УНИВЕРЗИТЕТ У НИШУ
ПРАВНИ ФАКУЛТЕТ

Превара као облик високотехнолошког криминалитета

(мастер рад)

Ментор:
Проф. др Драган Јовашевић

Студент:
Александар Арсић
Број индекса: М 003/17-УП

Ниш, 2018.

Садржај

УВОД

Појава компјутера и мобилних телефона сврстава се у најзначајнија открића у историји човечанства. Свакодневни развој и усавршавање ове области утиче како на откриће тако и на појаву и развој нових облика криминала. Нове технологије, с једне стране, имају посебан значај на процес друштвеног и економског развоја, док с друге стране имају утицај на сложеност и усавршавање нових облика криминала.

Савремени технолошки развој битно је проширио и променио појам криминала, пошто су се појавиле нове криминалне претње за које савремени системи сузбијања криминала морају пронаћи адекватне одговоре. Економска криза, велике миграције становништва, савремени облици тероризма, међународни организовани криминал, глобално загађење животне средине, развој информационо комуникационих технологија и науке и технике уопште, чине нужним укључивање већег броја друштвених и државних субјеката у систем сузбијања нових савремених облика криминала.

Унапређења у области науке, пронашла су примену у полицијској пракси савремених државних система, првенствено развој информационо комуникационих технологија. Нова научна достигнућа се користе ради формирања, одржавања и развоја електронских база података, различитих врста евиденција, форензике, криминалистичке анализе, стратешког планирања и слично. Примена нових технологија присутна је у законодавној пракси савремених земаља, као одговор на високу стопу криминала.

Требало би да постоји свест о огромном значају употребе компјутера, како у позитивном смислу, тако и у негативном смислу. Констатација да се компјутери у великој мери користе за различите врсте злоупотреба, доприноси промени схватања да криминал у највећој мери врше необразована лица. Савремене облике криминала карактерише висок степен организованости, интернационализација, рецидивизам, професионализам и специјализација, као и злоупотреба техничких достигнућа, латентност и висока тамна бројка, што све укупно знатно отежава откривање и доказивање кривичних дела. То говори да је компјутерска технологија, са повећањем примене и масовним коришћењем отворила врата разним злупотребама и криминалним радњама.

Високотехнолошки криминал се у последње време толико развио и усавршио, да су потребне савремене методе и одговорајући механизми како би се зауставио тај развој. Ефикасно супротстављање високотехнолошком криминалу представља изазов за сваку државу, нарочито његови организовани облици, са израженим последицама по сваког грађанина. Држава мора константно усаглашавати постојећи законодавни и институционални оквир, који омогућава коришћење не само специјалних истражних мера и радњи у кривичним поступцима, већ и системско праћење и истраживање нових трендова развоја ових механизама.

У Републици Србији високотехнолошки криминал је врста криминала која је у развоју, што указује на потребу праћења светских и европских трендова. Да би се створила објективна основа за доношење релевантних стратешких и оперативних одлука којима ће се унапредити правни и институционални капацитети Министарства унутрашњих послова и других органа за спровођење закона и постигао већи степен заштите основних права и слобода грађана Србије, Министарство унутрашњих послова израдило је у 2015. години, стратешки извештај „Процена претње од тешког и организованог криминала“ (SOCTA – *Serious and Organized Crime Threat Assessment*), без кога није могућ избор приоритета и дефинисање препорука за поступање полиције.

Полиција Србије је до сада потписала 21 споразум о полицијској сарадњи са трећим земљама, међу којима су 15 земаља чланице Европске уније, затим споразум о стратешкој сарадњи са Европолом, као и оперативни споразум (потписан у јануару 2014. године). Успостављен је комуникациони линк преко Европолове Мрежне апликације за безбедну размену информација (SIENA). Такође, потписана су 42 меморандума о разумевању и размени финансијско-обавештајних података са трећим државама, од којих су 17 државе чланице ЕУ (Ђурђевић, Радовић, 2015: 46).

Од посебног значаја за сузбијање високотехнолошког криминала је Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала[1], којим је у Републици Србији за поступање у предметима кривичних дела високотехнолошког криминала, за територију Републике Србије формирано Посебно одељење за борбу против високотехнолошког криминала (Посебно тужилаштво), при Вишем јавном тужилаштву у Београду, затим у Министарству унутрашњих послова Републике Србије образовано је Одељење за борбу против високотехнолошког криминала у оквиру Службе за борбу против организованог криминала, а у Вишем суду

[1] *Сл. гласник РС*, бр. 61/2005 и 104/2009.

у Београду, образовано је Одељење за борбу против високотехнолошког криминала за поступање у предметима кривичних дела високотехнолошког криминала. Оснивање посебних органа је условљено потребом посебне специјализације свих државних органа, који учествују у борби против високотехнолошког криминала, посебно из области информатичких технологија.

Законом о изменама и допунама Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала[2], а који је ступио на снагу 24.12.2009. године, извршено је његово усклађивање пре свега са Законом о изменама и допунама Кривичног Законика[3], али и изменама других важних закона (Законом о јавном тужилаштву[4], Законом о уређењу судова[5] и Законом о седиштима и подручјима судова и јавних тужилаштава[6]). Уведени су нови појмови као што је рачунарски систем и рачунари, проширена је надлежност државних органа за борбу против високотехнолошког криминала и на кривична дела против привреде и друга кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира и уставног уређења и безбедности Републике Србије, а у Вишем суду у Београду као надлежном суду на територији Републике Србије уместо већа формирано је одељење.

Једна од најзаступљенијих и друштвено најопаснијих облика високотехнолошког криминала препознатих у Србији, јесте сексуална експлоатација деце и малолетних лица, као посебно рањиве категорије, у порнографске сврхе. Поред тога, заступљени су и различити облици рачунарских превара на штету физичких и правних лица које се врше на различите начине, уз социјални инжењеринг и крађу и злоупотребу идентитета.

Финансијско пословање посебно угрожавају незаконите активности везане за платне картице, било да је реч о фалсификовању банковних картица или скидању новчаних износа са рачуна физичких и правних лица у електронском окружењу. За извршење ових кривичних дела користе се посебно осмишљени софтверски алати, технике и методе усмерене на нападе на рачунарске мреже и системе.

У мноштву богате базе метода извршења и појавних облика високотехнолошког криминала, у овом раду је настојано да се направи осврт на неке карактеристичне

[2] *Сл. гласник РС*, бр. 61/2005 и 104/2009.
[3] *Сл. гласник РС*, бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013 и 108/2014.
[4] *Сл. гласник РС*, бр. 116/2008, 104/2009, 101/2010, 101/2011 и 121/2012.
[5] *Сл. гласник РС*, бр. 116/2008, 104/2009, 101/2010, 31/2011, 78/2011, 101/2011, 101/2013, 40/2015, 106/2015 и 13/2016.
[6] *Сл. гласник РС*, бр. 101/2013.

појавне облике превара, износећи притом њихова обележја, начине на који се испољавају у пракси, тј. модусе којима се служе њихови учиниоци и све то, с крајњим циљем стицања, непосредно или посредно, противправне имовинске користи.

Циљ овог рада јесте указивање на експанзију и озбиљност штетних последица које могу настати извршењем неког од преварних појавних облика кривичних дела високотехнолошког криминала. Чињеница је да се њихов број константно повећава, јер развој ове области криминала прати развој интернет технологија и рачунарства. Сви људи су сведоци да се из дана у дан све више закорачује у нову сферу науке, и из дана у дан се руше неке, до скоро немогуће баријере, што, са једне стране, олакшава људски живот, а са друге стране,отвара простор за криминално деловање учинилаца кривичних дела високотехнолошког криминала.

Рад је конципиран у четири целине, идући, дедуктивном методом од општег ка посебном, почевши од основних одредница и карактеристика високотехнолошког криминала, нормативног – међународног и националног оквира за борбу против високотехнолошког криминала, преко система кривичних дела високотехнолошког криминала у Републици Србији, којих има, с обзиром на начин или средство извршења у готово свакој од глава Кривичног законика, па до дефинисања преваре, и прегледа најзначајнијих облика превара у високотехнолошком криминалу.

I ОПШТЕ ОДРЕДНИЦЕ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

1.1. Појмовно одређење високотехнолошког криминала

Високотехнолошки криминал је комплексан појам, повезан са организованим вршењем кривичних дела. У теорији се, чак сматра заједничким термином који покрива разноврсне криминалне активности од напада на компјутерске податке и системе, напада везаних за компјутере, садржаје или интелектуалну својину, па до напада на интернет сервисе, доступне на тржишту софтверских алата, који делују по моделу „злоћудни програм као услуга“ (CaaS), што омогућава злоупотребе легалних сервиса у криминалне сврхе. Реч је, заправо, о употреби високософистициране информационе технологије у планирању и извршавању кривичних дела, односно у експлоатисању „плодова“ кривичних дела (Мијалковић, Бајагић, 2012: 241).

Високотехнолошки криминал показује тенденцију пораста тако да се истраживање ових кривичних дела своди на национална законодавства и међународну сарадњу држава која се у знатној мери ослања на традиционална средства формалне међународне сарадње у кривичним стварима. У исто време, електронски докази налазе се на различитим местима широм света у оквиру једног случаја, а могућности за истраге су знатно отежане због различитих националних оквира (капацитети полицијских служби, тужилаштва и судови у различитим државама, технички ресурси и др.). Развој високотехнолошког криминала и злоупотреба компјутера подстакли су научну и стручну јавност да се позабави овим обликом криминалног понашања, његовим појавним облицима испољавања и мерама друштвене реакције према њиховим учиниоцима.

Компјутер постаје средство вршења различитих облика недозвољених, противправних и друштвено опасних делатности, односно кривичних дела. Наравно, компјутерски криминалитет под чијим збирним називом су обухваћени разнолики облици и форме понашања која су везана за злоупотребу компјутера и информационих система нема опште усвојену дефиницију. Тако се у кривичноправној литератури за ове разнолике облике компјутерског криминалитета употребљавају различити термини као што су: злоупотреба компјутера, компјутерска превара, деликти уз помоћ компјутера, информатички криминалитет, рачунарски криминалитет, компјутерски криминалитет и техно криминалитет.

Високотехнолошки криминалитет за разлику од других не представља још увек заокружену феноменолошку категорију те га је немогуће дефинисати јединственим и прецизно појмовним одређењем. Тешкоће у дефинисању ове појаве се јављају због тога што се ради о релативно новим облицима криминалног понашања, али и због велике разноврсности ове појаве која се тешко може обухватити једном општом дефиницијом. Најопштије речено, то је криминалитет који је усмерен против безбедности информационих (компјутерских, рачунарских) система у намери да се себи или другом прибави каква корист или да се другоме нанесе каква штета (Урошевић, Ивановић, Уљанов, 2012: 19).

Према енглеском речнику појам компјутерског криминала се одређује на следећи начин: „Компјутерски криминал обухвата незаконите активности које се врше на компјутеру или код којих је компјутер средство извршења. Обухвата криминални упад у други компјутерски систем, крађу компјутерских података, или коришћења on-line система за вршење или помоћ у извршењу превара“ (Урошевић et al, 2012: 20).

На 10. Конгресу Уједињених нација за превенцију криминалитета и третман делинквената, компјутерски криминалитет је одређен „као општи појам који обухвата кривична дела која се врше посредством комјутерског система или мреже, у компјутерском систему или мрежи, или против компјутерског система или мреже“. Уопштено, он представља свако кривично дело које се врши у електронском амбијенту (Урошевић et al, 2012: 20).

Аутор Ђорђе Игњатовић под појмом компјутерски криминал подразумева: “посебан вид инкриминисаних понашања код којих се рачунарски систем (схваћен као јединство хардвера и софтвера) појављује као средство извршења или као објект кривичног дела, уколико се дело на други начин, или према другом објекту, не би могло извршити или би оно имало битно другачије карактеристике“. Узимајући у обзир сва горе наведена сагледавања, дефиниције и истраживања у погледу појма високотехнолошког криминала, закључујемо да је неопходно имати широк приступ приликом дефинисања ове врсте криминалног понашања. Такође, закључујемо да дефиниција ове врсте криминала мора да садржи три битна елемента. То су:

- начин извршења,
- средство извршења и
- последица криминалног деловања (Игњатовић, 2000: 16).

Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала[7] први пут је и у српском законодавству дефинисан појам високотехнолошког криминала и то као "вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику".[8]

Према дефиницији рачунарског криминала коју је прихватио NCIS (Nacional Criminal Intelligence Service) на пројекту под називом "Тегљач" 1999. године у Великој Британији ова врста криминала се дефинише као "кривично дело у оквиру којег је рачунарска мрежа директно и значајно инструментална у његовом вршењу. Рачунарска међуповезаност је у овом случају од есенцијалног значаја" (Smith, Grabosky, Urban, 2004: 7).

Из наведеног излагања се може видети да постоје одређена криична дела за чије се извршење користе рачунарска, али и друга високотехнолошка средства, али која нису апсолутно неопходна (пошто представљају само средство) за извршење кажњивог акта. Као пример се може навести, рецимо, ситуација када се у извршењу кривичног дела злоупотребе службеног положаја створе скривени финансијски фондови на рачунару фирме који се користе за одређене трансакције, иако се ово кривично дело може извршити и без рачунара и рачунарских система, на пример, трансфером из једне банке у другу и сл.

Најбољи пример за ову врсту односа инструменталног и инцидeнталног (споредног) учешћа рачунарског система у кривичном делу је сексуална злоупотреба и искоришћавање малолетних лица (педофилија) путем интернета.[9]Ту се може радити о појави "намамљивања" деце преко одређених Chatroom сервиса да се са извршиоцем сретну и уживо, а након тога долази до вршења других кривичних дела, на пример силовања или недозвољених полних радњи.[10]

Дефиниција рачунарског криминала која се наводи у тротомном приручнику информационе безбедности (Bigholi, 2006: 211) је енумерациона и обухвата неколико области као што су:

[7]*Сл. гласник РС*, бр. 61/2005 и 104/2009.

[8]Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, *Сл. гласник РС*, бр. 61/2005.

[9]Овај термин се тренутно у ЕУ више користи, јер порнографија укључује и пристанак у овом случају детета – жртве, што, наравно, ни у ком случају није могуће.

[10]У последње време законодавци све чешће инкриминишу овакве акте посебним облицима кривичних дела – у Републици Србији је до инкриминације сексуалне злоупотребе и искоришћавања деце у порнографске сврхе дошло тек 2009. године.

- злоупотреба дозвољених начина употребе рачунара и рачунарских система, кибервандализам и кибертероризам, одбијање пружања услуга, уношење рачунарских вируса и других злоћудних програма,
- растурање криминалних материја: порнографије или дечје порнографије, онлајн игара или онлајн клађења, расистичког или антирелигијског садржаја,
- употреба комуникационих уређаја са циљем: изнуде, киберухођења,
- кривотворење или фалсификовање: крађа идентитета, кривична дела у вези са интернет протоколима (IP), програмска, CD, DVD пиратерија и кршење ауторских права и сл.,
- преваре: преваре са платним картицама и преваре лажним трансферима електронских фондова; крађа телефонских или интернет услуга; каталошке и аукцијске преваре; преваре потрошача и у вези са диретним продајама на интернету (на пример, кинеске масти или змијских уља) и
- остали облици: незаконито пресретање комуникација, комерцијална или корпорацијска шпијунажа, комуникацијске технологије у служби криминалног удруживања, електронско прање новца.

У литератури се могу наћи и дефиниције код којих се рачунарске мреже, односно информационо-комуникациона технологија појављују у вишеструкој "улози", односно као (Урошевић et al, 2012: 23-24):

1. **циљ напада** – нападају се сервиси, функције и садржаји који се налазе на мрежи. Краду се услуге, подаци или идентитет, оштећују се или уништавају делови или цела мрежа и рачунарски системи, или се ометају функције њиховог рада. У сваком случају, циљ учинилаца је рачунарска мрежа у коју се убацују рачунарски вируси или црви, обарају интернет сајтови, врше хакерски напади, врши се "одбијање услуга", познатије као DOS (Denial of Service) напади,
2. **алат** – криминалци од памтивека користе камен, нож, отров, пиштољ и слична оружја и оруђа. Данас модерни криминалци не "прљају" своје руке пошто користе интернет мрежу за вршење кривичних дела и реализовање својих криминалних радњи. Некада ова употреба мреже представља потпуно нови алат, док се у другим приликама чак спомињу и две варијанте: а) нова дела са новим алатима и б) стара дела са новим алатима. Коришћење новог оружја нарочито је популарно код злоупотребе малолетних лица у порнографске сврхе, злоупотребе

интелектуалне својине или онлајн продаје недозвољене робе (дроге, људских органа, деце, оружја и сл.),

3. **“окружење” у коме се напади реализују** – најчешће то окружење служи за прикривање криминалних радњи, као што то веома вешто успевају даураде педофили, а ни други криминалци нису ништа мање успешни и
4. **доказ** – као што се у класичном криминалу појављују нож, отров, пиштољ илидруго средство извршења кривичног дела, тако се и мрежа и информационо-комуникационе технологије (ИКТ) могу јавити у доказном поступку за ову врсту криминала. Истовремено, рачунарска мрежа служи као мрежа за повезивање разних субјеката, она је практично техничка подршка, али може бити и симбол – у случају када је ова последња улога везана за застрашивање или обмањивање.

Све наведене дефиниције дају могућност да се у различитим правним оквирима процесуирају различити облици високотехнолошког криминала, али је ипак неопходно за ову појаву дати свеобухватнију дефиницију.

Према једном схватању, рачунарски криминал је било који криминал извршен делимично или у целини у електронској средини, за који извршилац мора поседовати знања о компјутерској технологији (хардвер и софтвер) и мора поседовати одређену намеру. Та намера мора обухватити, како средство које се користи, тако и изазивање одређене последице овим средством.

Друга схватања одређују рачунарски криминал као посебан вид инкриминисаних понашања у којима се рачунарски систем (схваћен као јединство хардвера и софтвера) појављује или као средство извршења или као објекат кривичног дела уколико се дело на други начин или према другом објекту уопште не би могло извршити, или би оно имало битно другачије карактеристике (Игњатовић et al. 2000: 21).

Нешто потпунија дефиниција (Петровић, 2000: 42) је она која рачунарски криминал одређује као недозвољене активности у којима је рачунар објект или средство извршења кривичног дела, а чији је циљ:

- уништење или отуђење рачунарског система или његових компоненти,
- уништење, оштећење, отуђење и неовлашћена измена, објављивање или коришћење софтверских и прогамских производа,
- уништење, оштећење, отуђење и неовлашћена измена, објављивање или коришћење података,

- извршење кривичних дела,
- неовлашћено коришћење рачунарских ресурса и
- нарушавање или пробијање система заштите.

Имајући у виду све чињенице изложене у претходним дефиницијама, може се констатовати да је високотехнолошки криминал такав облик криминалног понашања код кога је киберпростор окружење у коме се компјутерске мреже појављују као средство, циљ, доказ, и/или симбол или окружење извршења кривичног дела. При томе се под овим простором подразумева или врста "заједнице" сачињене од мреже компјутера у којој се елементи традиционалног друштва налазе у облику бајтова и битова или "простор који креирају компјутерске мреже" (Прља, Рељановић, Ивановић, 2012: 120).

1.2. Карактеристике високотехнолошког криминала

Високотехнолошки криминал има своје специфичности у односу на друге врсте криминалних радњи које спадају у општи, класични, конвенционални криминал. То су: велика динамичност, константно ширење на нове области, тежина последице, велика тамна бројка, отежано откривање и доказивање, специфичност извршења, профил учиниоца, специфичност у прикупљању доказног материјала и слично. Карактеристике високотехнолошког криминала указују на опасност ове појаве и упућују да се сузбијању ове врсте криминала приступи са великом пажњом.

Штетне последице овог облика криминала су изузетно велике. Оне се могу испољити у наступању имовинске штете за правно или физичко лице, а понекад и за целу државу. И сами учиниоци кривичних дела у вези са злоупотребом компјутера представљају посебну, често специфичну категорију људи. Овде се углавном ради о неделинквентним, ненасилним, социјално прилагодљивим појединцима. То су, по правилу, лица која морају да поседују посебна стручна и практична знања и вештине у домену високе информатичке, рачунарске и компјутерске технологије и којима су оваква технолошка средства доступна.

Ова се кривична дела врше прикривено, често без неке видљиве и блиске просторне повезаности учиниоца дела и жртве (оштећеног). Најчешће се тешко откривају, а још теже доказују. При томе, ова дела дуго времена остају практично неоткривена, све док оштећени не претрпи какву штету која је видљива у систему

рачунарских информација. То је криминалитет који брзо мења форме и облике испољавања, границе међу државама као и врсту оштећеног тј. жртву.

Савремена информациона и компјутерска технологија унела је нове драстичне промене у све области друштвеног живота. Те промене су поред позитивних и корисних новина донеле и низ проблема везаних за појаву и ширење компјутерског криминала различитих облика, форми и видова испољавања. Све те промене се могу свести на следеће:

- нове форме вредности,
- концентрација података,
- нови амбијент деловања,
- нове методе и технике деловања,
- сужавање временске скале деловања,
- ширење географског простора деловања,
- покретљивост и
- стабилност ризика.

Такође, високотехнолошки криминал карактерише:

- доступност података, како овлашћеним, тако и неовлашћеним корисницима,
- висока концентрација на малом простору,
- провера и уређење података,
- проширен простор криминалног деловања,
- није потребна приступност извршиоца на месту извршења кривичног дела,
- скраћено време криминалног деловања,
- извршењем кривичног дела не омета се редован рад система,
- једном изграђен модус може се дуго користити,
- висок степен прикривености и тајности деловања и
- једноставност употребе компјутерске технологије од стране већег броја корисника проширује већи број потенцијалних извршилаца којима више није нужно посебно техничко образовање.

Опасност високотехнолошког криминала по друштво огледа се не само у јављању и већем броју појавних облика, већ и у развоју појединих облика традиционалних кривичних дела.

Високотехнолошки криминал има своје специфичности у односу на друге врсте криминалних деловања, које несумњиво указују на опасност ове појаве и упућују да се питању сузбијања исте, приступи са великом пажњом. Велика динамичност, константно ширење на нове области, тежина последица које наступају вршењем компјутерских кривичних дела, велика тамна бројка, отежано откривање и доказивање, специфичан профил учиниоца свакодневно утичу на развој, усавршавање и појаву нових облика кривичних дела из ове области.

Наведене карактеристике последица су специфичног амбијента у којем се високотехнолошки криминал врши. Тај амбијент карактеришу: висока концентрација на малом простору, претходно проверених и уређених података, доступних како овлашћеним, тако и неовлашћеним корисницима; знатно проширен простор криминалног деловања, који, за разлику од традиционалних видова криминалитета, не захтева присуство извршиоца на месту извршења кривичног дела; те скраћено време криминалног деловања, с обзиром на аутоматизовани амбијент, чија брзина спречава надзор и управљање. На тај начин, време потребно за извршење кривичног дела скраћује се на делове секунде, што имплицира висок ниво прикривености и значајне тешкоће у откривању такве делатности; на ово се надовезују и технике и методи који се врше истим механизмима као и легалне технике, не остављају трагове, нити ометају редован рад система, па је самим тим могућност откривања сведена на најмању меру; за разлику од традиционалног криминала, компјутерски карактерише стабилност ризика, с обзиром да се једном изграђен модус може веома дуго користити, са потпуно истим, ниским ризиком откривања; све једноставније могућности употребе компјутерске технологије од стране све већег броја корисника, којима више није нужно посебно техничко образовање.

Ситуација се сваког дана погоршава. Осим карактеристика високотехнолошког криминала, посебна забринутост се односи на уздржавање корпорација од пријављивања кривичних дела којима су оштећене путем вршења дела високотехнолошког криминала, јер сматрају да би тиме погоршале свој положај на тржишту. Овај проблем знатно повећава тамну бројку високотехнолошког криминала.

1.3. Типови високотехнолошког криминала

Различити документи на различите начине класификују облике ове врсте криминала. Тако се у материјалу за "радионицу" о криминалу на мрежи приликом Десетог конгреса УН констатује да постоје две субкатегорије овог криминала. То су:

- високотехнолошки криминал у ужем смислу – свако незаконито понашање усмерено на електронске операције сигурности компјутерских система и података који се у њима обрађују и
- високотехнолошки криминал у ширем смислу – свако незаконито понашање везано за или у односу на компјутерски систем и мрежу, укључујући и незаконито поседовање, нуђење и дистрибуирање информација путем компјутерских система и мрежа (Урошевић et al, 2012: 20).

У истом документу наводе се и конкретни облици овог криминалитета у складу са Препоруком Савета Европе и листом OECD-а из 1989., односно 1985. године. То су:

- неауторизовани приступ компјутерском систему или мрежи кршењем мера сигурности (хакинг),
- оштећење компјутерских података или програма,
- компјутерске саботаже,
- неовлашћено пресретање комуникација компјутерских система и мрежа и у тим системима и мрежама и
- компјутерска шпијунажа.

Сваки од ових облика криминала може се даље укрштати са другим јер у стварности готово да не постоји "чист" облик. Тако "хакинг", поред неовлашћеног уласка у компјутерске системе и мреже, често обухвата и уништење података или компјутерску шпијунажу као што је случај са упадима на интернет сајтове и уништење или "преправљање" података на њима или хакинг и трговина лозинкама. Измена компјутерских података и програма укључује и уношење компјутерских црва и вируса, што је најчешће праћено заустављањем рада компјутерског система, уништењем података и сл. У мрежама црви и вируси се у већини случајева преносе електронском поштом упућивањем на интернет линкове, а неретко то чине и хакери приликом неовлашћеног приступа.

Од дела високотехнолошког криминала у ширем смислу најчешће се појављују:

- компјутерски фалсификати,

- компјутерске крађе,
- техничке манипулације уређајима или електронским компонентама уређаја и
- злоупотребе система плаћања, као што су манипулације и крађе електронских података о платним картицама или коришћење лажних шифри у незаконитим финансијским активностима.

Овим кривичним делима се у новије време додају и дела подржана рачунарима. Тако ова дела високотехнолошког криминала обухватају "растурање" материјала или само њихово поседовање, при чему се рачунарска мрежа користи за постизање бољих резултата таквог деловања или у циљу избегавања законских санкција. У ова дела убрајају се поседовање и дистрибуција разних незаконитих и штетних садржаја, кршење ауторских и сродних права, продаја забрањене робе (оружја, крадене робе, лекова) или пружање недозвољених услуга (коцкање, проституција). Највише пажње у овој групи кривичних дела привлачи злоупотреба малолетних лица у порнографске сврхе и дистрибуција разних инкриминисаних материјала путем интернета.

Европска конвенција о високотехнолошком криминалу донета у Будимпешти 2001. године предвиђа четири групе кривичних дела високотехнолошког криминала. То су:

- дела против поверљивости, интегритета и доступности компјутерских података и система – њих чине незаконити приступ, пресретање, преправљање података или неовлашћено приступање системима, коришћење уређаја (производња, продаја, увоз, дистрибуција), програма, лозинки,
- дела везана за компјутере – код којих су фалсификовање и крађе најтипичнији облици напада,
- дела везана за садржаје – "дечја порнографија" је најчешћи садржај који се појављује у овој групи и обухвата поседовање, дистрибуцију, трансмисију, чување или чињење доступним и расположивим ових материјала, њихова производња ради дистрибуције и обрада у компјутерском систему или на носиоцу података и
- дела везана за кршење ауторских и сродних права - обухватају репродуковање и дистрибуцију неауторизованих примерака дела компјутерским системима.

Ова Конвенција под компјутерским системом подразумева и компјутерске мреже. У "Енциклопедији високотехнолошког криминала" наводи се да ФБИ и

Национални центар за криминал белих оковратника САД (National White CollarCrime Center) откривају и прате следеће облике:

- упад у компјутерске мреже,
- индустријску шпијунажу,
- софтверску пиратерију,
- дечју порнографију,
- бомбардовање електронском поштом,
- преузимање лозинки,
- "прерушавање" једног рачунара да електронски "личи" на други како би се могло приступити систему који је под заштитиом и
- крађу кредитних картица.

Зависно од типа извршених дела, високотехнолошки криминал може бити: а) политички (када је мотив извршења везан за политичке циљеве које извршилац кривичног дела жели да оствари), б) економски (када је мотив стицање противправне имовинске користи или наношење штете), в) производња и дистрибуција недозвољених и штетних садржаја (када су предмет производње, прибављања или дистрибуције материјали у електронском облику – текстови, слике, аудио-визуелни материјал и сл. чија је садржина везана за ширење говора мржње, педофилију и сл.) и г) повреде сајберприватности (када се, на пример, прибављају одређени подаци о личности на незаконит начин заобилажењем и кршењем мера заштите и сл.) (Урошевић et al, 2012: 28-29).

