идентификовано, а којима се може угрозити његова приватност.[150] То су, пре свега, подаци којима се могу угрозити живот, телесни и физички интегритет, част, углед, живот породице, идентитет и име. Ти подаци се односе на жива, умрла лица, као и лица проглашена умрлим. У савременим друштвима, већина људи оставља такозвани информациони траг своје комуникације са најразличитијим државним органима, јавним институцијама(на пример здравственим и образовним) и недржавним организацијама (на пример банкама, путничким агенцијама, робним кућама).[151]

Нарочиту опасност представља брзина размене података на интернету којој је готово немогуће ући у траг. Често корисници нису ни свесни да су њихови подаци ускладиштени у одговарајуће базе података или да они уопште и постоје.Најзначајнији међународни (европски) извори у погледу заштите података о личности су: Конвенција 108 Савета Европе о заштити лица у односу на аутоматску обраду података од 1981.године

[149]М. Дракулић, *Основи Компјутерског права*, , Београд ,1996, Друштво операционих истраживача Југославије - ДОПИС стр. 56.
[150] Ibid., стр. 66.
[151]С. Лилић , *Правни аспекти заштите података у аутоматизованим службеним евиденцијама*, Наша законитост 5/1989, стр. 614

заједно са Додатним протоколом у вези са надзорним органима и прекограничним протоком података од 2001. године ,као и Директива 95/46 Европског парламента и Савета Европске уније. У Републици Србији уставни основ овог права предвиђен је чланом 42. Устава РС док је законски оквир остварен Законом о заштити података о личности усвојеног 23.10.2008. године, у примени од 01.01. 2009. године. Правне мере заштите засноване су на одређеним принципима, које су прихватиле међународне организације и национална законодавства, како би се остварила хармонизација прописа. Најзначајнији принципи односе се на ограничавање прикупљања података, навођење сврхе, ограничавање употребе, суделовање и одговорности, забрану постојања тајних система за прикупљање и чување података, права субјеката о којима се и од којих се подаци прикупљају, обавезе и одговорност субјеката који прикупљање, обраду, меморисање и достављање обављају, принципе корисности, аутентичности и својине. Природа и степен правне заштите података, у крајњој линији, у зависности су од степена политичког значаја који се придаје личним правима, односно, заштити приватности и личних података у одговарајућим друштвено-политичким условима. Са своје стране, пак, ово зависи од општег степена материјалног и културног развитка одговарајуће друштвене заједнице. [152] Захваљујући развоју интернета и све напреднијим техникама злоупотребе личних података, право на заштиту података о личности додатно је угрожено кроз једно од најразорнијих дела компјутерског криминалитета која се односе на кршење права приватности са несагледивим последицама, а то су крађе идентитета на интернету.

- Крађа идентитета на интернету - Представља врсту компјутерске крађе а уједно и преваре код које се путем лажних порука у електронској пошти, онлајн причаоницама, веб сајтова и инсталирањем злонамерних софтвера на туђем компјутеру прикупљају енормне количине личних и финансијских података жртве. Крађа идентита на интернету инкриминисана је кривичним делом неовлашћено прикупљање личних података (члан 146 КЗ РС) и кривичним делом неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (члан 302 КЗ РС). Многи онлајн бизниси данас такође чувају личне податке о корисницима и купцима на својим веб сајтовима, и те информације се користе када се особа врати на веб сајт. Са овим информацијама преварант

[152] С. Лилић, *Право, информатичка технологија и заштита података*, Анали Правног факултета у Београду, бр. 2, стр. 211

би могао да изврши злоупотребе као што су подношење захтева за кредите или нове рачуне кредитних картица, затим они могу захтевати промену адреса за обрачун и користити туђу постојећу кредитну картицу без њиховог знања. Они такође могу да користе фалсификоване чекове и дебитне картице, или да обаве електронске трансфере у туђе име, да избришу нечији банковни рачун. Крађа идентитета може да иде даље од новчаних последица. Крадљивци могу да користе туђе информације да добију возачку дозволу или неки други документ на коме ће бити њихова фотографија, али туђе име и информације. Са тим документима крадљивци би могли да добију посао, поднесу захтев за путне исправе, или чак да учине да се и туђе име и поштанска адреса нађу у полицији и другим органима ако је лопов укључен у друге криминалне активности.[153]

Начин који омогућава најраспострањенији вид крађе, без видљивих знакова испољавања коришћење злонамерерног софтвера као што су тројански коњи који служе да се са жртвиног компјутера покупе лозинке, корисничка имена и бројеви кредитних картица које користе на рачунару и пошаљу их назад до починиоца дела. За разлику од конвенционалне крађе идентитета нпр. крађе новчаника са кредитним картицама, крађа идентитета на интернету може бити далеко разорнија јер је већина жртава крађе потпуно несвесна да је нешто украдено од њих док не буде прекасно. Према новим истраживањима, технологија препознавања лица може бити искоришћена за приступ личним подацима особе. Истраживачи Карниги Мелон Универзитета (енгл.Carnegie Mellon University) су комбиновали скениране слике и профиле на друштвеним мрежама како би идентификовали особе које нису на интернету. Овај нови метод додатно олакшава крађе идентитета на интернету при чему је неопходно детаљно преиспитивање ставова опште јавности у вези са приватношћу на интернету и оно што је на њему доступно о свакој појединачној особи. Спектар технологије за проналажење и прикупљање информација о интернет корисницима које користи влада једне државе су такође тема многих дебата између адвоката, судија и оних који сматрају да су такве мере неопходне како би спровођење закона могло бити у кораку са брзоразвијајућом комуникационом технологијом. На основу одлуку Савета министара Европске Уније у Бриселу, јануара 2009, министарство унутрашњих послова Велике Британије је прихватио план да се полицији дозволи приступ садржају компјутеру појединца без судског налога. Процес под

[153]Доступно на : www.webopedia.com/DidYouKnow/Internet/identity_theft преузето 08.05.2017.

називом „ даљинско претраживање “ је омогућавао једној страни да, са удаљене локације, прегледа туђи тврди диск и интернет саобраћај, укључујући имејл, историју претраживања и посећене странице. Полицији је сада дозвољено да затраже спровођење даљинског претраживања. Истраживање може бити одобрено и пронађен материјал предат и коришћен као доказ на основу сумње надређеног команданта који је сматрао да је овакав поступак био неопходан ради спречавања озбиљног преступа. Општа брига у вези са приватношћу интернет корисника је постала довољно велика брига за агенцију Уједињених Нација да је објавила извештај о опасностима крађе идентитета. [154] Највећу забежену бојазан опште јавности за своју приватност проузроковао је случај бившег службеника америчке Националне агенције за безбедност Едварда Сноудена(енгл. Edward Snowden) који је обелоданио на десетине поверљивих докуменама везаних за начине праћења и откривања података о грађанима Сједињених Америчких Држава.

Иако постоје неколико метода које настоје да сузбију или сведу на најмању могућу меру крађе идентита на интернету попут компјутерске форензике која у великој мери помаже полицијским службеницима да идентификују обе стране, жртве и починиоце крађе идентитета, од највеће је важности подићи општу свест грађана о ризицима доступности података, преиспитивати рад институција које се њима користе на који начин се подаци обрађују и складиште као и између којих институција постоји узајамна размена личних података.

- Компјутерско хаковање – Представља дело компјутерског криминалитета које се односе на кршење права на приватност али уједно и дело компјутерског криминалитета које се везује за економски криминал. Компјутерско хаковање је неовлашћено упадање у туђе информационе системе у намери да се сазнају одређене информације поверљивог карактера, или неовлашћено приступање информацијама ради њихове намерне преправке, уништења или оштећења.[155] Као најпогодније подручје деловања компјутерског хаковања на приватност лица јављају се друштвене мреже. Профил лица на друштвеним мрежама састоји се од мноштво података као што су; име, презиме, датум и година рођења, образовне установе које су похађане, подаци о сродницима као и пријатељима на конкретној друштвеној мрежи. Штету коју компјутерско хаковање може проузроковати

[154] Доступно на: http://news.bbc.co.uk/2/hi/technology/6199372.stm преузето 08.05.2017
[155]С.Константиновић-Вилић, В. Николић-Ристановић, М. Костић: оп. цит.,стр. 180.

упадом у туђи профил је пре свега нематеријалне природе и састоји се у нарушавању достојанства и части с обзиром на чињеницу да хакер може у потпуности онемогућити приступ профилу његовом власнику и тако га спречити увида у сам садржај профила и порука које се путем њега прослеђују. Иако мотиви извршења овог дела могу на први поглед деловати безопасно нарочито уколико се ради о вршњацима из школе, са спорта или других друштвених група последице које настају могу у одређеном броју случајева чак довести и до појаве самоубиства нарочито код млађе популације корисника друштвених мрежа који су током дужег времена изложена омаловажавању и порузи. Савети за безбедно коришћење друштвених мрежа могу у великој мери спречити појаву неовлашћеног упада у туђи профил и наношење штете при чему се они разликују код конкретних друштвених мрежа. Неки од њих су: постојање свести о подацима који се чине доступним, пажљив одабир пријатеља на мрежи, одређена доза сумње да је порука заиста од онога чије име пише на њој као и ургентно обавештавање администратора друштвених мрежа у случају немогућности уласка у сопствени профил.

- Компјутерска шпијунажа - Представља употребу широке категорије штетног софтвера или хардвера чија је намена да делимично пресреће или преузима контролу над компјутерима без знања или дозволе корисника. Иако сам назив сугерише да је реч о програмима и опреми која надгледа рад корисника, овај назив данас означава искоришћавање корисничког компјутера ради остваривања интереса за треће лице. Компјутерска шпијунажа је инкриминисана кривичним делима неовлашћени приступ заштићеном рачунару, и рачунарској мрежи и електронској обради података (члан 302 КЗ РС)и неовлашћено коришћење рачунара или рачунарске мреже (члан 304 КЗ РС).

Посебан вид компјутерске шпијунаже јесте компјутерско прислушкивање које постоји када се тајно, уз помоћ видео опреме, снима садржај нечијег компјутерског монитора или се прикључивањем на тај монитор обезбеђује контрола и праћење садржаја који се на њему емитује. Код компјутерског прислушкивања лице које преслушкује нема могућност мењања или избора садржаја, већ прати оно што овлашћени корисник емитује.[156] Најупечатљиви начин извршења компјутерске шпијунаже подразумева употребу веб камера, и то нарочито на преносним компјутерима (лаптоповима). Већина лаптоп рачунара са веб камерама поседује ЛЕД светло које би требало да се укључи сваки

[156] С.Константиновић-Вилић, В. Николић-Ристановић, М. Костић: оп. цит., стр. 181

пут када је укључена камера. Међутим, Федерални биро за истраге недавно је признао да је већ годинама агенција у могучности да искључи упозоравајуће светло веб камере тако да особа која је под надзором није не свесна чињенице да је камера укључена. Случај америчке мис тинејџерке Кесиди Вулф коју је уз помоћ софтвера на свом компјутеру и веб камере на њеном лаптопу шпијунирао Ђаред Абрахамс показао је да ЛЕД светло не представља поуздану одбрану ни када је реч о просечним шпијунима. Абрахамс је шпијунирао и друге девојке да би потом уцењивао своје жртве претећи им да ће објавити фотографије усликане за време њихових пресвлачења. [157] Овај случај који је потресао читаву америчку јавност недвосмислено показује опасност којој може просечни грађанин бити изложен. Нарочито отежавајућу околност представља чињеница да се софтвер за даљинско управљање веб камерама регуларно користи за управљање великим броја компјутера у институцијама нпр. на универзитетима што у великој мери онемогућава ефикасно проналажење учиниоца. С обзиром на све речено, иако помало хумористичка констатација светски познатог стручњака за безбедност Чарлија Милера(енгл.Charlie Miller) ни у ком случају не делује претерано „ најсигурнија ствар коју можете да урадити је да ставите траку на вашу камеру “.

Позната је чињеница да владе многих земаља, свесне зависности између могућности напредних технологија и економских перформанси, усмеравају своје напоре ка откривању и прибављању технологија развијених ван њихових граница.[158] Многе нације налазе у томе свој национални интерес, и то императиван, да користе све могуће расположиве начине, и офанзивне и дефанзивне, да би сачувале корак са новим технолошким развојем.[159]Детаљније о овоме биће изложено у делима компјутерског криминалитета којима се угрожава национална сигурност.

5.1.3 **Дела компјутерског криминалитета којима се угрожавају остали правно заштићени интереси (национална сигурност)**

Интернет и компјутерске мреже су моћан ресурс на који се савремено друштво умногоме ослања. Узимајући у обзир да инфраструктуре једне државе, попут брана ,електричних мрежа, финансијских трансакција ,транспортног саобраћаја, војних

[157] Више на : http://www.cnn.com/2013/09/26/justice/miss-teen-usa-sextortion/ преузето: 08.05.2017.
[158] G.D. Major,Espionage into the 21st century: A holistic approach to securiry, Datapro on CD, Originating report IS09-170-101 February 1994.
[159] Ibid.

одбрамбених система, све више ослањају свој рад на компјутерске системе, постоји оправдан страх да би компјутерски напад терористе озбиљно пореметио функционисање нападнутог система, довео до оштећења и угрожавање живота. Иако напади ове врсте нису до сада забежени, ова претња по националну сигурност државе се не сме игнорисати.

- Компјутерски тероризам – Дефинише се као акт уништавања или ометања компјутерских система у циљу дестабилизације једне државе или вршења притисака на њену владу и обухвата све намерно предузете, политички мотивисане нападе на компјутерске информације, компјутерске системе и мреже у циљу стварања опасности за живот или здравље људи, угрожавање јавне безбедности, застрашивање, изазивање немира или војних конфликата. [160] Компјутерски тероризам је инкриминисан следећим кривичним делима: тероризам (члан 391 КЗ РС), јавно подстицање на извршење терористичких дела (члан 391а КЗ РС), врбовање и обучавање за вршење терористичких дела (члан 391б КЗ РС), терористичко удруживање (члан 393а КЗ РС).

