УНИВЕРЗИТЕТ У НИШУ

ПРАВНИ ФАКУЛТЕТ

Компјутерска превара

(Мастер рад)

Ментор:

Проф. др Дарко Димовски

Студент:

Христина Стевић

Бр. индекса: М011/18-УП

Ниш, 2020

САДРЖАЈ

УВОД

Развој технологије довео је до тога да компјутер буде неопходан у савременом свету и то у свим сферама човековог живота. Компјутер је средство које нам олакшава и убрзава рад и омогућава лаку и брзу доступност жељеним информацијама, а управо смо због тога постали зависни од компјутера и сајбер простора и не можемо замислити сопствени живот без истих. Колико је развој технологије произвео позитивне ефекте у друштву, толико је и негативне управо због појаве кривичних дела код којих је карактеристична злоупотреба сајбер простора. Свесни смо тога да се константно спроводе ове врсте кривичних дела, та дела се и даље усавршавају и доводе до појаве нових дела за која не постоје конкретне методе сузбијања и борбе. Најучесталије су рачунарске преваре јер се помоћу рачунарских превара лако може доћи до туђег новца и података, с тога је предмет овог мастер рада усмерен на проучавање овог облика високотехнолошког криминалитета. Бавиће се проучавањем основних облика рачунарских превара у рачунарским системима, законском регулативом Републике Србије, надлежношћу државних органа у борби против високотехнолошког криминалитета и начином извршења преваре. Овим мастер радом је предвиђено да се подигне свест о опасностима којима смо изложени као корисници рачунара, пре свега интернета као и то да смо сви ми барем једном били потенцијалне жртве неког од облика високотехнолошког криминалитета.

У свету проблем високотехнолошког криминалитета није у потпуности разрађен и објашњен јер се ради о релативно новој појави која из дана у дан представља све већу опасност за становништво. Баш због тога морамо ускладити законску регулативу и рад надлежних органа и усмерити њихову активност на проналажење и отклањање извора, услова, околности или пропуста које су резултат неовлашћеног коришћења односно злоупотребе рачунара. Поред свега тога потребна је, ако не и најбитнија, шира друштвена акција, конкретно мислим на образовање корисника рачунара како да препознају преваре и на који начин се најбоље заштитити од истих. Највећа опасност коју једна рачунарска превара може произвести јесте финансијска безбедност појединца али и привредних и пословних субјеката и државе у целини. Зато је потребно детаљно регулисање кривичних дела рачунарских превара како би се казнило противправно присвајање имовинске користи. Мастер рад је, пре свега, усмерен на анализи појма високотехнолошког криминалитета, рачунарске преваре и постојећих облика превара, са дескрипцијом законске регулативе у области спречавања превара,

начином извршења преваре и надлежности државних органа у борби против високотехнолошког криминалитета.

Циљ мастер рада је да се укаже на опасност овог кривичног дела, као и на сам значај. Превара представља једну од најозбиљнијих безбедносних претњи која се одиграва у сајбер простору у 21. веку, потребно је упозорити јавност на последице које може произвести ово кривично дело. Такође, циљ рада јесте да се опише сам појам преваре, као и њена класификација и кроз примере који су се дешавали у свету укаже на постојећу опасност и на лаковерност становништва захваљујући којој су дошли до финансијског губитка. Несумњиво је да виртуелне мреже олакшавају социјализацију корисника, размену информација и комуникацију без временских и просторних баријера. Међутим, те погодности које пружају нове технологије, истовремено су створиле и могућност за појаву различитих врста злоупотреба и криминала.

I ВИСОКОТЕХНОЛОШКИ КРИМИНАЛИТЕТ

1. Појам високотехнолошког криминалитета

Готово неограничена моћ рачунара у меморисању и брзој обради података довели су до напретка неслућених размера у обиму, брзини и квалитету производње, тровине, науке, уметности, безбедности, саобраћаја и финансијског пословања са тенденцијом сталног усавршавања. Савремено пословање, свет науке, уметности, забаве и комуникације уопште постали су готово незамисливи без рачунара. Једна од најзначајнијих и најреволуционарнијих тековина развоја техничко- технолошке цивилизације јесте рачунар, који поред предности које носи са собом, брзо је постао средство злоупотребе несвених појединаца, група и организација.[1]

Ради се о области у којој постоји повећана могућност злоупотребе у случајевима све веће примене компјутеризованих информационих система с једне стране, а с друге стране у неадекватности односно недовољности постојећих законских прописа на новонастале ситуације. Такође, ово је област у којој је велика "тамна бројка" криминалитета због компликоване технологије, која отежава откривање и доказивање, неоспособљеност истражитеља и због тога што жртве не воде рачуна о мерама осигурања и већина се не осећа угроженим због таквих дела.[2]

Како се развијају искуства и технологије, тако се развијају и дефиниције високотехнолошког криминалитета. У потрази за дефиницијом, сматра се да, с обзиром на то да високотехнолошки криминалитет може укључити све категорије криминалитета, дефиниција мора да истакне посебност, знање или коришћење рачунарске технонологије. У Европи се први пут високотехнолошки криминалитет помиње на интернационалној конференцији Савета Европе о криминолошким аспектима економског криминалитета у Стразбуру 1976. године и дефинисан је као свака илегална активност у којој се рачунар користи било као средство, било као објекат кривичног дела. Три године касније, у првој свеобухватној презентацији високотехнолошког криминалитета, под називом "Сајбер криминалитет: Приручник извора кривичног права" високотехнолошки криминалитет дефинисан је у ширем

[1] Д. Јовашевић, *Кривично право-посебни део*, Ниш, 2014, Номос стр. 111
[2] С. К. Вилић, В. Н. Ристановић, М. Костић, *Криминологија,* Ниш, 2009, Пеликан принт, стр. 178

смислу као свако илегално дело за које је познавање компјутерске технологије од суштинске важности за успешно кривично гоњење.[3]

Савет Европе је 1989. године Препоруком усвојио функционални приступ и криминалитет везан за рачунаре описао као скуп кривичних дела која су набројана и дефинисана у смерницама и препорукама за национална законодавства. У препоруци која се односи на кривично процесно право из 1995. године појављује се израз "кривична дела везана за информационе технологије" која подразумевају сва кривична дела у чијем откривању и доказивању надлежни органи морају имати приступ информацијама које се обрађују или простиру кроз компјутерске системе или системе електронске обраде података.[4]

Јерковић у свом раду „Борба против високотехнолошког криминалитета у Србији“ високотехнолошки криминалитет дефинише као радњу која се предузима уз употребу рачунара и других средстава информационих технологија, која подразумева неовлашћен приступ заштићеном рачунару или неовлашћено пресретање електронских података који су упућени са рачунара ка другом рачунару. Такође, под високотехнолошким криминалитетом Јероковић подразумева „уништавање, измену и брисање електронских података, ометање или онемогућавање функционисања рачунарског система путем оштећења, брисања, мењања или уметања електронских података, дистрибуцију недозвољених садржаја и стварање и ширење вируса и малициозног софтвера“.[5]

Аутори књиге „Мач у World wide web-у“, Урошевић, Ивановић и Уљанов, дефинишу високотехнолошки криминалитет као криминалитет извршен у целини или делимично у електронској средини, за који учинилац мора имати познавање компјутерске технологије (хардвер и софтвер) и мора поседовати атрибут намере. Под намером аутори подразумевају како средство које се користи, тако и изазивање одређене последице овим средством. У истој књизи наводи се да је рачунарски криминалитет посебан вид инкриминисаних понашања у којима се рачунарски систем (схваћен као јединство хардвера и софтвера) појављује или као средство извршења или

[3] S. Schjolberg, *The histoy of cybercrime: 1976-2014,* Norderstedt, 2014, Cybercrime research institute, стр. 51.
[4] S. Schjolberg, *The History of Global Harmoniyation on Cybercrime Legislation- The Road to Geneva,* http://www.cybercrimelaw.net/documents/cybercrime_history.pdf , приступила 24.08.2019. године
[5] Р. Јерковић, „*Борба против високотехнолошког криминалитета у Србији*“, Телекомуникације- научно стручни часопис Републичке агенције за телекомуникације, бр. 3/2009, стр. 1

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.[6]

Имајући у виду наведене дефиниције, можемо доћи до закључка да је високотехнолошки криминалитет такав облик криминалног понашања у коме се рачунар, рачунарски систем, рачунарске мреже и рачунарски подаци појављују као средство, циљ, објекат, доказ или као окружење извршења ових дела.

Високотехнолошки криминалитет обухвата скуп кривичних дела где се као средство и објекат извршења могу јавити рачунари, рачунарски подаци и мреже.[7]

Дакле, разликују се кривична дела где се рачунар може појавити као средство извршења или као објекат извршења и кривична дела у којима се Интернет користи као незаконит. Тешко је проценити број и врсте кривичних дела из области високотехнолошког криминала, такође је тешко проценити и економску штету која настаје извршењем ових кривичних дела. Ипак, из године у годину, како број тако и економска штета у сталном је порасту. Начин извршења ових кривичних дела је разнолик због саме природе савремених информационих технологија.[8]

2. Појавни облици високотехнолошког криминалитета

У пракси, готово да не постоји "чист" облик наведеног дела. Многи аутори приликом одређивања појавних облика високотехнолошког криминалитета користе два приступа:

- Један полази од општег појма високотехнолошког криминалитета и овде спадају сва дела која имају својства особена овој појави или појму.
- Други примењују метод енумерације, где се набрајају или групишу дела која се под високотехнолошким криминалитетом подразумевају.