Политички високотехнолошки криминал чине следећа кривична дела:

- високотехнолошка шпијунажа,
- хакинг,
- саботажа,
- кибертероризам и
- ратовање.

Економски високотехнолошки криминал чине следећа кривична дела:

- рачунарска превара,
- хакинг,
- крађа интернет услуга и времена,
- копирање софтвера, микрочипова и база података,

- високотехнолошка индустријска шпијунажа и
- преварна интернет аукција (неиспоручивање производа, лажна презентација производа, лажна процена, надограђивање цене производа, удруживање ради постизања веће цене, трговина робом са црног тржишта, вишеструке личности).

Производњу и дистрибуцију недозвољених и штетних садржаја чине:

- "дечја порнографија",
- педофилија,
- верске секте,
- ширење расистичких, нацистичких и сличних идеја и ставова;
- злоупотреба жена и деце и
- манипулација забрањеним производима, супстанцама и робама: дрогом, људским органима и оружјем.

У повреде сајберприватности спадају:

- надгледање електронске поште,
- СПАМ поруке,
- фишинг,
- прислушкивање, снимање "причаоница",
- праћење е-конференција и
- прикачивање и алализа колачића (cookies).

Из наведених подела јасно се уочава да велики број различитих класификација сам по себи показује разноврсност њихових појавних облика испољавања и комплексност њихових појавних облика, али и различитост критеријума који се користе.

У сваком случају, осим упада у компјутерске системе и мреже, шпијунаже, саботаже, пиратерије, бомбардовања електронске поште примањем нежељених порука, "прикупљања" лозинки, "скривања" једног рачунара другим, рачунарских вируса, односно њихове производње и дистрибуирања, овој области припада и цео скуп недозвољених и штетних садржаја од "дечје порнографије" до растурања верских, расистичких и сличних садржаја. Посебно су бројна дела дисеминације недозвољене робе или пружања недозвољених услуга. Томе треба додати и киберсаботаже и

тероризам, као и крађу интернет времена, услуга, идентитета, разне злоупотребе кредитних картица.

Штете настале вршењем ових кривичних дела, зависно од појавног облика високотехнолошког криминалитета, могу се поделити на:

- финансијске – које могу да настану када учинилац врши кривично дело ради стицања противправне имовинске користи, па ту корист за себе или другога, заиста и стекне, или је не стекне, али својим делом објективно причини одређену штету другом лицу, или када учинилац не поступа ради стицања користи за себе или другог, али објективно учини финансијску штету,
- нематеријалне – које се огледају у неовлашћеном откривању туђих тајни или другом "индискретном штетном поступању" и
- комбиноване – када се откривањем одређене тајне или повредом ауторског права, путем злоупотребе компјутера или информатичке мреже наруши нечији углед, односно повреди морално право, при чему му се истовремено проузрокује и конкретна финансијска штета.

Неспорно је да је високотехнолошки криминал више везан за активности појединаца, а криминал везан за компјутерске мреже представља више дело група и то организованих, професионализованих, па све чешће и строго специјализованих (Урошевић et al. 2012:29). Те групе су, с једне стране, "традиционалне" групе организованог криминала које су се усавршиле и осавремениле применом информационо комуникационих технологија чимесу се припремиле за "излазак" на ову "сцену". С друге стране, јављају се и посебне организоване групе – "сајбермафија". Оне имају своја правила, другачији начин понашања од конвенционалних, као што имају и специфично "оружје".

Њихове активности су у многоме олакшане специфичностима окружења у ком делују и оружја која користе. Окружење је виртуелно, оружје је информационо, а знање је специјализовано. Интернационализам, транснационалност, мултидимензионалност само су нека од својстава тих група. Њихова организациона формула није толико једноставна, устаљена и једнообразна као што је то случај са другим облицима организованог криминала, што још више утврђује слику о њиховој посебности.

II НОРМАТИВНИ ОКВИРИ ЗА БОРБУ ПРОТИВ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА У РЕПУБЛИЦИ СРБИЈИ

2.1. Међународноправни оквир за борбу против високотехнолошког криминала

2.1.1. Конвенција о високотехнолошком криминалу Савета Европе

Неопходност међународног повезивања националних државних органа представља основни предуслов ефикасном супростављању високотехнолошком (компјутерском) криминалу. Република Србија је ратификовала Конвенцију о високотехнолошком криминалу Савета Европе[11] у марту 2009. године уз Додатни протокол[12] који се бави инкриминисањем аката расистичке и ксенофобичне природе путем рачунара. Конвенција је донета 23. новембра 2001.године у Будимпешти, и поред Србије ратификована је још од 31 државе чланице Савета Европе (потписале су је и Канада, Јапан, Јужноафричка Република и САД).

Основни циљеви доношења Конвенције су хармонизација националних законодавстава у домену материјалноправних одредби у области високотехнолошког криминала, увођење одговарајућих процесних инструмената ради бољег процесуирања ових кривичних дела и успостављање брзих и ефикасних институција и процедура међународне сарадње.[13]

У преамбули саме Конвеције наглашена је потреба за процесуирањем извршилаца кривичних дела високотехнолошког криминала, која имају међународни карактер. Унапређење сарадње надлежних националних органа један је од основних приоритета с циљем сузбијања високотехнолошког криминала.[14]

Европске државе су међу првима схватиле неопходност стварања међународног документа који би регулисао питање компјутерског криминалитета, а све већа опасност од последица компјутерског криминалитета, поспешила је настојања твораца Конвенције да се превазиђу различита ограничења у националним законодавствима, која доводе у питање делотворност правне заштите, заједно са међусобним настојањима држава да ускладе своја законодавства у овом погледу.

---

[11] *Сл. гласник РС - Међународни уговори*, бр. 19/2009.
[12] *Сл. гласник РС - Међународни уговори*, бр. 19/2009.
[13] http://www.aic.gov.au/statistics/hightech/cybercrime.htmlпреузето 08.06.2018. године.
[14] Члан 2. Закона о потврђивању Конвенције о високотехнолошком криминалу, *Сл. гласник РС*, бр. 19/2009.

Конвенција предвиђа обавезу за државе потписнице да у свом националном законодавству пропишу следећа кажњива понашања као кривична дела:

1. дела против поверљивости, целовитости и доступности рачунарских података и система: незаконит приступ; незаконито пресретање; ометање података; ометање система; злоупотреба уређаја,
2. дела у вези са рачунарима: фалсификовање у вези са рачунарима; превара у вези са рачунарима,
3. дела у вези са садржајем: дела у вези са дечјом порнографијом,
4. дела у вези са кршењем ауторских и сродних права и
5. други облици одговорности: покушај, помагање и подстрекавање; одговорност правног лица.

Конвенција је прописала минимум заједничких стандарда приликом инкриминисања ових кривичних дела. Тако је створен основ за сарадњу између надлежних органа држава, као и за размену искустава. Конвенцијом је искључен евентуални приговор услед недостатка двоструке инкриминисаности и у случају евентуалне екстрадиције.

За кривично дело незаконитог приступа подацима на рачунарима или систему, потребна је намера учинилица да те информације присвоји, измени или уништи. Државама потписницама остављена могућност да у својим законодавствима регулишу и посебне облике овог кривичног дела.

Незаконито пресретање је кривично дело које се састоји из намере пресретања, преноса података између два рачунара.

Кривична дела ометање података и ометање система се састоје из намере потпуног или делимичног брисања, оштећења, измене садржине, компресије или било ког другог начина измене података. Конвенција и овде даје могућност државама да сузе домет инкриминације, односно да се кривичним сматрају само она дела, где је причињена већа штета.

Злоупотреба уређаја је сложено кривично дело. Конвенција ово дело одређује као сваку намерну, противправну, производњу, употребу, набавку или продају, као и сваки облик чињења доступним и дистрибуције, било које врсте уређаја, под којима се подразумевају и рачунарски програми помоћу којих се могу извршити кривична дела одређена у Конвенцији. Имајући у виду неодређеност ове одредбе, творци Конвеције остављају могућност резерве државама потписницама када је реч о продаји или другом

начину дистрибуције лозинки или других података, помоћу којих се могу извршити кривична дела.

Фалсификовање се односи само на умишљајно, противправно брисање, измену, убацивање или сакривање података, које резултира измењеним садржајем тих података, без обзира на то, да ли они на било који начин добијају другу сврху или смисао, или постају неупотребљиви.

Превара је одређена као умишљајно, противправно брисање, измена, убацивање или сакривање података, као и свако друго мешање у рад система у циљу прибављања противправне имовинске користи за себе или другога.

Конвенција о високотехнолошком криминалу обавезује државе потписнице да као кривично дело дечје порнографије инкриминише следеће радње: производња дечје порнографије у сврху њене дистрибуције преко рачунарског система; нуђење или чињење доступним дечје порнографије преко рачунарског система; дистрибуција или преношење дечје порнографије преко рачунарског система; набављање дечје порнографије преко рачунарског система, за себе или за друго лице; поседовање дечје порнографије у рачунарском систему или на медијумима за чување рачунарских података.[15]

Ова Конвенција је инкриминисала свако понашање укључујући и прибављање и поседовање, што чини значајну разлику у односу на бића сличних кривичних дела везаних за кршење ауторских права путем рачунарске мреже. Творци Конвенције су на ауторитативан начин државама потписницама наредили да уреде своја законодавства и да на тај начин допринесу превенцији дечје порнографије.

Такође, Конвенција прецизно регулише шта се сматра порнографским садржајем. Тако се као порнографски материјал сматра сваки материјал који визуелно приказује:

1. малолетника који учествује у експлицитно сексуалној радњи,
2. лице које изгледа као малолетник, које учествује у експлицитно сексуалној радњи и
3. реалистичне слике, које представљају малолетника који учествује у експлицитно сексуалној радњи.[16]

[15]Члан 9. ств.1. Закона о потврђивању Конвенције о високотехнолошком криминалу, *Сл. гласник РС*, бр. 19/2009.
[16]Члан 9. ств.2. Закона о потврђивању Конвенције о високотехнолошком криминалу, *Сл. гласник РС*, бр. 19/2009.

Конвенција под децом подразумева сва лица узраста до навршене осамнаесте године живота, уз могућност да се ова граница спусти на шеснаест година**.**

Државе потписнице су обавезне да у складу са Конвенцијом усвоје законске и друге мере, коју су неопходне како би се одговорна лица казнила за нека од наведених кривичних дела високотехнолошког криминала као што су: а) покушај, б) подстрекавање и в) помагање у извршењу кривичних дела високотехнолошког криминала. Такође је предвиђена могућност да се за ова кривична дела пропише и кривична одговорност правних лица**.**

Члановима 14-22. Конвенције регулисана су процесна овлашћења државних органа приликом истраживања кривичних дела високотехнолошког криминала.

Поред тога, велика је пажња усмерена на начин прикупљања података који се налазе у рачунарима или преносним уређајима, као и на заштиту основних права појединца гарантованих Европском конвенцијом о људским правима и основним слободама из 1950.године, Међународним пактом Уједињених нација о грађанским и политичким правима из 1966. године и осталим важећим међународним докуменатима о људским правима, који садрже начело пропорционалности.[17]

Надлежни органи, у складу са Конвенцијом, имају право увида и заплене сваког рачунара или носача података, уколико постоје основи сумње, да се ту могу налазити недозвољени материјали, као и да од провајдера прикупљају податке, који се односе пре свега, на употребу интернета, телефона и картица. Такође је предвиђено и пресретање података, односно праћење електронске комуникације, посебно оне које се обавља путем интернета. Ова област је и најосетљивија, јер се њоме повређују основна права човека, а то су правона приватност и право на преписку. Како се пресретање односи само на тешка кривична дела, државе имају пуну слободу да саме одреде када ће и у којим случајевима ово право користити. При томе су државе дужне да обавежу даваоца услуга на чување у тајностиспровођење одређених радњи из оквира надлежности, као и сваке информације у вези са тим. Када се имају у виду истраге за кривична дела тероризма и злостављања деце оваква процедура је оправдана и прихватљива, иако не постоји механизам заштите грађана од могућих злоупотреба.

Конвенцијом није предвиђена ни обавеза провајдера да складишти податке о својим корисницима, који би можда касније били од користи надлежним органима, и то због очигледне повреде права на приватност корисника.

[17] Члан 15. Закона о потврђивању Конвенције о високотехнолошком криминалу, *Сл. гласник РС*, бр. 19/2009.

Члан 22. Конвенције предвиђа надлежност држава за процесуирање уколико је кривично дело извршено: а) на њеној територији, б) на броду под заставом те државе, в) у ваздухоплову регистрованом у складу са законима те државе и г) од стране њеног држављанина, ако је дело кажњиво по кривичном закону државе где је извршено или ако је дело извршено на месту изван надлежности било које државе. Такође, су државеобавезне да, уколико не изврше екстрадицију свог држављанина, му суде за дела која су извршена на територији друге државе.

Трећи део Конвеције је посвећен међународној сарадњи како би се превазишле препреке приспровођењу националног законодавства за кривична дела која подразумевају учешће неколико земаља, а често и појединце из више земаља. Сарадња држава се тако одвија путем размене података за извршена кривична дела, као и екстрадиције њихових учинилаца. У посебним случајевима може бити успостављена и директна сарадња између правосудних органа појединих држава, као и Интерпола,без икаквог посредовања органа извршне власти.

Такође државе могу тражити, једна од друге, спровођење истражних радњи у случају када: а) има основа да се верује да су одговарајући подаци нарочито подложни губитку или измени и б) инструменти, договори и закони налажу брзу сарадњу.[18]

Конвенција служи и као основ за екстрадицију уколико државе то питање нису регулисале.

Конвенција предвиђа оснивање дежурне службе која би радила данонoћно седам дана у недељи (24/7), за чије потребе државе морају да успоставе у својим полицијским службама јединицу за сарадњу, која би пружала тренутну помоћ истрагама или поступцима у вези са кривичним делима која се односе на рачунарске системе и податке, или ради прикупљања доказа у електронском облику о кривичном делу. Таква помоћ треба да обухвати олакшавање или, уколико то домаће право и пракса дозвољавају, непосредно спровођење следећих мера: давање техничких савета; заштиту података; прикупљање доказа, давање информација правне природе и лоцирање осумњичених.[19]

[18]Члан 31.став 3. Закона о потврђивању Конвенције о високотехнолошком криминалу, *Сл. гласник РС*, бр. 19/2009.
[19]Члан 35.став 1. Закона о потврђивању Конвенције о високотехнолошком криминалу, *Сл. гласник РС*, бр. 19/2009.

2.1.2. Додатни протокол уз Конвенцију о високотехнолошком криминалу

Додатни протокол уз Конвенцију о високотехнолошком криминалу[20] донет је 28. јануара 2003. године у Савету Европе у Стразбуру. Он се односи на инкриминацију радњи расистичке и ксенофобичне природе учињених уз помоћ рачунара. Протокол инкриминише понашања која није регулисала Конвенција, а која се тичу ширења мржње, нетолеранције и нетрпељивости путем рачунарских система, према расним, верским, националним групама и заједницама.[21] Ширење интернета и доступност рачунара постали су опасна средства за ширење погубних идеологија и ставова, попут величања нацизма, тероризма, позива на линч појединаца и сл. Интернет се не може благовремено контролисати, јер сваки корисник сматра да има право на изражавање свог става, тако да су злоупотребе огромне.

Протокол предвиђа обавезе за државе потписнице да у свом националном законодавству пропишу кажњавање следећих кривичних дела:

1. ширење или на други начин чињење доступним јавности, преко рачунарског система, расистичког и ксенофобичног материјала,
2. претња мотивисана расизмом и ксенофобијом,
3. увреда мотивисана расизмом и ксенофобијом,
4. порицање, значајно умањивање, одобравање или оправдавање геноцида или злочина против човечности и
5. помагање и подстрекавање.[22]

Ширење или на други начин чињење доступним јавности, преко рачунарског система, расистичког и ксенофобичног материјала подразумева сваку радњу којом се овакав материјал чини доступним јавности коришћењем рачунарског система.

Претња мотивисана расизмом и ксенофобијом представља стављање у изглед појединцу или групи да ће према њима бити извршено кривично дело предвиђено у закону, при чему се појединици и групе разликују по боји коже, раси, пореклу, националној, верској или етничкој припадности.

---

[20] *Сл. гласник РС - Међународни уговори*, бр. 19/2009.

[21] Члан 1. Закона о потврђивању додатног Протокола уз Конвенције о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе која су извршена преко рачунарских система, *Сл. гласник РС - Међународни уговори*, бр. 19/2009.

[22] Члан 3-7. Закона о потврђивању додатног Протокола уз Конвенције о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе која су извршена преко рачунарских система, *Сл. гласник РС - Међународни уговори*, бр. 19/2009.

Увреда мотивисана расизмом и ксенофобијом, поседује елементе као и претходно дело, само што се овде ради о вређању (повреди части и угледа), а не о претњи. Протокол је код овог дела оставио могућност државама да ограниче инкриминацију само на увреде којима се група или појединац понижавају или извргавају подсмеху или на увреде којима се шири мржња.

Порицање, значајно умањивање, одобравање или оправдавање геноцида или злочина против човечности односи се на случајеве који су били предмет одлучивања од стране међународних судова од 1945. године до данас под условом да је овакав садржај на било који начин учињен доступан јавности, односно већем броју људи.

Свака држава потписница треба да усвоји законодавне и друге мере, неопходне да би се као кривично дело у домаћем праву прописало намерно и противправно помагање и подстрекавање на извршење неког од наведених кривичних дела са намером да та дела буду учињена.[23]

2.1.3. Директиве ЕУ о борби против високотехнолошког криминала

2.1.3.1. Директива Савета Европске заједнице о правној заштити компјутерских програма

Директива Савета Европске заједнице о правној заштити компјутерских програма од 14. маја 1991. године представља једно од првих решења у области правне заштите компјутерских програма. Она је настала као резултат сарадње држава чланица на смањивању разлика у својим законодавствима у циљу сузбијања неовлашћеног умножавања компјутерских програма, које има негативан утицај на функционисање заједничког тржишта. Правна заштита пружена је сваком физичком и правном лицу које потпада под одредбе националних законодавстава у области ауторског права примењивог на књижевна дела. Директива обавезује државе чланице, да се као недозвољена правно санкционишу следећа понашања:

1. стављање у промет копије компјутерског програма, знајући да је копија недозвољена или имајући разлога за основану сумњу у њену недозвољеност,

[23]Члан 7. Закона о потврђивању додатног Протокола уз Конвенције о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе која су извршена преко рачунарских система, *Сл. гласник РС - Међународни уговори*, бр. 19/2009.

2. држање из комерцијалних разлога копије компјутерског програма, знајући да је копија недозвољена или имајући разлога за основану сумњу у њену недозвољеност и
3. стављање у промет или држање у комерцијалне сврхе сваког средства чија је једина сврха да олакша недозвољено уклањање или неутрализацију сваког техничког механизма евентуално направљеног у циљу заштите компјутерског програма.

Државе потписнице су у обавези да заплене сваку недозвољену копију компјутерског програма у складу са националним законом. Директива ауторима обезбеђује правну заштиту за живота и педесет година након смрти (уколико је реч о више аутора, до смрти последњег), док правним лицима и анонимним ауторима рок заштите тече од дана чињења програма доступним. Аутором компјутерског програма сматра се физичко лице, група лица и правно лице.

2.1.3.2. Директива о чувању података који су добијени или обрађени приликом пружања јавно доступних услуга електронске комуникације или јавних комуникационих мрежа

Директива о чувању података који су добијени или обрађени приликом пружања јавно доступних услуга електронске комуникације или јавних комуникационих мрежа од 15.03.2006. године донета је с циљем ефикасног откривања и процесуирања учинилаца кривичних дела чије извршење оставља електронске трагове. Она представља допуну Директиве 2002/58 о обради личних података и заштити приватности у области електронских комуникација.[24] Директива у складу са чланом 8. Европске конвеције о заштити људских права и основних слобода даје право државама потписницама, да под одређеним условима ограниче права грађана с циљем очувања јавног реда и мира, заштите националне сигурности, одбране и ради успешног процесуирања учинилаца кривичних дела неовлашћене употребе система електронске комуникације.

Основни циљ Директиве је усклађивање националних законодавстава држава која регулишу обавезе даваоца јавних услуга комуникација да чувају податке које у оквиру обављања своје делатности добијају и обрађују, како би подаци били доступни

[24]http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32006L0024 преузето 13.06.2018. године.

у случају откривања кривичних дела и процесуирања њихових учинилаца. Директива се не примењује на садржај електронске комуникације, као ни на информације до којих се долази коришћењем електронске комуникације, већ само на податке о локацији и промету правних и физичких лица који су потребни за тачну идентификацију претплатника или корисника услуга (Комлен Николић, 2010: 64).

Такође, Директива води рачуна између поштовања основних људских права и потребе ефикасног супростављања криминалу, имајући у виду начела сразмерности и оправданости ограничења права грађана. Право на приступ подацима имају само надлежни органи држава чланица у судским поступцима који су уређени домаћим законима. Чланом 5. извршена је категоризација података који се складиште, односно чувају сходно одредбама Конвенције.

У првој категорији налазе се подаци који су потребни ради проналажења и идентификације извора комуникације. Код мобилне и фиксне телефоније чувају су следећи подаци: а) телефонски број прикључка са ког позив долази и б) име и адреса уколико је претплатник, односно корисник регистрован. Код приступа интернету,мобилном интернету и електронској пошти чувају се следећи подаци: а) подаци о додељеном корисничком имену/именима, б) корисничко име и телефонски број додељен свакој комуникацији с којом се ступа у јавну телефонску мрежу и в) име и адреса претплатника или регистрованог корисника којем је у тренутку комуникације додељена адреса интернет протокола (IP), корисничко име и телефонски број.

Другу категорију чине подаци потребни ради откривања одредишта комуникације. Код мобилне и фиксне телефоније чувају су следећи подаци: а) бирани број или бројеви и у случају који укључује коришћење додатних услуга попут преусмеравања или преноса позива, број или бројеви на које је позив преусмерен и б) име или имена и адресу/адресе претплатника или регистрованог корисника.Код мобилног интернета и електронске поште, потребно је сачувати податке о: а) имену примаоца услуге или његов број телефона коме је упућен позив путем услуге мобилног интернета и б) имену и адреси претплатника, регистрованог корисника или податке о корисничком имену примаоца према коме је комуникација усмерена.

Директива у трећој категорији података одређује који се подаци чувају ради утврђивања времена, датума и трајања комуникације. Код мобилне и фиксне телефоније чувају се подаци о датуму и времену почетка и завршетка комуникације. Код приступа интернету,мобилном интернету и електронској пошти, чувају се следећи подаци: а) временски оквир пријаве и одјаве приступа корисника интернету према

одређеној временској зони, заједно са IP адресом, било да је статичка или динамичка, коју је комуникацији доделио давалац услуга приступа интернету, као и корисничко име претплатника односно корисника и б) време пријаве и одјаве од услуге електронске поште или услуге интернет телефоније према одређеној временској зони.

Откривање врсте комуникације постиже се захваљући подацима садржаним у четвртој категорији. Код фиксне и мобилне телефоније то је коришћена телефонска услуга, а код електронске поште и интернет телефоније у питању је коришћена интернет услуга.

Једна од најважнијих категорија података је она која се користи за откривање комуникацијске опреме корисника или њихове наводне опреме. Код фиксне телефоније чувају се телефонски бројеви са којих се позива и који су позивани. Код мобилне телефоније чувају се: а) телефонски бројеви са којих се позива и бројеви који се позивају, б) међународни идентитет мобилног претплатника странке која позива и која прима позив, в) међународни идентитет мобилног уредаја странке која позива и која прима позив и г) код унапред плаћених (pre paid) анонимних услуга, датум и време почетка употребе услуге и ознака локације са које је услуга активирана.

Код приступа интернету, електронској пошти и интернет телефонији чувају се подаци о телефонском броју с којег се позива у сврху телефонског приступа или дигитална претплатничка линија или друга крајња тачка лица које започиње комуникацију.

Директива у последњој категорији регулише који су подаци неопходни за откривање локације опреме за мобилне комуникације.

Државе су у обавези да податке чувају у року од шест месеци до две године од дана комуникације[25], с тим што се подаци могу чувати и дуже од предвиђеног рока, али уз обавезу обавештавања Комисије и друге државе о разлозима продужења. Комисија може у року од шест месеци да донесе одлуку којом одобрава или одбија примену националне мере након испитивања да ли је мера предузета као средство произвољне дискриминације или представља прикривено ограничење трговине међу државама чиме се стварају препреке за функционисање унутрашњег тржишта.[26]

[25]Члан 6. Директиве Европског парламента и Савета о чувању података који су добијени или обрађени приликом пружања јавно доступних услуга електронске комуникације или јавних комуникационих мрежа.

[26]Члан 12. Директиве Европског парламента и Савета о чувању података који су добијени или обрађени приликом пружања јавно доступних услуга електронске комуникације или јавних комуникационих мрежа.

Директива уређује и правну заштиту лица, чији се се подаци прикупљају и чувају. Тако је предвиђена обавеза предузимања потребних мера да сеспречи противправан приступ подацима који се чувају, као и прописан поступак утврђивања одговорности за такве радње у управном или кривичном поступку. Санкције које се изричу у овим случајевима морају по природи и тежини бити сразмерне, какоби одвратиле од даљег кршења закона.

2.1.4. Други међународни инструменти

Поред наведених међународних докумената (Конвенције, Протокола и Директива) који су дали допринос у процесу конституисања норми које се тичу правила "сајбер дисциплине" ипрописивања деликата (кривичних дела) које државе треба да предвиде у националном законодавству, велики значај и улогу у сузбијању и спречавању високотехнолошког криминала имају и одређене међународне организације. Ту се посебно издвајају Европска канцеларија криминалистичке полиције – Европол и специјализована група унутар ове организације која се бави искључиво проблематиком високотехнолошког криминала – Центар за борбу против високотехнолошког криминала.

Центар за борбу против високотехнолошког криминала (European cibercrime center – ECC) је почео са радом у јануару 2013. године са задатком да помогне у заштити државних органа, привредних субјеката и грађана од све растућег компјутерског криминалитета у Европској унији, који је последица велике информационе писмености, развијене информационе инфраструктуре, електронског банкарства и интернет трговине.

Главне области деловања Центра су:

1. борба против организованих криминалних група (поготово оних које је баве финансијским преварама на интернету),
2. борба против дечје порнографије и сексуалне експолатације на интернету,
3. заштите података од крађе и
4. заштита виталних информационих система Европске уније.

У овим областима Центар пружа помоћ полицијским службама појединих држава као: а) обавештајни и логистички центар, б) централна база података, в) центар за обуку, г) центар за вештачење и д) центар за сарадњу са невладиним сектором и привредом. Такође, Центар велику пажњу усмерава и на сузбијање злоупотреба

платних картица које на нивоу Европске уније сваке године направе штету од милијарду и по евра (Европол је спровео више успешних акција на овом пољу)[27]. Како је употреба платних картица раширена већ скоро две деценије на простору Европске уније и како је само у 2011. години укупна вредност плаћања картицама износила преко 3000 милијарди евра, јасно је зашто ова област од посебног значаја за Европол (Publications Office of the European Union, 2012: 3). До злоупотребе платних картица долази тако што извршиоци набављају податке са картица служећи се разним методама, а затим те податке продају или их сами користе. Само 2011. године у Европској унији било је 20.244 пријављених злоупотреба, што је скоро дупло више у односу на 2010.годину, када је било пријављено 12.383 злоупотреба (Publications Office of the European Union, 2012: 8).

Центар је као део Европола постигао добре резултате у борби против дечје порнографије. До сада је, захваљујући Центру, разбијено више криминалних група и ухапшено на стотинепедофила. Последња у низу успешних акција Центра је спроведена у сарадњи са америчком федералном полицијом (ФБИ) ирумунском полицијом у фебруару 2018.године када је спасена двогодишња беба из Румуније коју је њен отац злостављао и слике и видео записе злостављања постављао и нудио ради продаје на интернету.[28]

Центар је заслужан и за формирање Европске финасијске коалиције за борбу против сексуалне експлоатације деце на интернету која ради под патронатом Европске Комисије (eng. European Financial Coalition against commercial sexual exploitation of children online). Коалицију чине представници полицијских служби и невладиног сектора, привреде и истакнути појединци који се боре против злоупотребе деце и њихове експлоатације на интернету. Захваљући Центру и Коалицији годишње се обради преко милион сумњивих порнографских садржаја на интернету.[29]

Центар за борбу против високотехнолошког криминала бави се и обавештајним активностима. Тако у оквиру Центра ради тим специјализован за прикупљање

[27] Најпознатија акција Европола против организованих криминалних група које се баве преварама и злоупотребама картица била је "Плави ћилибар" (енг. Blue Amber), у којој је учествовало преко 50 полицијских служби. У овој операцији ухапшено је преко 130 лица која су у вишегодишњем периоду, злопотребом платних картица куповала и препродавала авио карте преко интернета и на тај начин оштетила 38 авио компанија и стекла противправну добит у износу од преко милијарду евра. http://www.computerweekly.com/news/4500248925/Police-arrest-130-in-global-anti-cyber-fraud-operation преузето 22.06.2018. године.