Први терористички напад на компјутере забележен је још 1969. године у Америчкој држави Мичиген, где су припадници једне антиратне организације под именом Beaver 55 напали центар за електронску обраду података познатог хемихског концерна Dow Chemical, за који се тврдило да производи бојне отрове, напалм и друго хемијско оружје.[161] Први службено регистровани компјутерско терористички напад извршен је 1998. године када је терористичка организација „Тамисли тигрови“ преплавила амбасаду Шри Ланке имејл вирусима. Треба разликовати компјутерски тероризам од обичног тероризма с обзиром на активност терористе у такозваном „виртуалном“ простору компјутерских система и мрежа. Терористичке организације користе интернет и компјутерске мреже за међусобну комуникацију, регрутовање својих присталица, прикупљање обавештајних података, илегално добијање пасоша и виза као и за дистрибуцију пропаганде. Ове активности могу изазвати страх, терор, панику и подићи степен безбедности државе међутим не могу директно изазвати смрт, повреду или физичко оштећење што представља јасну границу у односу на тероризам у класичном значењу. Као главне предности интернета као оруђа терористе наводе се : лак приступ; расположивост (сви језици, свако

[160] P. Galley, *Computer terrorism: what are the risks? Science, Tehnology and Society*, Swiss Federal Institute of Tehnology,1996, www.home.ch/spaw1165-infosec-sts en/ преузето 08.05.2017.
[161] Информативни кутак, Занимљивости; http://kompjuterskikriminalitet.blogspot.com/2009/02/zanimljivosti.html претражено 15.08.2017. године

време, електронска пошта, причаонице, дискусионе групе; блогови; звук; слика; отворена или кодирана комуникација); нерегуларност; одсуство цензуре и владине контроле; потенцијално велика публика у целом свету; анонимност комуникације и децентрализација; брз проток информација; ниски трошкови постављања интернет презентације; стално кретање и евазија (стварање и брисање адреса); широка лепеза оружја (вируси, црви, backdoor бомбе); критичне инфраструктуре као потенцијални циљеви.[162] Најважнија подручја примене интернета од стране терористa су: планирање и координација; управљање операцијама (практично више није потребан физички контакт између оних који управљају операцијама и оних који непосредно изводе акције); пропаганда; прикупљање средстава; публицитет; психолошки рат; прикупљање података; регрутовање и мобилизација; умножавање (енгл.networking); дељење информација; прање новца; кибернетички рат (енгл.cyberwar); лажне куповине софистициране опреме; биотероризам (нпр. оглашавање фалсификованих и лажних лекова), итд.[163] Компјутерским тероризмом не могу се сматрати хакерске активности које подразумевају неовлашћен улазак у компјутерске мреже с циљем нарушавања њиховог нормалног рада звог непостојања намере да се проузрукује штета великих размера и шири идеолошко-политичка пропаганда.

Све оно што се у данашњем свету догађа путем интернета, кроз злоупотребе од стране терористa није могуће ефикасно спречити управо због непостојања, најпре на националном нивоу држава, адекватних и делотворних закона који би регулисали ову област. Компјутерски тероризам није целовито регулисан ни једном међународном конвенцијом. Генерална скупштина УН усвојила је 2006. године резолуцију под називом „ Глобална стратегија против тероризма “, која, уколико би се компјутерских тероризам могао прихватити као једна од нових форми тероризма, би могла послужити као једно од средстава његовог сузбијања. Такође, Савет Европе је 2004. године донео „ Конвенцију о високотехнолошком криминалу “ која се потпуније бави питањима ове изузетно сложене проблематике. С обзиром на чињеницу глобалног карактера компјутерског тероризма сарадња на међународном нивоу је „ condicio sine qua non “ ефикасне и брзе реакције како на откривање и заштиту од истог тако и на само сузбијање.Оно што повећава опасност

[162] Ж. Кешетовић, *Интернет као оруђе терористa*, Ревија за безбедност-стручни часопис о корупцији и организованом криминалу, Центар за безбедносне студије, Година II, бр. 4/2008 Београд
[163] Ibid.

када је реч о могућности да терористи у наредном периоду све више користе интернет и компјутерске системе за остваривање својих циљева јесу извори таленана који су у стању да обезбеде експерте, довољно оспособљене да врше компјутерске саботаже и шпијунаже високог нивоа, да од терористе преузимају одговарајуће задатке или их обучавају у руковању компјутерском опремом. Глобални извор талената, представљају незапослени технолошки стручњаци из земаља трећег света, високостручни кадрови бивших обавештајних служби и изузетно надарени студенти. Интернет странице терористе су врло професионално урађене и садрже углавном информације о настанку и деловању терористичке групе којој припадају, о политичким циљевима групе, истакнутим припадницима, важним говорима, обавештења о активностима и аудио и видео презентације. Услед великог ризика од откривања својих чланова терористичке организације које делују у Сирији (Исламска држава Фронт Ал-Нусра и др.) не регрутују више своје чланове у Европи и Северној Америци на традиционалан начин уместо у џамијама као што је била пракса ранијих година, већину радикалних муслимана терористи регрутују јер активно користе друштвене мреже. Процес селекције, провере и посматрања нових чланова је дуг и сматра се да је око 4 000 чланова на овај начин регрутовано из западноевропских земаља, Сједињених Америчких Држава и Канаде.

- Компјутерска саботажа и шпијунажа -Као пример коришћења компјутерских система за извршење наведених дела ,која се сврставају и у дела којима се угрожава национална сигурност, може се навести Ирска републиканска армија која је 1997. године шокирала енглеску јавност, упућивањем претње да ће поред бомби, атентата и других облика терористичких аката почети да користи електронске нападе на владине компјутерске системе . Иако се компјутерске саботаже ,које представљају уништење или оштећење компјутера и других уређаја за обраду података у оквиру компјутерских система или брисању, мењању и спречавању коришћења информација садржаних у меморији компјутерских уређаја, најчешће приписују терористичким организацијама, нису тако ретки случајеви њиховог извршења и од стране појединаца. Саботери могу имати веома различите мотиве, који могу бити политичког, економског, војног, службеног или приватног карактера. [164] Тако на пример, у тржишној утакмици у којој нема милости и у којој се често не бирају средства, није искључено да нека компанија организује саботажу

[164]С. Петровић, оп.цит. стр. 140

на рачунару конкурентске фирме. [165] Далеко већу материјалну штету саботери могу нанети уколико своју активност усмере на државне органе, јавне службе или друга правна лица као што су установе, предузећа или друге организације. Радник у Национаној ваздухопловној и свемирској администрацији у САД је 2007. године намерно оштетио компјутер који је требало да буде испоручен на међународну свемирску станицу шатлом Ендевор.[166] У Србији је 2013. године шефица кабинета бившег директора јавног предузећа „ Нуклеарни објекти Србије “ пре него што је напустила то предузеће, са службеног рачунара обрисала пословну кореспонденцију и податке који су били од значаја за рад самог предузећа.

Као и компјутерска саботажа, компјутерска шпијунажа може бити мотивисана војним, политичким или економским разлозима, због чега се многе земље преко својих тајних служби ангажују у откривању политичких, војних, економских и службених тајни других земаља.[167]Подаци концентрисани у државним, војним, истраживачким и многим другим информационим системима представљају праву ризницу тајних података, чије је одавање и достављање сада могуће на много бржи и поузданији начин.[168] Како би се на брз и ефективан начин компјутерска шпијунажа извршила користе се читав спектар најразноврснијих метода и техника, почев од оних традиционалних до специфичних, високо софистицираних компјутерских техника. За ове активности се обично ангажују атешеи за науку и технологију, трговачки представници, припадници обавештајних служби, војни атешеи при амбасадама широм света, као и дописници новинских и радио-телевизијских агенција.[169] Многе владе користе и студенте који студирају у другим земљама да стажирају у циљним компанијама, као алтернатива обавезном служењу војске.[170]Оно што је уочљиво последњих година је чињеница да се фокус компјутерске шпијунаже све више помера са политичких и војних ка економским темама. На то указују и терминолошке промене које се огледају у све доминантнијем присуству економског и индустријског/ комерцијалног вида компјутерске шпијунаже који представља прикупљање

[165] Ibid.
[166]Доступно на :http://www.nbcnews.com/id/19981415/ns/technology_and_science-space/t/nasa-reports-computer-sabotage преузето 15.05.2017.
[167] С. Петровић, оп.цит. стр. 142
[168] Ibid., стр. 144
[169] G. D. Major, Espionage into the 21st century: a holistic approach to security, Datapro on CD, Originating Report ISO9-170-101,February 1994.
[170] B. N. Venzke, Economic/industrial espionage, 1996, http://www.infowar.com/class_2/class2_2.html-ssi

обавештајних података од страних влада или великих корпорација са циљем остваривања енормно велике финансијске користи кроз злоупотребе најзначајнијих података. Познат је случај шпијунског напада на ИБМ од стране двадесетак особа које су радиле за јапански Хитачи и током три године украле поверљиве информације вредне између 750 милиона и 2,5 милијарде долара. Акцију је пресекао 1982. године ФБИ у својој чувеној „sting"(жаока) операцији. [171]

[171] U. Sieber, оп.цит., стр. 14 R.Garner The growing professional menace, 1995, Open computing,стр. 36

6.Етиолошке карактеристике компјутерског криминалитета

Криминална етиологија је део криминологије који проучава опште изроке криминалитета као масовне друштвене појаве и појединачне, посебне, непосредне узроке, услове и поводе јављања криминалног понашања (криминогене факторе).[172]Општи узроци криминалитета који произилазе из одређене друштвене структуре, друштвено-економског система и односа у свим сферама друштвеног живота, повезани су са посебним и појединачним факторима који делују у породици, школи, професионалном, класном, друштвеном статусу, у оквиру појединих ужих и ширих друштвених група. [173]

Криминална етиологија се најчешће дели према природи фактора који делују на јављање криминалитета на две области: егзогену етиологију и ендогену етиологију.

Егзогена етиологија се односи на изучавање узрока криминалитета који произилазе из одређене друштвене културе и структуре, услова живота, деловање разних криминогених фактора везаних за породицу, школу, групу, средства масовне комуникације, сукоба култура, различитих схватања о вредностима, друга девијантна понашања итд.

Ендогена етиологија изучава утицај личних особина психолошких карактеристика, црта личности на јављање криминалног понашања. У оквиру ендогене етиологије треба разјаснити како се одвија процес „ криминализације личности “ зашто поједина лица врше кривична дела у одређеним социјалним условима, а друга у истим тим условима то не чине, какав утицај на криминалитет имају психолошки процеси (лични интелектуални процеси: мишљење, учење, интелигенција, опажање; емоционални процеси или осећања и вољни процеси-мотивација) и психичке особине (навике, способности, темперамент, потребе, интереси). [174]

6.1 Егзогени криминогени фактори

Егзогене факторе који су допринели појави и распрострањености компјутерског криминалитета потребно је најпре тражити у специфичностима брзине развоја и ширења информационе технологије као и у све већој зависности друштва од употребе компјутера и компјутерске технике у свакодневном животу. Динамичне промене на пољу

[172] С. Константиновић-Вилић, В. Николић-Ристановић, М. Костић, Криминологија, оп.цит. стр. 28,
[173] Ibid. стр. 30
[174] Ibid. стр. 29

информационе технологије, са снажним комерцијалним примесама, значајно поједностављају и олакшавају њено коришћење, чак и од стране нетехничких кадрова, ширећи тако лепезу оних којима „ компјутерска моћ “ постаје доступна, а ту моћ нико не сме да потцењује, јер карактеристике које олакшавају коришћење ове технологије су исте оне које олакшавају и неовлашћен продор у систем и приступ његовим ресурсима, функцијама и његовом садржају. [175] Компјутерски криминалитет је у непосредној вези са степеном друштвено-економског развоја одговарајуће средине. Што је степен развоја неке средине виши, његови су појавни облици разноликији, начини његовог извршења софистицираније, а починиоци стручнији и бројнији. [176] Неки од доминантнијих егзогених фактора су : 1) технолошки развој; 2) концентрација података; 3) нови амбијент деловања; 4) нове вредности; 5) нове форме старих вредности; 6) нове временске и просторне границе; 7) ширење информатичке писмености; 8) глорификација компјутерских криминалаца нове; 9) криминалне методе и технике итд.

У оквиру технолошког развоја интернет је као нови глобални медиј фундаментално променио начин друштвеног живота обезбеђујући нове и једноставније начине комуницирања, инфоримасања, образовања, рада и забаве. На пример, много је лакше написати електронску поруку преко електронске поште него класично папирно писмо. Ово посебно долази до изражаја ако исту поруку треба написати на већи број електронских адреса широм света. Електронска пошта може бити писана и читана у било ком тренутку и може бити слана и примана у свако доба дана и ноћи, независно од временске зоне у којој се налазе и пошиљалац и прималац.[177] Значајно је напоменути да је технолошки развој омогућио увођење информационе технологије у банкарске и финансијске системе чиме су новчана средства добила свој тзв. „ електронски облик“ и преселила се у тзв. „ електронске“ трезоре.

У двадесет и првом веку информација представља најважнији стратешки ресурс који може имати изузетно велику вредност, па чак бити и непроценљив. Информација је

[175] С.Петровић оп.цит. стр. 62-63
[176] Д. Драгичевић, *Компјутерски криминалитет и информацијски сустави*,Загреб,1999, стр. 146-148
[177] B. Guttman, R. Bagwill, Internet security policy: A technical guide, NISTнм special publication 800-XX, july 31, 1997., http:csrc.nist.gov/isptg/html/ISPTG.html, J. Honeycutt, A. M. Pike, Using the internet, Special Edition,Que Corporation, Indianopolis,SAD,1996, стр. 224; B. Sterling, Short history of the internet, The magazine of fantasy and science fiction, february, 1993., http://www.fortunecity.com/skyscraper/smiley/0/ history.htm

једина „ствар „ која се може украсти , а да и даље остане на свом месту. [178] У компјутерима могу бити концентрисани изузетно вредне информације (подаци) из области привреде, науке, медицине, безбедности и одбране државе као и подаци о личности појединца које у случају злоупотребе могу проузроковати велику како материјалну тако и нематеријану штету. Подаци се могу избрисати или изменити, а да о томе не остану докази. Аутоматска и даљинска обрада података омогућава обављање разноврсних трансакција без могућности ефикасног надзора или управљања њима. Изузетно динамичан развој медија за складиштење и пренос података попут стандардних и хард дискова, флеш меморија и тзв. „клауд“ (енгл. cloud) сервера додатно отежава ефикасно праћење тока њихове размене. И док се време потребно за реализацију класичних облика криминалних радњи мери данима или сатима, а у идеалним условима и минутима, реализација компјутерског криминала мери се хиљадитим или милионитим делова секунде, што указује на драстично сужавање временске скале деловања компјутерских криминалаца.[179]Све већа минијатуризација компјутера и компјутерске опреме, снижавање цена и поједностављање употребе допринели су ширењу информатичке писмености и повећању броја корисника изузетном брзином . Основна знања из области информатике пружена у оквиру школских програма могу у појединим случајева бити довољна за извршење појединих дела компјутерског криминалитета. Свој „ допринос“ у подстицању младих у пуној мери даје и филмска индустрија у чијим су филмовима често приказани млади хакери као хероји модерног доба достојни страхопоштовања и дивљења.

Могућности за извршавање компјутерског криминала постоје, до извесног степена, у скоро сваком амбијенту у којем се користи информациона технологија, из простог разлога што не постоји апсолутно заштићен систем. Колики ће тај степен бити, зависи пре свега, од пословне политике која се води на плану руковођења, организационом и кадровском плану, али и на плану заштите, надзора и контроле.