Првој групи припадају схватања Едвардса, Валдена и Сејвџа, сматрају да се ова кривична дела могу поделити у две групе. Првој групи припадају она кривична дела у којима рачунари имају "активну" улогу, другој групи припадају

[6] В. Урошевић, З. Ивановић, С. Уљанов, *Мач у Word wide web-у: Изазови високотехнолошког криминала,* Београд, 2012, Етернал микс, стр. 24

[7] Члан 2, Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала ("Сл.гласник РС", бр. 61/2005 и 104/2009)

[8] В. Спасић, *Актуелна питања у области сајбер криминала (чланак)*, Билтен судске праксе Врховног суда Републике Србије, број 1/2006, Београд, страна 107

она кривична дела у којима се рачунари појављују као периферни објект криминала.[9]

На сличан начин се може извршити класификација високотехнолошког криминалитета у ужем и ширем смислу. Ужем смислу припадају рачунарске преваре, шпијунажа, саботажа, ширем смислу припадају остала дела.[10]

Другој групи припадају схватања Зиебера, он прихвата поделу Комитета експерата ОЕЦД-а, и сматра да се ова кривична дела могу поделити у три велике групе и то:

- Дела везана за економски криминал, овде спадају превара, крађа, саботажа и компјутерска шпијунажа, хакинг и слично.
- Дела везана за кршење приватности: илегално прикупљање и чување личних података, коришћење нетачних података, илегално откривање и злоупотреба података и слично
- Дела везана за угрожавање осталих правно заштићених интереса: угрожавање националне сигурности, интегритет процедура везаних за рачунаре и мреже података и слично.[11]

Постоји подела која је наведена у књизи "Енциклопедија сајбер криминалитета", аутора Самјуел Мек Квејда. Категоризација облика високотехнолошког криминалитета извршена је на основу радње извршења:

- Несавесно коришћење информационих система, кршење политике или праксе безбедности и тиме излагање система и података сајбер нападима.
- Конвенционалан криминалитет који користи рачунаре или друге врсте електронских и других уређаја за информационо-технолошке комуникације као подршке незаконитих активности.
- Он-лајн преваре као што су фишинг (енг. P[12]hishing)[13], пуфинг (енг. Spoofing)[14], спаминг (енг. Spamming)[15] или други начин обмањивања људи на мрежи ради

[9] Ж. Миладиновић, *Кривично дело преваре као модел остваривања сајбер криминала, докторска дисертација,* Београд, 2016, стр. 67
[10] В. Водинелић, *Методика откривања, доказивања и разјашњавања рачунарског криминалитета,* Приручник, 4/1990, стр. 323-328
[11] *The International Handbook of Computer Crime,* Chichester, John Wiley and sons, 3-27

финансијске добити, као и преваре са кредитним картицама и крађом идентитета.

- Неовлашћени упад у рачунаре и информационе системе, уз откривање лозинки ради провале у системе и мрежне или оф- лајн злочине.
- Злонамерно писање и дистрибуција рачунарских кодова који подразумевају креирање, копирање, ширење малвера (деструктивни вируси, тројанци, црви или адер/ спајвер програми).
- Дигитална пиратерија музике, филмова или софтвера, посебно преко пир-ту-пир мрежа.
- Сајбер малтретирање, претње, намерно срамоћење или принуда, као и сајбер шиканирње.
- Он-лајн ухођење и друге увредљиве сајбер понуде, нпр. сексуалне понуде, заједно са слањем нежељених слика или текстова сексуалне природе, промовисање секс- туризма, или коришћење интернета за олакшавање трговине људима у сексуалне или друге сврхе. Под овим аутор одразумева и дела дечје порнографије као веома чест облик ухођења или размене недозвољених сексуалних садржаја у којима су главни актери малолетна лица.
- Академске преваре и научне злоупотребе од стране ученика, студената, наставника, професора као плагирање, варање на испитима или лажирање методе истраживања или резултата.
- Организовани криминалитет коришћењем интернета од стране етничких група за олакшавање комбинација илегалних и легалних активности, као што су кријумчарење људи, оружја, дроге.
- Владино шпијунирање, корпоративну шпијунажу, она обухвата незакониту употребу шпијунских и Key logger софтвера за откривање података који могу бити украдени или коришћени за извршење додатних кривичних дела.

---

[13]Фишинг представља вид интернет преваре, путем које се корисник обмањује на тај начин што приступа одређеној интернет страници која у ствари представља идентичну копију оригинал странице, на којој корисник оставља своје поверљиве податке који се касније користе за различите злоупотребе.

[14] Спуфинг представља још један вид интернет преваре, која се састоји у виртуелној крађи идентитета ради добијања одређених информација. Особа која шаље поруке представља се као ваш пријатељ и на тај начин вас доводи у заблуду ради добијања неопходних информација за даљу злоупотребу.

[15] Спаминг најчешће представљају поруке које се сматрају непожељним и које прималац није тражио, а које као такве садрже неку рекламу, оглас или обавештење о добитку неке награде, игре на срећу, пословне понуде и слично.

- Сајбер тероризам када се покушава испуњење „социјалних, верских или политичких циљева изазивањем страха или оштећењем или ремећењем критичне ингормационе инфраструктуре“.[16]

II КОМПЈУТЕРСКА ПРЕВАРА

1. Појам компјутерске преваре

Компјутерска тенологија данас се може злоупотребљавати на разноврсне начине. Један од начина јесу компјутерске преваре. Представљају најраспрострањенији вид компјутерског криминалитета и имају претежно имовински карактер. Питање злоупотребе инфорационих технологија није само правно питање. С обзиром да се ради о проблему који узрокује огромне финансијске губитке, потребно је обратити пажњу и на економске ефекте на привредне токове у свакој држави појединачно.

Компјутерска превара дефинисана је 1989. године у документу Савета Европе као уношење, мењање, брисање или потискивање података или компјутерских програма, или на други начин утицање на процес обраде података, које проузрокује штету другом лицу или имовини, са намером прибављања противправне економске користи за себе или друго лице.[17]

Поред кривичних дела која су усмерена против безбедности рачунарске технологије, постоји огроман број кривичних дела која се могу извршити помоћу коришћења рачунара доста брже и лакше, а учиниоцима се доста тешко улази у траг, док су последице доста веће и озбиљније.[18]

По својој природи, најближе су привредном криминалитету и проузрокују енормне штетне последице. Компјутерске преваре се врше у намери прибављања за себе или другога противправне имовинске користи, с тим што се код њих у заблуду не доводи или одржава неко лице, као у случају обичних превара, већ се та заблуда односи на компјутер у који се уносе нетачни подаци или се пропушта уношење истих или се на

[16] C. S. McQuade, *Encyclopedia of Cybercrime,* London, 2009, Greenwood press. стр. 44.
[17] Council of Europe, Recommendation No. R (89) 9 of the Committee of Ministers to member states on Computer- related crime, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804f1094, приступила 21.09.2019. године
[18] Ј. Матијашевић, М. Петковић, *Кривична дела против безбедности рачунарских података- анализа противправних решења и значај у контексту сузбијања високотехнолошког криминала,* Зборник радова са међународне научно-стручне конференције "Криминалистичко-форензичка истраживања", Бања Лука, стр. 599

неки други начин користи рачунар како би се остварила превара у рачунарском смислу.[19] Области у којима се најчешће врши компјутерска превара јесу финансијско пословање, пореске обавезе, осигурање, социјално осигурање, прање новца итд.[20] Компјутерске преваре се могу вршити на различите начине и компјутерски деликвенти у том погледу показују заиста велику инвентивност, а компјутер за варалице представља неку врсту лаког "залогаја", попут људског мозга лишеног моћи разликовања имагинарног од стварног, чиме се испољава као савршена жртва.[21]

Као главно обележје овог кривичног дела јесте довођење одређеног субјекта у заблуду да би се тиме прибавила противправна имовинска корист. Преваранти долазе до свог циља тако што врше своје активности преко рачунара у намери да наведу жртву преваре да им открије своје основне податке или пак да им исплати извесну суму новца уколико им је за узврат обећан знатно већи новчани износ. За успешан напад битно је да је извршилац кривичног дела упознат са циљним системом, његовим функцијама сервисима и политиком заштите тог система. Неопходно је да ефикасно користи програм који ће аутоматски експлоатисати рањивости за проваљивање у рачунар. Важно је да прекрије трагове да би избегао могућност да буде детекован и праћен и такође је битно да се напад изврши веома брзо јер то онда смањује могућност да се предузму мере заштите на време.[22]

Компјутерска превара и Интернет превара се разликују. Интернет превара није увек и рачунарска превара јер неке интернет преваре одговарају класничним преварама које као средство извршења користе интернет али не и рад рачунара. Интернет превара се односи на било коју превару при чијем извршењу, како би се набалила противправна имониска корист за себе или другога користи Интернет, као што су собе за ћаскање, електронска пошта итд. Док се рачунарском преваром подразумева коришћење

[19] Ж. Алексић, М. Шкулић, *Криминалистика,* Правни факултет Универзитета у Београду и Јавно предузеће "Службени гласник", Београд, 2007, стр. 389

[20] У банкама, карактеристичан начин извршења састоји се у заокруживању сума на рачунима клијената на целе бројеве, па се тако остварена разлика електронским путем усмерава на сопствени рачун. Сличне трансакције могуће су када долази до промена каматних стопа у корист штедиша, или промене курсева валута, па се та чињеница не евидентира на време... Тако је један службеник штедионице у Хамбургу издао наредбу рачунару да, приликом обрачунавања камата, заокружује стотинке и десетине пфенинга и остатке заокруженог броја, аутоматски пребацује на његов рачун у истој банци. На тај начин, за само две године, остварио је противправну корист од око 500.000 немачких марака.