[28] https://www.europol.europa.eu/content/international-police-action-leads-rescue-22-month-old-romanian-sex-abuse-victim. преузето 22.06.2018. године.

[29] http://www.europeanfinancialcoalition.eu/private10/images/document/2.pdf. преузето 22.06.2018.године.

информација на интернету, њихову анализу и препознавање потенцијалних претњи побезбедностЕвропске уније.

По Дигиталној агенди Европске комисије за Европске унију за 2020. годину информациона технологија је кључ привредног развоја. Зато је и безбедност на интернету постала један од приоритета обезбеђивања тог развоја (PublicationsOfficeoftheEuropeanUnion, 2012: 5).Центар у циљу спровођења Агенде интезивно сарађује са CERT-ом (eng. Computer Emergency Response Team) који представља службу ЕУ задужену за безбедност органа Европске Уније од претњи које долазе са интернета.

2.2. Национални правни оквир заштите од високотехнолошког криминала у Републици Србији

2.2.1. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала

Доношењем Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала[30] и оснивањем посебних органа за борбу против високотехнолошког криминала учињен је велики корак, што представља израз разумевања ризика који са собом носи извршење кривичних дела из ове области и допринос успостављању високотехнолошке безбедности. Чињеница да су информационе и комуникационе технологије постале незаменљиве у функционисању модерних друштава наметнула је потребу да се у светским оквирима успоставе мере и механизми за заштиту друштава и појединаца од високотехнолошког криминала усвајањем одговарајућих законодавних решења и унапређењем међународне сарадње. Резултат таквих напора је, између осталог, и доношење Конвенције о сајбер криминалу Савета Европе која успоставља минимум стандарда које је неопходно, по мишљењу међународне заједнице, да испуне национална законодавства у циљу ефикасне борбе против високотехнолошког криминала (Ранђеловић, 2012: 71).

С друге стране, питање организације правосудног система сваке државе у правцу стварања претпоставки за успешну борбу против нових појавних облика криминала, у овом случају високотехнолошког, јесте питање које намеће низ недоумица и на које није лако дати одговор. Да ли се определити за свеобухватну

[30] *Сл. гласник РС*, бр. 61/2005 и 104/2009.

системску промену која се огледа у промени и усклађивању низа прописа како би се створио адекватан законски оквир који би државним органима омогућио ефикасно деловање, или се одлучити за делимичну измену појединих законских одредаба у правцу измене постојећих овлашћења или надлежности, или успостављања нових, до тада непостојећих, органа који би били "уметнути" у већ постојећи и уврежени систем деловања, јесте питање чији одговор мора да помири различите захтеве и могућности.

С једне стране, избор прве варијанте пружа могућност да се одговори свим потребним захтевима, али, са друге стране, она захтева ангажовање великих материјалних и људских ресурса, постављање система на потпуно новим основама, за шта је потребна снажна политичка воља, али и друштвена свест о неопходности таквих промена. Избор друге варијанте пружа могућност бржих промена без задирања у основе система и уз ангажовање мањих средстава, али, с друге стране, може наметнути и друге проблеме као што су преплитање надлежности старих и нових органа, односно нерешено питање надлежности за поједина кривична дела, колизија нових законских решења са постојећим у погледу нових овлашћења, питање неприхватања, односно сарадње са новим органима који ремете већ устаљене и уобичајененачине сарадње.

Потпуно је јасно да је Република Србија у покушају да обезбеди ефикасну кривичноправну заштиту од нових појавних облика криминала, као што је високотехнолошки криминал, одабрала делимичне циљане промене појединих закона, уз доношење новог закона, којима се успостављају нови државни органи за поступање у овим кривичним предметима, што је, имајући у виду могућности Републике Србије, сасвим разумљиво. Међутим, начин како је то учињено у погледу надлежности, примене већ застарелих законских решења, како у погледу материјалног права, тако и у погледу процесних овлашћења у поступку откривања учинилаца кривичних дела и обезбеђивању доказа, у пракси ствара низ проблема.

Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, који је ступио на снагу 25. јула 2005.године (члан 3) се примењује ради откривања, гоњења и суђења за кривична дела против безбедности рачунарских података и за кривична дела против интелектуалне својине, имовине и правног саобраћаја код којих се као објекат или средство извршења јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику, ако број ауторских дела прелази 500 или настала материјална

штета прелази износ од 850.000 динара. Новелама овог закона из 2009. године[31] је направљена измена у погледу кажњивости, па је као услов у закону прописано да број примерака ауторских дела треба да прелази 2000 или настала материјална штета да прелази износ од 1.000.000 динара.

Овим Законом се предвиђа и оснивање посебних органа за борбу против високотехнолошког криминала у оквиру постојеће судске и тужилачке организације и Министарства унутрашњих послова. У Вишем јавном тужилаштву у Београду формирано је Посебно одељење за борбу против високотехнолошког криминала, тј. Посебно тужилаштво. Радом посебног тужилаштва руководи Посебни тужилац за високотехнолошки криминал кога поставља Републички јавни тужилац из реда заменика јавних тужилаца који испуњавају услове за избор за заменика вишег јавног тужиоца, уз писмену сагласност лица које се поставља. Предност имају заменици јавних тужилаца који поседују посебна знања из области информатичких технологија.[32]

Ради обављања послова органа унутрашњих послова у вези са високотехнолошким криминалом, у оквиру Министарства унутрашњих послова образује се Служба за борбу против високотехнолошког криминала, која поступа по захтевима Посебног тужиоца.[33] За поступање у овим предметима надлежан је Виши суд у Београду, за територију Републике Србије, односно у другом степену Апелациони суд у Београду.[34]У Вишем суду у Београду је образовано Посебно одељење за борбу против високотехнолошког криминала. Судије у одељење распоређује председник Вишег суда у Београду из реда судија тог суда, уз њухову сагласност. Предност имају судије које поседују посебна знања из области информатичких технологија. [35] Територијална надлежност наведених органа успостављена је на целој територији Републике Србије.

[31]*Сл. гласник РС*, бр. 104/2009.
[32] Члан 6. Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала, *Сл. гласник РС*, бр. 61/2005.
[33] Члан 9. Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала, *Сл. гласник РС*, бр. 104/2009.
[34]Члан 10. Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала, *Сл. гласник РС*, бр. 104/2009.
[35]Члан 11. Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала, *Сл. гласник РС*, бр. 104/2009.

2.2.2. Закон о потврђивању Конвенције о високотехнолошком криминалу и Додатног протокола уз Конвенцију о високотехнолошком криминалу

Народна скупштина Републике Србије је усвојила два закона из области сузбијања високотехнолошког криминалитета који су засновани на међународним стандардима: а) Конвенцији о високотехнолошком криминалу и б) Додатном протоколу уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система.[36]

2.2.3. Законик о кривичном поступку у функцији сузбијања високотехнолошког криминала

Ефикасно откривање и сузбијање високотехнолошког криминала укључује и веома специфичне оперативне мере и радње, као и посебне доказне радње. У питању су интернет патроле, пресретање телекомуникација у реалном времену, трагање на мрежи – *Tracing* и сл. Такве и сличне мере често се срећу у упоредном праву. Шта више, неке националне полицијске јединице "патролирају" интернетом да би обезбедиле јавну безбедност у тој области. Те јединице су развиле специфичне софтверске алате да би открили кривична дела као што су хаковање или дистрибуирање тзв. материјала насталог злоупотребом малолетних лица у порнографске сврхе (Прља et al, 2012: 128).

У Републици Србији је, нажалост, могућност Одељења за високотехнолошки криминал у Вишем јавном тужилаштву у Београду за примену специјалних истражних техника у дужем периоду била ограничена само на примену члана 144. Законика о кривичном поступку (закључно са Законником о кривичном поступку из 2011. године)[37] који се односи на достављање података о стању пословних и личних рачуна осумњичених, али само за кривична дела за која је прописана казна затвора од најмање четири године.Због тога су надлежни држави органи били принуђени да се користе постојећим, "класичним" овлашћењима (Урошевић et al, 2012: 38).

Ако се прибављање електронске поште осумњиченог, односно окривљеног од интернет провајдера, уз наредбу судије за претходни поступак, спроводи применом члана 168. ЗКП којим је регулисана предаја писама, телеграма и других пошиљки од субјеката регистрованих за пренос информација, упућених окривљеном или које он

[36] *Сл. гласник РС*, бр. 19/2009.
[37] *Сл. гласник РС*, бр. 72/2011 и 101/2011.

одашиље, ако постоје околности због којих се може основано очекивати да ће дате пошиљке послужити као доказ у кривичном поступку (Комлен-Николић, 2008: 20-25).

Поштанска, телеграфска и друга предузећа, друштва и лица регистрована за преношење информација су дужна да овлашћеним службеницима полиције (односно БИА и ВБА) омогуће извршење наведених мера. Неспорно је да то омогућава прикупљање комуникационих података у складу са одредбама Конвенције о високотехнолошком криминалу, али проблеми у пракси су настајали због специфичности начина прибављања доказа за тако софистицирана кривична дела, будући да се до њих често долази мониторингом на мрежи у реалном времену.

Према одредбама члана 153. ЗКП[38] у предмете који се могу привремено одузети се убрајају, поред оних оних којих могу представљати средство или објекат извршења кривичног дела високотехнолошког криминала, и уређаји за аутоматску обраду података и опрема на којој се чувају или се могу чувати електронски записи. Лице које се користи овим уређајима и опремом дужно је да органу који води поступак, на захтев суда, омогући приступ и да пружи обавештења потребна за њихову употребу. Пре одузимања ових предмета орган који води поступак ће у присуству стручног лица извршити преглед уређаја и опреме и пописати њихову садржину. Најзад, ако корисник присуствује овој радњи, може ставити примедбе. Очигледно је да је законодавац у овом случају уважио аргументоване захтеве тужилачке струке (Комлен-Николић, 2010: 34).

У теорији је изражен став да су кривичнопроцесне одредбе које су о посебног значаја за борбу против високотехнолошког криминала садржане у члану 167. ЗКП се даје могућност да судија за претходни поступак, на писмени и образложени предлог јавног тужиоца, нареди надзор и снимање телефонских и других разговора или комуникација другим техничким средствима оних лица за која постоје основи сумње да су сама или са другим лицима извршила одређена кривична дела. Такво схватање је било прихватљиво само делимично и условно, на пример када се конкретан случај високотехнолошког криминала односи на прање новца. С тим у вези треба нагласити да је за откривање неких од типичних дела високотехнолошког криминала може користити и мера рачунарског претраживања података, која је значајна због све израженије компјутеризације личних и других података, те великих могућности које ти подаци пружају у вези са прибављањем доказа, а с друге стране преставља гарант

[38] *Сл. гласник РС*, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 и 55/2014.

заштите у коришћењу личних података од државних органа у таквим поступцима (Урошевић et al, 2012: 39).

Закон о електронским комуникацијама [39] предвиђа тајност електронских комуникација, па се у члану 126. наводи да пресретање електронских комуникација којим се открива садржај комуникације није допуштено без пристанка корисника, осим на одређено време ради вођења кривичног поступка или заштите безбедности Републике Србије, на начин предвиђен законом. Оператор је дужан да омогући законито пресретање електронских комуникација. Надлежни државни орган који спроводи послове законитог пресретања дужан је да води евиденцију о пресретнутим електронским комуникацијама, која нарочито садржи одређење акта који представља правни основ за вршење пресретања, датум и време вршења пресретања, као и да ову евиденцију чува као тајну, у складу са законом којим се уређује тајност података. Оператор је дужан да, ради остварења ове обавезе, о свом трошку обезбеди неопходне техничке и организационе услове.

Чланом 161. ЗКП-а предвиђене су посебне доказне радње, као и услови за њихово одређивање. Посебне доказне радње могу се одредити према лицу за које постоје основи сумње да је учинило кривично дело из члана 162, а на други начин се не могу прикупити докази за кривично гоњење или би њихово прикупљање било знатно отежано.[40] Оне се, изузетно, могу одредити и према лицу за које постоје основи сумње да припрема неко од тих кривичних дела, а околности случаја указују да се на други начин дело не би могло открити, спречити или доказати, или би то изазвало несразмерне тешкоће или велику опасност. Под тим условима радња тајног надзора комуникације се може одредити и за следећа кривична дела: а) неовлашћено искоришћавање ауторског дела или предмета сродног права, б) оштећење рачунарских

[39] *Сл. гласник РС*, бр. 44/10 и 62/14.

[40] У кривична дела из члана 162. у односу на која се могу предузети посебне доказне радње, а која припадају делима високотехнолошког криминала, спадају кривична дела:
-За која је посебним законом одређено да поступа јавно тужилаштво посебне надлежности;
-приказивање,прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију (члан 185. ст. 2. и 3. КЗ), изнуда (члан 214. став 4. КЗ), фалсификовање новца (члан 223. ст. 1. до 3. КЗ), прање новца (члан 231. ст. 1. до 4. КЗ), напад на уставно уређење (члан 308. КЗ), позивање на насилну промену уставног уређења (члан 309. КЗ), шпијунажа (члан 315. КЗ), одавање државне тајне (члан 316. КЗ), изазивање националне, расне и верске нетрпељивости;
Под условима из члана 161. овог закона посебна доказна радња из члана 166. овог закона (Тајни надзор комуникација) може се одредити и за следећа кривична дела: неовлашћено искоришћавање ауторског дела или предмета сродног права (члан 199. КЗ), оштећење рачунарских података и програма (члан 298. став 3. КЗ), рачунарска саботажа (члан 299. КЗ), рачунарска превара (члан 301. став 3. КЗ) и неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (члан 302. КЗ).

података и програма, в) рачунарска саботажа, г) рачунарска превара и д) неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података.

У овако дефинисаном системском простору за надзор комуникација, нису обухваћени сви облици комуникације, већ је за сваки њен облик потребно посебно тумачење. Већ помињане, али и неке нове облике комуникационих карактеристика, на пример, MAC адресе уређаја који се користе, IP адресе, PROXY серверске маске, претраживачка историја одређеног корисника, историја "крстарења" интернетом, историја коришћења претраживачких сервиса (Google, Yahoo...); коришћење различитих социјалних мрежа и cloud computing могућности, које оне пружају (комуникацију и chat у оквиру cloud окружења, похрањивање података у оквиру истих, што се најчешће врши путем Facebook-а и Instagram-а) тешко се могу обухватити таквим решењима, без опширнијих образлагања и објашњења.

Уколико је неопходно да овакве одредбе буду унете у законски текст, треба неизоставно предвидети различите нивое услова у погледу прибављања наредби за издавање различитих комуникационих карактеристика, на пример листинга мобилних телефона, а различите за прибављање евиденција у вези са информационо-комуникационим технологијама (ИКТ) од IP адреса и MAC адреса уређаја до мејлова и римејлера коришћених у комуникацији. У сваком случају, неопходно је да такве наредбе доноси суд, али се у испуњавању услова за њих могу прописати различите одредбе. Могуће је предвидети и различите нивое судова надлежних за издавање различитих наредби, што такође може бити основ за олакшање прибављања наредбе. Такође, могуће је предвидети оне мере прописане конвенцијом и на тај начин решити овај проблем (Урошевић et al, 2012: 44).

Рачунарско претраживање података (растер потрага) састоји се у аутоматском претраживању већ похрањених личних и са њима непосредно повезаних података и њиховом аутоматском поређењу са подацима који се односе на кривично дело из члана 162. ЗКП-а и на осумњиченог, да би се као могући осумњичени искључила лица за која не постоји вероватноћа да су повезана са кривичним делом. По својој суштини то је негативна растер потрага која доприноси елиминацији одређених лица из круга осумњичених аутоматизованим претрагама у полицијским, административним и другим евиденцијама. Другим речима, тим методом елиминишу се одређена лица из круга оних која се служе лажним идентитетом, туђим кредитним картицама и слично.

Ова посебна доказна радња се може предузети ако постоје основи сумње да је учињено кривично дело из члана 162. ЗКП-а, а ако се на други начин не могу

прикупити докази за кривично гоњење или би њихово прикупљање било знатно отежано. Изузетно се ова радња може одредити и ако постоје основи сумње да се припрема неко од кривичих дела из члана 162. ЗКП-а, а околности случаја указују да се на други начин дело не би могло открити, спречити или доказати, или би то изазвало несразмерне тешкоће или велику опасност. Суштина овог метода је слободан приступ полиције свим евиденцијама које се воде аутоматизовано, што одудара од начела заштите права на приватност грађана и информатичко самоодређење (Бошковић, Кесић, 2015: 241-250).

III КРИВИЧНОПРАВНИ ОКВИР ЗА БОРБУ ПРОТИВ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

За кривичноправни оквир за борбу против високотехнолошког криминала најзначајнија су кривична дела против безбедности рачунарских података, или тзв. компјутерска кривична дела. Она се у највећој мери односе на ову проблематику и уско су повезана са институтима који се нападају и користе у извршењу аката високотехнолошког криминала. Наравно, поред ове, постоји још неколико група кривичних дела у Кривичном законику (КЗ) [41] која се могу сврстати у дела високотехнолошког криминала, с обзиром на објекат или средство извршења кривичног дела, о којима ће такође бити речи.

3.1. Кривична дела против безбедности рачунарских података

Ова кривична дела су предвиђена први пут у Кривичном закону Републике Србије (1977.) после новеле из априла 2003. године[42] (Јовашевић, 2014: 216). Према тадашњим одредбама ова кривична дела су била систематизована у XVI глави Кривичног закона под називом: "Кривична дела против безбедности рачунарских података". Кривичним закоником[43] из 2005. године, који је ступио на снагу 1. јануара 2006. године рачунарска кривична дела су обухваћена главом XXVII под називом: "Кривична дела против безбедности рачунарских података". Законик одређује појам високотехнолошког криминала као вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику.

Кривична дела против безбедности рачунарских података представљају по времену свог настанка најновију врсту криминалитета укривичном законодавству Републике Србије. Енормни и нагао развој компјутерске технологије ушао је у готово све области савременог друштвеног живота и пружио изванредне могућности у свим областима у којима се примењује. Значајне користи које из тога друштво има праћене су, међутим, и неким негативним појавама, пре свега појавом нових облика криминалитета који се повезују управо за примену рачунарске технологије. Ти нови облици криминалитета добили су и одговарајући назив – компјутерски (рачунарски)

[41] *Сл. гласник РС*, бр. 85/2005, 88/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013,108/2014 и 94/2016.
[42]" *Сл. гласник СРС*, бр.39/2003 и 67/2003.
[43]*Сл. гласник РС*, бр. 85/2005, 88/2005.

криминалитет. Стога је кривично законодавство на то брзо реаговало, па су се одговарајуће инкриминације појавиле у кривичним законодавствима савремених земаља – а међу њима је и Република Србија (Урошевић et al, 2012: 47).

Појавне облике компјутерског криминалитета у праву Републике Србије чине кривична дела која су садржана у глави XXVII Кривичног законика. Ова кривична дела се могу поделити у две групе. Једну групу чине дела којима се повређује сам систем компјутерске технологије оштећивањем или уништавањем рачунарских података или програма, или се омета њихово коришћење, или се врши неовлашћен приступ рачунарској мрежи и самој обради електронских података. Другу групу чине дела код којих се користи рачунарска технологија да би се помоћу ње вршила одређена кривична дела (Урошевић et al, 2012: 47). То су следећа кривична дела:

a. Кривична дела повреде рачунарских података:

1. оштећење рачунарских података и програма,
2. рачунарска саботажа,
3. прављење и уношење рачунарских вируса и
4. спречавање и ограничавање приступа јавној рачунарској мрежи.

b. Кривична дела злоупотребе рачунарских програма:

1. рачунарска превара,
2. неовлашћен приступ заштићеном рачунару, рачунарској мрежи и електронској обради података,
3. неовлашћено коришћење рачунара или рачунарске мреже и
4. прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података.

При дефинисању ових кривичних дела наведени појмови користе се у свом кривичноправном смислу, са садржајем одређеним чланом 112. Кривичног законика[44]. Тако се у ставу 17. овог члана рачунарски податак одређује као представљена информација, знање, чињеница, концепт или наредба који се уноси, обрађује или памти или је унет, обрађен или запамћен у рачунару или рачунарској мрежи.Под рачунарском мрежом се, у смислу става 18. истог члана, сматра скуп међусобно повезаних рачунара, односно рачунарских система који комуницирају размењујући податке, акао рачунарски програм се сматра уређени скуп наредби који служе за управљање радом рачунара, као и за решавање задатака помоћу рачунара, што је дефинисано ставом 19. овог члана.

[44]*Сл. гласник РС*, бр. 85/2005, 88/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 и 94/2016.

Даље, у члану 112. став 20. дат је појам рачунарског вируса, као рачунарског програма или другог скупа наредби који је 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. Рачунар је, у смислу става 33. овог члана, сваки електронски уређај који на основу програма аутоматски обрађује и размењује податке. И на крају, 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, што је предвиђено ставом 34. овог члана.

Сва кривична дела из ове групе врше се са умишљајем.

3.1.1. Оштећење рачунарских података и програма (члан 298. КЗ)

Кривично дело оштећење рачунарских података и програма има три облика, од којих су два тежа, а један основни.[45] Основни облик дела постоји када лице неовлашћено избрише, измени, оштети, промени или на други начин учини непотребљивим рачунарски податак или програм (Стојановић, Делић, 2018: 231-232).

Објект заштите је безбедност рачунарских података или рачунарских програма, а објект напада је рачунарски податак или програм.

Радња основног облика кривичног дела одређена је алтернативно, тако да се може извршити на следеће начине: брисањем, изменом, оштећењем или прикривањем рачунарског податка или програма. Генерална клаузула одређује да се ово кривично дело може учинити и на други начин, односно на начин који чини неупотребљивим рачунарски податак или програм (Ђорђевић, 2014: 171-172).

Постојање кривичног дела подразумева да се нека од делатности која има карактер радње извршења предузима неовлашћено, без одговарајуће дозволе. Брисање је уклањање рачунарских података у целини или делимично или рачунарског програма. Измена је делимична промена постојећих података или уношење нових података на начин, од стране лица и у поступку који није предвиђен одговарајућим прописима или по одговарајућој процедури. Оштећење је привремено, делимично или краткотрајно онеспособљавање коришћења рачунарског податка или програма изазивањем кварова или кидањем појединих делова, веза или склопова, тако да се рачунарски податак или

[45] Члан 298. Кривичног законика, *Сл. гласник РС*, бр. 85/2005, 88/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 и 94/2016.

програм не могу користити за одређено време за сврху за коју су намењени. Прикривање је премештање података или програма са места на коме је био похрањен или садржан и склањање на друго, најчешће непознато место. Чињење неупотребљивим на други начин је свако друго онеспособљавање за краће или дуже време или онемогућавање у већој или мањој мери коришћења рачунарског податка или програма (Јовашевић, 2014: 219).

Потребно је нагласити да се под другим начинима чињења неупотребљивим подразумева и чињење недоступнима, тако да се овај начин инкриминишу и случајеви деловања разних „тројанских“или „backdoor“ програма који служе како би се одређени програми сакрили у меморији компјутера, ради извршења припремне радње за неко кривично дело нпр. рачунарску изнуду (Прља, Ивановић, Рељановић, 2011: 142). Потребно је такође утврдити тачно време и место извршења кривичног дела, да ли се ради о неовлашћеном извршиоцу и начин на који је извршено кривично дело.

Кривично дело је довршено када је услед предузете радње рачунарски податак или програм постао неупотребљив.

Последица дела је повреда заштићеног добра – рачунарског податка или програма који припада физичком или правном лицу у смислу његове употребљивости, корисности уопште или за одређено време, на одређеном месту или за одређену намену.

Извршилац дела може да буде свако лице, а у погледу кривице потребан је умишљај.

За ово кривично дело прописана је новчана казна или казна затвора до једне године. Суд учиниоцу дела обавезно изриче меру безбедности одузимања уређаја и средстава ако су испуњена два услова: а) да се ради о средствима и уређајима којима је кривично дело учињено и б) да су средства и уређаји у својини учиниоца дела (Стојановић, 2018: 907-909).

Ово дело има два тежа облика испољавања.

Први тежи облик дела постоји уколико је предузетом радњом извршења основног облика дела причињена штета у износу који је већи од 450.000 динара. Висина причињене имовинске штете у време извршења дела у законом утврђеном износу представља квалификаторну околност. За ово дело је прописана казна затвора од три месеца до три године.

Најтежи облик кривичног дела одређен је у ставу 3. Он постоји ако је предузетом радњом извршењаосновног дела причињена штета у износу преко 1.500.000

динара, док је предвиђена казна затвора за ово дело од три месеца до пет година (Јовашевић, 2014: 219).

Најчешћи вид извршења овог кривичног дела представља рушење веб сајтова, што је свакодневна активност хакерских група. Објекат напада је обично само део сајта, најчешће насловна страна, која бива промењена тако да се на њој остави ауторски "потпис" групе, порука или поздрав, што јесте (али не само и једино) најчешћи елемент или чак и сврха акције хакивиста. Извршиоце је веома тешко открити јер они користе алате за скривање, који праве IP адресе, коју је извршилац користио у време извршења кривичног дела. У одређеним случајевима учиниоци иду, намерно, са постизањем ове околности, с тим да је ове податке веома тешко прибавити (обзиром да се на пример налазе на серверима у иностранству), чак и у оним случајевима када их нису сакрили или користили лажне. Тада временски протек игра своју улогу на многе елементе дела, од уништења и оштећења трагова до бекства извршилаца из државе (Прља et al, 2011: 143).

Оштећена лица углавном сама или уз туђу мање или више стручну помоћ, покушавају да поврате програме и податке који су предмет извршења овог кривичног дела јер им најчешће свакодневно пословање намеће то да често правна лица буду мета извршења овог кривичног дела, па стога настоје да не руше углед свог пословања и покушавају сама да реше проблем. На овај начин се најчешће уништавају непосредни докази, који би могли довести до откривања извршиоца, а надлежним органима остају само посредни докази који нису довољни за процесуирање извршилаца (Комлен Николић, 2010: 90).

3.1.2. Рачунарска саботажа (члан 299. КЗ)

Рачунарска саботажаје компјутерско кривично дело које чини лице које унесе, уништи, избрише, оштети, измени, прикрије или на други начин учини неупотребљивим рачунарски податак или програм или оштети рачунар или други уређај 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.[46]

[46] Члан 299. Кривичног законика, *Сл. гласник РС*, бр. 85/2005, 88/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 и 94/2016.

Објекат заштите рачунарске саботаже је двоструко одређен. Као прво, то може бити рачунарски податак или програм, али то може бити и рачунар, односно други уређај за електронску обраду и пренос података, али овде се мора радити о посебном својству оштећеног. Сви објекти заштите морају припадати државном органу, јавној служби или другим правним лицима (као што су нпр. установе, предузећа или друге организације), док у погледу радње извршења и осталих обележја бића овог кривичног дела нема разлике у односу на кривично дело оштећење рачунарских података и програма (Јовашевић, 2014: 220).

Разликују се два основна облика дела. То су: а) уништење или оштећење рачунарског податка или програма и б) уништење или оштећење рачунара или другог уређаја за електронску обраду и пренос података. Такође, поред већ поменутог својства оштећеног, овде је јако битно и да код извршиоца постоји одређена намера – намера да се онемогући или знатно омете поступак електронске обраде и преноса података. Није од значаја да ли је ова намера у конкретном случају и остварена (Ђорђевић, 2014: 173).

Радња извршења је алтернативно одређена као: 1) унос, 2) уништење, 3) брисање, 4) измена, 5) оштећење, 6) прикривање и 7) чињење неупотребљивим на други начин рачунарског податка или програма, односно уништење или оштећење рачунара или другог уређаја за електронску обраду и пренос података.