[178] B. Menkus, *Protecting corporate data*, Honeywell Source summer, 1994, p. 48
[179] С.Петровић оп.цит. стр. 90

6.2 Ендогени криминогени фактори

Неки од најзначајнијих ендогених фактора који доводе до појаве компјутерског криминалитета , односно који на појединца утичу да се укључи у криминалне активности су: [180]

- Отуђеност, као последица савременог начина живота и комуницирања, који се све мање одвија уз непосредан контакт, а све више посредно, путем информатичке и телекомуникационе технологије, може довести до асоцијалног понашања. Као последица такве зависности и анонимности при комуникацији, често се јавља жеља за нездравим доказивањем и презентовањем своје надмоћи, посебно међу хакерима, као специфичном категоријом извршилаца криминалних активности из ове области;

- Фрустрација изазвана информационим стресом, као последица све веће количине информација којом смо засипани свакодневно и нужност да међу њима одаберемо оне на основу којих ћемо доносити правовремене и ваљане одлуке, може довести до агресивности и различитих реакција појединаца у односу на информациону технологију и њено коришћење;

- Психичка обољења, као последица неконтролисане, временски дуготрајне, видљиво проблематичне употребе интернета, резултира социјалним, пословним или финансијским проблемима;

- Мотивација је неизоставни део расправе о узроцима ове појаве. Брзина којом се може извршити компјутерска злоупотреба, са великих удаљености, уз анонимност учиниоца и тешкоће њиховог откривања, велики су подстицај и чест мотив појединца да такво дело изврши, а посебно када се томе придода могућност брзог и лаког богаћења, тј. стицање незаконите имовинске користи;

Ставови и схватања све су чешћи разлог разних кажњивих дела, а посебно када су у питању идеолошки ставови који могу довести и до најтежих облика рачунарског криминалитета, као што је то случај са компјутерском саботажом.

Осећај незадовољства или фрустрације неким аспектом приватног или пословног живота, као што су недостатак љубави, нежности, пажње, присуство мобинга на послу , економска зависност и социјална запостављеност може за последицу имати формирање

[180] Д. Драгичевић, оп. цит.стр. 148-149

негативних карактерних црта личности. Неке од њих попут похлепе, зависти, љубоморе, или осветољубивости могу представљати изузетно јак мотив за извршење дела компјутерског криминалитета. Међу ендогеним факторима компјутерског криминалитета и злоупотребе друштвених мрежа треба поменути и синдром интернет зависности и то специфичан вид интернет зависности, који се односи на компулсивну употребу веб сајтова за сајбер дечију порнографију.[181] Када се ради о ендогеним узроцима везаним за дечију порнографију, анализе показују да не постоји значајна узрочна повезаност између појединих психолошких црта личности (морални избор хедонистичке вредности, морални избор социјалних вредности, екстраверзија, неуротицизам, отвореност према искуству, разумност и савесност) и злоупотребе дечије порнографије.[182] Корисници интернет дечије порнографије схватају можда да је њихово понашање друштвено забрањено, али не верују да је оно„ погрешно“ за њих лично, за разлику од корисника порнографије која није дечија, који верују да је понашање везано за дечију порнографију морално погрешно и на друштвеном и на индивидуалном нивоу .[183]Узрочност дигиталне пиратерије поједини аутори повезују са теоријом самоконтроле.[184] Приликом понашања које се квалификује као дигитална пиратерија, особе са ниском самоконтролом, не поштују поверење исказано у уговору о лиценцирању између онога ко је створио дигитални медиј и онога који има ауторска права. За већину људи дигитална пиратерија је узбуђење, а интернет једноставан

[181] М.Ковачевић-Лепојевић, *Појам и карактеристике интернет зависности*, Специјална едукација и рехабилитација, Vol. 10, br. 4, Београд, стр. 621, http://www.casopis.fasper.bg.ac.rs/izdanja/SEIR2011/vol10br4/1Spec_Edu_i_Reh_ISTRAZIVANJA/4-Marina_Kovacevic_Lepojevic.pdf, претражено 03. 09. 2017. године

[182] В. Вилић оп.цит стр. 247

[183] K.Siegfrid Spellar, R. Lovely, M. Rogers, *Self-Reported Internet Child Pornography Consumers*. *A Personality Assessment Using Bandura's Theory of Reciprocal Determinism*, наведено у Cyber Criminology, Exploring Internet Crimes and Criminal Behavior, 2011, CRC Press, p. 72

[184] Gottfredson и Hirschi су 1990. Формулисали теорију самоконтроле према којој је низак ниво самоконтроле на индивидуалном нивоу узрок криминалитета и девијантности. Ниска самоконтрола представља индивидуалну склоност ка криминалитету и девијантности, а може да буде резултат слабог или неефективног родитељства које дете искуси пре осме године живота. Како би се развио одређени ниво самоконтроле родитељи морају да развију емоционалну везу са својим дететом. Једном када се ова веза развије родитељи имају могућност да сакупе бихевијоралне информације о свом детету. Онда родитељи могу да анализирају ове информације како би одредили да ли је понашање девијантно или може да прерасте у девијантно. Када родитељи слабо или уопште не обављају ову улогу, дете има веће шансе да развије ниски степен самоконтроле. Особе са ниском самоконтролом склоније суизвршавању једноставнијих и лакших задатака, чешће бирају физичке а не менталне активности, ангажоване су у ризичним понашањима, фокусиране на себе и не могу да контролишу свој темперамент. Видети : M.Gottfredson,.and T.Hirschi, .: *A general theory of crime*, Stanford, CA: Stanford University Press, цит. Према G. Higgins,Value and Choice, Examining Their Roles in Digital Piracy, наведено у Cyber Criminology, Exploring Internet Crimes and Criminal Behavior, оп.цит., стр. 141

уређај за манипулацију и спровођење дигиталне пиратерије. На тај начин ниска самоконтрола има директан утицај на вршење дигиталне пиратерије.

6.3 Криминолошке теорије узрочности компјутерског криминалита

Посебну теорију о компјутерском (сајбер) криминалитету установио је Jaishankar 2008. године. [185] Теорију је назвао **теорија транзиције простора** (енгл. Space Transition Theory), објашњавајући да је потребно да постоји посебна теорија о узроцима криминалитета у сајбер простору, јер су уопштена теоријска објашњења феномена сајбер криминалитета недаекватна и недовољна. Теорија образлаже природу понашања особе која испољава прилагођено или неприлагођено понашање у стварном простору и у кибернетичком простору. Просторна транзиција се односи на померање особе из једног простора у други (на пример из стварног физичког простора у кибернетички простор и обрнуто). Према теорији транзиције простора, људи испољавају различито понашање у случају преласка из стварног, реалног, физичког простора у виртуелни простор.

Постулати ове теорије формулисани су у седам тачака:

1. Особе које су потиснуле криминално понашање у стварном или физичком простору због свог статуса или позиције, имају склоност да испоље криминалитет у виртуелном простору;

2. Флексибилност идентитета, дисоцијативна анонимност и недостатак страха у сајбер простору доводе до тога да преступник изабере сајбер простор за извршење недозвољеног дела;

3. Криминално понашање преступника у виртуелном простору ће највероватније бити пренето и у физички простор, као што се и понашање из физичког простора може пренети у сајбер простор;

4. Повремени „испади“ преступника у сајбер простору, заједно са динамичном просторно временском природом сајбер простора дају преступнику шансу„ да побегне “, односно не буде ухваћен;

5. а) Људи који се међусобно не познају имају шансу да се уједине у сајбер простору како би извршили неки злочин у физичком простору; б) Људи који се међусобно

[185] K.Jaishankar, Editorial: Establishing a Theory of Cyber Crimes, International Journal of Cyber Criminology, Vol 1 Issue 2 July 2007, стр. 7, http://www.cybercrimejournal.com/Editoriaijccjuly.pdf, претражено 28. 08. 2017. године

познају у физичком простору могу да уједине како би извршили неки злочин у сајбер простору;

6. Особе из друштва које су затвореније и репресивније имају веће шансе да изврше неко дело у сајбер простору него особе из отворених заједница;

7. Конфликт норми и вредности из физичког простора са нормама и вредностима у сајбер простору може да доведе до сајбер криминалитета.

Сајбер криминалитет, кога Wall (2001.) категоризује као четири главна типа: хакинг (илегални упад у компјутерски систем), сајбер преваре и крађе, сајбер порнографија и сајбер насиље, може се објаснити постулатима теорије транзиције простора.[186] Међутим, ова теорија је до сада остала само као теоријско објашњење узрока сајбер криминалитета и емпиријски није проверена[187] Према **теорији стила живота** (енгл. Lifestyle/exposure to risk perspective)[188], on line стил живота директно утиче на виктимизацију од компјутерског криминалитета. Студија у којој је анализиран овај утицај [189]полази од чињенице да је компјутерски криминалитет велика претња интернет корисницима и да им наноси огромну штету, посебно када дође до крађе личних података из персоналних досијеа. Истраживања у оквиру студије су показала да студенти који воде начин живота оријентисан на коришћење компјутера и немају одговарајуће антивирус програме, имају далеко већу шанску да постану жртве компјутерског криминалитета. Могућност виктимизације се значајно смањује уколико се повећа интернет сигурност и већина корисника поседује адекватан компјутерски програм за заштиту од злоупотребе.

Теорија диференцијалне асоцијације полази од утицаја криминалних и некриминалних понашања унутар групе и опредељивања чланова групе за једно или друго

---

[186] P.Danquah, O.B Longe,.An Empirical Test of The Space Transition Theory of Cyber Criminality: Investigating Cybercrime Causation Factors in Ghana, African Journal of Computing & ICT September 2011, Vol. 2. No. 2 Issue 1, pp. 37-48, http://www.ajocict.net/uploads/V4N1P62011_AJOCICT__An_Empirical_Test_Of_The_Space_Transition_Theory_of_Cyber_Criminality_-_The_Case_of_Ghana_and_Beyond.pdf, претражено 28. 08. 2017. године

[187] В. Вилић, оп.цит., стр. 236

[188] Hinderlang, M., Gottfredson, M., и Garofalo, J., међу првима су развили идеју о утицају стила живота на кретање стопе криминалитета. Утврдили су да висока стопа виктимизације неких друштвених група(млади мушкарци) може бити објашњена њиховим стилом живота, који се састоји углавном у активностима ван куће и у току ноћи. С. Константиновић-Вилић, ,В.Николић-Ристановић, М. Костић, *Криминологија*, op.cit., стр.. 307

[189] C. Kyung-Shick,Cyber-Routline Activities, Empirical Examination of Online Lifestile, Digital Guardians and computer Crime Victimisation“ наведено у Cyber Criminology, Exploring Internet Crimes and Criminal Behavior,оп.цит., p 243

понашање, зависно од утицаја који преовлађује. Битан аспект успеха терористичких група, које су своје чланство омасовиле користећи интернет и друштвене мреже, управо су објашњења ове теорије о прихватању криминалних утицаја. Захваљујући интернету, терористичке групе су биле у могућности да успешно остваре односе са младим људима широм света, са различитих географских подручја и да тако координирају терористичке активности.[190]

Према **теорији рационалног избора** [191] преступници ће увек тежити да изаберу оне мете које захтевају најмање напора, али које у исто време пружају високу награду и носе најмањи ризик у погледу откривања и последица неуспеха. Приликом коришћења интернета и укључивања на друштвене мреже управо стална доступност жртве, масовност корисника и отежана могућност откривања доприносе да се поједине особе одлуче на извршење дела. Свакако да се код крађе идентитета као један од криминогених фактора може сагледати олакшан приступ личним информацијама и подацима када корисници деле садржај са свим или већином корисника и на тај начин директно омогућавају повреду приватности и злоупотребу.[192]

[190]T. Freiburger , J.Crane J, The Internet as a Terrorist's Tool, A Social Learninig Perspective, наведено у Cyber Criminology, Exploring Internet Crimes and Criminal Behavior, op.cit., p.128
[191]С. Милићевић, С.Вујовић, Проблем савремене доби: облици крађе и злоупотребе идентитета и мјере превенције, Сузбијање криминала и европске интеграције, с освртом на високотехнолошки криминал,. Лакташи2 8-30.03.2012.,стр. 310
[192] В. Вилић оп.цит. стр. 237

7. Подела и основне карактеристике извршиоца дела која припадају компјутерском криминалитету

Уопштено би се извршиоци ових дела могли поделити на злонамерне, који могу да делују ради остварења имовинске користи, или само у циљу наношења штете, као и на учиниоце који нису мотивисани ни остварењем користи, нити проузроковањем штетних последица, већ једноставно траже задовољство у неовлашћеном продирању у неки добро обезбеђен информациони систем.[193]Злонамерни извршиоци дела компјутерског криминалитета су најчешће мотивисани користољубљем, а сматра се да подаци из праксе указују на одређени скуп особина које чине њихов криминални профил: око 80% ових делинквената чини дело по први пут, 70% је запослено више од пет година у оштећеном предузећу; њихово старосно доба је у просеку између 19 и 30 година; претежно су мушког пола; веома су интелигентни; имају углавном више година радног искуства и важе као савесни радници који приликом обављања радних задатака не проузрокују никакве проблеме; често су технички квалификованији него што то захтева радно место на које су распоређени; ови учиниоци, по правилу, себе не сматрају крадљивцима или уопште криминалцима, већ само позајмљивачима. [194] Компјутерски криминалитет који се врши из користољубља у великој мери је присутан у банкарском и финансијском пословању. Статистички подаци о извршиоцима дела овог типа криминалитета у области банкарских послова указују на најчешће професије учинилаца: 25% чине особе са специјалним овлашћењима и одговорностима у информатичким системима; 18% програмери, 18% службеници који располажу терминалима, 16% благајници, 11% оператери-информатичари и у 12% случајева учиниоци ових дела су лица ван оштећених корпорација, у шта су укључени и корисници услуга.[195]

Извршиоци дела компјутерског криминалитета који траже задовољство у неовлашћемом продирању у добро обезбеђен информациони систем припадају тзв. хакерима. Од изузетне је важности указати на значења термина хакер према Новом хакерском речнику [196] особа која ужива у истраживању детаља у програмираним

[193] Ј. Матијашевић, оп.цит. стр. 86
[194] Ibid.
[195] Ж. Алексић, М. Шкулић, *Криминалистика*, Београд,2007 стр.388-389
[196] Више на: http://svethakera.com/index.php?option=com_content&task=view&id=13&ltemid=32 претражено 06.08.2017.