[21] J. C. Bellour, *Међународна превара,* Избор бр.1, Загреб, 1981 год., стр. 76-77

[22] Вулетић Д., *Одбрана од претњи у сајбер простору* Одбрана, Београд 2011.година стр. 22

рачунара и електронска обрада података како би се дошло до противправне имовинске користи.[23]

2.Међународно-правни оквир борбе против компјутерске преваре

У складу са Уставом Републике Србије прописана су општеприхваћена правила међународног права и међународни уговори који представљају саставни део правног поретка Републике Србије који се примењују.[24] Реч је о следећим међународним актима који се боре против компјутерске преваре:

- **Конвенција о високотехнолошком криминалу Савета Европе са додатним протоколом**

Како би се спречио високотехнолошки криминал постало је неопходно међународно повезивање држава. Конвенција је донета 23. новембра 2001. године у Будимпешти. Република Србија је Конвенцију о високотехнолошком криминалу Савета Европе ратификовала у марту 2009. године уз Додатни протокол. Поред Републике Србије, конвенцију је ратификовало још 31 држава које су уједно чланице Савета Европе.[25]

Конвенцију чини преамбула и три поглавља:

- Употреба термина,
- Материјално и процесно право,
- Међународна сарадња и Завршне одредбе.

У *преамбули* је прописано да је потребно како би се сузбио високотехнолошки криминал свакако сарадња полицијских и других релевантних органа између држава света. Такође је прописано да је потребно казнити починиоца кривичних дела која су везана за коришћење рачунара и рачунарских мрежа.[26]

---

[23] М. Бабовић, *Хакерска субкултура и компјутерски криминал,* Правни живот- часопис за правну теорију и праксу, бр. 9/2004, Удружење правника Србије, Београд, стр. 749-750

[24] *Стратегија за борбу против високотехнолошког криминала, за период 2019-2023,* http://arhiva.mup.gov.rs/cms_cir/decaipolicija.nsf/Strategija%20za%20borbu%20protiv%20visokotehnolo%C5%A1kog%20kriminala%20(2019%20-%202023).pdf , приступила 23.05.2020.године

[25] Конвенцију је могуће ратификовати иако држава није чланица Савета Европе, међу тим држава се налазе Јапан, САД, Канада, Јужноафричка Република. Конвенцију од држава чланице Савета Европе нису потписале Андора, Монако, Русија и Сан Марино.

[26] Закон о потврђивању Конвенције о високотехнолошком криминалу ("Сл.гласник РС", бр.19. март 2009.)

Прво поглавље садржи само један члан, у коме су дефинисани основни термини који се користе у Конвенцији.

Друго поглавље Конвенције регулише материјалне и процесне одредбе на које се обавезују потписнице Конвенције да ће увести у своје законодавство.

- Материјалне одредбе се одређују на следећи начин:

- Дела против поверљивости, целовитости и доступности рачунарских података и система, где спадају: незаконит приступ, незаконито пресретање, ометање података, система, злоупотреба уређаја.

- Дела у вези са рачунарима, где спадају: фалсификовање и **превара**.

- Дела у вези са садржајем, где спадају: дела у вези са дечијом порнографијом.

- Дела у вези са кршењем ауторских и сродних права.

- Други облици: покушај, помагање и подстрекавање, одговорност правног лица, санкције и мере.[27]

- Процесне одредбе су везане за овлашћења државних органа приликом истраживања кривичних дела која су повезана са новом технологијом.[28] Конвенција прописује да сви органи који су надлежни за сузбијање високотехнолошког криминала могу запленити, прегледати сваки рачунар, носач података на коме се налазе, такође имају овлашћење да од провајдера електронских комуникација прикупе све податке који се односе на употребу интернета, кредитних картица, на основу чега надлежни органи могу доћи до имена или IP адресе могућег починиоца кривичног дела.[29]

Треће поглавље се бави међународном сарадњом држава на сузбијању високотехнолошког криминала. Државе су дужне да организовано и спонтано размењују податке који се тичу извршења кривичног дела која су везана за употребу рачунара, такође је дозвољена и екстрадиција починилаца кривичних дела из једне државе у другу.[30]

[27] Convention on Cybercrime – Explanatory Report, str. 8.
[28] Чланови 14-22 Конвенције
[29] Чланови 19 и 20 Конвенције
[30] Члан 26 Конвенције

Додатни протокол уз Конвенцију о високотехнолошком криминалу

Овај протокол је донет 28. Јануара 2003. године у Савету Европе у Стразбуру. Односи се на инкриминацију дела расистичке и ксенофобичне природе која су учињена уз употребу рачунара. Наиме, протокол инкриминише понашања која нису предвиђена у Конвенцији, а која се тичу ширења нетолеранције, нетрпељивости, мржње путем рачунарских система, према верским, националним, расним заједницама.[31]

- **Директиве ЕУ о борби против компјутерске преваре**

Европска унија је донела велики број директива које су везане за сузбијање високотехнолошког криминала уопште. Најзначајније директиве су:

- ***Директива Савета Европске заједнице о правној заштити компјутерских програма***

Ова директива је донета 17. маја 1991. године, једна је од првих решења у пружању правне заштите рачунарских програма.[32] У директиви је прописано да су државе потписнице у обавези да пруже сваком физичком и правном лицу правну заштиту. Такође, у обавези су да правно санкционишу противправна понашања која се односе на:

1) Стављање у промет недозвољене копије компјутеског програма, унапред знајући да је та копија недозвољена или постоји основана сумња у њену недозвољеност.
2) Држање истих копија које су наведене у тачки 1.
3) Стављање у промет или држање средства чија је сврха да олакша недозвољено уклањање неког техничког механизма који је направљен како би се заштитио рачунарски програм.

Државе чланице су обавези да заплене све недозвољене копије рачунарског програма са националним законом. У директиви је, такође, прописано да се обезбеди

[31] Члан 1. Закон о потврђивању додатног Протокола уз Конвенцију 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.)
[32] „Council Directive of 14 may 1991 on the Legal Protection of Computer Programs“, Directive 91/250/EEC, OJ no L 122/42.

правна заштита и 50 година након смрти[33], правним лицима и анонимним ауторима, заштита почиње да тече од дана када се програм учини доступним.

- ***Директива о чувању података који су добијени или обрађени приликом пружања јавно доступних услуга електронсиске комуникације или јавних комуникационих мрежа[34]***

Директива је донета 15.03.2006. године, како би се ефикасно открио и процесуирао починилац кривичног дела чије извршење оставља електронске трагове. Ова директива представља допуну Директиве 2002/58 о обради личних података и заштити приватности у области електронских комуникација.[35] Циљ директиве је да усклади национално законодавство држава чланица, које регулишу обавезу даваоца јавних услуга комуникација да чувају податке, како би ти подаци били доступни у случају откривања кривичног дела и санкционисања починилаца. Наиме, директива се примењује само на податке о локацији и промету правних и физичких лица који су потребни ради идентификације корисника услуга.[36]

У члану 5. су одређене категорије и подкатегорије података који се чувају:

Прву категорију чине подаци који се користе како би се идентификовао **извор комуникације**.

Друга категорија података одређује **одредиште комуникације**.

У *трећој категорији* реч је о **утврђивању времена, датума и трајања комуникације**.

Четврта категорија података се односи на **откривање врсте комуникације.**

У *петој категорији* се открива **комуникацијска опрема корисника или њихове наводне опреме.**

Шеста категорија регулише који су подаци неопходни за откривање **локације опреме за мобилне комуникације.**

[33] Уколико је реч о више лица, онда до смрти последњег лица.
[34] Директива 2006/24/ЕУ Европског парламента и Савета
[35]*Службени лист Европске уније,* http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32006L0024, приступила 24.05.2020. године
[36]Л. Комлен Николић, *Сузбијање високотехнолошког криминала",* Удружење јавних тужилаца и заменика јавних тужилаца Србије, Београд, 2010. стр. 64

Свака држава чланица има обавезу да шест месеци до две године од дана комуникације чува податке.[37] Прописано је, такође, да се подаци могу чувати и дуже од две године, али уз обавезу да се обавести Комисија и друге државе чланице због чега те податке чувају и даље.[38]

3.Правна регулатива компјутерске преваре у државама бивше Југославије

У циљу спречавања компјутерске преваре потребно је да у свакој држави постоји правни и законски оквир који може спречити вршење компјутерске преваре. Потребна је повезаност између правне и информационе области, уколико постоји заједничка сарадња између ове две области постоји могућност да се компјутерска превара расветли и да се санкционишу починиоци. Уколико не постоји адекватна законска регулатива, јасно је да ће постојати тешкоћа приликом откривања овог кривичног дела јер се намеће истражним органима обавеза да случајеве компјутерске преваре подводе под стандардне форме класичног криминала.[39] У наставку биће приказана правна регулатива држава бивше Југославије.

- **Компјутерска превара у законодавству Републике Словеније**

Нови закон о ауторском праву у Словенији је донет првим реформама 1995. године, тада је, такође, покренут процес усвајања кривичноправних стандарда у кажњавању појавних облика рачунарског криминала. Сви облици рачунарског криминалитета су концентрисани у Казненом законику Републике Словеније.[40] Постоји неколико поглавља Казненог законика у оквиру ког постоје кривична дела која се базирају на злоупотреби рачунара, рачунарске технологије, информационих система или мрежа. Ради се о следећим кривичним делима:

- Кривично дело злоупотреба личних података (члан 143) које је сврстано у групи кривичних дела против људских права и слобода,

[37] 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.
[38] 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.
[39] В. Полић, мастер дипломац, *Компаративна анализа компјутерског криминала у законодавствима Републике Србије и неких страних земаља*, Универзитет Сингидунум
[40] Казнени законик (КЗ-1), „Урадни лист Републике Словеније”, шт. 55/2008, issn 1318-0576, година XVII.