Унос је уписивање или похрањивање новог до тада непостојећег податка или измена већ постојећег рачунарског или другог податка у рачунарском програму. Уништење је потпуно и трајно разарање супстанце или облика одређеног предмета тако да више уопште не може да се користи за сврху, намену за коју је раније коришћен. Брисање је уклањање најчешће механичким или другим путем у целини или делимично рачунарског податка или програма. Измена је делимично мењање постојећих података у смислу њихове садржине, места где се налазе или њихове улоге или уношење других неистинитих података у рачунарски систем. Оштећење је привремено, делимично или краткотрајно онеспособљење рачунарског податка, програма, рачунара или другог уређаја за сврху за коју су иначе намењени. Прикривање је склањање податка или предмета са места на коме се до тада налазио и које је свима било познато и премештање на друго најчешће скривено место тако да се са њиховом садржином не могу упознати друга лица уопште или за одређено време. Чињење неупотребљивим рачунарског податка или програма представља сваку делатност којом се у већој или мањој мери утиче на употребљивост рачунарских података или програма (Јовашевић, 2014: 220). Радња другог облика овог кривичног дела је алтернативно одређена и

састоји у уништењу или оштећењу рачунара или другог уређаја за електронску обраду података. У принципу, овде видимо да је једина разлика између првог и другог облика овог кривичног дела у објекту напада, где су код првог облика рачунарски подаци и програми, а код другог су то рачунари и други уређаји за електронску обраду података. Намера учиниоца је у оба случаја иста (Стојановић, 2018: 909-910).

Последица дела је повреда рачунарског податка, програма, рачунара или уређаја за аутоматски пренос или обраду података у смислу њихове употребљивости и корисности.

Извршилац овог кривичног дела може бити било које лице, а у погледу кривице потребан је директан умишљај.

Прописана казна затвора за ово кривично дело је казна затвора од шест месеци до пет година.

Кривична дела рачунарска саботажа и оштећење рачунарских података и програма су слична према начину извршења и последицама које могу оставити, због чега надлежни органи морају бити опрезни приликом правне квалификације кривичног дела.Ова кривична дела се разликују по тежини последица које проузрокују, јер су последице кривичног дела рачунарске саботаже много теже и имају знатно шири спектар последица и објеката и правних субјеката (Лазаревић, 2011: 881). Последице кривичног дела рачунарска саботажа се манифестују у знатном онемогућавању или знатном отежавању функционисања државног органа за дужи временски период, заједно са огромном материјалном штетом и губицима (Комлен, Николић, 2011: 94).

Такође се као посебан облик извршења рачунарске саботаже јавља и уношење података и програма који нападнути податак или програм чине неупотребљивим или за последицу имају оштећење и уништење податка или програма (Јовашевић, 2014: 221).

3.1.3. Прављење и уношење рачунарских вируса (члан 300. КЗ)

Кривично дело прављење и уношење рачунарских вируса има свој основни и тежи облик.[47] Основни облик овог кривичног дела може учинити лице које направи рачунарски вирус у намери да га унесе у туђ рачунар или рачунарску мрежу.

Објект заштите је безбедност рачунара и рачунарске мреже од вируса различите врсте и природе, а објект напада је рачунарски вирус. Рачунарски вирус је рачунарски

[47] Члан 300. Кривичног законика, *Сл. гласник РС*, бр. 85/2005, 88/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 и 94/2016.

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 (Јовашевић, 2014: 221).

Радња извршења овог дела се састоји у: 1) прављењу – стварању рачунарског вируса који је подобан, довољан, који је у могућности да проузрокује одређене промене, оштећења у коришћењу или употребљивости рачунара или рачунарске мреже у целини или делимично. Судско веће у сваком конкретном случају мора утврдити шта су то компјутерски вируси, како се праве, које су њихове врсте и карактеристике, сврха и садржина. Такође, за постојање ове радње извршења потребно је да учинилац поступа са намером (као субјективним елементом) да тако створени рачунарски вирус унесе у туђи рачунар или рачунарску мрежу. Намера мора да постоји на страни учиниоца у време предузимања радње без обзира да ли је у конкретном случају она и остварена и 2) уношењу рачунарског вируса, непосредно или посредно, у туђи рачунар или рачунарску мрежу, без обзира ко је овај вируса направио. (Прља et al, 2011: 156).

Неопходну помоћ суду, односно судском већу у процесуирању овог кривичног дела могу да пруже вештаци информатичке струке. Ово дело се сматра свршеним самим моментом прављења оваквог вируса у намери да се он унесе у туђи рачунар или рачунарски систем, без обзира да ли се таква намера и остварила у конкретном случају (Стојановић et al: 2018: 232).

Извршилац дела може да буде свако лице, а у пракси су то лица која поседују посебна, специјална знања из области рачунарства и информатике. У погледу кривице потребан је директан умишљај који карактерише наведена намера. Уређаји и средства којима је учињено дело се обавезно одузимају применом мере безбедности одузимања предмета (Ђорђевић, 2014: 173-174).

За ово кривично дело алтернативно су предвиђене новчана казна или казна затвора до шест месеци.

Ако је пак, овако направљени вирус и унет у туђ рачунар или рачунарску мрежу чиме је проузрокована штета (било имовинска или неимовинска) ради се о тежем облику овог кривичног дела за које је прописана новчана казна или казна затвора од две године. Битно је да овако проузрокована штета представља резултат предузете радње основног дела и да у односу на њу учинилац поступа са нехатом (Стојановић, 2018: 910-911).

За успешно вођење кривичног поступка против извршилаца кривичног дела неопходно је прибавити следеће доказе (Прља et al, 2011: 156):

- утврдити време и место извршења кривичног дела,
- прибавити рачунарски вирус,
- одузети алате и уређаје помоћу којих је вирус направљен,
- установити начин на који је рачунарски вирус унет у туђи рачунар или мрежу и
- утврдити наступање штете.

3.1.5. Рачунарска превара (члан 301. КЗ)

Рачунарска превара је кривично дело које је прописано одредбама Кривичног законика Републике Србије, у групи кривичних дела против безбедности рачунарских података, чланом 301. КЗ. Такође, исто дело је предвиђено и одредбама Конвенције о високотехнолошком криминалу.

Дело се састоји у уношењу нетачног податка, пропуштању уношења тачног податка или на други начин прикривању или лажном приказивању податка чиме се утиче на резултат електронске обраде и преноса података у намери да се себи или другом прибави противправна имовинска корист и тиме проузрокује имовинска штета другом лицу (Јовашевић, 2014: 221-222).

Објект заштите је безбедност рачунарских система од уношења нетачних, неистинитих података и поверење у ове системе. Објект напада код рачунарске преваре представљају сами рачунари и рачунарски системи (Ђорђевић, 2014: 174).

Радња извршења се састоји из две алтернативно предвиђене делатности. То су: а) прикривање и б) лажно приказивање рачунарског податка. Прикривање је неуношење неког податка од стране лица које је обавезно да исти унесе у рачунар или рачунарску мрежу. Може се радити о било каквом податку. Лажно приказивање рачунарског податка постоји када се у рачунарској мрежи приказује, објављује, уноси или користи неистинити податак. Обе делатности морају бити предузете у односу на податак који је по свом значају, природи, карактеру, времену уношења или употребе такав да је подобан да утиче на резултат електронске обраде и преноса података у рачунарском систему (Урошевић et al, 2012: 51).

Било која од ових делатности у смислу кривичног дела мора бити предузета на законом одређен начин – уношењем нетачног, неистинитог податка у целини или делимично, пропуштањем да се унесе, неуношењем, неуписивањем каквог важног податка, или на други начин. Све делатности у смислу радње извршења овог кривичног дела морају бити предузете у одређеној намери – намери да учинилац за себе или другог прибави противправну имовинску корист. Та намера мора да постоји на страни учиниоца у време предузимања радње, али она у конкретном случају не мора бити и остварена (Стојановић, 2018: 911-912).

Последица дела је повреда која се огледа у проузроковању имовинске штете за друго физичко или правно лице, па и целу државу. Може се радити о штети у било ком износу која је у узрочно-последичној вези са предузетом радњом извршења без обзира да ли је оштећени власник или корисник рачунарске мреже (Јовашевић, 2014: 222)

Извршилац дела може да буде свако лице, а у погледу кривице потребан је директан умишљај који квалификује наведена намера. За ово дело прописана је новчана казна или казна затвора до три године.

Квалификовани облици овог дела постоје када је предузетом радњом извршења прибављена имовинска корист која прелази износ од 450.000 динара, за који је предвиђена казна затвора од једне до осам година, односно корист која прелази износ од 1.500.000 динара, за који је предвиђена казна затвора од две до десет година (Стојановић et al, 2018: 233).

Ово дело има и лакши, привилеговани облик који постоји када је дело учињено само у намери да се друго лице оштети, за који је прописана новчана казна или казна затвора до шест месеци (Јовашевић, 2014:222).

3.1.6. Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (члан 302. КЗ)

Кроз ово кривично дело, које је такође наведено у Конвенцији о високотехнолошком криминалу, иста настоји да изједначи, по третману, електронске комуникације са телефонским комуникацијама и, на овај начин, уводи инкриминацију пресретања електронске комуникације. У питању је неовлашћено пресретање приватних података који се преносе између два рачунарска система, садржинских

података о комуникацијама, али и о саобраћају укључујући ту и електромагнетну емисију са рачунара, који носи овакве податке. [48]

Кривично дело има основни и два тежа, квалификована облика испољавања.[49]

Први облик овог кривичног дела чини лице које се, кршећи мере заштите, неовлашћено укључи у рачунар или рачунарску мрежу, или неовлашћено приступи електронској обради података (Стојановић et al, 2018: 233).

Објект заштите овог кривичног дела јесте безбедност заштићених рачунара или рачунарске мреже, односно, података који се електронски обрађују. Објекат напада су заштићени рачунари, рачунарске мреже, односно подаци који се електронски обрађују.

Радња извршења основног облика је двојако одређена и састоји се у: 1) неовлашћеном укључивању у рачунар, кршењем мера заштите или у 2) неовлашћеном приступу електронској обради података. Рачунар је сваки електронски уређај који на основу програма аутоматски обрађује и размењује податке. Рачунарска мрежа се дефинише као скуп међусобно повезаних рачунара, односно рачунарских система који комуницирају размењујући податке. У оба случаја битно је да се радња предузима неовлашћено. Последица кривичног дела је неовлашћено укључивање или приступ заштићеном рачунару или рачунарској мрежи, односно употреба тако добијеног податка (Ђорђевић, 2014: 175-176).

Извршилац кривичног дела може бити свако лице, а у погледу виности потребан је умишљај. Извршилац мора имати свест да се врши неовлашћено укључење у рачунар или рачунарску мрежу, да се употребљава податак добијен на овакав начин и да, услед тога, могу наступити наведене последице (Лазаревић, 2006: 750).

За основни облик овог кривичног дела прописана је алтернативно новчана казна или казна затвора до шест месеци.

Тежи облик кривичног дела чини лице које предузимањем радње извршења основног облика дође у посед податка, па исти потом сними или употреби. За овај облик је прописана новчана казна или казна затвора до две године (Стојановић, 2018: 912-913).

Најтежи облик овог кривичног дела постоји када је услед предузимања радње извршења основног облика кривичног дела дошло до застоја или озбиљног поремећаја функционисања електронске обраде и преноса података или мреже или су настале

[48]http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legalisacion.pdf преузето 04.07.2018. године.

[49] Члан 302. Кривичног законика, *Сл. гласник РС*, бр. 85/2005, 88/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 и 94/2016.

друге тешке последице. За најтежи облик је прописана казна затвора до три године (Урошевић et al, 2012:52).

Ово кривично дело има интересантан савремени појавни облик испољавања који се јавља као крађа бежичне Интернет конекције. Облици напада на бежичне локалне мреже (WLAN) веома су широки простори за нападе на ове облике комуникација, неки од уобичајених су прислушкивање, анализа комуникационих саобраћаја, манипулација подацима, напади на клијенте вајерлеса, противправно одузимање и злоупотреба бежичног интернета, типовање оваквог места са којег се може бесправно користити ова услуга и сл. (Прља et al,2011: 176).

3.1.7. Спречавање и ограничавање приступа јавној рачунарској мрежи (члан 303. КЗ)

Ово кривично дело има основни и један тежи, квалификовани облик.[50] Основни облик дела чини лице које неовлашћено спречава или омета приступ јавној рачунарској мрежи.

Објекат заштите овог кривичног дела представља безбедност јавних рачунарских мрежа, доступних неограниченом броју лица, а које грађани користе у свакодневном животу за информисање, обављање финансијских трансакција, електронску трговину или одржавање друштвених контаката. Дакле, није реч само о Интернету, као глобалној мрежи, већ и о другим врстама мрежа – интранет, VPN и сл. Објект напада је јавна рачунарска мрежа (Стојановић, 2018: 913-914).

Радња извршења основног облика овог кривичног дела је двојако одређена као: 1) спречавање и 2) ограничавање приступа јавној рачунарској мрежи. Као рачунарска мрежа се дефинише скуп међусобно повезаних рачунара, односно рачунарских система који комуницирају размењујући податке.

Спречавање приступа јавној мрежи представаља потпуно онемогућавање другог лица да се користи јавној рачунарском мрежом, док се под ограничавањем подразумева свако отежавање приступа таквој мрежи.[51] Извршилац овог кривичног дела мора поступати неовлашћено, а уколико је постојао правни основ, тада не постоји ово

[50] Члан 303. Кривичног законика, *Сл. гласник РС*, бр. 85/2005, 88/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 и 94/2016.
[51] Члан 112. тачка 18. Кривичног законика, *Сл. гласник РС*, бр. 85/2005, 88/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 и 94/2016.

кривично дело. Последица кривичног дела се састоји у спречавању или ограничавању лица, тј. корисника да користе јавну рачунарску мрежу (Ђорђевић, 2014: 175).

Извршилац овог кривичног дела може бити свако лице које мора поступати са умишљајем. Кривично дело је свршено кад је од стране неког лица предузета било која радња којом се спречава или омета приступ јавној рачунарској мрежи, као и када дело изврши службено лице у оквиру вршења своје службене дужности, наравно, неовлашћено.

Квалификовани облик дела постоји ако радњу извршења основног овлика кривичног дела учини службено лице у вршењу службене дужности. Код овог кривичног дела квалификаторну околност представља својство извршиоца, које се у овом конкретном случају односи на службено лице које, вршећи своју службену дужност, преузме радњу извршења основног облика овог кривичног дела. Такође, за постојање тежег облика овог кривичног дела, потребно је да је радња извршења предузета неовлашћено – супротно закону и прописима службе (Стојановић et al, 2018: 234).

Што се тиче казни, за основни облик овог кривичног дела прописана је алтернативно новчана казна или казна затвора до једне године, док је за тежи облик прописана казна затвора до три године.

Један од најчешћих начина српечавања или ограничавања приступа јавној мрежи представљају такозвани DoS (енгл. Denial of service) и DDoS (енгл. Distribuited Denial of Service) напади. Организовању оваквих напада претходи стварање тзв. ботнета – мреже заражених рачунара, која настаје тако што се, помоћу одређеног малициозног софтвера, остварује контрола над великим бројем рачунара. Нападачи[52] претражују Интернет, проналазе рачунаре који нису адекватно заштићени и у њих убацују наведени софтвер. Број заражених рачунара може бити и неколико хиљада нпр. код DDoS напада. После преузимања контроле нападач издаје команду рачунарима у мрежи да на одређени сервер пошаљу велики број комуникационих захтева, чиме се саобраћај комуникационих портова, код рачунара жртве, загушује и тиме онемогућује приступ мрежи и услугама које она пружа (Прља et al, 2011: 180).

[52]То могу бити власници ових ботнетова, ботхерди креатори зломанерних софтверских програма који су створили ботнет, али и друга лица која закупљују услуге ботхерда.

3.1.8. Неовлашћено коришћење рачунара или рачунарске мреже (члан 304. КЗ)

Ово кривично дело има само један основни облик.[53] Дело чини лице које неовлашћено користи рачунарске услуге или рачунарску мрежу у намери да себи или другом прибави противправну имовинску корист (Стојановић et al, 2018: 235).

Објект заштите код овог кривичног дела представља безбедност рачунара или рачунарске мреже од неовлашћеног коришћења, док је објект напада рачунар или рачунарска мрежа (Ђорђевић, 2014: 176).

Радња кривичног дела одређена је као неовлашћено коришћење рачунарских услуга или рачунарске мреже. Ово је сувише широко постављена формулација, што може довести до значајних злоупотреба.

Рачунар је сваки електронски уређај који на основу програма аутоматски обрађује и размењује податке. Рачунарска мрежа се дефинише као скуп међусобно повезаних рачунара, односно рачунарских система који комуницирају размењујући податке. У оба случаја битно је да се радња предузима неовлашћено. Последица кривичног дела се састоји у угрожавању безбедности рачунара или рачунарске мреже (Стојановић, 2018: 914-915).

Извршилац може бити свако лице, а у погледу виности потребан је умишљај. За постојање овог кривичног дела је неопходно утврдити и намеру извршиоца да себи или другом прибави противправну имовинску корист. (Лазаревић, 2011: 751).

За ово дело запрећена је новчана казна или казна затвора до три месеца. Такође, предвиђено је да се гоњење за ово дело предузима по приватној тужби.

И у случају овог кривичног дела овлашћена службена лица дужна су да предузму радње из своје надлежности и да прикупе потребне доказе, уколико постоје основи сумње да је радњом извршења уз ово кривично дело извршено и неко друго кривично дело за које се гоњење предузима по службеној дужности. У том случају се и за ово кривично дело примењују овлашћења и одредбе које се односе на подношење кривичне пријаве (Прља et al, 2011: 182).

Овде треба указати и на обавезу да се оштећеном, и у случају извршења кривичног дела које се не гони по службеној дужности, учине доступним подаци о

[53] Члан 304. Кривичног законика, *Сл. гласник РС*, бр. 85/2005, 88/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013 и 108/2014.

извршиоцу како би се могло остварити гоњење по приватној тужби. Такође, може се размотрити и случај у којем се користи бежична интернет локална мрежа WLAN са постојећом фабричком заштитом у којој је и корисничко име и шифра исто. У овим познатим случајевима заштита постоји, али је она позната скоро већини људи, па се са основом поставља питање њене сврхе, као и значаја (Прља et al, 2011: 182).

3.1.9. Прављење, набављење и давање другом средстава за извршење кривичних дела против безбедности рачунарских података (члан 304а. КЗ)

Кривично дело прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских податакаје промењено најновијим изменама Кривичног законика из 2016. године[54], према којим ово дело чини свако лице које производи, продаје, набавља ради употребе, увози, дистрибуира и на други начин ставља на располагање уређаје и рачунарске програме пројектоване или првенствено ради извршења неког од кривичних дела против безбедности рачунарских података из члана 298. до 303. Кривичног законика, као и рачунарске шифре или сличне податке путем којих се може приступити рачунарском систему као целини или неком његовом делу са намером да буде употребљен у извршењу неког од кривичних дела из чл. 298. до 303. КЗ (Стојановић, 2018: 915).

Објект заштите је безбедност рачунарских система и података. Као објект напада могу се јавити: 1) одређени уређаји, 2) рачунари, 3) рачунарски програми, 4) рачунарске шифре и 5) слични подаци путем којих се може приступити рачунарском систему као целини или неком његовом делу.

Радња извршења јесте производња, продаја, набављање ради употребе, увоз, дистрибуирање или стављање на располагање на други начин одређених средстава ради извршења кривичних дела из чл. 298. до 303. КЗ. То су уређаји и рачунарски програми који су направљени искључиво или претежно у сврху извршења неког кривичног дела против безбедности рачунарских података. На овај начин је Закон о изменама и допунама КЗ[55] из 2016. годинене само, у већој мери, ускладио ово кривично дело с Конвенцијом о високотехнолошком криминалу, већ је прецизније одредио објект радње извршења (Стојановић, 2018: 916). Производња јесте процес у коме се на основу одређених компоненти и сировина као улазних материја добија као финални продукт

[54] *Сл. гласник РС*, бр. 94/2016.
[55] *Сл. гласник РС*, бр. 94/2016.

неки произво. Продаја је замена одређених предмета у замену за новац или неки други вид надокнаде (Јовашевић, 2014: 223). Набављање је долажење у посед предмета на било који начин, са накнадом или без накнаде, на дозвољени или недозвољени начин. Увоз је долажење у посед неких предмета који доспевају из неке друге државе у матичну државу. Дистрибуирање је процес допремања одређених предмета другим произвођачима ради њихове продаје, а стављање на располагање другом на употребу представља помагање, омогућавање другом лицу да дође у посед ових предмета (Ђорђевић, 2014: 176).

За постојање дела битно је да се радња извршења предузима у односу: а) уређаје, рачунаре, рачунарскепрограме, рачунарске шифре или сличне податке путем којих се може приступити рачунарском систему у целини, или неком његовом делу и б) у одређеном циљу – ради извршења неког од кривичних дела против безбедности рачунарских података, без обзира да ли је неко од ових кривичних дела уопште извршено или покушано. Такође, веома је битно овде напоменути да је код последње врсте објекта напада, а то су рачунарске шифре или слични програми помоћу којих се може нарушити безбедност рачунарских система, да је неопходно да буде испуњен и субјектибни елемент, а то је да намера учиниоца да их употреби ради извршења неког кривичног дела из чл. 298. до 303. КЗ. Овај услов је постављен из разлога што није реч о програмима и уређајима који су првенствено, по својој улози направљени и намењени за извршење неког од ових кривичних дела. (Стојановић et al, 2018: 236).

Извршилац дела може да буде свако лице, а у погледу кривице потребан је умишљај.

За ово кривично дело прописана је казна затвора у трајању од од шест месеци до три године.

Такође ово кривично дело има и други, лакши облик, који постоји онда када неко лице само поседује нека од средстава извршења првог облика овог кривичног дела, у намери да их употреби у сврху извршења неког од кривичних дела из чл. 298. до 303. КЗ. Радња извршења овог облика састоји се само у поседовању наведених предмета. Поседовање је фактичка, државинска власт над стварима. Поред тога, битан је и субјективни елемент, који се састоји у намери да се ова средства и предмети употребе у сврху извршења неког од кривичних дела против безбедности рачунарских података.

За лакши облик кривичног дела присана је алтернативно новчана казна или казна затвора до једне године (Стојановић, 2018: 916).

Уз казну суд обавезно изриче и меру безбедности одузимања предмета. (Јовашевић, 2014: 223).

Прво кривично дело овог облика рачунарског криминала у Републици Србији је откривено и расветљено 11. марта 2011. године по званичном саопштењу Министарства унутрашњих послова Републике Србије (Прља et al, 2011: 184).[56] На овај начин, законодавац је омогућио кривичноправну заштиту платних картица, али и свих других објеката кривичних дела из групе кривичних дела против безбедности рачунарских података чиме је уједно извршио и инкриминацију припремних радњи за вршење ових кривичних дела, и то посебно кривичних дела која у себи носе елементе крађе идентитета (Прља et al, 2011: 184).

3.2. Најзначајнија кривична дела против интелектуалне својине

Кривична дела против интелектуалне својине представаљају значајну групу кривичних делачије предвиђање у Кривичном законику, у глави двадесет, као кривична дела против интелектуалне својине,[57] има за циљ кривичноправну заштиту интелектуалне својине као једног од основних права човека које је утврђено Уставом (члан 73.), а чија је заштита регулисана већим бројем закона и других прописа који одређују ову материју (Урошевић et al, 2012: 52).

У кривична дела у надлежности Одељења за борбу против високотехнолошког криминала спадају ова дела само када се: а) као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, као и њихови производи у материјалном или електронском облику, б) ако број примерака ауторских дела прелази 2.000 и в) ако настала материјална штета прелази износ од 1.000.000 динара.

[56] Припадници Министарсва унутрашњих послова, односно Службе за борбу против организованог криминала су у сарадњи са Вишим јавним тужилаштвом у Београду лишили су слободе АА из Суботице због постојања основа сумње да је извршио следећа кривична дела против безбедности рачунарских података: прављење и уношење рачунарских вируса, рачунарска превара и прање новца. АА је путем Интернета претходно купљени компјутерски вирус, који је сачувао на серверу који је закупио, унео у преко хиљаду рачунара широм света стварајући ботнет мрежу. АА је затим путем заражених рачунара којима је управљао са свог сервера на торент сајтовима постављао заражене фајлове које је представљао као филмове, који су даље упућивали на рекламу за интернет страницу коју је направио АА, како би преко њега преузимали наводно филмове, АА је за ову услугу преко једне канадске компаније коју је довео у заблуду тим путем за девет месеци наплатио преко свог девизног рачуна износ од преко 70.000 америчких долара, знајући да та средства потичу од недозвољене рачунарске мреже сачињене од заражених рачунара којима је осумњичени управљао.

[57] *Сл. гласник РС*, бр. 85/2005, 88/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 и 91/2016.

Кривична дела из ове групе се могу сврстати у две групације, у зависности од објекта заштите, и то на:

a) Кривична дела против ауторских права:
- повреда моралних права аутора и интерпретатора и
- неовлашћено уклањање или мењање електронске информације о ауторском или сродним правима.

b) Кривична дела неовлашћеног коришћења туђе интелектуалне својине:
- неовлашћено искоришћавање ауторског дела или предмета сродног права,
- повреда проналазачког права и
- неовлашћено коришћење туђег дизајна.

Из ових решења произилази да су усклађене кривичноправна и материјалноправна заштита ауторских права, јер се по Закону о ауторским и сродним правима[58] ауторским делима сматрају „нарочито рачунарски програми у било којем облику њиховог изражавања, укључујући и припремни материјал за њихову израду, затим музичка дела са или без речи и припремни материјал за њихову израду, затим музичка дела са или без речи, као и филмска дела.[59]

3.3. Кривична дела против имовине

У склопу првих измена Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала[60] из 2009. године у исти у уврштена, и непрактично изостављена, кривична дела против имовине.[61]

У тој групи најинтересантнија су следећа дела:
- Превара;
- Изнуда.

[58] *Сл. гласник РС*, бр. 104/2009, 99/2011 и 119/2012.
[59] Члан 2. Закона о ауторским и сродним правима. *Сл. гласник РС*, бр. 104/2009, 99/2011 и 119/2012.
[60] Службени гласник РС, бр. 104/2009.
[61] У погледу надлежности Одељења за борбу против ВТК важе исти, општи услови као и за дела против интелектуалне својине.

3.4. Кривична дела против привреде

Кривична дела против привреде су изразито опасна по стабилност економског система и управо зато се овим кривичним дела посвећује посебна пажња. Утицај криминалаца у овој области изразито је видљив и рачуна се у милијардама евра на глобалном нивоу. Електронска трговина и банкарство све су израженије активности на интернету и данас се криминалне делатности све више селе у ту област (Урошевић et al, 2012: 74).

Из области привредног криминалитета, за сузбијање високотехнолошког криминала посебно су значајна следећа кривична дела:

- фалсификовање и злоупотреба платних картица,
- прање новца и
- неовлашћена употреба туђег пословног имена и друге посебне ознаке робе или услуга.

3.5. Кривична дела против полне слободе

Из групе кривичних дела против полне слободе у област високотехнолошког криминала спадају следећа кривична дела:

- приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију,
- навођење малолетног лица на присуствовање полним радњама и
- искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу.

3.6. Кривична дела против опште сигурности људи и имовине

Општа сигурност људи и имовине основни је задатак у раду свих полиција света. Управо у ери информационих технологија многи уређаји су директно везани за информационо комуникационе технологије и у великој мери зависе од интернета. То је управо и разлог због којег је високотехнолошки криминал веома брзо ушао и у ову сферу (Урошевић et al, 2012: 81).

Из ове групе се као кривично дело за које може бити надлежно одељење за борбу против високотехнолошког криминала издваја кривично дело:

- уништење и оштећење јавних уређаја.

3.7. Кривична дела против уставног уређења и безбедности републике Србије

Ова кривична дела могу бити предмет разматрања у оквирима високотехнолошког криминала због начина извршења или употребљених средстава, али са политичком намером – намером угрожавања уставног уређења и безбедности Републике Србије. У ову групу кривичних дела спадају:

- напад на уставно уређење,
- позивање на насилну промену уставног уређења,
- шпијунажа и
- одавање државне тајне.

3.8. Кривична дела против човечности и других добара заштићених међународним правом

Из ове групе кривичних дела се као кривично дело које може бити обухваћено облашћу високотехнолошког криминала издваја кривично дело расна и друга дискриминација (Прља et al, 2011: 190).

IV ПРЕВАРА КАО КРИВИЧНО ДЕЛО ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛИТЕТА

4.1. Опште карактеристике кривичног дела преваре

Превара је кривично дело из групе кривичних дела против имовине, које је уведено као још једно од могућих кривичних дела која могу бити предмет поступања Одељења за борбу против високотехнолошког криминала, и то први пут изменама Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала[62] 2009. године, заједно са кривичним делом изнуде. Кривично дело превара је прописано одредбом Кривичног законика Републике Србије, у члану 208.

Кривично дело преваре чини лице које, у намери да себи или другом прибави противправну имовинску корист, доведе у заблуду друго лице лажним приказивањем или прикривањем чињеница, или га одржава у заблуди и тиме га наведе да овај на штету своје или туђе имовине нешто учини, не учини или трпи.[63]

Објект заштите код овог кривичног дела је безбедност имовине лица које се доводи у заблуду или одржава у заблуди, или неког другог лица. Објект напада јесте имовина поменутог или неког другог лица. Под имовином се, у најопштијем смислу, подразумева скуп добара која припадају одређеном субјекту.