системима и побољшања њихове употребне моћи, супротно већини корисника који уче само неопхнодни минимум коришћења тих система:

1) особа која програмира са ентузијазмом или која више ужива у програмирању него теорисању о истом;

2) особа способна да процени праве вредности;

3) особа која је добра у брзом програмирању ;

4) особа која је експерт за неки кориснички програм или проводи много времена користећи га (на пример Unix hacker)

Хакери су особе опседнуте новом технологијом у тој мери да готово сваки аспект свог живота у већој или мањој мери повезују са компјутерима. Дневно за компјутером проведу и по 14 часова како би проширили своја знања о информационим технологијама и обезбедили себи што једноставнији продор у заштићене програме и системе. Нажалост, успешност ове активности веома често повлачи и ненамерну материјалну штету као и оштећење система. У сврху позитивног приступа термину хакер, наводе се подаци да је до сада пронађено више од 12. 000 пропуста у функционисању компјутерских програма и система на које су указали хакери како би произвођачи програма и система исправили своје пропусте, а корисници истих себе благовремено заштитили. За разлику од наведеног ужег појма хакера , шири појам обухвата различите врсте хакера у зависности од одговарајућих критеријума. У наставку ће бити изложена подела хакера према критеријуму поштовања етике и степену професионалности.

Према критеријуму поштовања етике постоје:[197]

- **White Hat Hackers (Беле капе) –** ови хакери се придржавају хакерске етике, баве се заштитом система и мрежа рачунара. Труде се да побољшају заштиту система да не би дошло до продирања у њих и наношења штета. По правилу се изнајмљују од компанија да би провалили у рачунар, а затим обавестили власника на који начин је то урађено и како поправити одређене недостатке;

- **Black Hat Hackers (Црне капе) -** ови хакери се не устручавају да краду и уништавају податке у мрежама и системима у које приступе. Хакерску етику интерпретирају на себи адекватан начин. Принцип да све информације треба да буду

[197] Ј. Матијашевић, оп.цит. стр. 88

слободне даје им оправдање да проваљују у туђе системе. Неретко се дешава да униште неки део система, а у њихове активности спада и креирање и ослобађање вируса и црва који наносе штету корисницима рачунара;

- Grey Hat Hackers (Сиве капе) - јесу нешто између црних и белих капа. Желе да се издвоје од тастера за безбедност неке компаније са једне стране и са друге стране да се дистанцирају од негативизма „ црних“ капа. Већином су то хакери који су у почетку кршили хакерску етику, да би касније стечено знање примењивали по свим њеним правилима;

Класификација хакера према степену професионалности, где је критеријум ниво познавања рачунарске технологије и озбиљност последица које проузрокују, разликују следеће групе извршилаца : [198]

- Аматери - најчешће имају легално занимање, а из различитих разлога се повремено упуштају и у криминалну активност. Најчешће врло брзо бивају откривени. У ову групу спадају: 1) Слаби и поводљиви појединци чији су криминални акти најчешће узроковани тренутном повољном приликом. Често нису ни свесни могућих последица својих радњи. Веома лако бивају изманипулисани од стране особа које их обећањима, претњама или уценама, наводе на злоупотребе рачунарских система; 2) Људи са пороком су особе са приватним проблемима, изазваним неким социо-патолошким понашањима, који излаз виде у криминалном понашању; 3) Фрустрирани појединци су незадовољне, разочаране и огорчене особе које на основу свог унутрашњег осећаја (сматрају да су преварене, неоправдано запостављене,...) оправдају своја чињења.

- Професионалци- су особе којима је једно од главних, а често и једино занимање бављење криминалом. Владају изузетним технолошким знањима, које константно усавршавају и доградњују. Поред високог нивоа стручности, изузетно су мотивисани, и у свом раду показују велику упорност и истрајност, услед чега се веома тешко откривају, а још теже се њихова дела доказују у судском поступку.У ову групу спадају: индивидуални криминалци, мотивисани остваривањем материјалне користи, немају разрађене дугорочне планове, нити самосталну стратегију деловања. Врло ретко се удружују са другим особама; Организоване групе компјутерских хакера, састављене

[198] Више о томе: М.Будимлић, П.Пухарић, оп. цит. стр. 33-38

су од појединаца који делују под заједничким интересима. Карактерише се чврстом организацијом и хијерахијском уређеношћу. Резултати које остварују у директном су односу са бројношћу и стручношћу чланова и квалитетом организације. Ове групе, поред класичних начела деловања организованих криминалних група, владају изузетним информатичким знањима, која користе у извршењу тешких дела из области рачунарског криминалитета, што их сврстава у професионале извршиоце највишег ранга.

Од изузетне је важности указати на посебну врсту хакера тзв. крекере који захваљујући великом степену познавања информационих технологија свесно и намерно продиру у заштићене компјутерске системе најчешће мотивисани користољубљем. Постоје следеће групе крекера: [199] 1) Вандали - имају за циљ да хакују рачунарске системе са намером да их униште (брисање фајлова, форматирање хард диска што проузрокује губитак информација,...); 2) Jokers (Џокери) - најбезопаснија врста крекера у погледу штете коју наносе рачунарима. Њихова намера је да приступе рачунарском систему, мењајући му звук, визуалне ефекте,...); 3) Breakers (Врекери) - професионални криминалци , који врше напад на систем са намером да украду новац, скуп софтвер итд. 4) Ламери - углавном малолетници, који користећи штетне програме написане од стране крекера, наносе штете другима (краду шифре, уништавају дискове, итд); 5) Cardels - криминалци који користе туђе кредитне картице за плаћање својих рачуна; 6) Collectors (codes kids) - прикупљају и користе софтвер пресрећући различите шифре, кодове и бројеве приватних телефонских компанија које имају приступ глобалној мрежи. Специфичну врсту кракера чине тзв. фрикери (Phreakers). Фрикерима се сматрају особе које у првом реду изучавају разне телефонске системе и располажу знањем из тог подручја, што им омогућава да се уз помоћ различитих средстава и метода неограничено и бесплатно користе њиховим услугама. Ово су хакери чија је уска специјалност крађа телефонских импулса, обављање међународних позива на рачун другог лица и све оне активности које се тичу телефонског саобраћаја. Основне карактеристике деловања фрикера јесу да их је веома тешко открити, због софистицираности телефонских система, као и то да својим

[199] В. Спасић, Актуелна питања у области сајбер криминала, Билтен судске праксе Врховног суда Србије, Intermex, br. 1/2006, Beograd

деловањем проузрокују енормне финансијске губитке.[200]Извршиоци дела компјутерског криминалитета који су изузетно ретки али истовремено и најопаснији су компјутерски шпијуни. Неовлашћено упадају у компјутерске системе, манипулишу информацијама, краду их и прослеђују наручиоцима. Компјутерски шпијуни у већини случајева настоје да себи обезбеде позиције унутар одговарајуће организације које ће им омогућити слободан приступ компјутерским система као што су место програмера, сарадника за одржавање компјутерских мрежа и других облика електронске комуникације, службеника који имају приступ финансијском пословању и др. У одређеном броју случајева неовлашћени упад у систем компјутерским шпијунима може бити олакшан захваљујући подацима којима располажу овлашћена лица за приступ систему. Корист коју овлашћена лица стичу активношћу компјутерских шпијуна искључиво је материјалне природе. На повећану опасност од њихових активности указује специфична мотивациона структура која може садржати назнаке терористичке идеологије. Способни су да неовлашћено приступе подацима садржаним у компјутерским системима са високим степеном заштите, који веома често могу бити од значаја за националну безбедност одређене државе.

Данашњег просечног извршиоца дела компјутерског криминалитета могуће је окарактерисати као углавном младу, интелигентну, високо мотивисану, узорну и поверљиву особу мушког пола са чврсто изграђеном логиком и одличном вештином коришћења компјутерских система. Још давне 1975. године Паркер Д. је навео карактеристике модерног компјутерског криминалца тог времена, базирајући их на 17 случајева које је он детаљно испитивао: [201]

- Извршиоци су млади(просечна старост 29 година)
- Управљачке и професионалне вештине су преовладавајуће (70% су били руководиоци или високо искусни технички професионалци)
- Нарушавање професионалног (радног) поверења било је евидентно у 65% случајева;
- Личне карактеристике:

– Виђен као веома пожељан радник: поуздан. Достојан поверења, бистар, паметан, мотивисан;

[200] Ј. Матијашевић, оп.цит. стр. 89

[201] L.Krauss, A. MacGahan, *Computer fraud and countermeasures*, New Jersey,1979,. стр. 39;I.C. Palmar, G. A. Potter, *Computer security risk management*,London 1989, pp. 117-118

– Није професионални криминалац који се поноси својом криминалном прошлошћу

– Највећи страх су имали од могућности да њихови криминални акти буду откривени и познати породици, пријатељима и колегама са посла.

Осам година касније (1983. године) Bequail A.[202]демонстрира сличан профил:

- Старост: 15-45 година;
- Криминална прошлост: обично раније нису били у сукобу са законом;
- Професионално искуство: од минималног до високо искусних информатичких професионалаца; мада су забележени случајеви да извршиоци нису имали било какво информатичко искуство;
- Личне особине: бистар, мотивисан и спреман да прихвати технички изазов, ангажован радник;
- Улога: у већини случајева делује самостално, ипак, расте број случакева са конспирацијом два или више криминалаца;
- Понашање: у јавности никад не нарушава важеће (стандардне) друштвене норме понашања;
- Позиција: најчешће је у позицији са које има лак приступ до рачунара;

[202] A. Beaquai, оп.цит. р. 43

II СТУДИЈА О КОМПЈУТЕРСКОМ КРИМИНАЛИТЕТУ У ПЕРИОДУ 2009-2015. ГОДИНЕ

8. Предмет,значај и циљ истраживања

Темељан и свеобухватан начин анализе компјутерског криминалитета захтева приступ који је најпре утемељен теоријским истраживањем, а затим и студијом о компјутерском криминалитету, као типу криминалитета с многобројним модалитетима испољавања. Предмет студијског приступа су кривична дела против: безбедности рачунарских података, интелектуалне својине, поједина дела из групе кривичних дела против полне слободе ,слобода и права човека и грађанина и привреде из Кривичног законика Републике Србије, као и „kaznena djela protiv računalnih sustava, programa i podataka“, „kaznena djela protiv intelektualnog vlasništva“ и остала дела која припадају компјутерском криминалитету из ранијег и тренутно важећег Казненог закона Републике Хрватске. Значај овог предмета истраживања огледа се у потпунијем сагледавању овог сложеног типа криминалитета, чиме је усмерена његова темељна анализа, како би се у будућности повећало превентивно деловање, и кроз различите активности надлежних органа, образовног система, разних семинара и едукативних програма уз укључивање друштва дошло до његовог ефикасног откривања и сузбијања.

Непосредни циљ спровођења студијског приступа у анализи компјутерског криминалитета је утврђивање феноменолошких и етиолошких карактеристика компјутерског криминалитета.

8.1 Просторни и временски оквир истраживања

У циљу спровођења студије за период од 01.01.2009. године закључно са 31.12.2015.године, обухватајући територију Републике Србије и Републике Хрватске, извршена је обрада и анализа статистичких података за наведена кривична дела Републичког завода за статистику и Државног завода за статистику Републике Србије и Републике Хрватске. Подаци наведених институција односе се на укупан број, пол, године живота, радни статус, изречене кривичне санкције, брачно стање, школску спрему и постојање саучесништва пунолетних учинилаца против којих је правноснажно окончан кривични поступак.

8.2 Хипотезе и методе истраживања

Спроведеним истраживањем су проверене следеће хипотезе:

1) Већину пунолетних лица осуђених за наведена кривична дела компјутерског криминалитета чине мушкарци, док се жене јављају у својству осуђених у малом броју случајева.

2) У највећем броју случајева приликом изрицања кривичних санкција , изрицана је условна осуда.

3) Већина осуђених пунолетних лица за наведена кривична дела компјутерског криминалитета имају између 30 и 39 година.

4) Постоји тренд раста броја осуђених пунолетних лица за наведена кривична дела компјутерског криминалитета.

5) У највећем броју случајева осуђена пунолетна лица за наведена кривична дела компјутерског криминалитета су запослена.

6) Мањина осуђених пунолетнх лица за наведена кривична дела компјутерског криминалитета има високо образовање .

7) Компјутерски криминалитет се најчешће врше од стране појединаца.

8) Мањина осуђених пунолетних лица за наведена кривична дела компјутерског криминалитета су неожењена.

Ово истраживање се заснива на статистичком методу, правно догматском методу, упоредно - правном методу и историјском методу. Статистички метод је примењен приликом прегледа статистичких извештаја РЗС-а и ДЗС-а за период од 2009. до 2015. године, правно- догматски приликом анализе позитивних прописа Републике Србије и Републике Хртватске у домену компјутерског криминалитета , као и упоредно - правни и историјски метод који је коришћен приликом анализе раније важећег Кривичног законика Републике Хрватске.

9. Студија случаја о компјутерском криминалитету у Републици Србији у периоду 2009-2015. године

9.1 Анализа резултата истраживања

Предмет анализе су следећа кривична дела из КЗ РС : [203]

- Оштећење рачунарских података и програма (члан 298 КЗ РС)
- Рачунарска саботажа (члан 299 КЗ РС)
- Прављење и уношење рачунарских вируса (члан 300 КЗ РС)
- Рачунарска превара (члан 301 КЗ РС)
- Неовлашћен приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (члан 302 КЗ РС)
- Спречавање и ограничавање приступа јавној рачунарској мрежи (члан 303 КЗ РС)
- Неовлашћено коришћење рачунара или рачунарске мреже (члан 304 КЗ РС)
- Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података (члан 304 а КЗ РС)
- Приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију (члан 185 КЗ РС),
- Искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу (члан 185 б КЗ РС)
- Повреда моралних права аутора и интерпретатора (члан 198 КЗ РС)
- Неовлашћено искоришћавање ауторског дела или предмета сродног права (члан 199 КЗ РС)
- Неовлашћено уклањање или мењање електронске информације о ауторском и сродним правима (члан 200 КЗ РС)
- Повреда проналазачког права (члан 201 КЗ РС)
- Неовлашћено коришћење туђег дизајна (члан 202 КЗ РС)
- Повреда тајности писама и других пошиљки (члан 142 КЗ РС)
- Неовлашћено прикупљање личних података (члан 146 КЗ РС)

[203] Кривични законик Републике Србије „Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 i 94/2016

- Фалсификовање и злоупотреба платних картица (члан 225 КЗ РС)
- Фалсификовање исправе (члан 355 КЗ РС и 356 КЗ РС)
- Фалсификовање службене исправе (члан 357 КЗ РС)

Табела 1. Број пунолетних лица осуђених за сва наведена кривична дела компјутерског криминалитета према полној структури у периоду од 2009. до 2015. године, а на основу података РЗС-а.