- Кривично дело напад на информациони систем (члан 221) које је сврстано у групи кривичних дела против имовине,
- Кривично дело упад у пословни инфомациони систем (члан 237) које је сврстано у групи кривичних дела против привреде.

Последња промена Закона о ауторском праву Републике Словеније, из 2004. године, увела је строже мере како би се смањила стопа пиратерије. Словенија је донешењем прописа и адекватним примењивањем свакако испунила све захтеве које је прописала Конвенција о високотехнолошлом криминалу.[41]

У Казненом законику Републике Словеније није предвиђена компјутерска превара.

- **Компјутерска превара у законодавству Републике Хрватске**

Република Хрватска је кривична дела која су повезана са рачунарским криминалом регулисала у Казненом закону.[42] У поглављу XXV садржана су кривична дела против рачунарског система, програма и података. Реч је о следећим делима:

- Неовлашћени приступ (члан 266),
- Ометање рада рачунарског система (члан 267),
- Оштећење рачунарских података (члан 268),
- Неовлашћено пресретање рачунарских података (члан 269),
- Рачунарско кривотворење (члан 270),
- Рачунарска превара (члан 271),
- Злоупотреба направе (272),
- Тешка кривична дела против рачунарског система, програма и података (члан 273).

У члану 271. дефинише се радња извршења кривичног дела рачунарска превара, и то на следећи начин:

(1) Ко с циљем да себи или другоме прибави противправну имовинску корист, унесе, измени, избрише, оштети, учини неупотребљивим или недоступним рачунарске податке или омета рад рачунарског система и на тај начин причини штету другоме, казинеће се казном затвора од шест месеци до пет година.

[41] Живанка Миладиновић, *оп. цит., докторска дисертација,* Београд, 2016, стр. 160
[42] Казнени закон, „Народне новине Републике Хрватске", бр. 110/97, 27/98, 50/00, 129/00, 51/01, 111/031, 190/03, 105/04, 71/06, 110/07, 152/08.

(2) Ако је кривичним делом из става 1 овог члана прибављена знатна имовинска корист или проузрокована знатна штета, извршилац ће се казнити казном затвора од једне до осам година.

(3) Подаци који су настали чињењем кривичног дела из става 1.и 2. овог члана ће се уништити.

С обзиром на то да су кривичноправна законска решења усклађена са одредбама Конвенције о високотехнолошком криминалу, Хрватска спада у круг земаља које су одлучне у супростављању овој врсти криминала.[43]

- **Компјутерска превара у законодавству Црне Горе**

У Црној Гори постоји неколико врста правних аката који чине темељ функционисања и основ за даљу надоградњу савременог концепта информационе безбедности. Реч је о следећим правним актима:

- Закон о потврђивању конвенције о рачунарском криминалу,
- Кривични законик,
- Законик о кривичном поступку,
- Закон о информационој безбедности,
- Закон о Агенцији за националну безбедност,
- Закон о тајности података,
- Закон о електронском потпису,
- Закон о електронским комуникацијама,
- Закон о електронској трговини.

Такође, као акти који играју битну улогу када је реч о високотехнолошком криминалу су:

- Елаборат са дефинисаним надлежностима државних органа у борби против рачунарског криминала којим је извршена процена стања и спремности државе у области сајбер безбедности,
- Уредба о ближим условима и начину спровођења информатичких мера заштита тајних података,
- Уредба о ближим условима и начину спровођења индустријских мера заштите података,

[43] Др.сц. Л. Сокановић, др.сц. А. Орловић, *Облици пријевара у казненом закону,* стр. 584, 2017.

- Уредба о начину вршења и садржају унутрашње контроле над спровођењем мера заштите тајних података.[44]

Кривични законик Црне Горе у поглављу XXVIII садржи кривична дела против безбедности рачунарских података и то:

- Оштећење рачунарских података и програма (члан 349),
- Ометање рачунарског система (члан 350),
- Прављење и уношење рачунарских вируса (члан 351),
- Рачунарска превара (члан 352),
- Неовлашћени приступ рачунарском систему (члан 353),
- Злоупотреба уређаја и програма (члан 354).

У члану 352 дефинише се радња извршења кривичног дела компјутерска превара на следећи начин:

(1) Ко унесе, измени, избрише, пропусти уношење тачног податка или на други начин прикрије или лажно прикаже рачунарски податак или изврши било какво ометање рада рачунарског система и тиме утиче на резултат електронске обраде, преноса података и функционисања рачунарског система у намери да себи или другом прибави противправну имовинску корист и тиме другом проузрокује имовинску штету, казниће се затвором од шест месеци до пет година.

(2) Ако је делом из става 1 овог члана прибављена имовинска корист која прелази износ од три хиљаде еура, учинилац ће се казнити затвором од две до десет година.

(3) Ако је делом из става 1 овог члана прибављена имовинска корист која прелази износ од тридесет хиљаде еура, учинилац ће се казнити затвором од две до дванаест година.

(4) Ко дело из става 1 овог члана учини само у намери да другог оштети, казниће се новчаном казном или затвором од две године.[45]

[44] *Стратегија сајбер безбједности Црне Горе 2013-2017,* стр. 12, Подгорица, јул 2013. године

[45] *Кривични законик Црне Горе*, ("Сл.лист РЦГ", бр. 70/2003, 13/2004-испр. и 47/2006 и "Сл.лист ЦГ"бр.40/2008, 25/2010, 32/2011, 64/2011- др.закон 40/2013, 56/2013-испр., 14/2015, 42/2015, 58/2015-др.закон, 44/2017, 49/2018 и 3/2020)

- **Компјутерска превара у законодавству Федерације Босне и Херцеговине**

Облици кривичног дела која спадају у област компјутерског криминала регулисана су ентитетским законодавством- Кривични закон Федерације Босне и Херцеговине и Кривични закон Републике Српске.

Када је реч о Кривичном закону Федерације Босне и Херцеговине, у поглављу XXXII садржана су кривична дела против система електронске обраде података. У овом поглављу су садржана следећа кривична дела:

- Оштећење рачунарских података и програма (члан 393),
- Рачунарско кривотворење (члан 394),
- Рачунарска превара (члан 395),
- Ометање рада система и мреже електронске обраде података (члан 396),
- Неовлашћени приступ заштићеном систему и мрежи електронске обраде података (члан 397),
- Рачунарска саботажа (члан 398),
- Искоришћавање детета или малолетника ради порнографије (члан 211),
- Упознавање детета са порнографијом (члан 212).[46]

У члану 395 дефинише се радња извршења кривичног дела компјутерска превара на следећи начин:

(1) Ко неовлашћено унесе, оштети, измени или прикрије рачунарски податак или програм или на други начин утиче на исход електронске обраде података с циљем да себи или другом прибави противправну имовинску корист и тиме другом проузрокује имовинску штету, казиће се казном затвора од шест месеци до пет година.

(2) Ако је кривичним делом из става 1.овог члана прибављена имовинска корист која прелази 10.000КМ, учинилац ће се казнити казном затвора од две до десет година.

(3) Ако је кривичним делом из става 1.овог члана прибављена имовинска корист која прелази 50.000КМ, учинилац ће се казнити казном затвора од две до дванаест година.

(4) Ко кривично дело из става 1.овог члана учини само с циљем да другог оштети, казиће се новчаном казном или казном затвора до три године.

[46] *Кривични закон Федерације Босне и Херцеговине*, ('Сл.новине ФБиХ", бр.36/2003, 21/2004- испр., 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 и 75/2017)

Кривични закон Републике Српске у поглављу XXXII садржана су кривична дела против безбедности компјутерских података и то:

- Оштећење компјутерских података и програма (члан 407),
- Компјутерска саботажа (члан 408),
- Израда и уношење компјутерских вируса (члан 409),
- Компјутерска превара (члан 410),
- Неовлашћени приступ заштићеном компјутеру, компјутерској мрежи, телекомуникацијској мрежи и електронској обради података (411),
- Спречавање и ограничавање приступа јавној компјутерској мрежи (члан 412),
- Неовлашћено коришћење компјутера или компјутерске мреже (члан 413).

У члану 410 дефинише се радња извршења кривичног дела компјутерска превара на следећи начин:

(1) Ко унесе нетачан податак, пропусти уношење тачног податка или на други начин прикрије или лажно прикаже податак и тиме утиче на резултат електонске обраде и преноса података у намери да себи или другом прибави противправну имовинску корист и тиме другом проузрокује имовинску штету, казниће се новчаном казном или казном затвора до три године.

(2) Ако је делом из става 1.овог члана прибављена имовинска корист која прелази износ од 10.000КМ, учинилац ће се казнити казном затвора од једне до осам година.

(3) Ако је делом из става 1.овог члана прибављена имовинска корист која прелази износ од 30.000КМ, учинилац ће се казнити казном затвора од две до десет година.

(4) Ко дело из става 1.овог члана изврши само у намери да другог оштети, казниће се новчаном казном или казном затвора од шест месеци.[47]

[47] *Кривични законик Републике Српске (*"Сл.гласник РС", бр.64/2017 и 104/2018- одлука УС)

- **Компјутерска превара у законодавству Северне Македоније**

Облици кривичног дела која спадају у област компјутерског криминала регулисана су Кривичним законом

Када је реч о Кривичном закону, у поглављу XXIV садржана су кривична дела против имовине. У овом поглављу су садржана следећа кривична дела[48]:

- Штета и неовлашћени упад у рачунарске систем (члан 251),
- Прављење и уношење рачунарских вируса (члан 251-а),
- Компјутерска превара (члан 251-б),

У члану 251-б дефинише се радња извршења кривичног дела компјутерска превара на следећи начин:

(1) Ко са намером да себи или другом прибави илегално имовинску корист уносом у рачунар или рачунарски систем неистините податке, брисање или прикривање рачунарских података, уз фалсификовање електронског потписа или на неки други начин проузрокује погрешан резултат у електронској обради и пренос података биће кажњен новчаном казном или казном затвора до три године.