Радња основног облика кривичног дела је навођење другог лица да учини, не учини нешто или трпи на штету своје или туђе имовине. Навођење представља стварање или учвршћивање, већ постојеће, одлуке код другог, да предузме неку активност, односно, да се уздржи од тога и, оно мора бити усмерено на имовину. Услов за постојање овог кривичног дела јесте да је оштећени под утицајем погрешно створене представе о некој чињеници нешто учинио, или пропустио да учини, односно нешто трпео чиме је нанео штету својој или туђој имовини. За доказивање овог дела неопходно је утврдити и намеру извршиоца кривичног дела, која се састоји у прибављању себи или другом противправне имовинске користи или, за привилеговани облик, само наношење штете другоме (Ђорђевић, 2014: 99).

---

[62] *Сл. гласник РС*, бр. 61/2005 и 104/2009.

[63] Члан 208. Кривичног законика, *Сл. гласник РС*, бр. 85/2005, 88/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 и 94/2016.

Та радња извршења се предузима на законом одређени начин: а) лажним приказивањем, саопштавањем или б) прикривањем чињеница које су од значаја на доношење одређене одлуке пасивног субјекта.

Извршилац кривичног дела може бити свако лице, које мора поступати са директним умишљајем, с обзиром на то да намера која је основни елемент бића није остварива у другим облицима виности (Лазаревић, 2006: 585).

За основни облик дела запрећена је новчана казна или казна затвора од шест месеци до пет година.

Осим основног, постоји и привилегован (лакши) облик овог кривичног дела. Ово дело постоји када је извршилац преузео радњу извршења основног облика дела само с намером да другог оштети, а не и да прибави било какву имовинску корист (субјективни елеменат). Битно је да на страни учиниоца постоји умишљај у погледу наношења штете другом лицу. Поред тога, потребно је да је другом лицу нанета штета у износу до 15.000 динара (објективни елеменат). За привилеговани облик преваре је запрећена новчана казна или казна затвора до шест месеци (Ђорђевић, 2014: 100).

Поред наведених, кривично дело преваре има такође и два квалификована, тј. тежа облика, која су одређена висином прибављене противправне имовинске користи извршењем основног облика кривичног дела. Код првог тежег облика ради се о прибављеној имовинској користи, односно проузрокованој штети која прелази износ од 450.000 динара, за шта је прописана кумулативно новчана казна и казна затвора од једне до осам година. Код другог, најтежег облика дела, ради се о прибављеној имовинској користи или проузрокованој имовинској штету у износу од преко 1.500.000 динара, за шта је прописана новчана казна и казна затвора од две до десет година.

Специфичност на којој се заснива надлежност органа у области високотехнолошког криминала јавља се код преваре која је у вези са рачунарима, рачунарским системима и мрежа. Интернет представља нову област деловања извршилаца кривичних дела, који на преваран начин остварују имовинску корист. Та глобална мрежа је ново оружје у рукама криминалаца за вршење класичних облика кривичних дела, дајући им нова средства за прикривање извршилаца, за олакшавање проналаска жртава, вишеструко и вишезначно олакшавање варања, за прикривање преваре. Искоришћавање интернета створило је неограничене могућности за вршење различитих кривичних дела чинећи доступним неограничен број потенцијалних жртава и, скоро у потпуности, елиминисало трошкове неопходне за организовање овог кривичног дела (Урошевић et al, 2012: 72).

Извршиоци се у овом случају служе погодностима које им пружа интернет, скоро потпуну анонимност, као и чињеницом да је дигиталне финансијске токове, који обично воде преко више држава, веома тешко пратити и утврдити крајњу дестиннацију средстава. Социјални профили оштећених се веома разликују, а жртва преваре извршене путем интернета може постати готово свако лице. Због тога је неопходно увек бити на опрезу, јер извршиоци оваквих кривичних дела усавршавају начине обављања својих криминалних активности, прилагођавајући се најразличитијим условима и новостима на свом "тржишту" чиме мењају циљне групе свог деловања, у зависности од сопствених потреба и могућности. У том смислу, значајно је да и држава предузме све што је могуће на спречавању догађања ове врсте превентивним акцијама и обраћањем широј јавности са указивањем на могућности заштите различитих група, могућих мета оваквих кривичних дела, као и пружањем смерница оваквим фокус групама како да поступају у датим околностима.

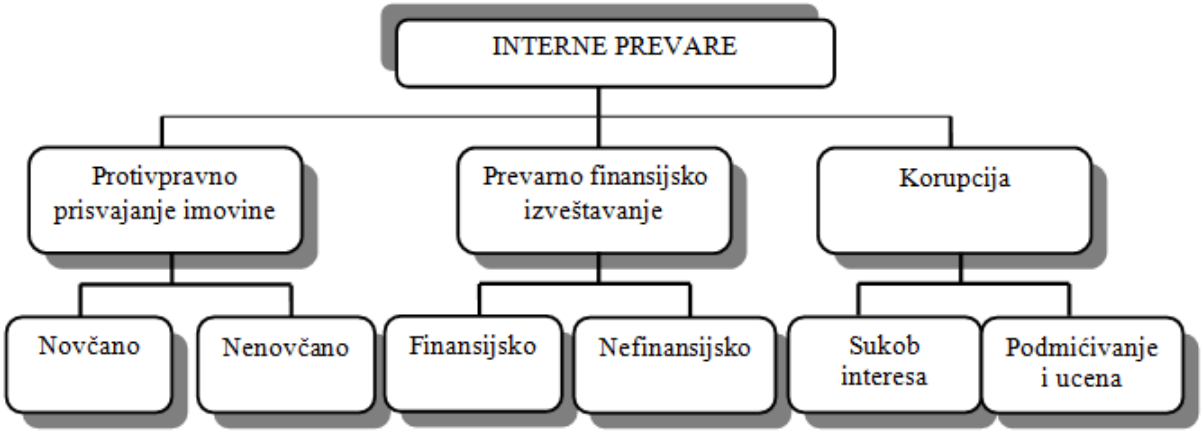
Групе извршилаца оваквих кривичних дела су веома добро организоване, специјализоване за одређене регионе, а да би интернет преваре биле успешне, служе се најразличитијим методама за прибављање података о потенцијалним жртвама и склапање њиховог социјалног профила. Најбољи извор информација представљају сами оштећени, који посетом лажним рекламним интернет сајтовима или одговором на посебну врсту рекламних и електронских порука (spam) остављају своје личне податке, а на основу прикупљених материјала се прави механизам преваре.

У овом смислу значај оштећених, али и њиховог страха и стида, и потребу за хитним поступањем препознали су у САД где је уведена онлајн могућност пријављивања на интернет сајту IC3[64], без страха да ће неко открити њихов идентитет, осим примаоца пријаве, да ће бити осрамоћени или да ће процес пријављивања трајати дуже од неколико секунди. С друге стране, они на овај начин остварују скоро тренутним увид у разноврсност и променљивост овог облика криминалитета, па могу лакше и брже да обавештавају ширу општу, али и стручну јавност о појавним облицима превара и тако остваре ширу превенцију (Прља et al, 2011: 47).

Joseph T. Wells, оснивач и председник Удружења овлашћених испитивача преваре – ACFE, потврђује да је појам малверзације или преваре много шири од појма криминалних радњи. Он указује и на то да малверзације у ширем смислу могу обухватити било коју криминалну радњу да би се стекла корист која употребљава

[64]http://www.ic3.gov/. Преузето дана 08.07.2018. године.

обману као основни начин извршења. Међутим, иако су преваре или малверзације шири појам (категорија) од појма криминалних радњи, оне се исто тако морају разврставати и класификовати у посебне подгрупе. Потреба овакве класификације јавља се првенствено због интерних превара на које се до пре неколико година и није обраћала пажња као што су преваре унутар ентитета које могу проузроковати велику штету том истом ентитету. Да постоје различите врсте интерних превара најбоље потврђује следећа слика (Влаовић Беговић, Томашевић, 2016: 91-92).



Слика 1. Типови интерних превара[65]

Листа Федералне комисије за трговину од класичних 12 превара (Урошевић et al, 2012: 73) садржи:

- лажне пословне прилике,
- ланчана писма,
- преваре са радом у кући,
- здравствене и дијеталне преваре,
- лаке прилике за зараду,
- бесплатна роба,
- прилике за инвестиције,
- преварне масовне електронске поруке,
- пакети за дешифровање сигнала кабловске телевизије,
- гарантовани кредити или зајмови,
- промотивне понуде наградних путовања и
- преваре у вези са побољшањем кредитних способности.

[65] Извор: Влаовић Беговић, С., Томашевић С., *Одговорност ревизора за откривање рачуноводствених превара*, Школа бизниса, 1/2016, стр. 92.

Лажне пословне прилике подразумевају понуде и обећања прилика за зараду веће количине новца, уз веома мало труда. Уобичајено садрже бомбастичне крилатице, као на пример: „Будите свој шеф, одредите себи време за рад, радите само неколико часова недељно, радите од куће“. Те врсте превара у предмету често садрже:

- остварите регуларни приход кроз онлајн аукције,
- обогатите се, кликните,
- оставите свој рачунар да зарађује новац за Вас,
- искористите интернет да зарадите и
- *eBay Insider Secrets Revealed 6228*.

Такве преваре, у ствари, представљају пирамидалне шеме за преваре. Пре или касније ова превара се открива од стране државних органа, жртве се тада повлаче, па и превара престаје. За такве се преваре обично каже да изгледају превише добро да би биле истините.

Ланчана писма – код ове врсте превара које су познате и на простору Републике Србије, али не у виртуелном окружењу, већ у стварности и заснива се на сујеверју, које је веома присутно у народу и рачуна се на вероватне, компулзивне потезе преварених. Нарочито су значајне нове врсте оваквих превара присутне у окружењу социјалних мрежа. Такве преваре са собом носе карактеристике и елементе других кривичних дела, на пример црве увезане у линк који нуде у поруци или уношење неког злонамерног програма обавезног за читање дате поруке и сл.

Преваре “еликсира живота и здравља” као и “дијеталне преваре” користе несигурност људи у сопствено тело и здравствене околности. Таква стања жртве чине веома подложним и сугестибилнима за преваре. И остали облици преваре слично изгледају – увек је то превише лепо да би било стварно (Прља et al, 2011: 48).

4.2. Рачунарска превара као кривично дело

Рачунарска превара је кривично дело које је прописано одредбамаКривичног законика Републике Србије, у групи кривичних дела против безбедности рачунарских података, чланом 301. КЗ. Такође, исто дело је предвиђено и одредбама Конвенције о високотехнолошком криминалу.

Дело се састоји у уношењу нетачног податка, пропуштању уношења тачног податка или на други начин прикривању или лажном приказивању податка чиме се утиче на резултат електронске обраде и преноса података у намери да се себи или

другом прибави противправна имовинска корист и тиме проузрокује имовинска штета другом лицу (Јовашевић, 2014: 221-222).

Објект заштите је безбедност рачунарских система од уношења нетачних, неистинитих података и поверење у ове системе. Објект напада код рачунарске преваре представљају сами рачунари и рачунарски системи.

Радња извршења се састоји из две алтернативно предвиђене делатности. То су: а) прикривање и б) лажно приказивање рачунарског податка. Прикривање је неуношење неког податка од стране лица које је обавезно да исти унесе у рачунар или рачунарску мрежу. Може се радити о било каквом податку. Лажно приказивање рачунарског податка постоји када се у рачунарској мрежи приказује, објављује, уноси или користи неистинити податак. Обе делатности морају бити предузете у односу на податак који је по свом значају, природи, карактеру, времену уношења или употребе такав да је подобан да утиче на резултат електронске обраде и преноса података у рачунарском систему (Стојановић et al, 2018: 234).

Било која од ових делатности у смислу кривичног дела мора бити предузета на законом одређен начин – уношењем нетачног, неистинитог податка у целини или делимично, пропуштањем да се унесе, неуношењем, неуписивањем каквог важног податка, или на други начин. Све делатности у смислу радње извршења овог кривичног дела морају бити предузете у одређеној намери – намери да учинилац за себе или другог прибави противправну имовинску корист. Та намера мора да постоји на страни учиниоца у време предузимања радње, али она у конкретном случају не мора бити и остварена (Ђорђевић, 2014: 174-175).

Последица дела је повреда која се огледа у проузроковању имовинске штете за друго физичко или правно лице, па и целу државу. Може се радити о штети у било ком износу која је у узрочно-последичној вези са предузетом радњом извршења без обзира да ли је оштећени власник или корисник рачунарске мреже (Јовашевић, 2014: 222)

Извршилац дела може да буде свако лице, а у погледу кривице потребан је директан умишљај који квалификује наведена намера. За ово дело прописана је новчана казна или казна затвора до три године (Стојановић, 2018: 911).

Квалификовани облици овог дела постоје када је предузетом радњом извршења прибављена имовинска корист која прелази износ од 450.000 динара, за који је предвиђена казна затвора од једне до осам година, односно корист која прелази износ од 1.500.000 динара, за који је предвиђена казна затвора од две до десет година.

Ово дело има и лакши, привилеговани облик који постоји када је дело учињено само у намери да се друго лице оштети, за који је прописана новчана казна или казна затвора до шест месеци (Јовашевић, 2014: 222).

Намера законодавца је да прописивањем овог кривичног дела заштити веродостојност и интегритет података, који се електронски обрађују или се врши њихово преношење електронским путем. Као неопходни елемент бића овог кривичног дела потребно је утврдити, у сваком конретном случају, и намеру учиниоца да за себе или другог прибави противправну имовинску корист и да, тиме, другом проузрокује имовинску штету.

За правну квалификацију кривичног дела рачунарска превара и његово успешно доказивање неопходно је утврдити време и место извршења кривичног дела, тачну радњу која је предузета, као и начин и средство којим је унет нетачан податак.[66] У погледу унетих података потребно је установити њихову неистинитост, у чему се та неистинитост огледа, и како је, тиме, податак утицао на резултат електронске обраде и преноса података, затим уколико је у питању пропуштање уноса тачног податка, на који начин је то пропуштено, односно на који други начин је прикривен или лажно приказан податак, а све у циљу утицања на резултат обраде и преноса података.

У вези овог питања потребно је утврдити начин уношења податка (или уколико је пропуштено његово уношење), да ли је то учињено путем физичког приступа уређају подобном за електронски пренос или обраду података или је то учињено путем мреже. Неопходно је утврдити који је софтвер био коришћен, као и колики је износ имовинске користи био обухваћен умишљајем учиниоца, наравно и висину износа наступеле штете, па и у случајевима да корист и није остварена. За доказивање дела из става 4. потребно је утврдити врсту штете која је била обухваћена намером учиниоца и њено наступање, као и постојање намере учиниоца да својим деловањем проузрокује такву штету. Потребно је, такође, утврдити којим је средствима извршено кривично дело и уколико је могуће, извршити њихово одузимање како би били обезбеђени сви неопходни докази (Прља et al, 2011: 173).

Електронска обрада података и очување њеног интегритета и веродостојности су од изузетног значаја за сваку државу, нарочито због тога што електронско пословање постаје доминантан вид активности привредних субјеката и државних органа. Пословне

[66] У Немачкој употреба податка у преварне сврхе, на пример, трансфера средстава са банкарског рачуна употребом хакерски прибављених података представља посебан облик преваре, у овом случају рачунарске преваре из чл. 263 Казненог закона Немачке (Прља et al, 2011: 172).

трансакције које се обављају електронским путем нарочито су погодне за разне видове злоупотреба, а са растом њиховог обима повећава се број кривичних дела из те области, а последице постају све теже. Овим кривичним делом могу бити погођени сви привредни субјекти од великих корпорација и државних предузећа, банака, до најмањих попут књиговодствених фирми или спортских кладионица. У овој области од значаја је и примена Закона о електронској трговини.[67]

4.3. Нигеријска превара

Појава интернета, као и све већа, глобално распрострањена употреба информационих и телекомуникационих технологија, утицала је на пораст илегалних активности у сајбер простору. Употреба рачунарских сервера који пружају опције анонимног коришћења интернета, могућност отварања Web електронске поште и коришћења лажних електронских адреса, постављање лажних интернет сајтова и др., данас су основно оруђе у рукама извршилаца кривичних дела превара које се врше помоћу савремених информационих технологија.

„Преваре 419“ као облик кривичних дела превара које се врше уз помоћ рачунара данас су постале честа и распрострањена појава, која је од стране многих полицијских служби широм света означена као велика опасност по финансијску безбедност, како појединаца, тако и држава. Од стране многих организација 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.[68]

Као специфичан облик преваре који има међународне размере и који изазива оштећења која се могу исказати стотинама милиона америчких долара, „нигеријска превара“ заслужује посебну пажњу и посебну анализу.

Грађани Републике Србије који су корисници интернета, као и државне институције, јавне установе и предузећа са територије Републике Србије у којима се користи интернет у пословању, изложени су ризику који је настао као последица деловања тих криминалних група.

---

[67] *Сл. гласник РС*, бр. 41/2009.

[68] http://en.wikipedia.org/wiki/Advance-fee_fraud. преузето 20.07.2018. године.

4.3.1. Појам нигеријске преваре

„Нигеријска превара“, или превара позната под називом „превара 419“, појавила се раних 80-тих година прошлог века, са наглим економским развојем Републике Нигерије, који се заснивао на употреби нафтних ресурса. Неколико незапослених студената са нигеријског универзитета почело је у раним 80-тим и средином 90-тих да употребљава методе те преваре како би довели у заблуду пословне људе са Запада који су били заинтересовани за „тајанствене“ послове у нигеријском нафтном сектору, а касније су те методе почели да употребљавају и на широј популацији. У току прве деценије 21-ог века „превара 419“ постала је популаран начин извршења кривичних дела преваре у Африци, Азији и Источној Европи, а у последње време и у Северној Америци, Западној Европи (углавном Великој Британији) и Аустралији (Урошевић, 2009: 2).

„Превара 419“, као израз за „нигеријску превару“, добила је назив по члану број 419 *Нигеријског кривичног закона* (који је део поглавља 38) под називом „Прибављање имовине помоћу преварних радњи: Превара“, који дефинише ово кривично дело (Chawki, 2009: 2). Америчко друштво за дијалектику је утврдило да се израз „превара 419“ користи од 1992. године.

„Нигеријска превара“ је метода вршења кривичног дела преваре уз помоћ рачунара. Њено извршење најчешће почиње писмом или електронском поруком којаје тако осмишљена да изгледа као да је намерно послата примаоцу поруке. Радња извршења „нигеријске преваре“ углавном почиње убеђивањем „жртве“ преваре да учествује у подели одређених новчаних фондова под условом да унапред уплати одређени новчани износ који је, у највећем броју случајева, неупоредиво мањи од оног износа који би требало да добије као корист одтог фонда (Smith et al. 1999: 1).

Електронском поруком (најчешће SPAM поруком) од примаоца поруке се тражи помоћ за трансфер великих новчаних износа, за који ће након обављеног трансфера добити одређени проценат као надокнаду. У таквим порукама се нпр. наводи да је:

- реч о великој суми новца која је позната само пошиљаоцу поруке, и да он чека да буде исплаћена као резултат одређених банкарских малверзација и сл.,
- пошиљалац поруке је члан нигеријске владе или нигеријске војске који покушава да изнесе већу количину новца из Нигерије, али му је за то потребна помоћ из иностранства,

- пошиљалац поруке спреман да новац подели са оним ко му помогне да изврши трансфер одређене суме новца (нпр. прање новца) и
- тајност посла је апсолутна потреба, пошто би корумпирани званичници Нигерије присвојили новац за себе уколико би сазнали да он постоји (Buchanan et al. 2001: 40).

4.3.2. Начин извршења нигеријске преваре

Извршиоци кривичног дела преваре шаљу електронске поруке корисницима интернета, са намером да понуде неки примамљив посао у нади да ће жртва преваре на крају уплатити одређени износ новца на име његове реализације (нпр. разне измишљене надокнаде за ангажовање стручних лица или адвоката, за издавање потребних дозвола за реализацију посла, уплата административних такси и друго). Те електронске поруке насловљене су генерално на било ког примаоца поруке. Из њих се не може видети коме се пошиљалац обраћа, а њихов контекст је такав да прималац поруке лако може помислити да се порука односи управо на њега.

Уколико жртва преваре одговори на прву поруку, она се методом социјалног инжењеринга наводи да помисли да је њена помоћ неопходна да би се одређена радња извршила (нпр. трансфер новца, уручивање наследства и др.).[69] Детаљи у порукама могу да се разликују, али садржина самог писма које стиже жртвама преваре најчешће се односи на то да лице које је наводни пошиљалац поруке није у могућности да само изврши одређене радње, те да му је зато потребна помоћ примаоца поруке. Лица која се наводе у тим порукама најчешће стварно постоје, али су њихови идентитети украдени без њиховог знања и тако се користе неовлашћено од стране извршилаца кривичних дела како би се прикрио њихов прави идентитет, или како би се снагом ауторитета одређених лица улило поверење жртвама преваре и придобило њихово поверење (Урошевић, 2009: 4).

У тим порукама помињу се суме новца које се крећу и до неколико милијарди америчких долара, затим злато, „прљав“ новац на банковним рачунима, „крвави

[69]Социјални инжињеринг је акт манипулације којим се људи наводе да одају поверљиве информације о себи. Та техника заснива се на ометању пажње одређеног лица у циљу прикупљањаинформација које оно иначе не би одало, а како би се ти подаци касније злоупотребили (радиодавања корисничких имена, лозинки или, нпр. података о платним картицама). Све методе социјалног инжињеринга заснивају се на специфичним правилностима у процесу доношењаодлука, познатијем као „погрешна когниција“, која представља образац неправилног просуђивања људи који се појављују у одређеним, специфичним ситуацијама (Прља et al, 2011: 57).

дијаманати“, серије чекова и др. Суме новца укључују милионе долара које ће наводни инвеститори на крају посла поделити са жртвом преваре, а проценат зараде који се обећава креће се и до 40 % од суме новца која је предмет „посла“.

Већина прималаца ових електронских порука на те поруке најчешће не одговара (пошто знају да се ради о врсти преваре), а Интернет сервис провајдери их приликом филтрирања на својим серверима најчешће одвајају, и пре него што дођу до крајњих корисника, помоћу “црних листа” у оквиру којих се за анализу и елиминацију користе ажурирани спискови IP адреса са којих се електронске поруке најчешће пристижу. Мали проценат корисника ипак прима овакве поруке, које пролазе кроз филтере Интернет сервис провајдера, чиме се ствара могућност да они ступе у контакт са извршиоцима кривичних дела. То је довољно да “идејни творци” ових превара шаљу милионе електронских порука, пошто рачунају да ће један мањи проценат корисника ступити у контакт са њима, након што их прочита.

Овде је модус извршилаца такав да циљају на неодређене жртве, без неких специфичних карактеристика. Насупрот томе, постоје и циљане клопке чији је модус карактеристичан за друге облике кривичних дела као нпр. код циљаног (спир) фишинга (Прља et al, 2011: 58).

Оштећена лица се методама социјалног инжењеринга при комуникацији наводе да уплате један мали проценат од укупне суме новца која је предмет „посла“. Уплату тих новчаних износа извршиоци кривичних дела траже како би се нпр. надокнадили одређени трошкови које сноси неко измишљено лице (нпр. трошкови подмићивања, накнаде у банкама, трошкови адвоката и др.) да би дошли до предметног новца.

Највећи број извршилаца ових кривичних дела припада мањим организованим криминалним групама, али се понекад дешава да извршиоци функционишу и самостално. Уколико извршиоци кривичних дела нису добро организовани, онда не могу да изврше преваре већих размера и на тај начин оштете веће компаније, али су јако опасни за средњу класу грађана и мала предузећа.

Ако жртва преваре пристане на понуђени „посао“, извршиоци кривичних дела јој шаљу један или више фалсификованих докумената са лажним печатима, потписима, лажном садржином и сл. Извршиоци који врше ове врсте преваре често користе лажне податке и крађу идентитета, те тако при свом представљању користе фотографије других лица које су прикупилиса интернета како би се лажно представили оштећенима. Након што оштећени уплати одређени новчани износ према инструкцијама извршилаца кривичних дела следи одлагање новчаних трансакција везаних за исплату обећане суме

новца. Стално се појављују нови трошкови за оштећеног на име реализације посла, па се траже нова одлагања, стално сеобећава „експресна“ исплата новца, уз убеђивање жртве преваре да ће јој се улагање у договорени посао вишеструко исплатити (Прља et al, 2011: 59).

Психолошки притисак се на жртве преваре додатно врши и навођењем да је тајност „посла“ јако потребна, пошто би корумпирани званичници неке државе присвојили новац за себе уколико би сазнали да он постоји (Buchanan et al, 2001: 40). Такав притисак понекад жртва преваре додатно врши и сама над собом (нпр. када и након што сазнају да су преварене, жртве преваре наставе комуникацију да би повратиле новац, пронашле извршиоце и сл.).

Извршиоци кривичних дела се ослањају на чињеницу да ће за време које прође док жртва схвати да је преварена (тј. док схвати да обећани новац не постоји), новчани трансфер који је она извршила на њихове рачун бити исплаћен, те да оштећени неће стићи на време да блокира трансфер.

Од оштећених се најчешће тражи да новац уплате преко Western Union-a или Money Gram-a због брзине преноса новчаних средстава и анонимности примаоца уплате, чиме се смањује могућност откривања извршилаца. Електронске поруке, као што су SPAM-ови са оваквом садржином, најчешће се шаљу из интернет кафеа. У Нигерији, у областима као што су нпр. Лагос или Фестак, постоје многи интернет кафеи који су отворени управо у те сврхе, а радно време им је од 22,30 часова до 07,00 часова, ради избегавања контроле од стране државних службеника.

Чињеница је да извршиоци ових кривичних дела користе информационе технологије да би сакрили свој идентитет и физичку локацију, како би осујетили напоре полицијских служби да их открију и сл. (Chawki, 2006: 5). Поред тога што успоравају рад рачунара корисника на интернету, ове поруке подижу и цену коришћења употребе интернета крајњим корисницима пошто интернет сервис провајдери морају додатно да улажу у своју опрему како би их заштитили од нежељене електронске поште овог типа (Longe et al, 2008: 138).

У многим државама постоје и предузећа која уз новчану надокнаду обезбеђују лажна документа која се користе у овим преварама.[70] Са жртвама кривичних дела

[70]Након једне преваре која је укључивала лажни потпис нигеријског председника Olusegun Obasanjoy лето 2005. године, нигеријске власти извршиле су претресе на тржници у делу Лагоса под називом Oluwole. Заплењене су хиљаде нигеријских и других пасоша, 10.000 бланко British Airways карата, 10.000 налога за исплату новца из САД, царинска документација, лажна уверења универзитета, 500 компјутера са скенираном документацијом који су служили за прављење фаслификоване документације и др.

извршиоци комуницирају и преко мобилних телефона, користећи припејд SIM картице, које лако могу да баце и потом купе нове картице ради даље комуникације.

У најекстремнијим случајевима жртва преваре не схвата да је преварена ни након што се трансфер новца реализује. Верзије Нигеријске преваре су тако осмишљене да се стварају чак и лажни уговори по којима се новац, који жртва преваре уплаћује на име реализације неког посла, сматра легалним пословним улагањем, тако да жртва није убеђена да ради било шта илегално, па тако и не сумња да може доћи до злоупотребе њеног поверења. Због постојања уговора, који представља вешто укомпоновано средство социјалног инжењеринга, жртва преваре је убеђена и да је правно заштићена. У случају да оштећени и посумња у истинитост "приче", извршиоци кривичних дела ће понудити и да се лично упознају са жртвом преваре, инсистираће на томе да је повежу са "стручним људима" као што су нпр. брокери, банкари и др., који могу да потврде истинитост њихових навода и сл.

На такав начин жртва преваре уплаћује новац без осећаја да је учинила било шта на своју штету. У оваквом емоционалном стању жртве, извршилац кривичног дела може тражити још новчаних зајмова и исплату одређене суме новца унапред, уз већ поменуте фиктивне уговоре, држећи оштећеног константно у заблуди. Овакви случајеви, често, се и не пријављују пошто жртва преваре не схвата да је оштећена а, понекад, не жели да призна ту чињеницу или пријављивање одлаже све док, након дужег времена, сама не схвати да је преварена. Наравно, и оваква писана акта могу бити веома значајна приликом доказивања кривичног дела, а посебно уколико су она размењивана путем електронске поште са жртвом (Миладиновић Богавац, 2017: 101).