Година	Мушкарци	Жене
2009.	843	128
2010.	419	87
2011.	600	105
2012.	608	89
2013.	466	95
2014.	534	100
2015.	379	78

На основу података приказаних у Табели 1. може се закључити да је у периоду обухваћеним истраживањем, број осуђених пунолетних лица мушког пола и по неколико пута био већи у односу на број осуђених пунолетних лица женског пола.

Табела 2. Број изречених кривичних санкција за сва наведена кривична дела компјутерског криминалитета у периоду од 2009. до 2015. године , а на основу података РЗС-а.

Година	Затвор	Новчана казна	Условна осуда
2009.	136	80	742
2010.	64	20	417
2011.	107	47	544
2012.	142	43	504
2013.	159	31	367
2014.	198	19	414

2015.	160	19	266

На основу података приказаних у Табели 2. може се закључити да је у периоду обухваћеним истраживањем, број изречених условних осуда далеко већи у односу на број следеће највише изречене кривичне санкције тј. казне затвора.

Табела 3. Број осуђених пунолетних лица за кривична дела против безбедности рачунарских података и интелектуалне својине у периоду од 2009. до 2015. године по годинама старости , а на основу података РЗС-а.

Година	25-29	30-39	40-49	50-59
2009.	23	81	52	18
2010.	23	44	31	12
2011.	23	38	33	18
2012.	16	35	27	16
2013.	12	22	28	12
2014.	8	19	29	14
2015.	4	8	11	7

На основу података приказаних у Табели 3. може се закључити да је у периоду обухваћеним истраживањем, већина осуђених лица за наведена дела компјутерског криминалитета имала између 30 и 39 година на основу поређења са осталим бројнијим старосним групама.

Табела 4. Подаци о радном статусу осуђених пунолетних лица за кривична дела против безбедности рачунарских података и интелектуалне својине у периоду од 2009. до 2015. године, а на основу података РЗС-а.

Година	Запослен/а	Незапослен/а
2009.	85	90
2010.	42	73
2011.	43	72
2012.	29	32
2013.	18	54

2014.	11	47
2015.	11	17

На основу података приказаних у Табели 4. може се закључити да је у периоду обухваћеним истраживањем, највећи број осуђених пунолетних лица за наведена дела компјутерског криминалитета био незапослен .

Табела 5. Подаци о школској спреми осуђених пунолетних лица за кривична дела против безбедности рачунарских података и интелектуалне својине у периоду од 2009. до 2015. године, а на основу података РЗС-а.

Година	непотпуна основна (1–7 разр.)	основна школа	средња школа	виша школа	висока школа
2009.	8	33	142	3	8
2010.	6	16	100	6	2
2011.	7	24	97	4	5
2012.	7	22	73	3	4
2013.	6	18	53	-	4
2014.	6	16	46	3	5
2015.	3	4	20	3	1

На основу података приказаних у Табели 5. може се закључити да је у периоду обухваћеним истраживањем, по неколико пута био већи број осуђених пунолетних лица са завршеном средњом школом у односу на наредни бројчано највећи степен образовања.

Табела 6. Подаци о постојању саучесништва приликом извршења кривичних дела против безбедности рачунарских података и интелектуалне својине у периоду од 2009. до 2015. године, а на основу података РЗС-а.

Година	Укупан број извршених кривичних дела	Није саучесништво	Саучесништво
2009.	205	185	20
2010.	134	119	15
2011.	141	133	8
2012.	115	111	4
2013.	90	79	11
2014.	81	69	12
2015.	36	31	5

На основу података приказаних у Табели 6. може се закључити да је у периоду обухваћеним истраживањем, незнатно постојање саучесништва приликом извршења дела компјутерског криминалитета у односу на извршење истих од стране појединаца.

Табела 7. Подаци о брачном стању осуђених пунолетних лица кривична дела против безбедности рачунарских података и интелектуалне својине у периоду од 2009. до 2015. године, а на основу података РЗС-а.

Година	Неожењен/неудата	Ожењен/удата	Разведен/разведена
2009.	64	117	15
2010.	56	71	
2011.	55	59	11
2012.	37	54	10
2013.	25	41	11
2014.	23	38	14
2015.	8	16	8

На основу података приказаних у Табели 7. може се закључити да је у периоду обухваћеним истраживањем, већи био број ожењених пунолетних лица осуђених за наведена дела .

10. Студија случаја о компјутерском криминалитету у Републици Хрватској у периоду 2009-2015. године

10.1 Анализа резултата истраживања

Предмет анализе су следећа кривична дела из раније важећег КЗ РХ [204] :

- Повреда тајности, цјеловитости и доступности рачуналних података програма или сустава (члан 223 КЗ РХ)
- Рачунална пријевара (члан 224 КЗ РХ)
- Искориштавање дјеце или малољетних особа за порнографију (члан 196 КЗ РХ)
- Дјечја порнографија на рачуналном суставу или мрежи (члан 197 КЗ РХ)
- Повреда права аутора или умјетника извођача (члан 229 КЗ РХ)
- Недозвољена упораба ауторског дјела или изведбе умјетника извођача (члан 230 КЗ РХ)
- Повреда права из пријављеног или заштићеног изума (члан 232 КЗ РХ)
- Повреда тајности писама и других пошиљака (члан 130 КЗ РХ)
- Недозвољена употреба особних података (члан 133 КЗ РХ)
- Рачунално кривотворење (члан 223 КЗ РХ)
- Кривотворење исправе (члан 311 КЗ РХ)
- Кривотворење службене исправе (члан 312 КЗ РХ)
- Злоупораба чека и кредитне картице (члан 226 КЗ РХ)

Предмет анализе су следећа кривична дела из тренутно важећег КЗ РХ [205] :

- Ометање рада рачуналног сустава (члан 267 КЗ РХ)
- оштећење рачуналних података (члан 268 КЗ РХ)
- рачунална пријевара (члан 271 КЗ РХ)
- неовлаштени приступ (члан 266 КЗ РХ)
- злоупораба направа (члан 272 КЗ РХ)
- искориштавање дјеце за порнографију (члан 163 КЗ РХ)
- искориштавање дјеце за порнографске представе (члан 164 КЗ РХ)

[204] Казнени закон Републике Хрватске „Народне новине“, бр 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08, 57/11, 143/12)
[205] Казнени закон Републике Хрватске (пречишћен текст „Народне новине“, бр. 125/11, 144/12 и 56/15,61/15)

- повреда особних права аутора или умјетника извођача (члан 284 КЗ РХ)
- недозвољена упораба ауторског дјела или изведбе умјетника извођача (члан 285 КЗ РХ)
- Повреда других ауторском сродних права (члан 286 КЗ РХ)
- Повреда жига (члан 288 КЗ РХ)
- повреда тајности писама и других пошиљака (члан 142 КЗ РХ)
- недозвољена употреба особних података (члан 146 КЗ РХ)
- рачунално кривотворење (члан 270 КЗ РХ)
- Кривотворење исправе (члан 278 КЗ РХ)
- Кривотворење службене или пословне исправе (члан 279 КЗ РХ)
- Злоупораба чека и кредитне картице (члан 239 КЗ РХ)

Табела 1. Број пунолетних лица осуђених за сва наведена кривична дела компјутерског криминалитета према полној структури у периоду од 2009. до 2015. године, а на основу података ДЗС-а.

Година	Мушкарци	Жене
2009.	631	153
2010.	569	130
2011.	479	101
2012.	469	68
2013.	384	86
2014.	376	75
2015.	414	69

На основу података приказаних у Табели 1. може се закључити да је у периоду обухваћеним истраживањем, број осуђених пунолетних лица мушког пола и по неколико пута био већи у односу на број осуђених пунолетних лица женског пола.

Табела 2. Број изречених кривичних санкција за сва наведена кривична дела компјутерског криминалитета у периоду од 2009. до 2015. године , а на основу података ДЗС-а.

Година	Затвор	Новчана казна	Увјетна осуда
2009.	91	56	619
2010.	84	44	556
2011.	61	30	481
2012.	72	31	431
2013.	58	26	378
2014.	50	14	388
2015.	56	8	413

На основу података приказаних у Табели 2. може се закључити да је у периоду обухваћеним истраживањем, број изречених увјетних осуда далеко већи у односу на број следеће највише изречене кривичне санкције тј. казне затвора.

Табела 3. Број осуђених пунолетних лица за „kaznena djela protiv računalnih sustava, programa i podataka i intelektualnog vlasništva“ у периоду од 2013. до 2015. године по годинама старости , а на основу података ДЗС-а.

Година	21-24	25-29	30-39	40-49
2013.	20	35	45	49
2014.	24	8	22	22
2015.	13	12	27	6

На основу података приказаних у Табели 3. може се закључити да је у периоду обухваћеним истраживањем, већина осуђених лица за наведена дела компјутерског криминалитета имала између 30 и 39 година на основу поређења са осталим бројнијим старосним групама.

Табела 4. Подаци о школској спреми осуђених пунолетна лица за „kaznena djela protiv računalnih sustava, programa i podataka i intelektualnog vlasništva“ у периоду од 2013. до 2015. године, а на основу података ДЗС-а.

Година	Без школе и 1-7 разреда основне школе	Основна школа	Средња школа у трајању од 1-3 год.	Средња школа у трајању 4 год. и гимназија	Виша школа и 1. ступањ факултета	Факултети и уметничка академија
2013.	2	24	53	66	6	4
2014.	6	28	23	33	1	2
2015.	3	18	31	26	3	3

На основу података приказаних у Табели 4. може се закључити да је у периоду обухваћеним истраживањем, био већи број осуђених пунолетних лица са завршеном средњом школом у трајању од 4 године и гимназијом у односу на наредни бројчано највећи степен образовања.

Табела 5. Подаци о постојању саучесништва приликом извршења свих наведених дела компјутерског криминалитета у периоду од 2009. до 2015. године, а на основу података ДЗС-а.

Година	Укупан број извршених кривичних дела	Није саучесништво	Саучесништво
2009.	784	610	174
2010.	699	541	158
2011.	580	459	121
2012.	537	436	101
2013.	470	354	116
2014.	451	362	89
2015.	483	415	68

На основу података приказаних у Табели 6. може се закључити да је у периоду обухваћеним истраживањем, незнатно постојање саучесништва приликом извршења дела компјутерског криминалитета у односу на извршење истих од стране појединаца.

Табела 6. Подаци о брачном стању осуђених пунолетних лица за „kaznena djela protiv računalnih sustava, programa i podataka i intelektualnog vlasništva“ у периоду од 2013. до 2015. године, а на основу података ДЗС-а.

Година	Неожењен/неудата	Ожењен/удата	Разведен/разведена
2013.	79	60	15
2014.	47	34	10
2015.	40	28	14

На основу података приказаних у Табели 6. може се закључити да је у периоду обухваћеним истраживањем, већи био број неожењених пунолетних лица осуђених за наведена дела.

11. Анализа постављених хипотеза

1. Већину пунолетних лица осуђених за наведена кривична дела компјутерског криминалитета чине мушкарци, док се жене јављају у својству осуђених у малом броју случајева.

Ова хипотеза је потврђена како у Републици Србији тако и у Републици Хрватској с обзиром на чињеницу да је разлика у броју мушкараца осуђених за наведена дела био далеко изнад броја жена током свих година за које је истраживање спроведено. Док је у Републици Хрватској разлика најмање била изражена 2014. године, за Републику Србију је то случај 2015.

2. У највећем броју случајева приликом изрицања кривичних санкција , изрицана је условна осуда.

Ова хипотеза је потврђена како у Републици Србији тако и у Републици Хрватској с обзиром да је укупан број изречених условних осуда и по неколико пута већи од збира преосталих највише изречених кривичних санкција. Наведена разлика израженија је у Републици Хрватској где број изречене казне затворе ни у једној години обухваћеној истраживањем није достигао 100, насупрот Републици Србији где је 2014. године достигнут број од чак 198 изречених казни затвора.

3. Већина осуђених пунолетних лица за наведена кривична дела компјутерског криминалитета имају између 30 и 39 година.

Ова хипотеза је потврђена како у Републици Србији тако и у Републици Хрватској. Ова хипотеза је потврђена анализом кривичних дела против безбедности рачунарских података и интелектуалне својине у Републици Србији и анализом kaznenih djela protiv računalnih sustava, programa i podataka i intelektualnog vlasništva“. Преостала кривична дела која припадају компјутерском криминалитету нису могла бити предмет анализе због немогућности њиховог појединачног издвајања из одговарајуће групе кривичних дела којима припадају, међу којима су присутна и дела других типова криминалитета. У Републици Хрватској је ова хипотеза потврђена за период од 2013. до 2015. године због непостојања за ранији период групне класификације кривичних дела која припадају „kaznenim djelima protiv računalnih sustava, programa i podataka i intelektualnog vlasništva“. Док је у Републици Хрватској број осуђених лица старости од 30 до 39 година за наведена дела у 2015. години био знатно већи у односу на број осуђених лица старости од 40 до 49

година. У Републици Србији је у последње три године та разлика присутна у изузетно великом распону.

4. Постоји тренд раста броја осуђених пунолетних лица за наведена кривична дела компјутерског криминалитета.

Ова хипотеза није потврђена. У Републици Србији је једино 2014. у односу на 2013. годину и 2010. у односу на 2009. годину био присутан раст броја броја осуђених пунолетних лица за наведена кривична дела компјутерског криминалитета. У Републици Хрватској је присутан тренд постепеног пада броја осуђених пунолетних лица за наведена кривична дела компјутерског криминалитета из године у годину са изузетком 2015. Наведени подаци могу послужити као показатељ постојања изузетно велике „ тамне бројке" компјутерског криминалитета.

5. У највећем броју случајева осуђена пунолетна лица за наведена кривична дела компјутерског криминалитета су запослена.

Ова хипотеза није потврђена. У Републици Хрватској постављена хипотезе није могла бити проверена због непостојања података Државног завода за статистику о радном статусу осуђених лица. Приликом провере хипотезе у Републици Србији анализирана су кривичних дела против безбедности рачунарских података и интелектуалне својине. Преостала кривична дела која припадају компјутерском криминалитету нису могла бити предмет анализе због немогућности њиховог појединачног издвајања из одговарајуће групе кривичних дела којима припадају, међу којима су присутна и дела других типова криминалитета.У Републици Србији је једино 2009. године постајала незнатна разлика у броју запослених и незапослених лица осуђених за наведена кривична дела компјутерског криминалитета док је у преосталим годинама обухваћеним истраживањем та разлика све израженија, достижући и по неколико мањи пута мањи број запослених у одноу на незапослене.

6. Мањина осуђених пунолетних лица за наведена кривична дела компјутерског криминалитета има високо образовање .