(2) Ако је учинилац прибавио већу имовинску корист, казниће се казном затвора од три месеца до пет година.

(3) Ако је учинилац прибавио значајну имониску корист, казниће се казном затвора од једне до десет година.

(4) Уколико се радња из става 1 учини само са намером да нанесе штету другом, казниће се новчаном казном или казном затвора до једне године.

(5) Ако је случај из става 4 починио већу штету, учинилац ће бити кажњен казном затвора од три месеца до три године.

(6) Ко неовлашћено производи, набавља, продаје, држи или прозводи специјалне уређаје, алате, рачунарске програме или рачунарске податке који се користе за извршење предмета из члана 1, казиниће се новчаном казном или казном затвора до једне године.

(7) Увреда за случај из става 1 и 4 је кажњива.

(8) Ако случај из овог члана учини правно лице, казниће се новчаном казном. Чланови (8) и (9) постају чланови (9) и (10).

[48] Наведена су само кривична дела која се тичу високотехнолошког криминала.

(9) Посебни уређаји, средства, рачунарски програми или подаци који се користе за спровођење дела биће заплењени.

(10) За случај из става 4 кривично гоњење се покреће приватном тужбом.[49]

- **Компјутерска превара у законодавству Републике Србије**

Познато је да право веома споро реагује на нове технологије. У прошлом веку, када је реч о технологији, право се бавило стварањем нових правила у ваздушном саобраћају, у вези са генетским инжињерингом и слично.[50]

Република Србија се касно прикључила решавању проблема компјутерског криминала. Наиме, до 2003. године није постојала законска регулатива у овој области, због тога учиниоци компјутерског криминала, укључујући и компјутерску превару, нису били кривично гоњени, те су могли несметано да врше све облике компјутерског криминала.

Основни закон у Републици Србији који регулише област компјутерског криминала је Кривични законик Републике Србије, у коме постоји поглавље XXVII, под називом "Кривична дела против безбедности рачунарских података" (чл. 298-304). У овом поглављу спадају:

- Кривична дела против безбедности рачунарских података,
- Прављење и уношење рачунарских вируса,
- Рачунарска превара,
- Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података,
- Спречавање и ограничавање приступа јавној рачунарској мрежи,
- Неовлашћено коришћење рачунара или рачунарске мреже.

Најчешће санкције које се изричу за дела компјутерског криминалитета су новчана казна, казна затвора и забрана обављања делатности, у зависности о ком делу се ради. Након што пресуда постане правоснажна, кривичне санкције се уносе у казнену евиденцију, с тим што постоје само одређена лица која могу имати приступ тим подацима. Како би постојало успешнп праћење и сагледавање узрока, последица и

[49] *Кривичен законик Република Северна Македонија* ("Сл.весник на Република Северна Македонија" број 80/99, 4/2002, 43/2003, 19/2004, 81/2005, 60/06, 73/06, 7/08, 139/08, 114/09, 51/11, 135/11, 185/11, 142/12, 166/12, 55/13, 82/13, 14/14, 27/14, 28/14, 115/14, 132/14)

[50] П. Димитријевић, *Право информационе технологије*, Internet Law, Sven, Ниш, 2011, стр. 54.

најуобичајених дела и починилаца компујтерског криминалитета потребно је обезбедити систематско и континуирано евидентирање.[51]

У ставу 1 члана 301. дефинише се радња извршења кривичног дела рачунарска превара, и то на следећи начин: „Ко унесе нетачан податак, пропусти уношење тачног податка или на други начин прикрије или лажно прикаже податак и тиме утиче на резултат електронске обраде и преноса података у намери да себи или другом прибави противправну имовинску корист и тиме другом проузрокује имовинску штету, казниће се новчаном казном или затвором до три године.” У ставу 2 тог члана наводи се да ће се учинилац казнити затвором од једне године до осам година ако је делом из става 1 тог члана прибављена имовинска корист која прелази износ од 450.000 динара. Ставом 3 предвиђено је да ће се учинилац казнити казном затвора од две године до десет година ако је делом из става 1 тог члана прибављена имовинска корист која прелази износ од 1.500.000 динара. Чланом 4. предвиђени су новчана казна или затвор до шест месеци уколико је дело из става 1 тог члана извршено само у намери да други буде оштећен.[52]

Поред Кривичног законика, постоји и Закон о потврђивању Конвенције о високотехнолошком криминалу[53]. У члану 8. је предвиђена превара у вези са рачунарима, где се наводи да свака страна уговорница треба да усвоји законодавне и друге мере које су неопходне како би се као кривично дело у домаћем праву прописало наношење имовинске штете другом лицу, када је учињено са намером и противправно:

- Свако уношење, мењање, брисање или прикривање рачунарских података,
- Свако ометање рада рачунарског система, са преварном или нечасном намером да се неовлашћено прибави противправна имовинска корист за себе или другога.[54]

[51] То су предвиделе и: Recommendation No.R (89) 9 on computer relating crime i Recommendation No.R (95) 13 of Committee of Ministers to Member States Concering Problems of Criminal Procedure Law Connected with Information Tehnology

[52] Кривични законик ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009 i 111/2009)

[53] Објављен је 18.03.2009. године у "Службеном гласнику Републике Србије", број 19-09

[54] Закон о потврђивању Конвенције о високотехнолошком криминалу, "Сл. гласник РС", бр.19

4. Појавни облици компјутерске преваре

Компјутерска технологија данас се може злоупотребљавати разнолико. Компјутерске преваре могу да се врше на разноврсне начине и рачунарски деликветни у том погледу показују заиста велику обученост и оспособљеност, док рачунар за варалице представља средство које се овде испољава као лака мета за злоупотребу.[55] Због масовности и свакодневног проналажења све софистицираних начина да се изврши компјутерска превара, тешко је одредити њену класификацију која би могла обухватити све елементе. Постоје одређене компјутерске преваре на које је насело велики број жртава. Основни критеријум за ову поделу је како жртва учествује у извршењу кривичног дела преваре као облика високотехнолошког криминала. На основу наведеног критеријума, постоји следећа класификација рачунарске преваре:

- Нигеријска превара
- Преваре ауторитета
- Спам преваре
- Преваре са наградама
- Преваре са злонамерним апликацијама
- Преваре из области електронског банкарства.[56]

Временом ови облици компјутерских превара су се све више развијали и њихов начин извршења је све више усавршаван од саме појаве нигеријске преваре до осталих превара.

Самим развојем интернета олакшана је међусобна комуникација људи широм света. Многи корисници су користећи комуникацију путем интернета платили огроман цех читајући поруке непознатих пошиљаоца. Преваранти су продавајући бајковите приче о огромним добицима наводиле жртве да наседну на њихове преваре.

Мањак на рачуну код жртве је само подсетник да ништа није бесплатно, иако је развој интернета допринео томе да се олакша међусобна комуникација људи.

Наведени облици компјутерских превара су се базирале на комуникацију са жртвом уз њено активно учешће у извршењу преваре. Употребом злонамерних апликација, на рачунарима и телефонима, жртве без знања и учешћа бивају оштећене. Међутим, навођењем облика компјутерских превара, запажамо еволуцију коју су

[55] Bellour J. C. *Међународна превара,* Избор бр. 1. Загреб, 1981. година
[56] Ж. Миладиновић, *Кривично дело преваре као модел остваривања сајбер криминала, докторска дисертација,* Београд, 2016, стр.84

доживеле и тенденцију да жртва све мање учествује у извршењу преваре. Жртва учествује на тај начин што једним кликом сва финансијска средства жртве постају имовина преваранта, сем код нигеријске преваре која обухвата комуникацију, преговоре и уплату новца на рачун преваранта.

4.1.Нигеријска превара

Нигеријска превара или "превара 419" представља један од најраспрострањенијих облика кривичних дела преваре која се обавља уз помоћ рачунара[57]. Нигеријска превара је настали због све веће употребе савремених информационих технологија и захваљујући глобалној улози интернета од стране великог броја корисника широм света.

Нигеријска превара се појавила раних 80-их година, са наглим економским развојем Републике Нигерије. Превару је започело неколико студената како би довели људе у заблуду који су заинтересовани за "тајанствене" послове у нигеријском нафтном сектору, касније и широм света. Готово на свим континетима Нигеријска превара је постала популаран начин извршења кривичних дела (Африка, Азија, Источна Европа, Америка).[58]

Као метод за извршење Нигеријске преваре користи се рачунар, првенствено се шаље писмо или електронска порука која је осмишљена тако да изгледа као да је намерно послата примаоцу поруке. Жртва преваре се убеђује да учествује у расподели одређене суме новца, али је услов да унапред уплати одређени новчани износ.[59]

Постоје следеће фазе, на основу којих је лако описати Нигеријску превару:

- Првенствено стиже писмо, мејл или факс од стране службеног представништва стране владе или агенције,
- Ради се о пословном предлогу за трансфер више милиона долара на банковни рачун жртве, а жртви се нуди одређени проценат као знак захвалности,
- Писмом се тражи од жртве да обезбеди личне податке и то бланко меморандум компаније, информације о банковном рачуну и телефонски број,

[57] Израз 419 преузет је из члана 419 Нигеријског кривичног закона. То је део поглвља 38 који се односи на добијање имовине лажним представљањем, тј варањем. Данас се број 419 односи на сложену листу кривичних дела која говоре о крађи, варању, фалсификовању, лажном представљању и обмањивању.