Како би извршили кривично дело преваре овог типа, извршиоци најчешће користе фалсификовану документацију којом преузимају новац који је оштећени уплатио, бежичне трансфере новца за пренос противправно стечених новчаних средстава, техничка средства која им омогућују анонимну комуникацију, Web-базирану електронску пошту, електронске налоге који су 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, постављају лажне странице на интернету којима оштећене доводе у заблуду да комуницирају и сарађују са представницима легалних и легитимних институција, уговарају пословне састанке са оштећенима (приликом комуникације извршиоци

http://web.archive.org/web/20051029165224/http://news.yahoo.com/s/latimests/20051020/ts_latimes/iwilleatyourdollars.преузето 21.07.2018. године.

кривичних дела обећавају специјалне аранжмане, као што је нпр. улазак у Нигерију без визе и слично, након чега се жртве ових кривичних дела које дођу у контакт са извршиоцима киднапују, уз захтевање откупа за њихово ослобађање и сл. (Dyrud, 2005: 4).

4.3.3. Извршиоци нигеријских превара

Коришћење Интернет сервиса и програма на Интернету, за прикривање IP адреса такође је веома распрострањена појава приликом вршења Нигеријских превара. Ови сервиси извршиоцима омогућавају анонимно слање електронских порука, без остављања трага о правој IP адреси извршиоца кривичног дела, на тај начин што целокупан Интернет саобраћај према одређеним Интернет адресама и страницама иде преко сервиса којим потом као траг оставља своју IP адресу, а адреса правог корисника се налази на серверу ових сервиса (Прља et al, 2011: 63).

Прикривање идентитета извршилаца врши се на много различитих начина, а већина случајева прикривања везана је за сакривање идентитета лица који је осмислио превару и лица које злоупотребљава податке о "жртвама" преваре.

Пошто се ради о простору где се време реакције своди на секунде, кључна је брза и ефикасна реакција. Шанса за проналазак доказа у оваквом окружењу зависи од саме конфигурације умрежених рачунара који се појављују у комуникацији као рачунарски сервери, улазне капије, рутери и др. Лог фајлови су главни извор проналаска трагова и доказа о извршеном кривичном делу. У зависности од броја корисника и процеса који је у току, број ових лог фајлова све више расте, тако да поједини Интернет сервис провајдери у само једном дану стварају лог фајлове величине неколико стотина мегабита.

Прве информације о илегалној активности најчешће не воде до правог идентитета лица, већ је прикупљају подаци са више локација, често и широм света, преко ИНТЕРПОЛ-а. На међународном нивоу у полицијској и правосудној сарадњи још није постигнут довољно висок квалитет сарадње потебан за овакве врсте истрага. Разлози томе нису само у спорости правних система, већ и у потреби обавештајне заштите држава (Урошевић, 2009: 6).

Након сазнања да је извршено кривично дело које садржи елементе Нигеријске преваре, али и друге врсте превара из ове области, и да је дошло до злоупотребе података који су од стране извршилаца кривичних дела прикупљени на наведене

начине, полицијски службеници прикупљају доказе и трагове у виду електронских података о оствареној комуникацији која се одвијала између извршилаца кривичних дела и оштећених, као и податке о финансијским трансакцијама које је оштећени извршио према инструкцијама које је добио од извршилаца. Врше се провере лог фајлова у потрази за IP адресом, како би се лоцирао сервис преко кога је извршилац кривичног дела слао електронске поруке оштећеном, као и преглед целокупне електронске поште коју је оштећени примио, како би се уочили пропусти направљени од стране извршиоца који могу указати на постојање кривичног дела и места одакле је извршена превара.

Након изоловања IP адресе и времена слања електонских порука из лог фајлова преко ИНТЕРПОЛ-а се, у зависности од државе са чије је територије извршено кривично дело, врше провере у вези корисника коме је она била додељена у тренутку вршења кривичног дела.

Како би се детекција електронских порука свела на што мањи ниво, данас извршиоци нигеријских превара шаљу мање количине спам порука са рачунара заражених рачунарским вирусима, како би се обезбедило што дуже функционисање њиховог слања. Неки комерцијални спам сервиси укључују botnet мреже за слање ових порука, које помажу да се избегну анти-спам мере на рачунарима корисника и заштите на серверима Интернет провајдера, које функционишу на тај начин што се блокирају IP адресе које су постављене на "црне листе". Данас постоји велики број IP адреса са којих је вршено слање ових порука и које су идентификоване као носиоци спам активности.

"Црне листе" се често ажурирају, па извршиоци кривичних дела који користе слање оваквих порука за прибављање података морају да ангажују botnet мреже како би избегли блокирање њиховог пријема. Овакав начин слања спам порука додатно отежава рад полицијских служби, пошто корисници Интернета на територији Републике Србије и не сумњају да поруке које им стижу могу бити штетне. Из наведеног разлога сматра се да постоји велика "тамна бројка" када су у питању Нигеријске преваре пошто оштећена лица или нису свесна да су преварена (нису свесни да су постали жртве), или их је срамота да пријаве да су оштећени због своје околине. Оштећени се често и плаше да пријаве овакве случајеве пошто их извршиоци кривичних дела убеђују да су сами криви за то што посао није могао да се реализује, прете им да ће их тужити и сл. (Прља et al, 2011: 63-64).

У случајевима „нигеријских превара“ чије су жртве држављани Републике Србије радило се о преварама извршеним на неколико начина, и то: слањем обавештења о лажним добицима на лутрији помоћу којих су жртве превара методама социјалног инжењеринга навођене да поверују да су добитници награда, након чега су уплаћивали одређене суме новца да би им се омогућило подизање награде, и слањем обавештења о наследству помоћу којих су жртве превара методама социјалног инжењеринга навођене да поверују да су наследиле одређену количину новца, након чега су уплаћивали одређене суме новца да би им се омогућила исплата наслеђеног новца. Кривична дела су иницирана са подручја Нигерије, Сенегала и Бенина, а међународна полицијска сарадња са наведеним државама до данас није довела до значајнијих резултата (Урошевић, 2009: 10).

4.3.4. Искуства Републике Србије у сузбијању нигеријских превара и мере превенције

Интернет је још увек правно нерегулисан простор, у коме извршиоци кривичних дела имају доста простора за вршење криминалних активности. Развој савремених информационих технологија, посебно на пољу електронске трговине и комуникације, створио је нови простор за деловање криминалаца и криминалних група. „Нигеријске преваре“ су, из наведених разлога, постале један од најчешћих облика превара на интернету, због честог мењања начина извршења и прилагођавања брзим променама у области информационих технологија.

Наведена појава се може ефикасно спречавати једино акцијама на глобалном нивоу, како би се створила свест о опасности коју она са собом носи. Потребно је да се предузму активности на расветљавању начина извршења тих кривичних дела и њиховог презентовања широј јавности путем јавних гласила (новине, телевизија). Такође је потребно појачати и сарадњу на националном, регионалном и глобалном плану, посебно када су у питањумеђународна полицијска и кривичноправна сарадња.

Правна регулатива у Републици Србији пружа добру основу за ефикасно спречавање овог вида кривичног дела преваре. Међутим, као основни проблем јавља се чињеница да се ова кривична дела врше од стране лица која се налазе ван територије Републике Србије, углавном са територије афричког континента, са којима је међународна полицијска сарадња знатно отежана.

Чињеница је да феномен „нигеријских превара“ код нас није довољно познат широј јавности и корисницима интернета, посебно зато што та тема није довољно заступљена у медијима. Превентивно деловање државних органа као што су полиција и тужилаштво има кључну улогу у спречавању ове недозвољене појаве. Пошто сарадња са државама из којих се врши ова врста кривичних дела није на завидном нивоу, потребно је што хитније деловати проактивно, искористити потенцијал медија и скренути пажњу домаћој јавности на финансијске губитке који могу настати као последица тих кривичних дела.

Превентивна улога полиције у заштити корисникаинтернета са територије Републике Србије од „нигеријских превара“ би била успешнија и сврсисходнија од репресивних активности које се предузимају након сазнања да је кривично дело већ извршено (Урошевић, 2009: 10-11).

4.4. Клик преваре

У прошлости, онлајн рекламирање заснивало се на тзв. Cost-Per-Impression (плаћање на основу утиска који корисник има о реклами) моделу наплате за рекламирање. Цена рекламирања се наплаћивала по принципу Cost Per Mile (“цена по пређеним миљама”), који практично представља цену за сваких 1000 коментара одређене рекламе од стране корисника интернета. Ова метода је била заснована на моделу који је примењиван на телевизији и у штампи, где је клијенту који рекламира своје производе услуга била наплаћивана на бази броја појављивања рекламе која је објављивана, у одређеном временском периоду. Тај модел је био омиљен међу власницима интернет сајтова због тога што су услуге наплаћиване без обзира на учешће корисника и ефекте које реклама код њих изазива (Урошевић et al, 2012: 226-227).

На интернет претраживачима компанија као што је Google почели су да се примењују тзв. Pay-Per-Click модели за онлајн рекламирање на интернету. Овај тип “аранжмана” подразумева да лица или предузећа која се рекламирају на одређеном интернет сајту плаћају ономе ко објави њихову рекламу за сваку посету неког од корисника интернета који је кликнуо на рекламу (на пример, преко линка) и затим био усмерен на интернет сајт компаније. Дакле, овом методом врши се наплата услуге на основу активности корисника везаних за рекламу. Такав начин рекламирања је омиљен међу клијентима тј. компанијама које желе да привуку кориснике преко својих реклама

како би, доласком на њихов интернет сајт платили одређене услуге, извршили наручивање или куповину одређене робе и сл.

На Google-овом претраживачу по систему AdWord оглашивачи реклама се путем аукција опредељују на основу којих ће се кључних речи у резултатима претраге појавити њихова реклама. Њихова реклама се појављује одмах поред резултата претраге коју је извршио корисник на интернет претраживачу, и то на основу задате кључне речи. Ова форма рекламирања познатија је као "спонзорисана претрага". Очигледна корист за оглашивача рекламе је што је корисник, који види рекламу већ, заинтересован за тему која је везана за кључну реч (пошто је ту кључну реч и унео у поље за претраживање и покренуо претрагу). Самим тим постоји већа шанса да ће такво лице такође бити заинтересовано и за производ или услугу која се рекламира поред добијених резултата претраге. На пример, кориснику који тражи резултате на основу кључне речи "сат" може се у пољу за рекламирање приказати реклама произвођача Fossil. Корисници интернета такође имају корист од такозваног "циљаног рекламирања", пошто се преко њих приказују само оне рекламе за производе за које су највероватније и заинтересовани.

По систему AdSense фирме Google-а, на сличан начин као и по систему AdWords, након што се оглашивачи рекламе определе за рекламу која ће се појавити на основу кључне речи, на основу анализе садржаја интернет сајта, фирма Google смешта рекламу на интернет сајт који има сличан садржај који је повезан са том кључном речи. Сваки пут када неко лице кликне на ту рекламу власник интернет сајта добија проценат од зараде коју Google као фирма оствари од оглашивача рекламе, тако да Google практично зарађује само део тог новца, односно провизију (Урошевић et al, 2012: 227).

Разликују се два типа ових превара. То су: а) преваре од стране учесника и б) преваре од стране објављивача.

Први вид ове преваре најчешће се не врши ради стицања противправне имовинске користи, пошто ње заправо ни нема, већ у намери да се оштети или сузбије пословна конкуренција. Ова превара везује се најчешће за рекламе које се обављају по систему AdWords, када конкуренција врши превару према конкурентној фирми која је објавила рекламу. Извршилац, знајући да сваки клик на рекламу кошта његову пословну конкуренцију доста новца, смишља превару у оквиру које ће на одређеном интернет сајту где је реклама објављена она бити вишеструко пута посећена, понекад и аутоматским путем, вештачки преко botnet-а. Тиме се пословној конкуренцији наноси велика материјална штета, пошто заправо нема користи која настаје када се врше праве

посете рекламама од стране корисника. Такве нападе често врши пословна конкуренција коришћењем савремених рачунарских метода из области високотехнолошког криминала (Урошевић et al, 2012: 228).

Превару од стране оглашивача врши лице које је објавило рекламу, тј. сам власник интернет сајта на коме је реклама објављена (или где је објављено више реклама). То власници интернет сајтова, где су објављене рекламе, чине са унапред смишљеном идејом: да остваре противправну имовинску корист вршењем кривичног дела рачунарске преваре на штету својих клијената који су код њих објавили рекламу. Пошто лице, компанија или друга организација која објављује рекламу власнику интернет сајта плаћа за сваку посету реклами од стране корисника, власнику интернет сајта је у интересу да рекламу коју је објавио преко њега посети што више корисника. Извршиоци кривичних дела на чијим су интернет сајтовима објављене рекламе вештачки повећавају број таквих посета у жељи да зараде више новца. Најпростији облик таквих превара своди се на то да се ангажују различита лица која ће посећивати рекламе. На интернету постоји много интернет сајтова и сервиса који пружају могућност за упознавање, дружење и забављање (Урошевић, Ивановић, 2010: 88).

И ту могућност извршиоци кривичних дела користе како би ангажовали лица за помоћ при извршењу клик превара. Професионалци у области високотехнолошког криминала ангажују велики број лица која се овим послом баве организовано или који користе аутоматизоване методе за посету. Облик у коме се користи аутоматизовање посета је најтежи и најопаснији, пошто производи велики број напада у кратком временском року. Најтежи проблем при вршењу тих кривичних дела је утврђивање да ли је реч о правим или лажним посетама које су вештачки генерисане. Преваре које чине власници интернет сајтова на којима су објављене рекламе најчешће представљају класичне злоупотребе поверења, као и кршење уговорних обавеза. Иако се у многим уговорима овог типа правно регулишу права и обавезе оглашивача и власника интернет сајта који рекламира производе или услуге, међу којима су и спречавање коришћења аутоматизованих и организованих посета, као и вештачки генерисаних посета, овај проблем још увек није адекватно решен, посебно када се у обзир узме глобална природа интернета и начин његовог функционисања (принципи функционисања као мреже која нема власника, анонимност корисника и сл.).

Компанија *Google* може да послужи као одличан пример како би се виделе размере ове врсте рачунарске преваре. Многе компаније данас користе рекламирање на интернету као 99% свих начина рекламирања. Тако се комерцијалне активности многих

интернет сајтова изражавају у милионима и милијардама долара. Ако се ова врста преваре у скорије време не реши и не прекине, такав облик наплате рекламирања могао би да буде угрожен. Сама чињеница да је сервис *Google* зараду од 6,7 милијарди долара у 2005. години повећао на 10,4 милијарди долара у 2006. години говори о размерама овог посла и његовом значају. У 2006. години 60% ове зараде је потицао од сервиса *GoogleAdWords,* система који је иначе подложан преварама од стране конкурентских фирми, а осталих 40% од сервиса *AdSense,* система подложног преварама од власника интернет сајтова који објављују рекламе (податак из годишњег извештаја за 2006. годину компаније *GoogleInc*који је објављен 2007. године). Поред сервиса за претраге, *Google* је у наведеним годинама, као и многи други интернет сервиси који се баве оваквим видом рекламирања, драстично увећао свој профит.

Иако се број клик превара још увек не може тачно проценити, студије које су изведене указују на то да је око 14% таквих активности заправо лажно (Прља et al, 2012: 229). Према Bernard J. Jansen-у, ванредном професору Државног универзитета у Пенсилванији, из Одељења за компјутерски инжињеринг, не може се тачно рећи колика је тачност интернет претраживача при филтрирању лажних посета путем генерисаних кликова на линкове реклама, али се може закључити да она износи око 80% или више, што води до закључка да лажне посете чине око 6% од свих посета рекламама преко интернет претраживача (Jansen, 2007: 102).

Компаније као што је *Google* практично имају мало избора како би избегле ову опасност. Оне могу да отворе нове сервисе у намери да избегну да буду економски зависне од клијената који рекламирају своје производе путем њихових интернет сајтова или да предузму одређене кораке како би превентивно деловали, пре него што настане штета. Без обзира на то које се техничко решење примењује, потребно је што боље разумети начин извршења овог вида кривичног дела рачунарске преваре како би јој се адекватно супротставило на свим нивоима.

4.4.1. Начини извршења клик превара

Клик преваре врше се на више различитих начина, и то такозваним „симулованим кликом", нападима преко *botnet* мрежа, пребацивањем скрипти злонамерних рачунарских програма на рачунаре посетиоца које затим покрећу поновне посете интернет сајтовима и симулирају прави клик корисника на основу претходне посете реклами.

Сви начини извршења су веома специфични, па их треба објаснити детаљније.

4.4.1.1. Симуловани клик

Суштина оваквог начина извршења кривичног дела је у томе да се ради о аутоматизованом процесу који доводи до симулације клика на одређену рекламу, односно интернет линк где се она налази. Како би се разумео принцип функционисања ове врсте преваре, прво се мора разумети принцип функционисања технологије која подржава рекламу на интернет сајту, то јест технички принцип њеног функционисања.

Типични интернет сервиси за онлајн рекламе функционишу на тај начин што власницима интернет сервиса обезбеђују одређене кодове написане у *JavaScript* програмском језику, како би их поставили на интернет странице свог сајта. Ови кодови се затим покрећу у оквиру интернет претраживача који корисник користи и преузимају рекламе са рачунарског сервера на коме је она постављена у реалном времену. Покретачи преузимања затим врше трансфер кодова који су у *JavaScript* формату у *HTML* формату (практично мењају врсту програмског језика, а садржај рекламе остаје исти), како би се реклама појавила у облику који је потребан да би је корисник видео. Када корисник посети интернет линк рекламе, подаци о томе практично пролазе преко сервера, дајући тако прилику власнику интернет сајта да региструје број посета и, касније, на основу тога наплати своје услуге власнику рекламе. Након тога корисник се пребацује - редиректује на интернет сајт где се налази реклама (Gandhi, 2006: 131-132).

Евидентно је да програм који симулира клик корисника мора да функционише и врши одређене функције као претраживач. Прво мора да изврши *JavaScript* код који повлачи *HTML* код интернет странице где се налази реклама, да пребаци ове *HTML*кодове у потрази за интернет линком и потом да пошаље *HTTP* захтев серверу на коме се налази веб страница на одређеној *URL* адреси.

4.4.1.2. Клик превара путем botnet мрежа

Симуловање клика је, у суштини, прилично лако. Откривање основног вида овакве преваре је понекад јасно уочљиво самом анализом логова на серверима. Разлог за то је следећи: када програм пошаље *HTTP* захтев према серверу лица које је поставило рекламу, IP адреса рачунара корисника се у логовима појављује као захтев за пребацивање конекције између клијента и сервера. Практично све што треба да се

открије да је извршена клик превара јесте провера лог фајлова, посебно са освртом на оне фајлове где се појављује једна IP адреса са великим бројем захтева за конекцију. Да би избегли да их на овај начин открију, извршиоци кривичних дела често ангажују *botnet* мреже рачунара који су под њиховом контролом или плаћају извршиоце других кривичних дела који имају велики број заражених рачунара под својом контролом да за одређену суму новца преко тих рачунара врше клик преваре. Такве мреже се понекад састоје од неколико хиљада рачунара који су заражени тзв. злоћудним програмима, који су под контролом извршиоца кривичног дела (Soubusta, 2008: 136-141).

Овакве мреже настају на тај начин што извршиоци кривичних дела преузимају контролу на рачунару и потом преко мреже врше контролу рачунара коме задају и одређене задатке. Такве задатке рачунари потом извршавају на њихов знак, односно извршни код који је унапред одређен од извршиоца кривичног дела.

Као добар пример ове врсте рачунарских превара може се навести случај под називом *Ghost Click* који је спровела агенција *FBI* из САД. Откривено је да је широм света у стотину држава заражено 4 милиона рачунара у року од пет година. Ти заражени рачунари су омогућили да криминалци манипулишу радом рачунара и претрагама које врше на интернету и интернет реклама које посећују. Саопштено је том приликом да је ухапшено шест естонских држављана у истрази која је трајала две године. Превара је започета 2007. године, када су извршиоци овог кривичног дела почели да користе рачунарски вирус *DNS Changer* да би заразили рачунаре кућних корисника, али и корисника у компанијама, државним институцијама, па чак и у самој агенцији *NASA*.

Овај рачунарски вирус је вршио преусмеравање корисника на интернет странице и рекламе које су се појављивале приликом замене интернет страница оригиналне претраге онима које су биле потребне извршиоцима кривичних дела. Процена је да су извршиоци овог кривичног дела зарадили око 13,8 милиона америчких долара путем илегалних надокнада за рекламирање које су им плаћале компаније које су мислиле да се ради о легалним посетама њиховим страницама са рекламама. Тај вирус је, такође, имао опцију да онемогући нормалан рад антивирус програма, пружајући даљу могућност да се уносе рачунарски вируси типа тројанац у систем рачунара који је заражен. *FBI* је утврдио да су учиниоци били естонске националности, као и један руски држављанин (Урошевић et al, 2012: 231).

Ова акција је координирана са Одељењем за високотехнолошки криминал Краљевине Холандије, агенцијом NASA, компанијом *Trend Micro,* полицијом Естоније и већим бројем универзитетских установа у САД.[71]

Сличне примере познаје и Република Србија, тј. њени органи гоњења.[72]

4.4.1.3. Преузимање рачунара

Рачунаре извршиоци кривичних дела често компромитују експлоатисањем сигурносних пропуста и слабости рачунарског система (лоше антивирусне заштите, пропуста и оперативним системима и сл.). Програм који врши истраживање ових пропуста и слабости најчешће се назива *exploit* (слободан превод би био „истраживач"). Извршиоци кривичних дела ове програме некада пишу сами или, што је чест случај, користе већ познате програме овог типа који су написани за познате сигурносне пропусте и који су доступни на интернету (најчешћи су они везани за сигурносне пропусте у оперативним системима Microsoft Windows).

Када се одлучи за одређени тип злоћудног програма, извршилац кривичног дела почиње да скенира одређени опсег IP адреса у потрази за рачунарским системом који испуњава услове за употребу злоћудних програма то јест за оним системом који има одређену верзију оперативног софтвера или неки други рачунарски програм који је погодан за напад и експлоатисање. Када се открије слабост система, користи се злоћудни програм типа *exploit* да се добије даљински приступ рачунару (remote access)и како би се остварила контрола над њим. Након што *exploit* пронађе сигурносне пропусте у рачунарски систем се убацује малициозни програм – вирус који након тога преко унапред задатих команди контактира рачунар који контролише читаву мрежу

71 http://www.theage.com.au/it-pro/security-it/operation-ghost-click-busts-cybercrime-ring-that-hit-4m-computers-20111110-ln8v3.html. преузето 30.07. 2018. године.

[72]У саопштењу МУП-а Републике Србије од 11. марта 2011. године наводи се да је А. А. стар 27 година из Суботице ухапшен, у сарадњи са Вишим јавним тужилаштвом у Београду, због сумње да је извршио кривична дела која се односе на прављење и уношење рачунарских вируса, рачунарске преваре и прање новца. Осумњичени је у јуну 2010. године купио рачунарски вирус, потом га сачувао на закупљеном серверу, а затим га путем интернета унео у више од 1.000 рачунара широм света, стварајући такозвану „ботнет" мрежу којом је управљао са свог сервера. Користећи заражене рачунаре, осумњичени се регистровао на торент сајтовима и постављао фајлове са називима филмова, који нису садржавали филм већ рекламу која је упућивала на интернет сајт који је креирао, како би се преко њега преузимали софтверски садржаји, лажно приказујући да је садржај постављеног фајла филм. Овако нерегистровану услугу, А. А. је наплаћивао од једне канадске компаније коју је довео у заблуду и од ње за девет месеци наплатио преко свог девизног рачуна више од 70.000 америчких долара.
http://www.blic.rs/Vesti/Hronika/240864/Uhapsen-osumnjiceni-za-pre-nos-racunarskih-virusa.
преузето 30.07.2018. године.

заражених рачунара тј. botnet мрежу, са којег се задају команде за контролу и за давање инструкција тј. задатака зараженом рачунару (Урошевић et al, 2012: 232).

4.4.1.4. Начин контроле и задавања команди рачунарима зараженим рачунарским вирусом (функција Comand&Control)

У највећем броју случајева за контролу и задавање команди користе се *IRC (Internet Related Chat)* сервиси и њихови канали комуникације. Ти сервиси се најчешће састоје од једног или више сервера који служе за размену порука и/или команди за повезивање између клијената. Путем тих сервиса власник мреже заражених рачунара може да, преко канала за комуникацију, једновремено и централизовано зада команду сваком зараженом рачунару преко унапред задатих параметара и команди, да пошаље и покрене рачунарски програм на зараженом рачунару који ће даље вршити клик преваре са зараженог рачунара на интернет сајту где се налази циљана реклама (Урошевић et al, 2012: 232).

Алтернативни начин контролисања мреже заражених рачунара је и употреба корисничког интерфејса путем којег се заражени рачунар конектује на рачунарску мрежу. Та метода је јако захтевна пошто злоћудни програм стално при конекцији захтева *update,* тј. посету серверу који контролише заражене рачунаре, како би пријавио да се заражени рачунар конектовао на интернет и да се може покренути одређена функција. На тај начин се генерише и већи интернет саобраћај од зараженог рачунара и на њему, па је и могућност откривања већа.

4.4.1.5. Пребацивање скрипти на рачунаре посетилаца интернет сајтова

Један од најсофистицираних начина извршења овог типа рачунарске преваре је постављање „скрипти" на интернет сајтове на којима се реклама налази и то од власника интернет сајта који врши кривично дело рачунарске преваре. Те скрипте се приликом посете интернет сајту аутоматски пребацују на рачунар посетиоца. Скрипта потом покреће активност на зараженом рачунару (без знања корисника рачунара) којом се имитира прави клик посетиоца, иако он то није учинио. Лог фајлови оглашивача рекламе при таквој посети бележе идентитет посетиоца и његову IP адресу на серверу и на основу тога се касније врши наплата власнику објављене рекламе.

Овај начин извршења се ипак може открити и пратити. У случају сумње да се врши такав вид рачунарске преваре, власник објављене рекламе би требало да посети интернет сајт оглашивача без посете реклами коју је објавио, те да касније провери да ли су његова IP адреса и ID број регистровани као да су кликнули на линк рекламе, иако то нису учинили.

Међутим, извршиоци кривичних дела често знају за овај начин провере од стране власника објављених реклама, па су смислили начин да избегну да буду откривени. То решење подразумева постојање два интернет сајта, првог који пребацује скрипте и другог који је сасвим регуларан, на коме је објављена реклама. Интернет сајт који не пребацује скрипте је потпуно регуларан, и при посети се не може уочити ништа сумњиво.

За превару служи други сајт који није повезан са првим и над којим извршилац у потпуности има контролу. То може бити сајт који је извршилац отворио са намером да изврши превару или сајт лица које се појављује као саизвршилац, помагач и слично. На други интернет сајт се поставља скрипта која аутоматски учитава лажну страницу која је у ствари копије прве, регуларне стране сајта на коме је реклама објављена, и то сваки пут када корисник посети другу интернет страницу, при чему IP адресе остају забележене као да је посета била намењена правој интернет страници где се налази реклама (Урошевић et al, 2012: 233).

Напредни начини вршења рачунарских превара постали су претња савременом начину рекламирања на интернету. Многе организације су данас посвећене решавању безбедносних проблема. Зато оне одвајају додатне ресурсе везане за заштиту система, особља, технике и предузимају друге потребне радње како би заштитили информације и рачунарске системе. Иако те активности помажу да се ризик смањи, оне га свакако не елиминишу (Ianelli, Hackworth, 2007: 19-39).

Неке од тих заштитних мера подразумевају модификацију система наплате по систему наплате по основу активности посетиоца након регистровања посете (на пример, куповина, попуњавање формулара и сл.), наплате по једном појављивању рекламе, наплате по проценту појављивања рекламе на основу кључне речи, преко откривања корелација са сајтовима са којих је честа посета преко алгоритама које користе интернет провајдери, путем дупле провере преко удруживања са корисницима и остављањем тзв. *cookies-a* којима се детектује индивидуални корисник и сл. Ипак, ниједна од ових мера није довољно ефикасна да заштити власнике реклама од ових врста напада везаних за клик преваре.

Интернет је мрежа у оквиру које извршиоци често прикривају свој идентитет користећи његову инфраструктуру, али и пријављивањем података при регистрацији на различитим интернет сервисима који су измишљени или су прибављени крађом података о туђем идентитету. Истраживање кривичних дела у којима је дошло до крађе идентитета на интернету веома је тешко, посебно када се у виду има чињеница да интернет не познаје границе и да докази о извршеним кривичним делима могу да се налазе на серверима који се налазе у било којој држави на свету. Ову чињеницу посебно треба имати у виду када је реч о нападима преко *botnet* мрежа, чијег је власника веома тешко пронаћи (Урошевић et al, 2012: 234).