Ова хипотеза је потврђена како у Републици Србији тако и у Републици Хрватској анализом кривичних дела против безбедности рачунарских података и интелектуалне својине у Републици Србији и анализом kaznenih djela protiv računalnih sustava, programa i podataka i intelektualnog vlasništva".У Републици Хрватској је ова хипотеза потврђена за

период од 2013. до 2015. године због непостојања за ранији период групне класификације кривичних дела која припадају „kaznenim djelima protiv računalnih sustava, programa i podataka i intelektualnog vlasništva“. У Републици Србији је присутна знатна разлика у броју осуђених пунолетних лица за наведена кривична дела са завршеном средњом школом у односу на преостале мање бројчане степене образовања. У Републици Хрватској је највећи број осуђених лица за наведена кривична дела са завршеном средњом школом у трајању од 4 године или гимназијом. Једино је 2015. године број осуђених лица са завршеном средњом школом у трајању до 3 године био највећи са 31 наспрам 26 осуђених лица са завршеном средњом школом у трајању од 4 године или гимназијом

7. Компјутерски криминалитет се најчешће врше од стране појединаца.

Ова хипотеза је потврђена како у Републици Србији тако и у Републици Хрватској анализом кривичних дела против безбедности рачунарских података и интелектуалне својине у Републици Србији и анализом свих наведених дела компјутерског криминалитета у Републици Хрватској. Број извршених дела компјутерској криминалитета од стране појединца је по неколико пута већи у обе републике у односу на број извршених дела у саучесништву.

8. Мањина осуђених пунолетних лица за наведена кривична дела компјутерског криминалитета су неожењена.

Ова хипотеза је потврђена у Републици Србији, али не и у Републици Хрватској. Приликом провере хипотезе анализирана су кривична дела против безбедности рачунарских података и интелектуалне својине у Републици Србији и „ kaznena djela protiv računalnih sustava, programa i podataka i intelektualnog vlasništva“. У Републици Хрватској је ова хипотеза проверавана за период од 2013. до 2015. године због непостојања за ранији период групне класификације кривичних дела која припадају „kaznenim djelima protiv računalnih sustava, programa i podataka i intelektualnog vlasništva“. У Републици Србији је ,за све године које су обухваћене истраживањем, присутан значајно већи број ожењених осуђених лица на неведена дела за разлику од Републике Хрватске у којој ниједне године број ожењених није био већи у односу на број неожењених лица.

III ПРЕВЕНЦИЈА, ЗАШТИТА И СУЗБИЈАЊЕ КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА

12.Облици формалне друштвене контроле

Супротстављање компјутерском криминалитету обухвата два механизма: превентивно и репресивно деловање, одвраћање од злоупотребе компјутера и стварање услова за брзо откривање и доказивање у случајевима када је злоупотреба извршена. Превентивне мере се односе на установљавање стратегија заштите информационих система и њихову имплементацију, као и унапређивање законске регулативе на глобалном и националном нивоу. На глобалном плану ОУН се активно укључује у превентивно деловање кроз рад својих Специјализованих тела и радних група, као што су на пример Међународна телекомуникациона унија (International Telecommunication Union – ITU), Канцеларија УН за контролу наркотика и превенцију криминала (United Nations Office on Drugs and Crime – UNDOC) и Канцеларија УН за послове разоружања (Office for Disarmament Affairs – UNODA).[206]Важно је напоменути глобалне тежње ка систематском супростављању компјутерском криминалитету од стране регионалних међувладиних организација, пре свега Организације за европску безбедност и сарадњу – ОЕБС (Organization for Security and Co-operation in Europe – OSCE), у оквиру које је оформљена Радна група за безбедност информација и приватност.

За изградњу превентивног система заштите од компјутерског криминалитета посебно су важне Препоруке Савета министара Европског савета [207], које се тичу: побољшања техничких могућности за аутентификацију корисника података; побољшања техничких могућности праћења комуникација преко интернета и посебно на друштвеним мрежама, како би се заштитила приватност корисника и спречило непотребно и неовлашћено прикупљање личних података о корисницима; побољшања мера заштите од злоупотребе анонимности на интернету, нпр. увођење сертификата који би у одређеним случајевима злоупотребе могли да открију име и локацију са које одређени корисник који се крије иза своје анонимности чини неко кривично или противправно дело; побољшање

[206] В. Вилић оп.цит. стр. 342
[207] Recommendations to the European Council Europe and the global information society, http://channelingreality.com/Digital_Treason/Brussels_1995/Bangemann_report.pdf, претражено 04.8.2017.године

технологија којима би се заштитиле новчане трансакције преко интернета као и ауторска права.

Препоруке су такође усмерене на индустрију која се бави информационим и комуникационим технологијама, којој се саветује да: повећа степен сигурности корисника на свим интернет локацијама и друштвеним мрежама, као и саму сигурност рачунарских система; саветује кориснике и интернет провајдере како да безбедно користе рачунарске системе и информационе технологије и процедуре; побољша сарадњу са владиним агенцијама и званичним телима која се баве информационим технологијама и питању безбедности података на њима; утврде правила понашања на тај начин што би се прописало који садржај се сматра противправним и који је као такав санкционисан; створи међународну мрежу контаката на којој би стално на располагању као упозорење била база противправних садржаја и њихових аутора, како би корисници знали да са њима не ступају у контакте а интернет провајдери да им, у складу са законом, онемогуће приступ интернету и друштвеним мрежама; у сарадњи са специјалним одељењима у полицији и са тужилаштвима створи протоколе и процедуре, ради проналажења извршилаца и откривања кривичних дела компјутерског криминалитета. Један од начина на који Препоруке предвиђају превенцију и заштиту од компјутерског криминалитета јесте кроз јачање међународноправних механизама сузбијања кривичних дела компјутерског криминалитета, стварање листе минималних правила и процедура које свака земља мора да примењује (нпр. за дела попут упада у рачунаре и рачунарске системе, компјутерску шпијунажу, компјутерску превару, повреде ауторских права и сл.) и процесуирање и санкционисање објављивања противправних и незаконитих садржаја на интернету, нпр. дечија порнографија, дискриминаторско понашање, глорификција насиља и аката насиља, говор мржње и сл. Поред законских и институционалних мера које треба да створе успешан механизам заштите од компјутерског криминалитета, у Србији је донета Стратегија развоја информационог друштва у Републици Србији до 2020. године [208] која као једну од области приоритета одређује информациону безбедност, а посебно унапређење правног и институционалног оквира за информациону безбедност, заштиту критичне инфраструктуре, борбу против високотехнолошког криминала и научно-

[208] Стратегија развоја информационог друштва у Републици Србији до 2020. године(„Службени гласник РС“ бр. 51/2010)

истраживачки и развојни рад у области информационе безбедности. Поред тога што Стратегија предвиђа да ће до 2020. године бити уређени сви аспекти информационе безбедности и формирани одговарајући институционални оквири, један од циљева је да се развојем информационе безбедности створи поверење корисника у безбедно функционисање информационих система, поверење грађана у заштићеност података о личности у информационим системима, ширење свести о неопходности спровођења мера информационе безбедности, заштита података, информационих и телекомуникационих система, безбедност електронских трансакција и да се створе ефикасни механизми заштите и остваривање права у процесима електронског пословања и електронске размене података. Стратегија такође предвиђа доношење одговарајућих прописа из области информационе безбедности, којима ће се додатно уредити стандарди информационе безбедности, подручја информационе безбедности, као и надлежности и задаци појединих институција у овој области, као и формирање институције која ће у области информационе безбедности обављати послове верификације и сертификације метода, софтверских апликација, уређаја и система, истраживања и развоја и надзирати примену стандарда информационе безбедности у државним органима Упркос правног регулативи, успешна реализација заштите и сузбијања претпоставља, најпре, подизање колективне свести грађана о свим опасностима и последицама до којих може довести компјутерски криминалитет. Најзначајнију улогу у остварењу овог амбициозног циља имају образовне институције кроз константне едукације и семинаре као и сами медији путем објективног и непристрасног извештавања .

Први корак у заштити информационих система је постављање физичке и софтверске заштите. Физичким мерама се мора осигурати заштита од случајних оштећења опреме (непосредним путем или путем телефонске линије) и неовлашћене уградње делова опреме или програма. Софтверска заштита подразумева предузимање мера заштите оперативног система, спречавање неовлашћеног улажења у поједине корисничке програме (лозинке, кључне речи), регистровање свих активности у компјутеру и шифрирање података који се преносе од једног до другог корисника у систему [209], ризицима доступности података, преиспитивати рад институција које се њима користе на који

[209] Компутерски криминал/ИПФ-радна база, http://promocije.net/proba/krivicno-pravo/materijalno-krivicno-pravo/kompjuterski-kriminal/, претражено 19.07.2017. године

начин се подаци обрађују и складиште као и између којих институција постоји узајамна размена личних података.

Свакодневни развој интернета захтева велику пажњу и умешност у откривању компјутерског криминалитета. Повреде приватности на друштвеним мрежама је веома тешко доказати а извршиоце је готово немогуће открити. Неки од проблема доказивања повреде приватности корисника друштвених мрежа су: [210]

- трагови који остају су специфични, а огледају се у променама електронских записа који су настали у софтверском делу рачунара,

- анонимност извршиоца кривичног дела и тешко проналажење трагова које иза себе оставља,

- проналажење трагова најчешће и само представља неовлашћено продирање у туђе компјутерске системе и базе података,

- IP адреса није увек поуздано средство за праћење извршиоца дела, зато што и њоме може да се манипулише,

- откривање, тумачење и доказно коришћење промена насталих у софтверу захтева изузетну стручност и ангажовање компјутерских експерата високог нивоа,

- различито место и време деловања извршиоца кривичних дела.

Савети за безбедно коришћење друштвених мрежа могу у великој мери спречити појаву неовлашћеног упада у туђи профил и наношење штете при чему се они разликују код конкретних друштвених мрежа. Неки од њих су: постојање свести о подацима који се чине доступним, пажљив одабир пријатеља на мрежи, одређена доза сумње да је порука заиста од онога чије име пише на њој као и ургентно обавештавање администратора друштвених мрежа у случају немогућности уласка у сопствени профил.

За ефикасно сузбијање компјутерског криминалитета неопходно је створити одговарајуће законске механизме и правну регулативу за откривање и санкционисање ових друштвено неприхватљивих криминалних понашања. Такође, веома је важна благовремена пријава сваког облика злоупотребе и онлајн напада на приватност лица како би надлежни органи благпвремено деловали и како би се утицало на смањење велике „ тамне бројке “ компјутерског криминалитета. Нажалост, иако је од изузетног значаја благовремена

[210] В. Вилић оп.цит., стр. 348

пријава жртве и делотворна сарадња са надлежним органима у току поступка, када су у питању дела компјутерског криминалитета која се врше у великом корпорацијама широко је распрострањена пракса интерног решавања. Неки од разлога су :[211]

- Већина жели да одржава низак ниво информисаности о томе шта се код њих дешава, због могућих потенцијалних проблема који могу настати пријављивањем криминалног дела, као што су:
  - Негативан публицитет у јавности ;
  - Губитак угледа и поверења код пословних партнера у њихову стабилност, финансијску репутацију и кредитни рејтинг;
  - Страх да осигуравајуће компаније могу због тога повећати премије за осигурање или, чак, да одбију да обнове полисе осигурања;
- Могућност да се губици од компјутерског криминала пренесу са жртве на купца умањује интерес за његово пријављивање;
- Страх руководства од покретања питања и њихове одговорности због пропуста у предузимању одговарајућих мера заштите, што би могло омести њихов професионални опстанак и напредовање унутар организације;
- Компјутерски криминалац, чак и ако је осуђен, често добија условну осуду, па ниска казна дестимулише жртву да дело пријављује. Један менаџер је ово сумирао на следећи начин: „ Након што потрошите хиљаде долара и радних сати на случај, ви га видите како хода као слободан човек. То фрустрира“;

Због наведених разлога корпорације најчешће прибегавају дискретном премештају извршиоца дела на друго радно место или давању отказа.

[211] Information systems security survey, WarRoom Research, LLC, 23 November 1996., http://www.infowar.com/sample/survey.html-ssi; A. Beaquai, *How to prevent computer crime,1983,* John Wiley & Sons, Inc. str. 45-47; A. P. Collier, J. B. Spaul, Problems in policing computer crime, Woolwich Centre for Computer Crime Reseach, University of Exeter, 1990, http://www.ex.ac.uk/~BJSpaul/ais/computercrime.html; M. Tenhuen, Combating computer crime, Interpol Review, No 417,1989,(Confidential Supplement), no. 11, стр. 3; L. J. Cobbs, Canadian computer crime legislation: a review, Datapro on CD, Originating Report IS80-050-301, December 1992.

13. Облици неформалне друштвене контроле

У погледу превенције појаве компјутерског криминалитета од стране појединачног корисника компјутера, осталих компјутерских уређаја и интернета могуће је издвојити неколико начина:

– Увек укључен заштитни програм на компјутеру тзв. „firewall“ штити компјутер од покушаја извршилаца дела компјутерског криминалитета да приступе компјутерском систему, оштете или чак избришу важне податке као и да искористе лозинке које омогућавају приступ осетљивијим базама података унутар самог система.

– Инсталиран и редовно ажуриран антивирусни програм спречава продирање компјутерског вируса у компјутерски систем корисника. У већини случајева корисник се обавештава о присуству компјутерског вируса пре аутоматског брисања истог.

– Неки од садржаја на интернету осмишљени су и направљени тако да могу да заобиђу и најсавременију антивирусну заштиту. Електронска пошта која је приспела од непознатих особа не би се требало отварати. Нарочито је важно обратити пажњу на поруке у чијим прилозима се налази одговарајући садржај с обзиром на могућност да пошиљалац ни сам није свестан додатног садржаја који је накнадно убачен у прилог поруке са циљем извршења могуће злоупотребе.

– Опрезност приликом коришћења бесплатног бежичног интернета на јавним местима , посебно приликом коришћења услуга електронског банкарства и провере електронске поште. Постојање одговарајућег нивоа заштите на серверу преко кога се врши приступ интернету у великој мери може онемогућити извршење дела компјутерског криминалитета од стране лица која не морају ни бити повезана на исту бежичну интернет мрежу, већ је довољно да се налазе у близини потенцијалне жртве.

– Пажљив одабир лозинки (енгл.password) које служе да ограниче приступ компјутегским ресурсима. Потребно је избегавати коришћење информација из приватног или пословног живота као могуће лозинке .Многи безбедносни системи онемогућавају корисницима да користе једноставне речи од неколико слова или чак и имена за своје лозинке. Софтвери који контролишу приступ заштићеним подацима корисницима могу дозволити искључиво преглед али не и промену њиховог садржаја. Веома је важна периодична промена лозинки нарочито уколико се односи на присуп

пословним подацима с обзиром на чињеницу да су управо те лозинке чешће изложене злоупотребама.