[58] *Нигеријска превара у Републици Србији,* http://arhiva.mup.gov.rs/cms/resursi.nsf/Nigerijska_prevara.pdf, приступила 12.08.2019. године

[59] Smith R., Holmes M., Kaufmann P., *Nigerian Advance Fee Fraud, Trends and Issues in crime and criminal justice,* Australian Institute of Criminology, Australia, 1999

- Преварант шаље жртви као доказ на аутентичност понуде различита документа са службеним маркама, печатима, логом и слично,
- И на крају, од жртве се тражи да унапред уплати новац за различите таксе, регистрацију, дозволе и слично.[60]

- **Начин извршења нигеријске преваре**

Први корак у извршењу ове преваре је креирање налога на бесплатним платформама *Gmail, Hotmail* или *Yahoo,* како би контактирали мете. Имејл адреса мора бити уверљива, да асоцира на ауторитативну особу или институцију, коју жртве неће проверавати.[61] Затим се тражи жртва. Имена и имејл адресе се могу узети приликом пријаве на бесплатне портале. На тај начин могу се прикупити неколико хиљада адреса за пар дана. Текст порука углавном је писан енглеским језиком да би био разумљив људима широм света. Садржина поруке је углавном срцепарајућа, романтична и бајковита, где се жртва приказује као херој, храбри помагач у великим делима.

Према држављанима Србије који су били жртве овог облика преваре, радња извршења је изведена на неколико начина, и то:

- Може се послати о обавештење о лажном добитку игре на срећу, након чега жртве уплаћују одређену новчану суму да би им се омогућило подизање награде.
- Такође, може се послати обавештење о наследству, у шта жртве поверују па због тога уплаћују одређену суму новца да би им се омогућила исплата наслеђеног новца.[62]

Прва порука коју преварант шаље односи се на помоћ при пребацивању новца на рачун у њиховој земљи, а за шта ће бити награђен, не спомиње се да прималац треба да уплати одређени новац. У следећој поруци се већ преварант "неочекивано" сусреће са разним трошковима, које једино жртва потенцијалне преваре може да измири било због блокираног рачуна, било због немогућности плаћања у другој држави. Углавном су то трошкови подмићивања, накнаде у банкама, трошкови адвоката итд. Реч је о огромној

[60]С. Петровић, *Компјутерски криминал*, Војноиздавачки завод, Београд, 2004, стр. 148–150.
[61] Као пошиљалац може да се јави лице које стварно постоји, али његов идентитет је украде без његовог знања и извршиоци кривичних дела их користе да би прикрили свој прави идентитет или да би снагом ауторитета одређених лица улило поверење жртвама преваре и придобило њихово повреље.
[62] В. Урошевић, *"Нигеријска превара у Р. Србији"*, Безбедност- часопис Министарства унутрашњих послова Р. Србије, бр.3/2009, Београд, стр. 145- 156

суми новца, тај новац се на крају посла дели са жртвом преваре, жртва може зарадити и до 40% укупне суме новца која је предмет измишљеног посла.[63]

Након пристанка жртве на понуђени посао, преваранти имају задатак да у кратком року креирају лажни налог, фотографије, фалсификована документа са лажним печатима, потписима, како би жртва поверовала у истинитост посла.[64] Да би деловали убедљивије, ангажују и адвокате, банкарске службенике и друга стручна лица, како би жртву довели у заблуду и уверили да се заиста ради о правом послу, не о фиктивном. Жртве преваре пристају на то да пошаљу своје личне податке, број банковног рачуна, како би за кратко време зарадили велику своту новца. Уплате се најчешће врше преко *Western Union*-а и *MoneyGram*-а, због брзине преноса средстава и анонимности примаоца уплате, како би се теже открио извршилац. Након уплате од стране оштећеног, следи одлагање новчаних трансакција које су повезане са исплатом обећане суме новца. Стално се појављују нови трошкови, нова одлагања, стално се обећава исплата новца... Психолошки притисак на жртве се додатно врши навођењем да је тајност "посла" неопходна, јер ако би корумпирани званичници неке државе сазнали да тај новац постоји, онда би новац присвојили за себе.[65]

Извршиоци преваре се ослањају на чињеницу да ће, за време које прође док жртва схвати да је преварена, новчани трансфер који је она извршила бити исплаћен на њихове рачуне и да оштећени неће стићи да блокира трансфер на време. Након уплате преварант се жртви више не јавља, а могућност да се превараноту уђе у траг је минимална. Да би сакрили свој идентитет и локацију, поруке се углавном шаљу из интернет кафеа који су отворени у те сврхе, а радно време им је од 22,30 часова до 07,00 часова како би се избегла контрола од стране државних службеника.[66]

---

[63] Холандска компанија Ultrascan бави се истраживањем последица Нигеријских превара још од 1996. год. Резултати показују да су Нигеријске преваре свој врхунац достигле у 2009. години, када су жртве превара изгубиле готово 50% више новца него у 2008. години. Рађена је анализа на 8.503 случаја у више од 152 земље током 2009. године, на основу анализе жртве су изгубиле 9.3 милијарде долара, док су током 2008. године изгубили 6.3 милијарде долара. Према извештају, 51.761 превара је почињена из 69 других земаља, док је осталих 250.000 почињено из Нигерије. На пример, у Кини се обично користе преваре са лутријом или преваре "готовина на доставу", у Индији се обично користе преваре са понудама за брзо запослење и преваре са студентским визама. Ове врсте превара постају све опасније, теже их је открити и сузбити, што говори чињеница да је до данас изгубљено више од 41 милијарде долара, и то само када су у питању откривени случајеви, док су реалне процене експанзивног развоја ове појаве далеко веће.

[64] Dyrud M., (2005), *I brought You a good news An analysis of Nigerian 419 Letters,* Proceedings of 2005 Annual Association for Business Communications, Convention Association for Business Communication, USA, str. 11

[65]Buchanan J., Grant A., (2001), *Investigating and Prosecuting Nigerian Fraud, ''U.S. A ttomeys''* Bulletin, vol. 49., no. 06, USA, str. 39-47

[66]*Nigerian spam,* https://www.nigerianspam.com/, приступила 12.08.2019. године

Извршилац преваре је на добитку, за разлику од жртве. Када је откривена Нигеријска превара, новинар са Запада је упитао једног преваранта колико кошта извођење преваре. На то питање преварант је рекао да превара кошта свега два долара, долар да плати сат интернета у кафеу и долар да попије кафу.[67]

На територији Републике Србије у току 2008. и 2009. године од стране оштећених лица пријављено је девет кривичних дела преваре са елементима Нигеријских превара, против непознатих учинилаца. Укупна имовинска штета износила је 60.000 еура. Углавном се радило о следећим преварама:

- Слањем обавештења о лажним добицима на лутрији помоћу којих су жртве поверовале да су добитници награда и због тога уплаћивали одређене суме новца да би им се омогућило да подигну награду.
- Слањем обавештења о наследству помоћу којих су жртве поверовале да су наследиле одређену количину новца, након чега су уплаћивали одређену суму новца како би дошло до исплате наслеђеног новца.[68]

4.1.1.Случајеви нигеријске преваре

Основни циљ Нигеријске преваре јесте у томе да превари људе посредством добро осмишљених прича како би стекли одређену количину новца уз обећање да ће људима који пристану да пруже помоћ у име измиривања одговарајућих трошкова уплатити знатно већу суму новца од оне коју је жртва уложила. Постоје различити случајеви који су забележени у свету, а који спадају у категорију Нигеријске преваре. Извршиоци преваре користе се различитим причама како би придобили поверење код жртве, користе различита имена, на различите начине покушавају да прикупе новчана средства. У наставку ће бити наведени неки од најпознатијих случајева Нигеријске преваре у свету.

- **Случај Mrs Tema Wiliams**

Овај случај преваре се разликује од осталих по томе што се извршилац преваре одмах на почетку извињава због неочекиваног јављања, пошто жртва до сада није имала преписку са наводном особом којом се преварант представља. Пре свега,

[67] N*igerian Cyber Scammers – LA Times,* http://www.latimes.com/la-fg-scammers20oct20-story.html, приступила 12.08.2018. године.
[68] Др Владимир Урошевић, *"Нигеријска превара" у Републици Србији,* МУП Републике Србије, 2009 година, страна 8

објашњава на који начин је добио контакт жртве, затим прича да је до информација дошао тако што је тражио помоћ у земљи у којој жртва живи и да нема ни једног другог пријатеља коме се може обратити за помоћ, па се зато нада да ће му пре нека непозната особа помоћи када буде чула детаље његове приче која је измишљена. Ради се о особи која се зове Тема Вилиамс, удовица је и њен муж је био диретор фирме која је производила какао, он је убијен од стране побуњеника у политичком устанку. На његовом рачуну, који је отворен у Јужној Африци, налази се 6,5 милиона долара и удовица жели да та средства прималац пребаци на неки сигуран рачун или на рачун банке чији је он корисник у земљи у којој живи како би сачувала тај новац јер јој може бити одузет од стране државе. Она даје две могућности жртви. Прва могућност је да узме 5% од укупне суме новца, уколико јој помогне да пребаци новчана средства или да учествује у партнерству са родбином породице Вилиамс и да тако пренети новац уложе у нове послове који ће им донети знатно већи приход. Имагинарна удовица инсистира да јој жртва што пре одговори како би реализовали предлог и тако могли њој и њеном сину. Такође, удовица саветује жртву који је најбољи начин да уложи новац. У овом случају не постоји претерана маштовитост, речитост, већ се одмах прелази на предмет преваре, а то је да жртва пребаци новац на рачун у држави примаоца ове електронске поште.[69]