4.5. Вирусне преваре

4.5.1. Појам вируса у рачунарским технологијама

Вирус је мали програм написан са намером да измени начин рада рачунара, без дозволе или знања корисника тог рачунара. Под вирусом се сматра програм који инфицира одређени изабрани систем, као на пример датотеку, и који се може ширити даље по систему, па чак и изван њега. Но, у теорији се вирус може одредити и као паразитска апликација која се самореплицира (Прља et al, 2011: 156). За постојање вируса потребно је испуњење следећих услова:

- мора се сам активирати, често убацује свој код (програмску секвенцу) на место путање за извршавање другог програма,
- мора се реплицирати. На пример, може заменити друге стартујуће програме копијама вирусом инфицираних фајлова. Они могу инфицирати кућне рачунаре као и мрежне сервере и
- мора имати носиоца, како би се неко други у контакту са носиоцем могао инфицирати.

Неки вируси су програмирани тако да оштете рачунар преко програма за уништавање или програма који могу нанети штету, брисање датотека (фајлова). Други вируси пак нису дизајнирани за ту сврху већ да би се, просто, самореплицирали и на тај начин приказало њихово присуство у меморији путем текстуалних, видео или аудио порука. Чак и ови „бенигни" вируси могу створити проблеме за кориснике рачунара.

Обично они заузимају меморију намењену другим програмима, услед чега се као резултат јављају погрешна понашања и евентуални пад система.

Већина вируса је везана за багове[73] који могу довести до пада система. Према систематизацији Симантек корпорације постоји пет типова познатих вируса.

Први тип је вирус који инфицира фајлове (датотеке). Овај вирус инфицира програмске датотеке, обично извршне (егзекутабилне) програме као што су датотеке са екстензијама .com и .exe. Ови вируси могу својим извршавањем инфицирати друге датотеке, када се стартују са флопија, ХД-а, флеша или са мреже. Већина ових вируса је резидентна (отпорна и егзистирајућа) у меморији рачунара. Након инфицирања меморије, било који извршни фајл који се стартује такође бива инфициран. Примери овог типа вируса су Jerusalem и Cascade вирус.

Други тип је вирус бут сектора[74] било ког медија, флопија, HD-a, CD, DVD или флеш меморије. Неки аутори ове типове вируса сматрају праисторијским. Они имају мали сектор на својој меморијској површини који се активира када се исти „утакну" у рачунар. Описани тип вируса се прикачи за овај сектор на диску и активира се када корисник покуша да дигне систем преко ових медија који су заражени. Ови вируси су увек резидентни у меморији, већина их је написана у DOS -у, али сви кућни рачунари су потенцијалне жртве ових вируса. Све што је потребно је да се покуша стартовање система са оваквих медија и да се тако зарази систем. У овако зараженом систему неопходно је да се незаштићен медиј укључи и он ће бити заражен. Примери за овај тип су: Form, DiskKiller, Michelangelo и Stoned.

Трећа група су вируси **главног boot сектора.** Они функционишу на исти начин као и претходни вируси, с тим што су објекат њиховог напада системски сектори. Разлика између ове две групе вируса се огледа и у локацији депоновања вирусног кода. Ова група, по правилу, легалну копију стартних (бутабилних) датотека памти на неуобичајеној локацији, и као резултат се добија немогућност подизања система.

Мултипартитни вируси јесу четврта кагегорија (познати су и као полипартитни) вируса. Они инфицирају бут сектор и програмске датотеке, па су веома тешки за брисање и повраћај система који су напали. Ово из разлога непотпуности мера за чишћење оваквих вируса (ако обришемо и очистимо бут сектор, остаће у програмским датотекама и обратно). Примери су: OneHalf, Emperor, Anthrax and Tequilla.

[73]Баг – наенглеском bug – програмска грешка или недостатак, који изазива проблеме у раду система.
[74]Бутсектор – Boot sector је системска област на диску, он представља скуп датотека које иницирају стартовање система.

Макро вируси су пета категорија вируса. Они нападају датотеке које нису извршне, већ оне које садрже податке, оне су најчешће и највише коштају оштећене (Прља et al, 2011: 157-158).

Поред наведених типова вируса, у теорији постоји још типова рачунарских вируса, али ће сада бити поменуто још неколико карактеристичних из реда малициозних програма.

Тројански коњи (тројанци) су програми који се представљају као легитимне софтверске апликације, а који, у ствари, врше прикривене активности и штетне функције. Они су датотеке које наизглед представљају неке пожељне елементе, али, у ствари, су злоћудни. Значајна разлика вируса и тројанаца се огледа у чињеници да се ови потоњи не реплицирају. Тројански коњи садрже злоћудни код који када се активира проузрокује губитак или чак крађу података. Како би се постигло ширење тројанских коња неопходно је да неки други програми буду активирани на рачунару корисника, на пример отварањем и мејл поруке, у ствари додатка исте (attachment) или даунлоадовањем или извршавањем одређених датотека са Интернета. Битно је да тројанци немају носиоце, већ се они могу шетати, са инфицираног сајта, користећи недостатке и мањкавости браузера улазе на туђи рачунар и врше свој посао. Тројански коњ је нпр. Trojan Vundo.

Постоје и PCW тројанци који претражују машину у покушају да нађу фајлове у којима се чувају поверљиви подаци и да их пошаљу нападачу.

Trojanclickers представљају тројанце који преусмеравају рачунар корисника на одређени веб сајт, било са циљем да изазову DDoS напад на тај сајт, било да се корисник приступом том сајту зарази неким другим тројанцем или вирусом.

Trojandropper је тројанац који врши прикривену инсталацију других тројанаца или програма.[75]

Слично „тројанцима" делују и „логичке бомбе", штетни програми попут вируса, али без могућности самосталног извршавања, све док не добију команду од корисника нападнутог рачунара која се, најчешће, састоји у покретању одређеног програма.

Црви су програми који се реплицирају потпуно самостално, од система до система, не користећи никакве датотеке домаћине. Сматрају се подврстом вируса, па се одређују уобичајено као злоћудни програми који су свесни мреже (network-aware malware)[76]. Они су самостални програми, који немају потребу коришћења других

[75]http://www.singi.com/podrska/crvi.htm преузето 05.08.2018.
[76]http://www.sophos.com/blogs/chetw/g/2010/04/03/3-types-viruses-demystified преузето 05.08.2018.

датотека. Ово и представља основ за њихово разликовање од вируса којима је потребан неки облик домаћина - датотеке.

Иако црви постоје унутар других датотека, постоје разлике у начинима како вируси и црви користе датотеке домаћине. Уобичајено је да црв емитује датотеку која има „макро" црва унутар себе. Цео документ (датотека) путује од система до система тако да се цео документ сматра црвом. Пример за то је W32.Mydoom.AX@mrn. У сваком случају када се говори о црвима мисли се на програме који се користећи ЛАН (или Интернет) реплицирају са једних на друге рачунаре. Значајно је да се могу јавити и црви тројанци.

4.5.2. Појам и карактеристике вирусне преваре

Вирусна превара представља облике порука, најчешће трансмитоване путем и мејла, у количинама нешто мало вишим од уобичајених количина ланчаних писама. Следећи су примери ових облика вирусних превара, који садрже ове фразе:

- If you receive an email titled [email virus hoax name here], do not open it! (уколико примите имејл под насловом (назив и мејл преваре), немојте га отварати),
- Delete it immediately! (Одмах обришите!),
- It contains the [hoax name] virus. (Ово садржи (назив преваре) вирус),
- It will delete everything on your hard drive and [extreme and improbable,
- dangerspecifiedhere]. (Ово ће обрисати све на ХД вашег рачунара и још многе екстремне и невероватне опасности које се сете навести),
- This virus was announced today by [reputable organization name here],
- (Овај вирус је објављен данас од стране (име неке организације са добром репутацијом)) и
- Forward this warning to everyone you know! (Пошаљите ово упозорење свима које знате)

Ове преваре се често врше на све популарнијим социјалним мрежама као што су фејсбук, инстаграм, твитер итд. Наводи се да постоји велики број различитих облика превара ове врсте које иду од преваре која вас упозорава на неки нови злоћудни програм који се појавио на Интернету, или од вас тражи да проследите даље ову

поруку, или од вас тражи помоћ за прибављање веће количине новца у некој страној држави, па до позива да покупите награду коју сте остварили на лутрији[77].

Шта не представља вирус? Обзиром на публицитет који вируси имају, веома је лако окривити их за све проблеме на рачунару. Из овог разлога наводи се неколико ситуација чији настанак није условљен вирусима или другим злоћудним кодовима:

Табела бр. 1: Проблеми у раду рачунара који нису узроковани деловањем вируса[78]

хардверски проблеми	Ни један вирус не може физички уништити или оштетити хардвер рачунара, као што су чипови, плоче, процесори, матичне плоче или монитори
Рачунар пишти при стартовању без приказивања било чега на дисплеју	Обично је резултат проблема на хардверу приликом дизања система.
Рачунар не региструје или не пријављује 640 KB уобичајене меморије	Ово може бити знак постојања вируса, али не у сваком случају, неки драјвери (програми за покретање одређених уређаја под Windows системима) за мониторе или СЦСИ картице или дискове могу узимати део своје меморије.
Постојећа су два антивирус програма и један од њих пријављује проналазак вируса	Могуће је постојање вируса, али је вероватно и да други антивирус програм региструје први као вирус.
Микрософтов програм Word вас упозорава да документ садржи макро	Обично не значи да има и вирус.
Не можете отворити одређени документ	Не значи присуство вируса, покушајте отворити други или његову сигурносну копију.

У литератури се наводи да постоје одређена правила именовања вируса, па на пример, Симантек/Нортон (Symantec/Norton) антивирус има своје услове и правила. Име вируса се састоји од префикса, имена и често и суфикса. Префикс означава платформу на чијој се основи вирус репликује или тип вируса. DOS вируси не садрже префиксе. Име означава име фамилије вируса. Суфикс не мора увек постојати, а означава варијанте у оквиру исте фамилије, иобично га чине бројеви који означавају величину вируса или мање често слова. Примери су: префикси: АОЛ - овакви вируси су

[77]Неке од ових превара представљају средство или увертиру у фишинг.
[78]Извор (Прља et al, 2011: 160-161).

карактеристични за окружење Америка Онлајн или Backdoor Бекдор (задња врата или тајни пролаз) ове претње могу омогућавати недозвољени приступ извршиоцима са Интернета приступ вашем систему, итд. Суфикси: @m - означава да је вирус или црв мејлер, везан за електронску пошту, @mm - означава масовну пошту, Worm - значи да је у питању црв, а не вирус.

У сваком случају видљиво је да скоро сваки од безбедносних програма даје свој назив одређеним категоријама. Чак и без присуства тројанаца у рачунару, Windows може да омогући другима да приступе диску преко Интернета. Реч је у ствари о једном сервису који се користи код умрежених рачунара, дакле, тамо где постоји локална мрежа, а који извршиоци злоупотребљавају за извођење својих злонамерних и противзаконских активности. Назив сервиса је NetBIOS и, преко њега, се размењују фајлови у локалној мрежи. Овако створен проблем је релативно лако решити простим искључивањем овог сервиса, али поред овако простих проблема постоје многи који нису тако лако решиви (Прља et al, 2011: 161).

4.6. Преваре при куповини путем интернета

Ове врсте превара су данас прилично заступљене, с обзиром на чињеницу да се куповина и продаја најразноврснијих роба често одвија помоћу интернет огласа, без непосредног контакта купца и продавца, односно купца и робе. У њима посебно место припада преварама при куповини аутомобила, како због учесталости, тако и због значајне имовинске штете која наступа за жртву. Превара почиње тако што продавац – преварант поставља оглас да продаје, најчешће скупоцен аутомобил на одређени вебсајт, тражећи знатно нижу цену од његове тржишне вредности[79]. По правилу, такво возило не постоји, односно продавац није његов власник, нити са њим располаже, већ се детаљи о возилу, укључујући његове фотографије и опис, често преузимају са сајтова специјализованих за продају аутомобила.

Заинтересовани купац, надајући се повољнијој куповини, шаље email превараранту на контакт адресу из огласа, наводећи да је заинтересован за аутомобил. У одговору, преварант истиче, да аутомобил још увек није продат, по правилу у шпедитерској компанији. Након тога се жртви дају инструкције како и где да пошаље депозит или целу уплату продајне цене, најчешће електронским трансфером у циљу иницирања

[79] Реч је о популарним и добро опремљеним моделима аутомобила, са малим бројем пређених километара, сервисном књижицом, у јако добром стању. Цена таквих аутомобила готово је врло ниска, по правилу свега 50-60 % стварне вредности таквог аутомобила.

процеса шпедиције. Како би цела трансакција изгледала што реалније, преварант нуди купцу услуге агента продаје, коме овај може послати новац и који ће гарантовати за купопродају, у смислу да ће продавац добити новац тек када аутомобил буде испоручен купцу. У стању заблуде, при настојању да искористи повољну прилику за набавку доброг возила, жртва уплаћује средства, након чега се продавцу и (лажном) агенту губи сваки траг.

Већ при првом контакту купца и продавца, овај други објашњава зашто је аутомобил тако јефтин – нпр. смишља причу о томе како се сели у Велику Британију, где не може да вози аутомобил са воланом на десној страни. На питање купца где се аутомобил може погледати, преварант говори како је већ неколико пута долазио у државу са аутомобилом (нпр. из Велике Британије у Немачку), при чему се најављени купац није појављивао, због чега сада предлаже за себе сигурну опцију – тражи уплату новца за аутомобил на рачун шпедитерске фирме, која ће потом аутомобил допремити у државу купца. Након што купац прегледа аутомобил и потврди куповину, шпедитер ће новац пребацити на рачун продавца. При томе фирма за шпедицију, у ствари, не постоји, већ купац новац уплаћује директно на рачун преваранта.

Према другом сценарију, продавац захтева да купац уплати пола износа од продајне цене аутомобила WesternUnion-ом, на име и адресу коју му продавац наложи (по правилу, то је адреса града где се, наводно, налази аутомобил). Након што то уради, купац продавцу шаље потврду о уплати и одлази у место где се аутомобил налази да би га погледао, те заједно са продавцем, из пословнице Western Union-а подигао новац који је претходно послао и исплатио аутомобил. Међутим, одмах након уплате захтеване суме, преварант преко свог саучесника у Western Union-у подиже новац пре него што купац уопште крене на пут (Маринковић, Лајић, 2014: 193).

4.7. Превара усвојења

Превара усвојења (преваре у добротворне сврхе) представља облик преваре који често стиже нежељеним и мејлом и углавном као облик спам-а. У суштини, овде преварант апелује и циља на лица која су посебно осетљива на туђу муку и која су веома осетљива на добротворне позиве. Пошиљаоци оваквих порука се лажно представљају као представници неких добротворних организација (на пример УНИЦЕФ или УНЕСЦО, а специфично за Велику Британију БААФ (British Association for Adoption and Fostering – BAAF), регистрована организација за адоптивно и

тазвинско сродство) и у њихово име а, у ствари, за свој рачун траже уплате одређених средстава. Оно чиме преварант заокупљује пажњу жртве је носећа прича, обично, о неком убогом детету – сирочету или напуштеном од стране родитеља у циљу убеђивања лица да поднесе захтев за његово усвојење, након чега се од жртве тражи да плати трошкове процесуирања захтева.

Једна друга варијација ове врсте преваре се врши тако што и мејл садржи број рачуна родитеља детета које је у питању, уз шта се објашњава да је тај једини живи родитељ оболео од неке смртоносне болести и да му није остало много времена, уз шта се још истиче да је овај родитељ енормно богат, те би требало да том детету остави већу суму новца након смрти. У овом случају се често користи лого БААФ у циљу мамљења новца за захтев и формуларе. И у Републици Србији је било случајева везаних за преваре овог облика у смислу трансфера новчаних средстава намењених лицима у иностранству – у државама Африке (Прља et al, 2011: 50-51).

4.8. Романтичне преваре

Романтичне преваре за предмет напада имају лица који користе мреже за "судare на слепо" и социјалне мреже. Након контакта, овим путем, преварант тежи задобијању поверења жртве кроз различите облике изјава о наклоности или изливима љубави. Често преваранти живе далеко од жртве (у вечини случајева у другој држави), након чега преварант изражава незадрживу жељу да се са жртвом физички сретне. Уколико жртва пристане на сусрет, онда креће зачкољица – преварант нема довољно новца да допутује на место које је договорено за сусрет и захтева од жртве да му пошаље новац како би могао да допутује да би се видели.

Након пријема новца превара се развија на различите начине. Тада се дају најразличитија објашњења типа да је преварант због скупа непредвиђених догађаја у међувремену (или чешће у току путовања, услед, на пример, незгоде на путу) напрасно упућен у болницу при чему је неопходно да се покрију трошкови његовог лечења, да је брат преваранта отет, па је неопходно да се прикупе средства за његово ослобађање итд.[80]У даљем току догађаја преварант тражи још новца, док жртва не пресуши или престане да верује обмани.

[80] Више о овоме на http://www.prevara.info/index.php?option=com_content&task=view&id=283&Itemid=7 преузето 05.08.2018. године.

4.9. Он лајн аукцијске преваре

Ова врста превара такође представља један од веома честих облика превара. Наиме, у последње време се организују на Интернету лажне продаје или аукције предмета, ствари и робе кроз или преко аукцијских сајтова, али без намере да се роба (ствар, предмет) испоручи. Посебан облик ове врсте преваре "румунска аукцијска превара"[81]. У овом случају извршиоци отварају налог на e-bay-у (или неком другом сајту) и врше неколико значајних транскација, како би остварили добар чланski рејтинг[82] чиме би привукли могуће жртве. Оног тренутка када остваре контакт са жртвом, почињу са продајом скупе робе за своје жртве.

Интересантан је облик аукцијских превара у виду тзв. "напумпај и одбаци" (pump and dump) преваре. Овај облик превара злоупотребљава правила берзе и комбинује берзанско пословање са класичним уличним варањем. Ова превара користи обрнуту психологију панике, користећи позитивне вибрације масовним облицима спама[83] повезујући Интернет кориснике да купују одређену врсту акција на берзи, које су са великим потенцијалом услед неког неочекиваног догађаја.

Од посебне вредности су тзв. "лажне преваре", код којих је основна карактеристика давање бомбастичног и веома продорног наслова у новинама или медијима уопште, типа "Samsung продаје brand name rootkit" који је усмерен на наношење комерцијалне штете неком од произвођача и дистрибутера (Прља et al, 2011: 50-51).

4.10. Остали облици превара

У пракси се јављају и други различити облици рачунарских превара.

Превара плаћених убица представља врсту преваракоја је подтип изнуђивачких или уцењивачких превара. Жртва прима електронску пошту од члана организације нпр.

[81]Ово је ништа друго до посебан облик за који је везана вероватно организована група која води порекло из Румуније, карактеристике су да се продавац представља као особа из САД, али она обично упућује на лице које је њен сарадник у некој европској држави, користећи MoneyGram за пренос новца. Због необавезности постојања потпуне идентификације лица које преузима новац, нема потребе ни заMTCN money transfer control number (MTCN) бројем, нити за тајним одговором на питање пошиљаоца.

[82]Овај рејтинг није замишљен као начин превенције специфичних одређених преварних радњи, он представља субјективне утиске искустава корисника сумира на једном месту. У одређеним случајевима извршиоци преузму идентитет неког од добрих продаваца у циљу вршења преваре, зато треба обратити пажњу на постојање скоријих продаја и трансакција које је продавац вршио и на њихов бонитет.

[83]Уобичајено је да се оваква порука шири путем инфициране мреже ботова. Један од примера је Prime Time stores напад из, сада већ давне 2005. године. Тада је извештај са берзе о овој фирми стигао у облику ПДФ датотеке, која је тада лакше пролазила филтере маил сервера.

“Ishmael Ghost Group” који тврди да је послат да убије примаоца поруке и његову породицу. Као разлог овог смакнућа пошиљалац наводи наводни злочин против члана своје братије који је жртва “наводно” раније учинила. У изненадном обрту који је уследио када је неки члан братства указао пошиљаоцу ове поруке да познаје неког од рођака из седмог колена примаоца ове поруке и тој информацији следећег захтева за помиловање жртве од стране тог члана братства, неопходно је да жртва плати свој и живот својих ближњих (800 долара које ће послати преко Western Union-a или Money Gram-a у Велику Британију за миграцију Исламских патриота из САД) дајући му обично 72 часа да то уради (Прља et al, 2011: 54).

Превара астролошког читања функционише тако што жртва прима спам или искачућу поруку о бесплатном астролошком очитавању информација, где жртва даје податке о датуму и месту свог рођења. Након бесплатног текста о судбини по основу астролошких карактеристика, од жртве се тражи одређена новчана сума за пуну наталну карту уз обећавање постојања нечег позитивног као догађаја садржаног у овој карти. Тада жртва плаћа новац, али наравно заузврат не добија ништа, док је у већини случајева астролог недоступан за накнадни пријем мејлова (Прља et al, 2011: 54).

Превара економске стимулације је настала коришћењем ситуације велике економске кризе. У такво време жртви стижу информације о пакетима економске помоћи у САД, уз говоре и исечке тих говора председника САД Обаме, где је одређени број америчких грађана варан путем нежељених телефонских позива са снимцима говора који личе на Обамине, којима их позива на приступање одређеним сајтовима, типа www.nevergiveitback.com или www.myfedmoney.com у циљу добијања економске стимулативне помоћи. Наравно, да би се добила ова економска помоћ, неопходно је да се претходно унесу многи лични подаци и плате трошкови обраде ових информација у износу од 28 долара, након чега нема никакве економске помоћи (Прља et al, 2011: 54).

Преваре за сајтове о пословима постоје када жртве дају мношто личних података, при чему им се обећавају послови код куће, слање посебних софтвера за обављање тих послова, плаћање на сат, или плате од неколико хиљада долара недељно. Овакви сајтови су веома убедљиви, толико да су многе жртве уновчавале преварне чекове или примале непостојеће или постојеће новчане дознаке са потребом даљег трансфера већих сума новца и сл. Као подврста ове преваре постоји када се оглашавају оваква лица жртве као незапослени, али да би се огласили, извршиоци од жртава траже копије последњих чекова плата, након чега користе овакве податке за даље криминалне активности.

Лажни антивирус програми и искачући рекламни садржаји постоје када се тест скенирањем на рачунару жртве наводно проналазе вируси и тројанци. Затим им се препоручује неки софтвер којим се такви вируси могу скинути, под условом да жртва кликне на тај линк. Тог тренутка се на жртвин рачунар даунлоадује злоћудни (малициозни) код у облику тројанаца, вируса или килогера.

Посебно се наглашава потреба заштите од стручних превара које представљају врсту инсајдерске преваре. Овде запослени у одређеној добростојећој фирми злоупотребљава ресурсе фирме како би варао жртве, али и саму фирму. Проблем код ове преваре се јавља у виду протека времена од извршења преваре до њеног откривања од стране оштећених (Прља et al, 2011: 54-55).

ЗАКЉУЧАК

Високотехнолошки криминал представља вршење кривичних дела код којих се као објекат или средство извршења јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски програми, као и њихови подаци у материјалном или електронском облику. У кривично законодавство Републике Србије компјутерска (рачунарска) кривична дела су први пут уведена новелама Кривичног закона из 2003. године. Кривичним закоником из 2005. године ова кривична дела су систематизована у глави XXVII под називом Кривична дела против безбедности рачунарских података".

Компјутерска, тј. рачунарска кривична дела су дефинисана како одредбама међународних докумената, тако и у националном праву.

На међународном плану, ова кривична дела су прописана одредбама Конвенције Савета Европе о високотехнолошком криминалу из 2001. године. У њеном првом одељку прописано је да се она примењује у односу на кривична дела која за објект заштите имају поверљивост, интегритет и доступност компјутерских података и система, а то су:

- "неовлашћени приступ", под којим се подразумева неовлашћено приступање компјутерском систему или неком његовом делу, које је учињено са одговарајућом намером учиниоца (члан 2.);

- "недозвољено пресретање", које представља, уз помоћ одговарајућих техничких уређаја, извршено неовлашћено пресретање компјутерских података који нису јавне природе приликом њиховог "кретања" ка компјутерском систему, из компјутерског система или унутар самог компјутерског система, које је учињено са одговарајућом намером учиниоца (члан 3.);

- "оштећење података", које обухвата противправно оштећење, брисање, кварење, мењање или прикривање компјутерских података, уз постојање одговарајуће намере учиниоца (члан 4.);

- "ометање система" које постоји када се неовлашћено и у већој мери омета функционисање компјутерских система путем уношења, преношења, оштећења, брисања, кварења, мењања или прикривања компјутерских података, уколико је нека од наведених радњи преузета са одговарајућом намером учиниоца (члан 5.) и

- "злоупотребу уређаја", која се састоји у производњи, продаји, набављању ради употребе, увозу, дистрибуцији или на други начин стављању на располагање средстава и опреме који су намењени извршењу неког од кривичних дела прописаних у чл. 2-5.

(члан 6.). Објект радње такође могу бити и компјутерске лозинке, шифре за приступ или слични подаци путем којих се може приступити компјутерском систему као целини или неком његовом делу уколико се нека од предвиђених радњи извршења преузима са намером да они буду употребљени за извршење неког од кривичних дела предвиђених у чл. 2-5.

На националном плану, најзначајнији је, *lex specialis* закон из области сузбијања кривичних дела високотехнолошког криминала у Републици Србији, и то Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала у коме су дати појмови икарактеристике, односно врсте кривичних дела високотехнолошког криминала, као и систем надлежних државних органа за њихово откривање и сузбијање.

Овде се под компјутерским криминалитетом подразумева вршење кривичних дела код којих се као објекат или средство извршења јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски програми, као и њихови подаци у материјалном или електронском облику.

Овим законом се предвиђа и оснивање посебних органа за борбу против високотехнолошког криминала у оквиру постојеће судске и тужилачке организације и Министарства унутрашњих послова. У Вишем јавном тужилаштву у Београду формирано је Посебно одељење за борбу против високотехнолошког криминала, тј. Посебно тужилаштво. Радом посебног тужилаштва руководи Посебни тужилац за високотехнолошки криминал кога поставља Републички јавни тужилац из реда заменика јавних тужилаца који испуњавају услове за избор за заменика вишег јавног тужиоца, уз писмену сагласност лица које се поставља. Предност имају заменици јавних тужилаца који поседују посебна знања из области информатичких технологија.

Ради обављања послова органа унутрашњих послова у вези са високотехнолошким криминалом, у оквиру Министарства унутрашњих послова образује се Служба за борбу против високотехнолошког криминала, која поступа по захтевима Посебног тужиоца. За поступање у овим предметима надлежан је Виши суд у Београду, за територију Републике Србије, односно у другом степену Апелациони суд у Београду. У Вишем суду у Београду је образовано Посебно одељење за борбу против високотехнолошког криминала. Судије у одељење распоређује председник Вишег суда у Београду из реда судија тог суда, уз њухову сагласност. Предност имају судије које поседују посебна знања из области информатичких технологија. Територијална надлежност наведених органа успостављена је на целој територији Републике Србије.

Најважније карактеристике високотехнолошког криминала су:

- објект заштите је безбедност рачунарских података или информационог система у целини или његовог појединог дела (сегмента),

- посебан, специфичан карактер и природа противправних делатности појединаца,

- посебна знања и специјализација на страни учиниоца ових кривичних дела која искључује могућност да се свако, било које лице нађе у овој улози,

- посебан начин и средство предузимања радње извршења – уз помоћ или употребом (злоупотребом) рачунара,

- намера учиниоца као субјективни елемент у време предузимања радње која се огледа у намери прибављања за себе или другог користи или наношења штете другом физичком или правном лицу и

- велика динамичност и изузетна шароликост појавних облика, форми и видова испољавања.

Ефикасно откривање и сузбијање високотехнолошког криминала укључује и веома специфичне оперативне мере и радње, као и посебне доказне радње. У питању су интернет патроле, пресретање телекомуникација у реалном времену, трагање на мрежи – *Tracing* и сл. Такве и сличне мере често се срећу у упоредном праву. У Републици Србији је сам поступак откривања и доказивања кривичних дела уопште, па и кривичних дела високотехнолошког криминала регулисан одредбама Законика о кривичном поступку.

У Републици Србији је, нажалост, могућност Одељења за високотехнолошки криминал Вишег јавног тужилаштва у Београду за примену специјалних истражних техника у дужем периоду била ограничена само на примену члана 144. Законика о кривичном поступку који се односи на достављање података о стању пословних и личних рачуна осумњичених, али само за кривична дела за која је прописана казна затвора од најмање четири године. Због тога су надлежни државни органи били принуђени да се користе постојећим, "класичним" овлашћењима.

Ако се прибављање електронске поште осумњиченог, односно окривљеног од интернет провајдера, уз наредбу судије за претходни поступак, спроводи применом члана 168. ЗКП којим је регулисана предаја писама, телеграма и других пошиљки од субјеката регистрованих за пренос информација, упућених окривљеном или које он одашиље, ако постоје околности због којих се може основано очекивати да ће дате пошиљке послужити као доказ у кривичном поступку.