– Сладиштење важних података на одговарајућим медијумима у случају неовлашћеног брисања истих са централног компјутерског система. Постојање неколико примерака копија важних података на више различитих медијума додатно обезбеђује њихово очување .Као најпоузданији медијуми издвајају се :

- оптички дискови који могу очувати ускладиштене податке, према проценама стручњака, и по неколико деценија попут Блу-реј дискова (BD-R HTL)
- USB екстерни хард дискови најновије генерације (3.0)

ЗАКЉУЧНА РАЗМАТРАЊА

Успешно откривање и сузбијање компјутерског криминалитета и успостављање безбедности свих корисника информационих технологија подразумевају ревидирање постојећих и доношење нових прописа којима се регулишу област телекомуникација, заштита људских права и интелектуалне својине.

Може се закључити да примена неодговарајуће методологије у изради закона несумњиво представља један од основних разлога због којих је досадашња правна регулатива у овој области била неодговарајућа. Разлоге за такво стање свакако треба потражити и у чињеници да је реч о криминалитету који својом виталношћу и мноштвом појавних облика ставља законодавца у неравноправан положај с обзиром на отежану могућност константног праћења његовог развитка и преображаја.

Динамика развоја компјутерског криминалитета изискује континуирану непрекидну обуку свих учесника у борби против овог вида криминалитета, при чему је одговарајућа техничка опремљеност само предуслов за примену тако стечених знања и вештина. С обзиром на чињеницу да одговарајућа техничка опремљеност може представљати знатне финансијским издатке ,које многе државе из нису у стању да издвоје, неопходно ја помоћ и сарадња економски развијенијих земаља које би у превенцији и сузвијању компјутерског криминалитета морале да препознају како националне тако и међународне интересе.

Улога појединачног грађанина без обзира на својство жртве или извршиоца дела компјутерског криминалитета такође се не сме занемарити. Поред штете нематеријалне природе која проузрокује душевну бол, страх, панику или повреду части и достојанства, материјална штета може у појединим случајевима достићи износе који се на индиректан начин могу одразити и на економију једне земље . Оно што сваки грађанин може учинити на заштити својих података као завршном циљу напада појавних облика компјутерског криминалитета јесте стално развијање способноси препознавања, превремене заштите и пријављивања сваког назнака извршења дела надлежним органима.

ЛИТЕРАТУРА

Попис коришћене литературе, извори на српском језику:

А

Алексић Живојин, Шкулић Милан., *Криминалистика,* Београд, 2007, Правни факултет универзитета у Београду;

Б

Бановић Божидар ,*Обезбеђење доказа у криминалистичкој обради кривичних дела привредног криминалитета*, Београд, 2002, Виша школа унутрашњих послова;

Бошковић Мило, *Криминилогија и социјална патологија*, Нови Сад, 1995, Матица Српска;

Будимлић Мухамед, Пухарић Предраг, *Компјутерски криминалитет – криминолошки, кривичноправни и сигурносни аспект*, Сарајево, 2009, Факултет за криминалистику, криминологију и сигурносне студије;

В

Вилић Вида , *Повреда права на приватност злоупотребом друштвених мрежа као облик компјутерског криминалитета (докторска дисертација)* ,Ниш, 2016 , Правни факултет Универзитета у Нишу;

Видојковић Милош , *Компјутерски криминалитет* (мастер рад),Ниш,2015, Правни факултет Универзитета у Нишу;

Д

Дропулић Јулијано, *Право на приватни живот и друштвени интегритет* , Загреб, 2002, Визура;

Дракулић Мирјана, *Основи Компјутерског права*, , Београд ,1996, Друштво операционих истраживача Југославије;

Драгичевић Дражен, *Компјутерски криминалитет и информацијски сустави*, Загреб,1999, Инфориматор стр. 146-148;

Ј

Јовашевић Драган, Хашимбеговић Тарик, *Кривичноправна заштита безбедности рачунарских података*, Тара, 2004, Правни информатор стр. 3 ;

Јовашевић Драган, *Кривично право-посебан део*, Ниш, 2014, Номос ;

Јерковић Ранко , *Борба против високотехнолошког криминалитета у*

Србији, Телекомуникације- научно-стручни часопис Републичке Агенције за телекомуникације, бр. 3/2009, стр.1, http://www.telekomunikacije.rs/arhiva _brojeva/treci_broj/ranko_jerkovic:_borba_protiv_visokotehnoloskog_kriminaliteta_u_srbiji_.161.html претражено 07.08.2017 године;

К

Ковачевић-Лепојевић Марина , *Појам и карактеристике интернет зависности*, Специјална едукација и рехабилитација, Vol. 10, br. 4, Београд, стр.621,http://www.casopis.fasper.bg.ac.rs/izdanja/SEIR2011/vol10br4/1Spec_Edu_i_Reh_ISTRAZIVANJA/4-Marina_Kovacevic_Lepojevic.pdf, претражено 03.09. 2017. године;

Комплен-Николић Лидија, Гвозденовић Радоје, Радуловић Саша, Милосављевић Александар, Јерковић Ранко, Живковић Владан, Живановић Саша, Рељановић Марио, Алексић Иван ,*Кратак приказ развоја правне регулативе о високотехнолошком криминалитету на међународном нивоу*, Београд, 2010, Удружење јавних тужилаца и заменика јавних тужилаца Србије;

Кнежевић Саша, Кривично процесно право: општи део, Ниш, 2015, Правни факултет Универзитета у Нишу;

Константиновић-Вилић Слободанка , Николић-Ристановић Весна , Костић Миомира, *Криминологија*, Ниш,2012 Правни факултет Универзитета у Нишу;

Кешетовић Желимир, *Интернет као оруђе терориста*, Ревија за безбедност-стручни часопис о корупцији и организованом криминалу, Центар за безбедносне студије, Година II, бр. 4/2008 ,Београд;

Комплен-Николић Лидија, Гвозденовић Радоје, Радуловић Саша, Милосављевић Александар, Јерковић Ранко, Живковић Владан, Живановић Саша, Рељановић Марио, Алексић Иван , *Сузбијање високотехнолошког криминала*, Београд, 2010,Удружење јавних тужилаца и заменика јавних тужилаца Србије;

Кораћ Срђан, *Сузбијање дечије порнографије на Интернету: ЕУ стандарди*, Ревија за безбедност, бр. 11, 2008, стр. 47-51;

Л

Лилић Стеван , *Правни аспекти заштите података у аутоматизованим службеним евиденцијама*, Наша законитост 5/1989, стр. 614;

Лилић Стеван , *Право, информатичка технологија и заштита података*, Анали Правног факултета у Београду, бр. 2, стр. 211;

М

Матијашевић Јелена , *Кривичноправна регулатива рачунарског криминалитета*, Нови Сад, 2013 Правни факултет за привреду и правосуђе;

Миладиновић Живанка, *Кривично дело преваре као модел остваривања сајбер криминала (докторска дисертација)*, Београд, 2016 ,Факултет за право, јавну управу и безбедност ;

Милићевић Слободанка , Вујовић Срђан, *Проблем савремене доби: облици крађе и злоупотребе идентитета и мјере превенције, Сузбијање криминала и европске интеграције, с освртом на високотехнолошки криминал*,Лакташи,2012, Зборник радова, међународна научностручнаконференција,, стр. 310 http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2017.године;

П

Петровић Борислав , Јовашевић Драган, *Кривично/Казнено право Босне и Херцеговине – Општи дио,* Сарајево, 2005, Правни факултет универзитета у Сарајеву

Писарић Милана, *Претресање рачунара ради проналажења електронских доказа*, Зборник радова Правног факултета у Новом Саду, 1/2015, стр. 233

Петровић Слободан, *Компјутерски криминал*, Београд, 2000, Министарство унутрашњих послова Србије

Прља Драган, Рељановић Марио, Ивановић Звонимир , *Интернет право*, Београд, 2012, Институт за упоредно право Београ д стр. 50

Р

Радуловић Саша, *Специфичност прибављања електронских доказа о извршењу кривичних дела високотехнолошког криминала*, Београд, 2008, Центар за безбедносне студије, стр. 17-18

Ромић Миодраг , Грбић-Павловић Николина ,*Међународноправни документи којима се уређује област високотехнолошког криминала ,Сузбијање криминала и европске интеграције, с освртом на високотехнолошки криминал*, Лакташи,2012, Зборник радова, међународна научностручнаконференција,, стр. 196 http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2017.године;

С

Спасић Видоје, *Актуелна питања у области сајбер криминала*,Београд, 2006, Билтен судске праксе Врховног суда Републике Србије

Китаровић Никола , Компјутерски криминалитет, Београд, 1998, Билтен судске праксе Врховног суда Србије бр.2

Ф

Фејеш Иштван, *Компјутерски криминалитет- криминалитет будућности, изазов садашњости*, излагање на конференцији COBISS.SR-ID 159876620 ,2000. година

Ш

Шкулић Милан , *Компјутерски криминалитет- како одговорити на изазов*, написан за саветовање о рачунарским наукама и информационим технологијама YU ИНФО 98 - програмска област - Правни аспекти информатике, Копаоник.

Попис коришћене литературе, извори на страном језику:

A

Anderson E. Kent, International intrusions: motives and patterns, The proceedings of the 1994 Bellcore/Bell South Security Simposium, May 1994,

B

Bellour C., *Međunarodna prevara,* Zagreb, 1998, Izbor ,br. 1,76-77;

Beaquai A., *How to prevent computer crime,1983,* John Wiley & Sons, Inc,45-47;

Boer M., *Cooperation contre le piratage enregistrements sonores,* Lyon, 1996

Brvar Bogo , *Pojavne oblike zlorabe računalnika*, Ljubljana, ,1982, Revija za kriminalistiko in kriminologijo

C

Carter D. L.,Computer crime categories: How techno-criminals operate, FBI law Enforcement Bulletin, http://nsi.org/Library/Compsec/crimecom.html

Cobbs L. J., Canadian computer crime legislation: a review, Datapro on CD, Originating Report IS80-050-301, December 1992.

Collier A. P., Spaul J. B, Problems in policing computer crime, Woolwich Centre for Computer Crime Reseach, University of Exeter, 1990,
http://www.ex.ac.uk/~BJSpaul/ais/computercrime.html

D

Danquah P. , Longe O.B.,An Empirical Test of The Space Transition Theory of Cyber Criminality: Investigating Cybercrime Causation Factors in Ghana, African Journal of Computing & ICT September 2011, Vol. 2. No. 2 Issue 1, стр.. 37-48,
http://www.ajocict.net/uploads/V4N1P62011_AJOCICT__An_Empirical_Test_Of_The_Space_Transition_Theory_of_Cyber_Criminality__The_Case_of_Ghana_and_Beyond.pdf, претражено 28. 08. 2017. Године

Dyrud Marilyn, I *brought You a good news An analysis of Nigerian 419 Letters*, Proceedings of 2005 Annual Association for Business Communication, Convention Association for Business Communication, USA,2005, p. 11.

F

Freiburger Tina , Crane J. Jeffrey, The Internet as a Terrorist's Tool, A Social Learninig Perspective, Cyber Criminology, Exploring Internet Crimes and Criminal Behavior, p. 128

G

Garner Rochelle, The growing professional menace, 1995, Open computing

Gottfredson Michael, Hirsch Travis, *A general theory of crime*, Stanford, CA: Stanford University Press,

H

Honeycutt J., Pike A. M, Using the internet, Special Edition, Indianopolis, SAD,1996 Que Corporation,

Higgins George,Value and Choice, Examining Their Roles in Digital Piracy, Cyber Criminology, Exploring Internet Crimes and Criminal Behavior, p. 141

Jaishankar K., Editorial: Establishing a Theory of Cyber Crimes, International Journal of Cyber Criminology, Vol 1 Issue 2 July 2007, p.7,
http://www.cybercrimejournal.com/Editoriaijccjuly.pdf, претражено 28. 08. 2017. године

K

Krauss Leonard.,MacGahan Aileeen., *Computer fraud and countermeasures*, New Jersey,1979,Englewood Cliffs

Kyung-Shick Choi,Cyber-Routline Activities, Empirical Examination of Online Lifestile, Digital Guardians and computer Crime Victimisation,Cyber Criminology, Exploring Internet Crimes and Criminal Behavior,p. 243

M

Major G.D.,Espionage into the 21st century: A holistic approach to securiry, Datapro on CD, Originating report IS09-170-101,1994.

Menkus Belden, *Protecting corporate data*, Honeywell Source summer, 1994,p 48

Muncie John, McLaughlin Eugene, *The problem of Crime*, London, 2001, SAGE publications

P

Parker B. Donn , *Computer Abuse*, 1973, Springfild

Parker B. Donn, *Fighting computer crime*, New York, 1983, p.120 Wiley computer publishing

Palmar C,. Potter G. A , *Computer security risk management*,London 1989, Van Nostrand Reinhold Co

R

Revjako I. , *Computer terrorists: The latest technologies as a tool of committing crimes*, Minsk1997 Encyclopedia of crimes and accidents, Minsk, p.34
Galley Patrick, *Computer terrorism: what are the risks? Science, Tehnology and Society*, Swiss Federal Institute of Tehnology,1996, www.home.ch/spaw1165-infosec-sts en/ преузето 08.05.2017.

S

Schjolberg Stein,*Computers and Penal Legislation – A Study of the Legal Politics of a new Technology*,Oslo 1986, CompLex 3/86, Universitetforlaget

Siegfrid -Spellar Kathyryn, Lovely Richard, Rogers Marcus, *Self-Reported Internet Child Pornography Consumers. A Personality Assessment Using Bandura's Theory of Reciprocal Determinism*, Cyber Criminology, Exploring Internet Crimes and Criminal Behavior, 2011, CRC Press, p.72

Sieber Ulrich, *Computer Crime and Criminal Justice*, Köln,1977, C. Heymanns Verlag

Sieber Ulrich, *The international Emergence of Criminal Infromation Law*, Köln, 1992, C. Heymanns Verlag p. 5

Sterling Bruce, Short history of the internet, The magazine of fantasy and science fiction, february, 1993., http://www.fortunecity.com/skyscraper/smiley/0/ history.htm

T

Taylor Paul , *Hackers: Crime in the Digital Sublime*, 1999,Routledge,

Tan K., *Phishing and Spamming via IM (SPIM).*, Internet Storm Center, (2006); преузето 08.05.2017.