- **Случај Sgt. Joey Jones**

У овом случају примаоцу се обећава велика сума новца у замену за пренос средстава и уколико помогне у плаћању трошкова трансфера. Ради се о америчком војнику који је стациониран у иностранству и има код себе велику количину новца који припада бившем ирачком диктатору Садаму Хосеину. У поруци се налази и линк који треба да отвори прималац, а који садржи све битне детаље о овој ситуацији. Примаоцу поруке се објашњава да се новац чува у безбедносним условима у надлежној фирми и да њему као војнику није дозвољено да задржи тај новац, и зато тражи помоћ да се тај новац пребаци на рачун који се налази у другој земљи. Уколико жртва пристане, њој припада 30% од укупне суме и наглашава јој се да договор чува у тајности и да не треба да сумња у истинитост овог споразума. Када жртва пристане онда имагинарни војник тражи од примаоца да му достави личне податке, имејл адресу, број телефона или факса ради боље комуникације. Поред крађе украденог новца, постоји и крађа

[69] *Mrs Tema Wiliams Nigerian Scam,* https://www.hoax-slayer.net/tema-williams-nigerian-scam/, приступила 12.08.2019. године

идентитета с обзиром да извршилац преваре путем овог писма може добити и поверљиве информације примаоца поруке.[70]

- **Случај Mother Sarah Alan Rowland**

Како би се добило поверење жртве, у овом примеру нигеријске преваре користе се вера и побожност.[71] Ради се о монахињи по имену Сара Ален Ровленд, супрузи немачког амбасадора у Дубаију, који је тамо боравио девет година и умро 2004. године. Извршилац преваре пласира причу о томе да Сара и њен муж нису могли да имају деце и да је муж умро у кратком периоду од момента када је открио да је болестан, затим да је Сара одлучила да се не удаје и да не жели да има децу. Она је наследила богатство од 48 милиона долара у шпанској банци, али због болести јој је остало још три месеца живота пошто је оболела од рада и има проблема са ходом. Због свега наведеног она жели да своје богатство подели међу удовицама и да један део новца поклони сиротиштима. Она тражи помоћ од примаоца поруке да уплати одговарајућу суму новца као трошкове трансфера средстава и да новац који је наводно наследила искористи у божанске сврхе, ради благостања и помоћи верницима.[72]

4.2.Преваре ауторитета

Ауторитет се може дефинисати као друштвени положај који се може приписати особи услед односа моћи и утицаја у друштвеним односима.[73] Како би се привукла пажња жртве преваре на друштвеним мрежама користи се ауторитет. Преварантима у прилог иде то што велики број људи некритички прихвата ставове и захтеве особе која ужива ауторитет. Жртву преваранти убеђују на основу свог угледа и утицаја и на тај начин жртва занемарује да спроведе безбедносне провере. Прва грешка коју жртва прави јесте што прихвата захтеве особа које уживају велики ауторитет. Највише могу настрадати деца и млади, зато што они без готово икакве опрезности прихватају информације на друштвеним мрежама, које наводно прослеђује особа са ауторитетом.

Злоупотреба ауторитета личности на друштвеним мрежама може се извршити на следећи начин:

---

[70] *Sgt. Joey Jones Nigerian Scam*, http://www.hoax-slayer.com/sgt-joey-jones-scam.shtml, приступила 12.08.2019. године

[71] Живанка Миладиновић, *оп. цит., докторска дисертација,* Београд, 2016, стр. 93

[72] *Mother Sarah Alan Rowland Nigerian Scam,* http://www.hoax-slayer.com/sarah-alan-rowland-scam.shtml, приступила 12.08.2019. године

[73] Милан Вујаклија, *Лексикон страних речи и израза*, Штампар Макарије, Београд, 2011

- Прављењем лажних профила особа које уживају ауторитет,
- Хаковањем, компромитовањем постојећих профила или на други начин преузимањем контроле над профилом особе која ужива ауторитет.[74]

Када је у питању прављење лажног профила, није потребно да извршилац познаје дотичну особу под чијим именом прави лажни профил, потребно је једино да има неке основне информације о тој особи, слике... Лажан профил се може открити уколико се запази да нема довољно приватних фотографија већ само оних професионалних, с јавних догађаја које су свима доступне. Такође, преваранти много више означавају особе на фотографијама, а када мало боље размотримо познате личности би супротно урадиле, склониле своју ознаку са фотографија да не би биле доступне широј јавности. Када се наиђе на профил јавне личности која креће да пропагира насиље, да се вулгарно изражава преко статуса, да прати мали број страница и има мало лајкова на својим објавама, знамо да је реч о лажном или хакованом профилу. Многи на основу броја пратилаца закључују да ли се ради о правој особи или је реч о преваранту.

Према *New York Times*-у, који је недавно открио целу индустрију лажних профила купаца и компанија, установљено је да је лажне профиле све теже открити јер су почели да користе и праве податке корисника на овој друштвеној мрежи без њиховог знања. Поред свега тога постоји и проблем што корисници инстаграма траже лажне пратиоце да би што више подигли своју популарност на датој мрежи која се мери тиме колико пратилаца нека особа има. Данас је лажне пратиоце лако купити а чак су и јефтини. Компанија за заштиту података тврда да лоши ботови чији је циљ крађа лозинки и слање вируса чине 28,9% ботова на Instagramu. Уколико је профил јаван онда постоји већи ризик да ће их искористити преваранти, да ће злоупотребити податке и фотографије тог профила.[75] Мотиви за превару ауторитета могу бити поред ових наведених и стицање имовинске користи. То се постиже злоупотребом нечијег профила које ужива популарност и углед да би кроз акције прикупљања помоћи. Као један од примамљивих случајева јесу добровољне акције прикупљања помоћи. Тада преваранти користе лажне профиле да изгледа као да их лице које ужива ауторитет позива да се укључе у акције прикупљања помоћо након елементарних непогода или за потребе лечења одређене особе. И тада се уместо рачуна стварно угрожених на профилу налази

[74] Живанка Миладиновић, *оп. цит., докторска дисертација,* Београд, 2016, стр. 95
[75] *Лажни профили,* https://www.medijskapismenost.hr/kako-se-zastititi-od-krade-online-identiteta/, приступила 25.09.2019. године

рачун преваранта.[76] Како би се сачувала безбедност на друштвеним мрежама потребно је, пре свега, подесити приватност својих објава и слика, као и да се примају захтеви само од пријатеља које познајете. Уколико особа примети да међу пријатељима има лажних профила, потребно је пријавити администраторима друштвене мреже, а помоћу опције репорт уклонити са листе пратилаца.

Када говоримо о правној регулативи, у многим земљама крађа идентитета сматра се кривичним делом. Предвиђа се и затворска казна као и новчана накнада за причињену штету али то зависи од тежине преваре која је спроведена, а зависи и од разлога због чега је извршена злоупотреба ауторитета. У ситуацијама када се открије идентитет особе која је злоупотребила нечији профил, хаковала или направила лажни профил под именом неке особе која ужива ауторитет, онда оштећена страна може да покрене поступак ради санкционисања извшилаца ове преваре. Оштећена лица могу поднети тужбу због повреде свога угледа и части. Тако Кривични законик Републике Србије у члану 172. у ставовима 1. и 2. прописује следеће: „Ко износи или преноси штогод из личног или породичног живота неког лица а да при том то може нашкодити његовој части или угледу, казниће се новчаном казном или казном затвора до шест месеци, а у случају да је ово дело учињено путем медија, штампе, радија или сличних средстава или на јавном скупу, учинилац ће се казнити новчаном казном или казном затвора у трајању од годину дана.“[77] Злоупотреба личних података и крађа ауторитета ће се стално прилагођавати технолошким иновацијама, тако да ће увек постојати опасност од повреде угледа, части, хаковања профила и крађе личних података. Константно морамо пратити и трендове заштите од оваквих претњи и да будемо обазриви на лажне пратиоце и профиле.

Интернет провајдери могу веома лако сазнати ко стоји иза спорног налога. Када постоји основана сумња да је дело учињено, интернет провајдери су дужни да полицији дају податке који су потребни за истрагу. На основу овога Конвенција о високотехнолошком криминалу у члану 21 прописује да је потребно да свака чланица треба да усвоји легислативне и остале мере како би омогућила надлежним органима да приморају даваоца услуга да у оквиру својих техничких могућности на тој територији прикупе или сниме применом техничких уређаја или да међусобно сарађују.[78]

[76] *Лажни профили,* http://rs.n1info.com/Vesti/a192303/Izbegnite-prevaru-na-Internetu.html, пристипила 25.09.2019. године

[77] Кривични законик Републике Србије (Службени гласник РС) члан 172, (ставови 1 и 2).

[78] *Конвенција о високотехнолошком криминалу*, члан 21, став 1.

4.2.1.Случајеви преваре ауторитета

- **Случај америчког морнаричког заповедника Адмирала Џејмса Ставридиса**

Адмирал Џејмс Ставридис је познат по активном коришћењу Фејсбука и Твитера, самим тим је привукао велики број заповедника и војника да користе друштвене мреже.[79] Сајбер преваранти су искористили његову популарност и тиме отворили профил на Фејсбуку са његовим именом и презименом и повезали се са другим војницима. Потврђено је да су најмање један од тих лажних профила покренули кинески шпијуни који су на тај начин шпијунирали Америчке војнике и заповеднике.[80] Ослањући се на подешавања приватности на Фејсбуку, војници су у потпуности веровали у сигурност Фејсбука, па су без провере прихватали позиве за пријатељство од познатих лица, без размишљања ко се крије иза тих профила. Поред војника, ризик од опасности могу произвести и пријатељи и породице војника уколико са њима поделе информације о војним операцијама, о локацијама на којима се налазе, тако што на друштвеним мрежама поделе битне информације. Злоупотреба туђег имена и презимена, као и ауторитета на друштвеним мрежама представља кршење услова који су те мреже прописале, те друштвене мреже су одлучне у намери да заштите жртве тих злоупотреба.