Поштанска, телеграфска и друга предузећа, друштва и лица регистрована за преношење информација су дужна да овлашћеним службеницима полиције (односно БИА и ВБА) омогуће извршење наведених мера. Неспорно је да то омогућава прикупљање комуникационих података у складу са одредбама Конвенције о високотехнолошком криминалу, али проблеми у пракси су настајали због специфичности начина прибављања доказа за тако софистицирана кривична дела, будући да се до њих често долази мониторингом на мрежи у реалном времену.

Према одредбама члана 153. ЗКП у предмете који се могу привремено одузети се убрајају, поред оних оних којих могу представљати средство или објекат извршења кривичног дела високотехнолошког криминала, и уређаји за аутоматску обраду података и опрема на којој се чувају или се могу чувати електронски записи. Лице које се користи овим уређајима и опремом дужно је да органу који води поступак, на захтев суда, омогући приступ и да пружи обавештења потребна за њихову употребу. Пре одузимања ових предмета орган који води поступак ће у присуству стручног лица извршити преглед уређаја и опреме и пописати њихову садржину. Најзад, ако корисник присуствује овој радњи, може ставити примедбе. Очигледно је да је законодавац у овом случају уважио аргументоване захтеве тужилачке струке.

У теорији је изражен став да су кривичнопроцесне одредбе које су о посебног значаја за борбу против високотехнолошког криминала садржане у члану 167. ЗКП се даје могућност да судија за претходни поступак, на писмени и образложени предлог јавног тужиоца, нареди надзор и снимање телефонских и других разговора или комуникација другим техничким средствима оних лица за која постоје основи сумње да су сама или са другим лицима извршила одређена кривична дела. Такво схватање је било прихватљиво само делимично и условно, на пример када се конкретан случај високотехнолошког криминала односи на прање новца. С тим у вези треба нагласити да је за откривање неких од типичних дела високотехнолошког криминала може користити и мера рачунарског претраживања података, која је значајна због све израженије компјутеризације личних и других података, те великих могућности које ти подаци пружају у вези са прибављањем доказа, а с друге стране преставља гарант заштите у коришћењу личних података од државних органа у таквим поступцима.

Такође, за откривање и доказивање рачунарских кривичних дела од великог значаја је и мера рачунарског претраживања података (растер потрага), која се састоји у аутоматском претраживању већ похрањених личних и са њима непосредно повезаних података и њиховом аутоматском поређењу са подацима који се односе на кривично

дело из члана 162. ЗКП-а и на осумњиченог, да би се као могући осумњичени искључила лица за која не постоји вероватноћа да су повезана са кривичним делом. По својој суштини то је негативна растер потрага која доприноси елиминацији одређених лица из круга осумњичених аутоматизованим претрагама у полицијским, административним и другим евиденцијама. Другим речима, тим методом елиминишу се одређена лица из круга оних која се служе лажним идентитетом, туђим кредитним картицама и слично.

Из наведених карактеристика, шароликости и мноштва појавних облика, произилази да посебан значај у структури кривичних дела високотехнолошког криминала има рачунарска превара. Ово је, иначе, кривично дело предвиђено у члану 301. Кривичног законика Републике Србије.

У великом броју држава као узор у стварању правног оквира за супротстављање високотехнолошком криминалу послужила су решења садржана у Конвенцији о високотехнолошком криминалуи Допунском протоколу уз њу (које је ратификовала Република Србија 2009. године). Не умањујући допринос Конвенције у сузбијању кривичних дела високотехнолошког криминала имајући у виду да је тренутно технолошко окружење далеко од тога да је идентично стању од пре више од десет година, процесноправне одредбе која се заснивају на решењима из поменуте Конвенције су неприхватљива и застарела, па не могу дати одговарајуће резултате у откривању и обезбеђењу доказа за потребе вођења кривичног поступка.

Данас је у далеко већој мери комликованије ући у траг извршиоцу ових кривичних дела, открити криминалне активности на Интернету и обезбедити електронске доказе него 2001.године, јер процес својеврсне "дигиталне глобализације" наставља да се убрзава, а постављени оквир је више реактиван, него проактиван, а није ни технички неутралан. Примера ради, постоји обиље комуникационих мрежа и средстава: подаци се размењују уз помоћ привремених *online* датотека и сервера, а у све широј употреби су паметни мобилни телефони којима се приступа Интернету, *VOIP* технологија, апликацијеса систематском енкрипцијом (*Skype*), те софтвери који прикривају комуникациони канал и онемогућавају утврђивање адресе извора и одредишта комуникације (какав је *TOR –The Onion Roter*), па је потребно експедитивно деловати да би се открио траг или извор комуникације.

Проналажење извршиоца кривичних дела високотехнолошког криминала преко IP адреса није више толико једноставно, као пре неколико година, из више разлога: тачно је да се уз помоћ IP адресе може открити веза са одређеним пружаоцем Интернет

услуга и територијом одређене државе, али то не значи да ће се та адреса довести у везу са крајњим корисником јер су све више у употреби динамичке IP адресе. Осим тога, могуће је коришћење одређених програма прикривати, односно исте мењати. Стога је неопходно преиспитати основне постулате на којима почива Конвенција Савета Европе, а тиме и решења у националним системима држава потписница, међу којима је и Република Србија, односно размотрити потребу унапређења постојећих и предложити увођење нових решења у кривичном процесном праву.

Поред закључка да је у националним законодавствима неопходно у што краћем року усвојити адекватне материјалноправне и процесноправне законе који ће инкорпорирати мере усаглашене са Конвенцијом о високотехнолошком криминалу, а у складу са могућностима на простору сваке државе појединачно, неопходно је истаћи и чињеницу да је потребан и већи степен пажње научне и стручне јавности, макар у оном сегменту који је потребан да се карактеристике злоупотреба информационих технологија уваже на адекватан начин.

Исто тако, питање злоупотреба информационих технологија, нарочито уколико су у питању појавни облици који обухватају различите врсте преварних манипулација са елементима рачунарских система, није само правно питање. Наиме, сасвим је јасно да се одређеној појави друштво адекватно може супротставити само уколико сагледа све њене карактеристике и уђе у све поре њенихспецифичности. С обзиром да се ради о проблему који узрокује огромне финансијске губитке великог броја, не само развијених земаља, већ и држава које пролазе кроз процес транзиције, потребно је обратити пажњу на економске ефекте ових појава на привредне токове у свакој држави појединачно.

Иако је данас немогућ живот и функционисање друштва у целини без употребе рачунара и савремене информатичке технологије, сазрела је свест да се ова корисна и потребна средства могу користити за недопуштене, противправне циљеве, у првом реду, за прибављање противправне имовинске користи за неко лице или за наношење штете другима.Како у великом броју држава нису предвиђене адекватне радње и мере ради откривања и обезбеђења доказа за потребе вођења кривичног поступка за кривична дела високотехнолошког криминала, постоји потреба да се одговарајућим прописима у националним законодавствима надлежним органима дају овлашћења која су неопходна за истрагу и гоњење кривичних дела учињених у вези са рачунарским системима, као и других кривичних дела за гоњење којих је неопходно прикупити податке у електронском облику.

Ова овлашћења би требало да одговарају различитим циљевима, као што су прикупљање доказа, лоцирање извора и идентификовање учиниоца кривичног дела. У том смислу, поставља се питање, да ли правном регулисању тих овлашћења треба приступити реактивно или проактивно. Такође, неопходно је одредити у односу на која кривична дела се специфична овлашћења надлежних државних органа предузимају: да ли у односу на кривична дела која су у законима одређена као дела против рачунарских система, дела чије радње су предузете злоупотребом рачунара или у случају када је потребно обезбедити доказ у електронском облику без обзира о ком кривичном делу се ради.

Веома је важно истаћи значај сузбијања рачунарских превара.

Под рачунарском преваром се, према одредбама члана 301. Кривичног законика Републике Србије сматра уношење нетачног податка, пропуштање уношења тачног податка или на други начин прикривање или лажно приказивање податка чиме се утиче на резултат електронске обраде и преноса података у намери да се себи или другом прибави противправна имовинска корист и тиме проузрокује имовинска штета другом лицу. У овом раду је дат приказ неких карактеристичних превара из домена високотехнолошког криминалитета.

Најпре се спомиње нигеријска превара, која представља методу вршења кривичног дела преваре уз помоћ рачунара. Њено извршење најчешће почиње писмом или електронском поруком којаје тако осмишљена да изгледа као да је намерно послата примаоцу поруке. Радња извршења „нигеријске преваре“ углавном почиње убеђивањем „жртве“ преваре да учествује у подели одређених новчаних фондова под условом да унапред уплати одређени новчани износ који је, у највећем броју случајева, неупоредиво мањи од оног износа који би требало да добије као корист од тог фонда.

Такође, значајне су и клик преваре. Разликују се два типа ових превара. То су: а) преваре од стране учесника и б) преваре од стране објављивача.

Први вид ове преваре најчешће се не врши ради стицања противправне имовинске користи, пошто ње заправо ни нема, већ у намери да се оштети или сузбије пословна конкуренција. Ова превара везује се најчешће за рекламе које се обављају по систему AdWords, када конкуренција врши превару према конкурентној фирми која је објавила рекламу. Извршилац, знајући да сваки клик на рекламу кошта његову пословну конкуренцију доста новца, смишља превару у оквиру које ће на одређеном интернет сајту где је реклама објављена она бити вишеструко пута посећена, понекад и аутоматским путем, вештачки преко botnet-а. Тиме се пословној конкуренцији наноси

велика материјална штета, пошто заправо нема користи која настаје када се врше праве посете рекламама од стране корисника. Такве нападе често врши пословна конкуренција коришћењем савремених рачунарских метода из области високотехнолошког криминала.

Превару од стране оглашивача врши лице које је објавило рекламу, тј. сам власник интернет сајта на коме је реклама објављена (или где је објављено више реклама). То власници интернет сајтова, где су објављене рекламе, чине са унапред смишљеном идејом: да остваре противправну имовинску корист вршењем кривичног дела рачунарске преваре на штету својих клијената који су код њих објавили рекламу. Пошто лице, компанија или друга организација која објављује рекламу власнику интернет сајта плаћа за сваку посету реклами од стране корисника, власнику интернет сајта је у интересу да рекламу коју је објавио преко њега посети што више корисника. Извршиоци кривичних дела на чијим су интернет сајтовима објављене рекламе вештачки повећавају број таквих посета у жељи да зараде више новца. Најпростији облик таквих превара своди се на то да се ангажују различита лица која ће посећивати рекламе. На интернету постоји много интернет сајтова и сервиса који пружају могућност за упознавање, дружење и забављање.

Поред наведених, дат је приказ и најважнијих обележја других преварних облика, и то: вирусне преваре, преваре при куповини путем интернета, преваре усвојења, романтичне преваре, on line аукцијске преваре и други мање присутни облици превара, попут преваре плаћених убица, превара астролошког читања, превара економске стимулације и преваре за сајтове о пословима.

Ради се различитим преварним облицима из домена високотехнолошког криминала. Наведена појава се може ефикасно спречавати једино акцијама на глобалном нивоу, како би се створила свест о опасности коју она са собом носи. Потребно је такође да се ефикасно и квалитетно предузму активности на расветљавању начина извршења тих кривичних дела и њиховог презентовања широј јавности путем јавних гласила (новине, телевизија). Такође је потребно појачати и сарадњу на националном, регионалном и глобалном плану, посебно када су у питању међународна полицијска и кривичноправна сарадња.

Чињеница је да феномен нигеријских превара, али и свих других превара у високотехнолошком криминалу у Републици Србији није довољно познат широј јавности и корисницима интернета, посебно зато што татема није довољно заступљена у медијима. Превентивно деловање државних органа као што су полиција и

тужилаштво има кључну улогу када јеспречавање ове појаве у питању. Пошто сарадња са државама из којих севрши ова врста кривичних дела (државе Африке) није на завидном нивоу, потребно је штохитније деловати проактивно. То значи да треба искористити потенцијал медија и да се на тај начин скрене пажња домаћој јавности на финансијске губитке који настају као последица различитих облика кривичних дела рачунарских превара. Превентивна улога полиције у заштити корисникаинтернета са територије Републике Србије од „нигеријских превара“ таквим активностима сигурно би била успешнија и сврсисходнија од репресивних активности које се предузимају након сазнања да је кривично делоизвршено.

Данас живимо у времену када је коришћење Интернета постална сасвим нормална и уобичајена “активност” људи, почевши од најмлађих, па до људи у позном животном добу. Постало је готово немогуће имати мобилни телефон који нема могућност приступа Интернету. Социјалне мреже, попут Facebook-a и Instagram-a су постале веома приступачне, које се користе сада путем мобилних телефона, таблета и других електронских уређаја. Масовном употребом Интернета, јавило се доста последица, што позитивних, што негативних.

С једне стране, интернет је умногоме олакшао живот и рад људи, компанија, привреде и државе у целини. Тако је олакшано и убрзано обављање свакодневних послова уз многе друге погодности које савремена информациона технологија са собом носи. Но, са друге стране, исто тако се повећала, и стално се повећава могућност злоупотреба таквих технологија од стране несавесних појединаца и група. У томе се огледа предност високотехнолошког криминала, он се развија и “расте” са развојем Интернет технологија и рачунарства.

То је довело до пораста “информатичке писмености” људи, што је довело и до пораста свести о штетним ефектима и преварним радњама које се врше на Интернету. Такође, многе апликације које се данас пројектују и социјалне мреже које су у употреби су развиле својеврсне заштитне механизме попут шифровања, кодирања преписки, двоструке потврде идентитета и сл., у циљу заштите софтвера, повећања сигурности и веће безбедности корисника социјалних мрежа. Судећи по тренутној тенденцији и брзини развоја и осавремењивања науке и Интернет технологије, каква ће ситуација бити наредних година може се само претпостављати.

ЛИТЕРАТУРА

1. Бошковић, А. Кесић, Т. (2015). *Кривично процесно право*. Београд: Криминалистичко-полицијска академија.
2. Bidgoli, H. (2006). *Handbook of Information Security*. Hoboken: John Wiley & Sons.
3. Buchanan, J. Grant, A. (2001). *Investigating and Prosecuting Nigerian Fraud*, U.S. Attorneys' Bulletin, Vol 49, No 06. USA.
4. Влаовић-Беговић, С. Томашевић, С. (2016). *Одговорност ревизора за откривање рачуноводствених превара*. Нови Сад: "Школа бизниса".
5. Gandhi, M. (2006). *Badvertisements: Stealthy click-fraud with unwitting accessories. Journal of Digital Forensic Practice*. Taylor & Francis, Great Britain.
6. Dyrud, M. (2005). *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.
7. Ђорђевић, Ђ. (2014). *Кривично право – посебни део,* Београд: Криминалистичко-полицијска академија;
8. Ђурђевић, З. Радовић, Н. (2015). *Стратешки правци Европске уније за супротстављање криминалитету и њихов значај за Републику Србију*. Београд: Криминалистичко-полицијска академија.
9. Ianelli, N. Hackworth, A. (2007). *Botnets as a Vehicle for Online Crime, The International Journal of Forensic computer science.* Great Britain.
10. Игњатовић, Ђ. (2000). *Појмовно одређење рачунарског криминала*. Београд: Компјутерски криминал.
11. Jansen, B. (2007).*Click Fraud*. SAD: The Pennsylvania State University.
12. Јовашевић, Д. (2014). *Кривично право – Посебни део*. Ниш: Досије студио.
13. Комлен-Николић, Л. (2008). *Проблеми домаћег правосуђа у борби против високотехнолошког криминала*. Београд: Ревија за безбедност.
14. Комлен-Николић, Л. (2010). *Сузбијање високотехнолошког криминала*. Београд: Удружење тужилаца и заменика јавних тужилаца Србије.
15. Лазаревић, Љ. (2011). *Коментар Кривичног законика РС*. Београд.
16. Longe, B. Chiemeke, C. (2008). *Cyber Crime and Criminality in Nigeria – What Roles are Internet Access Points in Playing?* European Journal of Social Sciences – Volume 6, Number 4, Great Britain.
17. Маринковић, Д. Лајић, О. (2016). *Криминалистичка методика,* Београд: Криминалистичко-полицијска академија.
18. Матијашевић, Ј. Игњатијевић, С. (2012). *Врсте интернет превара – појам, значај и утуцај на економске и моралне аспекте друштвене заједнице*. Јахорина.
19. Матијашевић-Обрадовић, Ј. (2015). *Европски стандарди за борбу против високотехнолошког криминала*, Правни факултет у Новом Саду.
20. Мијалковић, С. Бајагић, М. (2012). *Организовани криминал и тероризам*. Београд: Криминалистичко-полицијска академија.
21. Миладиновић-Богавац, Ж. (2017). *Пословне преваре у сајбер простору*. Ниш: Друштво економиста "Економика".
22. Петровић, С. (2000). *Рачунарски криминал*. Београд: Министарство унутрашњих послова РС.
23. Писанић, М. (2013). *Потребни нормативни одговор на проблеме откривања и доказивања дела високотехнолошког криминалитета.* Правни факултет у Новом Саду.

24. Прља, Д. Ивановић, З. Рељановић, М. (2011). *Кривична дела високотехнолошког криминала*. Београд: Институт за упоредно право.
25. Прља, Д. Рељановић, М. Ивановић, З. (2012). *Интернет право*. Београд: Институт за упоредно право.
26. *Процена претње од тешког и организованог криминала (SOCTA)*, (2015). МУП Републике Србије.
27. Ранђеловић, Д. (2012). *Високотехнолошки криминал*. Београд: Криминалистичко-полицијска академија.
28. Рељановић М. Ивановић З. Цвијовић М. (2015). *Превенција и борба против ВТК и безбедност при комуникацији на интернету*, Београд.
29. Smith, R. Grabosky, P.N. Urban, G.F. (2004). *Cyber criminals on trials, defining and measuring cyber crime,* Newyork: Cambridge University Press.
30. Smith, R. Holmes, M. Kaufmann, P. (1999). *Nigerian Advance Fee Fraud*, Trends and Issues in crime and criminal justice, Australian Institute of Criminology, Australia.
31. Soubusta, S. (2008). *On Click Fraud, Dusseldorfer Informations wissenschaft*. Germany: Information swissenschaft & Praxis.
32. Стојановић, З. (2018). *Коментар Кривичног законика*, Београд: "ЈП Службени гласник".
33. Стојановић, З. Делић, Н. (2018). *Кривично право – посебни део*, Београд: Правна књига.
34. Урошевић, В. (2009). *Нигеријска превара*. Београд: Безбедност. МУП Р. Србије.
35. Урошевић, В. Ивановић, З. Уљанов, С. (2012). *Мач у World Wide Web-у – Изазови високотехнолошког криминала*. Београд: Eternal mix.
36. Chawki, M. (2009). *Nigeria Tackles Advance Fee Fraud*. Journal ofInformation, Law & Technology, University of Warwick, Great Britain.

Остала истраживачка грађа

Правни прописи

1. Закон о ауторским и сродним правима, *"Службени гласник РС"*, бр. 104/2009, 99/2011 и 119/2012.
2. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, *"Службени гласник РС"*, бр. 61/2005 и 104/2009.
3. 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 – Међународни уговори"*, бр. 19/2009.
4. Закон о потврђивању конвенције о високотехнолошком криминалу, *"Службени гласник РС – Међународни уговори"*, бр. 19/2009.
5. Законик о кривичном поступку*, "Службени гласник РС"*, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 и 55/2014.
6. Кривични законик Републике Србије. *"Службени гласник РС"*, бр. 85/2005, 88/2005 - испр. 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 и 94/2016.

Електронски извори

1. http://www.ic3.gov/
2. http://theage.com.au/it-pro/security-it/operation-ghost-click-bosts-cybercrime-ring-that-hit-4m-computers-20111110-1n8v3.html
3. http://www.singi.com/podrske/crvi.html
4. http://www.sophos.com/blogs/chetw/g/2010/04/03/3-types-viruses-demystified
5. http://www.prevara.info/index.php?option=com_content&task=view&id=283itemid=7
6. http://www.aic.gov.au/statistics/hightech/cybercrime.html
7. http://www.b92.net/tehnopolis/vesti.php?yyyy=2011&mm=04&nav_id=505734
8. http://www.beograd.vtk.jt.rs/
9. http://www.bos.rs/cepit/idrustvo/sk/regulacijasajberkriminala.php
10. http://www.bos.rs/cepit/idrustvo/sk/tipovisajberkriminala.php
11. http://www.google.rs/search?hl=sr&source=hp&q=provaljivanje+u+kompjuterski+sistem&meta=&aq=f&aqi

САЖЕТАК

Непрестана и континуирана експанзија информационих технологија је, поред многобројних предности које је донела савременом човеку у свим облицима живота и рада, довела и до настанка новог облика криминалног понашања, и то високотехнолошког криминала, и до његове експанзије и константног развоја. То је, по мишљењу аутора, најфлексибилнији вид криминалитета, јер свака иновација која буде откривена из домена информационих технологија и рачунарства, с циљем развоја нове функције и омогућавања обављања неких делатности путем Интернета, истовремено бива и злоупотребљена од стране софистицираних извршилаца зарад стварања новог појавног облика, модуса извршења кривичних дела високотехнолошког криминала. На тај начин се развијају и умножавају преваре извршене коришћењем рачунара, односно путем Интернета.

Сам рад је конципиран у неколико целина, тј. глава. Најпре се говори о неким основним постулатима и карактеристикама високотехнолошког криминала, врстама тог криминалитета и њиховим појавним облицима. У наредној глави се говори о правном оквиру за борбу против високотехнолошког криминала, и то најпре на међународном плану, уз приказ најзначајнијих одредби међународних докумената који имају круцијални значај за сузбијање високотехнолошког криминала.

Потом следи излагање националног правног оквира уз приказ законских решења из српског законодавства у овој области. Надаље је у раду изложен кривичноправни оквир, у оквиру кога је дата систематска подела кривичних дела која спадају у домен високотехнолошког криминала, према одредбама Кривичног законика Републике Србије. Тежиште је овде на групи кривичних дела против безбедности рачунарских података, код које је објашњено свако кривично и након тога дат осврт на остале групе кривичних дела из Кривичног законика, који садржи дела која, на основу начина или средства извршења, могу квалификовати као кривична дела високотехнолошког криминала, уз назначење о којим кривичним делима је реч.

Централна глава мастер рада се односи на, кривично дело преваре као дело имовинског криминалитета, његово појмовно одређење, карактеристике, након чега се разматрање наставља са облицима превара из домена високотехнолошког криминала. Овде је изложено неколико најзначајнијих врста, тј. појавних облика превара, почевши

од рачунарске преваре која има статус кривичног дела, па преко нигеријске преваре до клик и осталих облика преваре.

Таквим приступом је настојано да на свеобухватан, систематски начин буду приказана најважнија обележја високотехнолошког криминала уопште и да се на основу тога уради анализа његових облика испољавања у виду преваре. Преваре у високотехнолошком криминалу су нешто што све више интригира људе, а нажалост и погађа, тј. оштећује њихову имовину. Многи људи још увек немају праву представу о рачунарским преварама, начинима и средствима њиховог извршења, као и могућностима њиховог сузбијања. Стога је жеља аутора да оваквим приступом рад приближи и лаицима, односно онима који немају адекватна знања из домена високотехнолошког криминала и његовог сузбијања.

Кључне речи: високотехнолошки, криминалитет, превара, рачунар, имовинска корист, интернет.

SUMMARY

FRAUD AS A FORM OF HIGH-TECH CRIME

The ongoing and continuous expansion of information technology, in addition to the numerous advantages it has brought to modern man in all forms of life, has also led to the emergence of a new form of criminal behavior, high-tech crime, and its expansion and constant development. In my opinion, this is the most flexible type of crime, because any innovation that emerges, or is discovered in the field of information technology and computing, with the goal of developing some new functions and the enabling of performing of some of the activities on the internet, is being abusedat the same time by sophisticated perpetrators in order to create the new forms, the modus operandi of high-tech crime. In this way, the fraudscommitted by using the computers or (and) the internet are being developed and multiplied.

The master's thesis itself is conceived in several parts, ie chapters. In its opening, some basic postulates and characteristics of high-tech crime, its types of crimes and their forms are discussed. The next chapter discusses the legal framework for the fight against high-tech crime, at first, on the international level, with the presentation of the most important provisions of international documents of crucial importance for high-tech crime, and then the national legal framework, and the presentation of legal solutions from our legislation in this area. Furthermore, in my work, I presented the legal framework, within which the systematic division of criminal offenses that belongs to the domain of high-tech crime was provided, according to the provisions of our Criminal code.The focus here is on a group of criminal offenses against the integrity and safety of computer data, where every offence has been explained. Afterwards, I presented the overview of other groups of criminal offensesfrom our Criminal code, which contains criminal offenses that, based on the modus operandi or means of execution, can be parts of high-tech crime, with the indication of the type of the crimal offense. The central chapter of my master's thesis refers to, firstly, the criminal act of fraud as the act of „property crime", its conceptual determination, characteristics, and after that its connection with frauds in the domain of high-tech crime. Here are some of the most important forms of fraud, starting with the computer fraud that has the status of the criminal offense, then through Nigerian fraud, click frauds and others.

In this way, with such an approach, I tried to show the most important features of high-tech crime in a comprehensive and systematic manner, and on that basis, tomake a good

introduction to the forms of frauds. Frauds in high-tech crime are something that intrigues people more and more, and unfortunately, it damages them too, and many of them have no real idea of how it comes to them, whether and how are they punitive, and, most importantly, how to resist them, how to stay safe from them. Therefore, I wanted to bring this work closer to laymen, or to those who do not have adequate knowledge in the domain of high-tech crime.

Key words: high-tech, crime, fraud, computer, material gain, internet.

БИОГРАФИЈА

Александар Арсић је рођен 12.06.1994. године у Прокупљу. Основну школу "Милоје Закић" је завршио у Куршумлији, где је за одличан успех током школовања награђен дипломом "Вук Караџић". Такође, у Куршумлији је завршио и средњу школу, гимназију – природно-математички смер, са одличним успехом. Након завршетка средњег образовања, 2013. године је уписао основне академске студије криминалистике на Криминалистичко-полицијској академији у Београду.

Током школовања на Криминалистичко-полицијској академији био је члан и учесник разних секција и студентских конференција, како на националном, тако и на међународном нивоу, углавном из области међународне полицијске сарадње, илегалних миграција и трговине људима. Неке од њих су чланство у криминалистичкој секцији "Др Арчибалд Рајс", учешће на "Међународној зимској школи безбедности" у Крушеву, у Македонији, у априлу 2017. године. Такође је у статусу студента Криминалистичко-полицијске академије радио у Прихватном центру за мигранте у Прешеву, током трајања мигрантске кризе крајем 2016. године, где је испомагао припаднике Управе граничне полиције у евидентирању и процесуирању миграната који су тражили азил, односно транзитирали кроз Републику Србију.

Основне студије криминалистике је завршио у октобру 2017. године, са просечном оценом 9,18. Исте године у октобру, уписао је мастер студије на Правном факултету Универзитета у Нишу – смер унутрашњих послова.

У децембру 2017. године засновао је радни однос у Управи криминалистичке полиције у Београду.

Познаје рад на рачунару и говори енглески језик.

ИЗЈАВА О ИСТОВЕТНОСТИ
ШТАМПАНОГ И ЕЛЕКТРОНСКОГ ОБЛИКА МАСТЕР РАДА

Име и презиме аутора мастер рада: Александар Арсић

Наслов мастер рада: „Превара као облик високотехнолошког криминалитета“

Ментор: проф. др Драган Јовашевић

Изјављујем да је електронски облик мастер рада у pdf формату истоветан штампаном облику, који сам предао/ла Правном факултету Универзитета у Нишу.

У Нишу, _____

Потпис аутора

_____

ИЗЈАВА О АУТОРСТВУ И ОДОБРАВАЊУ ОБЈАВЉИВАЊА МАСТЕР РАДА

Изјављујем да је мастер рад, под насловом: „Превара као облик високотехнолошког криминалитета“

пријављен и одбрањен на Правном факултету Универзитета у Нишу:

• резултат сопственог истраживачког рада;

• да овај мастер рад у целини, нити у деловима, нисам пријављивао/ла на другим факултетима, нити универзитетима;

• да нисам повредио/ла ауторска права, нити злоупотребио/ла интелектуалну својину других лица.

Дозвољавам да се овај мастер рад чува у библиотеци и објави на сајту Правног факултета Универзитета у Нишу, са подацима о датуму одбране и комисији пред којом је рад брањен.

Аутор мастер рада: Александар Арсић

У Нишу, _____

Потпис аутора

_____