Tenhuen M. , *Combating computer crime*,1989, Interpol review, No. 417, (Confidental Supplement), no. 11 p. 2

Toren P. J. ,*Intellectual Property and Computer Crimes* (Intellectual Property usiness Crimes Series), New York USA, 2003, p.6-41

V

Venzke H. Ben, Economic/industrial espionage, Boston,1996, Intelligence Watch Report http://stealth-iss.com/documents/pdf/Economic.pdf претражено 21.07.2017 године

Violino B., high-tech thieves, Information Week, may 29, 1995., no. 529 p. 14(3)
Identity Theft: Is there Another You?: Joint hearing before the House Subcommc. On Telecommunications, Trade and Consumer Protection, and on Finance and Hazardous Materials, of the Comm. On Commerce, 106th Cong. 16(1999)(testimony of Rep. John B. Shadegg) http://www.usdoj-crm/mis/jam претражено 08.08. 2017. године

W

Walden Ian, *Information Technology & The Law*, Basingstoke, 1990, Macmillan Publishers p.12

Wiley John, *The International Handbook of Computer Crime*, Chichester,1991, John Wiley and Sons Publishers ,3–27;

Попис коришћене истраживачке грађе:

Стратегија развоја информационог друштва у Републици Србији до 2020. године(„Службени гласник РС“ бр. 51/2010)

Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in electronic communications services or of public communications networks and amending Directive 2002/58/EC,

Закон о потврђивању Европске конвенције о сузбијању тероризма(“Службени лист СРЈ– Међународни уговори“ бр 10/2001 од 09. 11. 2001. године

Законик о кривичном поступку („Сл. гласник РС“, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014)

Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала(„Службени гласник РС” бр.61/2005 и104/2009)

Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима(„СлужбенигласникРС” бр.32/2013)

Закон о ауторским и сроднимправима („СлужбенигласникРС“ бр. 104/2009, 99/2011 и119/2012 и 29/2016- одлука УС).

Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине(„Службени гласника РС“ бр. 46/2006, 104/2009 – др. закони)

Кривични законик Републике Србије „Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 i 94/2016

Казнени закон Републике Хрватске „Народне новине“, бр 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08, 57/11, 143/12)

Казнени закон Републике Хрватске (пречишћен текст „Народне новине“, бр. 125/11, 144/12 и 56/15,61/15)

Коришћене електронске адресе:

Recommendation No. R (89) 9, adopted by the Committee of Ministers of the Council of Europe on September 13, 1989 and Report by the European Committee on Crime Problems: Computer-relatedcrime,https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&Secmode=1&DocId=702280&Usage=2 п ретражено 08.08.2017

Recommendation No. R (95) 13, approved bz the European Committee on Crime Problems (CDPC) at its 44th plenary session May 29- june 2, 1995: Concerning problems of criminal procedural law connected with information technology ,http://www.justice.gov/criminal/cybercrime/crycoe.htm претражено 08.08.2017

Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders,2000, Background paper for the workshop on crimes related to the computer network: Crime-fighting on the Net, http://www.un.org/events/10thcongress/2088h.html преузето 15.05.2017.

www.caida.org/publications/papers/2003/sapphire/sapphire.html претражено 07.05.2017.

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html
A Paper for the 12th Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime, Strasbourg, 15-18 November 1976, стр. 225 - 229, https://openlibrary.org/works/OL11001385W/Criminological_aspects_of_economic_crime, претражено 08. 06. 2017. године

Препорука Савета Европе о криминалитету везаном за рачунаре бр. 89 (9), (Council of Europe Computer-related crime Recommendation No. R (89) 9, 1989) http://www.oas.org/juridico/english/89- 9&final%20Report.pdf, претражено 07. 08. 2017. Године

Recommendation No. R (95) 13 of the Committee of Ministers to Member States concering problems of Criminal Procedural Law connected with Information Technology, www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(1995)013_EN.asp, претражено 07.08. 2017. године

Council of Europe, European Committee on Crime Problems (CDPC), http://www.coe.int/t/DGHL/STANDARDSETTING/GDPC/defaul_en.asp. претражено 07.07. 2017.

Council of Europe, Convention on Cybercrime, European Treaty Series (ETS)- No. 185, Budapest, 23, XI 2001., http://conventions.coe.int/Treaty/en/Treaties/Word/185. doc претражено 07.09.2017. године

Закон о потврђивању Додатног протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система(„Службени гласник РС”, бр. 19/2009) и Додатни протокол уз Конвенцију Савета Европе о високотехнолошком криминалитету бр .185 који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених путем компјутерских система (Additional Protocol on the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems), 2005, http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm, претражено 09. 07. 2017. године

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, the 28 January 1981(Entry into force: 01.10.1985); http://conventions.coe.int/treaty/en/treaties/html/108.htm претражено 07.09. 2017. године

Council of Europe, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No. : 201, Lanzarote, the 23 October 2007. (Entry into force 01.07. 2010); http://conventions.coe.int/Treaty/EN/Treaties/Word/201.doc претражено 07.10.2017 . године

Препорука Савета Министара Савета Европе CM/Rec(2012)4 државама чланицама која се односи на заштиту људских права на друштвеним мрежама(Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services), 2012, https://wcd.coe.int/ViewDoc.jsp?id=1929453, претражено 07. 07. 2017. године

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market(Directive on electronic commerce), Official Journal of the European Comuunities, L 178,17.07.2000 PP. 1-16; http://europa.eu.nint претражено 20.07.2017 године

Овирна одлука о нападима на информационе системе Комисије европских заједница(Framework Decision on attacks against information systems of the Commission of the European Communities), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222&from=EN, претражено12. 08. 2017. Године

Стратегија за безбедно информационо друштво у Европи–Strategy for a Secure Information Society in Europe “Dialogue, partnership, and empowerment”, http://ec.europa.eu/information_society/doc/com2006251.pdf , претражено 21.07.2017.године

Акциони план за заштиту критичне информационе инфраструктуре,, Заштита Европе од бројних кибернетичких напада и ометања: побољшати спремност, безбедност и отпорност“ – Communication on Critical Information Infrastructure Protection “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, secuirty and resilience”, 2009, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF, претражено 07. 11. 2017. Године

Директива Савета Европске заједнице о правној заштити компјутерских програма (Council Directive of 14.may 1991. On the legal proctection of computer Programs) са обавезном

применом у државама чланицама ЕУ почев од1.1.1993. године, објављена је у„Службеном листу Европске заједнице бр. Л122/42“ од 1 7.5.1991. године

Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in electronic communications services or of public communications networks and amending Directive 2002/58/EC, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32006L0024, претражено 17. 08. 2017. године

Directive 2013/40/EU of the European Parliament and of the Council 12. 08. 2013, Offical Journal of the European Union 218/8, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040, претражено19. 08. 2017. године

Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in electronic communications services or of public communications networks and amending Directive 2002/58/EC,
Практични водич кроз савремено кривичноправо и примери из праксе , OSCE, Подгорица, март 2014, www.osce.org/me/montenegro/117630?download=true, претражено 15. 08. 2017. године
РезолуцијаУједињених Нацијао законодавству у области компјутерског криминалитета(UN resolution on computer crime legislation), http://www.unodc.org/documents/congress//Previous_Congresses/8th_Congress_1990/028_ACONF.144.28.Rev.1_Report_Eighth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders.pdf, претражено дана 11. 08. 2017. године

Приручник УН о спречавању и контроли компјутерског криминала (United Nations Manual on the Prevention and Control of Computer-related Crime), 1994,
РезолуцијаУједињених Нација(тзв. Женевска резолуција) о злоупотреби интернета у сврху сексуалне експлоатације(UN Resolution on Missuse of the Internet for the Purpose of Sexual Exploatation), http://www.uri.edu/artsci/wms/hughes/ppr.htm, прераженo 05. 07. 2017. године

Ревидирана Резолуција Уједињених Нација A/res/55/63 о борби против злоупотребе информационих технологија(UN resolution A/res/55/63 on combating the criminal misuse of information technologies), 2001, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf, претражено11. 08. 2017. године

РезолуцијаУједињених НацијаA/res/56/121 о борби против злоупотребе информационих технологија(UN resolution A/res/56/121 on combating the criminal misuse of informationtechnologies), 2002, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf, претражено20. 08. 2017.године

Резолуција 2007/20 од 26. 07. 2007. године, www.un.org/.../ecosoc/.../2007 /Resolution%2020, претражено 25. 04. 2017. године

Comprehensive Study on Cybercrime – Draft, United Nations office on drugs and crime, Vienna, February 2013, United Nations, New York 2013, стр. Ix,
http://www.unodc.org/documents/organized-

crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, претражено 12. 08. 2017. године
Глобална платформа о сајбер сигурности Међународне телекомуникационе уније (Global Cybersecurity Agenda (GCA) of the International Telecommunication Union), www.itu.int/osg/csd/cybersecurity/gca, претражено 11. 08. 2017. године
Јутарњи лист , www.jutarnji.hr, претражено 22. 08. 2017. године
Ultrascan Advanced Global Investigations, http://www.ultrascan-agi.com/ претражено 07.07. 2017. Године
http://www.nigerianspam.com/people-affected-419-scam.htm, претражено 07.07.2017.године

www.informationweek.com/medco-sys-admin-pleads-guilty-to-computer-sabotage/d/d-id/1059395? 07.08.2017. године

www.politika.rs/rubrike/Ekonomija/Piraterija-odnosi-milijarde-dolara.lt.html дана05.07.2017.године

http://torrentfreak.com/europe-has-the-highest-online-piracy-rates-by-far-160801/ преузето 08.05.2017.
www.webopedia.com/DidYouKnow/Internet/identity_theft преузето 08.05.2017.

http://news.bbc.co.uk/2/hi/technology/6199372.stm преузето 08.05.2017

http://www.cnn.com/2013/09/26/justice/miss-teen-usa-sextortion/ преузето: 08.05.2017.

Информативни кутак, Занимљивости;
http://kompjuterskikriminalitet.blogspot.com/2009/02/zanimljivosti.html претражено 15.08.2017. године

http://www.nbcnews.com/id/19981415/ns/technology_and_science-space/t/nasa-reports-computer-sabotage преузето 15.05.2017.

http://svethakera.com/index.php?option=com_content&task=view&id=13&ltemid=32 претражено 06.08.2017.

Recommendations to the European Council Europe and the global information society, http://channelingreality.com/Digital_Treason/Brussels_1995/Bangemann_report.pdf, претражено 04.8.2017.године

Компутерски криминал/ИПФ-радна база, http://promocije.net/proba/krivicno-pravo/materijalno-krivicno-pravo/kompjuterski-kriminal/, претражено 19.07.2017. године

Information systems security survey, WarRoom Research, LLC, 23 November 1996., http://www.infowar.com/sample/survey.html-ssi;;

САЖЕТАК И КЉУЧНЕ РЕЧИ

Прва целина мастер рада „ Криминолошки аспект компјутерског криминалитета “ посвећена је криминолошком и кривичноправном концепту компјутерског криминалитета. Поред одређења појма, кратког приказа историјског развоја и навођења основних карактеристика компјутерског криминалитета, детаљно је обрађен институционални оквир и правна регулатива за борбу против компјутерског криминалитета како на међународном тако и на националном нивоу. Сагледани су појавни облици уз анализу узрочности компјутерског криминалитата. На самом крају прве целине приказана је подела и основне карактеристике извршиоца дела компјутерског криминалитета.

Друга целина рада је усмерана искључиво на студију о компјутерском криминалитета у периоду 2009-2015. године за територију Републике Србије и Републике Хрватске. Непосредни циљ спровођења студијског приступа у анализи компјутерског криминалитета је утврђивање феноменолошких и етиолошких карактеристика компјутерског криминалитета. Приликом студијског приступа у анализи компјутерског криминалитета примењени су статистички метод, правно догматски метод, упоредно - правни метод и историјски метод. Неки од резултата до којих се дошло захваљујући наведеној студији су : број осуђених пунолетних лица мушког пола је и по неколико пута већи у односу на број осуђених пунолетних лица женског пола, приликом изрицања кривичних санкција изрицана је у највећем броју случајева условна осуда, незнатно је постојање саучесништва приликом извршења дела компјутерског криминалитета у односу на извршење истих од стране појединаца итд.

Трећа целина рада односи се на превенцију, заштиту и сузбијање компјутерског криминалитета.Успешна превенција и заштита од компјутерског криминалитета претпоставља примену одговарајуће методологије приликом израде правних прописа. Неопходно је константно праћење развоја и преображаја компјутерског криминалитета како би правна регулатива увек била у корак са новим облицима његовог испољавања и тиме обезбедила брзо и ефикасно сузбијање

Кључне речи: компјутерски криминалитет, појавни облици, превенција,сузбијање

SUMMARY AND KEYWORDS

The first section of the master's thesis „ Criminological aspect of computer crime “ is dedicated to criminological and criminal concept of computer crime. In addition to defining the subject, short review of the historical development and bringing into view the basic characteristics of computer crime, the institutional framework and legal regulation for fighting against computer crime both globally and nationally is in detail analyzed. The appearing forms have been put into perspective with the analysis of causation for computer crime. The divison and basic characteristics of the computer crime offenders have been presented in the very end of the first section.

The second section of the thesis is solely aimed at the study of computer crime in the period of 2009-2015 regarding the territory of both the Republic of Serbia and Republic of Croatia.The main purpose of carrying out the studical approach in the analysis of computer crime is to determine the phenomenological and etiological characteristics of computer crime. The statistical method, legal-dogmatic method, comparative-legal method and historical method have been applied during the studical approach of analyzing computer crime. Some of the results that have been discovered with the help of the mentioned study are : the number of the convicted male adults is several times greater than the number of convicted adults that are of female gender, in most cases during the pronunciation of criminal sanctions a conditional sentence has been pronounced,the existence of complicity during the commiting of computer crimes is insignificant considering the commiting of the same crimes from the individuals.

The third section of the thesis relates to the prevention, protection and repression of computer crime. The successful prevention and protection from computer crime presupposes the use of the required methodology during the making of legal documents. There is a necessity for the constant monitoring of development and conversion of computer crime so that the legal regulation would be able to keep up with the new forms of its manifestations and therefore provide fast and efficient repression.

Keywords: computer crime, appearing forms, prevention, repression

БИОГРАФИЈА АУТОРА

Драган Мирковић је рођен 11.11.1993. године у Нишу. Основну школу „ Радоје Домановић“ завршио је одличним успехом са Вуковом дипломом. Прву нишку гимназију „ Стеван Сремац “ (филолошко одељење) такође је завршио са одличним успехом и Вуковом дипломом. Правни Факултет у Нишу уписао је школске 2012/2013 године и дипломирао 5. 10. 2016. године са просечном оценом 9,55. и тиме стекао звање дипломирани правник. Мастер студије на Правном факултету у Нишу уписао је школске 2016/2017. Испите на кривично-правном смеру мастер студија положио је са просечном оценом 10,00 . Вишегодишњи је стипендиста Министарства просвете Републике Србије и Оксфорд центра у Нишу због успеха и ангажовања у савладавању енглеског језика. Такође, стипендиста је и Фонда за младе таленте Министарства омладине и спорта. Течно говори енглески и немачки. Од 29.05. 2017. године уписан је у Именик адвокатских приправника-волонтера Адвокатске коморе у Нишу, на вежби код адвоката Срђана Алексића из Ниша.