- **Случај крађа идентитета- Пакао због двојника**

Иза све чешћих крађа идентитета у Србији стоји уносан бизнис. На туђе име се отварају фирме, дижу се кредити, купује се роба. Један од примера је случај када је непознати "двојник" злоупотребио лична документа, па отворио фирме, подигао кредите и куповао робу на име једног Смедеревца Јована Николића и Бечејца Николе Вујков, а након тога су почеле да стижу казне за царинске и друге прекршаје. Крађа идентитета је према Америчкој федералној комисији за трговину "нај превара", што је пракса показала у Србији, где се из године у годину повећава број људи којима на кућне адресе стижу рачуни за разна дуговања или пријаве за утају пореза, или им стиже да плате робу и услуге које никад нису користили. Како би се заштитили од преваре, потребно је обратити пажњу где остављамо личне податке. Стално смо у ситуацији у

[79] *Адмирал Џејмс Ставридис,* https://www.facebook.com/james.stavridis , приступила 09.04.2020. године
[80]*Крађа идентитета,* http://www.telegraph.co.uk/technology/9136029/How-spies-used-Facebook-to-steal-Nato-chiefsdetails.html , приступила 09.04.2020. године

којој нам траже јединствени матични број, а ЈМБГ представља најопаснију шифру за улазак у различите базе.[81]

- **Случај Тимоти Повел, Флорида**

У Флориди је ухапшен мушкарац средњих година које је користећи лажне исправе искористио рачун старијег мушкарца, узевши неколико хиљада долара, како би купио пса и направио нове зубе. Тимоти Повел из Плантона, на Флориди је признао да је извршио крађу идентитета како би направио нове зубе јер му је био потреван нови нормалан изглед због будућих превара које је планирао са својом локалном бандом. Признао је да је идентитет украо од 80-годишњака који је патио од деменције преко дарк веба[82], превару је власт открила тако што је на рачун жртве стигао огроман рачун од стоматолошке ординације.[83]

4.3. Спам преваре

Спам се односи на слање исте поруке великом броју корисника интернета, у намери да порука стигне и до људи који сами не желе да је добију. Најчешће се користи за рекламирање производа и услуга. Углавном су то сумњиви производи или различити програми за "брзо богаћење" који могу резултовати и финансијским губитком примаоца поруке. Поред имејла, спамери користе и дискусионе групе, као и социјалне мреже како би поруке стигле до што већег броја корисника интернета. Аутоматски спам програми чак нападају и разговоре путем инстант порука, тако што насумично бирају корисничка имена и шаљу поруке надајући се да ће оне стићи до некога на другом крају.[84]

Према статистици корпорације " *Symantec*"[85], у првих шест месеци 2005. године, "спем" поруке су представљале 61% укупно размењених порука електронске поште у свету. Од тог броја, 51% потиче из САД.[86]

Забрињавајући податак је да су три четвртине свих имејл порука на интернету заправо спам имејлови. Данас је лако и јефтино послати много порука путем имејла, и

[81] *Крађа идентитета,* https://www.novosti.rs/vesti/naslovna/drustvo/aktuelno.290.html:428129-Kradja-identiteta-Pakao-zbog-dvojnika
[82] "Dark Web" је термин који се односи на специфичну колекцију веб сајтова која постоји на енкриптиваној мрежи и не може се пронаћи коришћењем традиционалних интернет претраживача.
[83] *Тимоти Повел, Флорида,* https://www.blic.rs/slobodno-vreme/vesti/hteo-je-nove-zube-i-novog-psa-ali-nije-imao-novca-pa-se-odlucio-na-najbizarniji-korak/4q9xf5k
[84] *Спам преваре,* https://www.techopedia.com/definition/23763/spamming, приступила 25.09.2019. године
[85] "*Symantec*" је светски лидер у производњи софтвера за заштиту рачунара и мрежа од сајбер напада
[86] "*Symantec",* https://www.it-klinika.rs/, приступила 25.09.2019. године

међу тих неколико милиона прималаца готово је сигурно да ће следити нпр линк који некоме осигурава наплату рекламе. Постији разлика између обичног и циљаног спама. Код обичног спама се одмах види да га је послала непозната особа, док се код циљаног види да спам шаље позната особа или фирма. То је мејл за који прималац мисли да га је послала позната особа, а у ствари то је урадио хакер користећи безбедносне пропусте мејл сервера. Постоји могућност да хакер тај мејл налог није отео, већ га је само виртуелно дуплирао и преко њега послао.

Постоје различите методе за слање спама.

- Спамери могу ставити линк на крај поруке који може изгледати овако: "Уколико не желите да примате овакве поруке, кликните овде како бисте зауставили примање". Уколико корисник кликне на тај линк, спамери корисника траже у адресару и тако стављају списак особа које тренутно читају спам поруке.
- Такође, спамери могу ставити слику, која је невидљива. Када корисник отвори спам поруку, захтев за отварање слике се шаље серверу који је поседује. Када добије захтев, корисник, читајући спам поруку, може ту поруку да пошаље на друге рачунаре.[87]

Како се заштитити од спама?

- Корисник треба да има макар две имејл адресе, од којих ће једну користити за личну преписку, а другу за пријављивање на јавним форумима, у собама за четовање и сл.
- Приватна адреса за личну преписку не сме да буде лака преварантима за разоткривање, не сме да буде једноставна, да садржи корисниково име и презиме, већ мора бити креативна и персонализована, да само кориснику њено име има смисла.
- С друге стране, јавна адреса се не сме користити у дужем временском периоду јер ће спамери врло брзо да дођу до ње и да злоупотребе имејл адресу у виду коришћења података корисника без његовог знања и одобрења.
- Никада не смемо да одговарамо на спам јер већина спамера прати пријем и лог одговора.

[87] Живанка Миладиновић, *оп. цит., докторска дисертација,* Београд, 2016, стр. 108

- Не сме се никада објављивати приватна адреса на местима која су свима доступна.
- Корисници никако не смеју да отварају *„unsuscribe"* линкове који се налазе у мејловима чији су извори под знаком питања пошто користе писма са овим изразом и уколико их корисник отвори онда обавештава у истом тренутку спамера да је жртва добила поруку након чега ће спамер још више да засипа корисника нежељеном поштом.
- Неопходно је да се стално проверавају најновије верзије *web browsera* и да се увек скидају сигурносне опције за њега.
- И на крају, у случају да су спамери открили адресу корисника, онда та особа мора да промени имејл адресу, то може бити комплексно али ће макар корисник да избегне даље нападе спам криминалаца, барем на неко време.[88]

У методе које се користе за проналажење и филтрирање нежељене поште спадају метода "беле листе", "црне листе" и Бајесова техника филтрирања спама.

Метода "беле листе" подразумева прихватање свих пристиглих порука са различитих имејл адреса који се налазе на листи познатој под називом "бела листа". То је најчешће локални попис адреса који провереним корисницима омогућава несметану комуникацију без додатних контрола у случају да се утврди да није реч о нежељеној електронској пошти. Када се утврди да се IP адреса са које је послата порука не налази на белој листи, онда се доставља обавештење кориснику о могућој спам поруци како би на време могао да спречи реализовање преваре.

Метода "црне листе" користи попис адреса које се налазе на датој листи и које су у претходном периоду означене као спам поруке. Попис тих порука врши се са сервера који су и одређени за проналажење нежељене поруке. Ти сервери имају велику флексибилност и у сваком моменту ажурирају постојеће црне листе које садрже актуелне спам поруке. Ова метода је веома ефикасна пошто има за циљ да корисника у право времевреме обавести да ли је пристигла спам пошта.

Бајесова техника филтрирања спама[89] користи статистичке методе за класификацију докумената у категорије. Карактеристично је да је ефикасан у

[88] *Како се заштити од спама,* https://www.informacija.rs/Anti-spam/Sta-je-spam-i-kako-se-zastititi-od-njega.html, приступила 25.09.2019. године

[89] У случају да кориснику пристигне порука која садржи реч Нигерија, која се често појављивала у најпознатијим спам порукама и преварама. Бајесовски филтер ће означити највероватније ову реч као спам реч, али ће такође у обзир узети и остали садржај поруке да би се утврдило да ли је реч о легитимној пошти без обзира што садржи спам реч. На пример име члана породице може бити од

разликовању нелегитимне и нежељене поште од легитимне. Ова метода има велики значај јер ради ефикасно у погледу избегавања класификовања легитимних мејлова као спама.[90]

Спам мејлови су неизоставни део виртуелног живота корисника интернета. Први корак који преваранти предузимају када шаљу спам поруку јесте проналажење мејл адресе циљане особе. Имејл адресе у фирмама и уставоновама у Србији обично су у форми: име.презиме@називфирме.рс. Када се пронађе имејл адреса, преварант приступа писању и слању спама. Уколико сајт нуди услугу да се спам пошаље, на пример Emkei's Fake Mailer, онда се може путем сајта послати или путем програма који покреће са свог рачунара. Међутим, ови сајтови и програми су често компромитовани и због тога их имејл сервери могу лако препознати као спам. Може се користити и *php* скрипта за слање циљаних спамова, ове мејлове веома тешко детектују имејл сервери. На пример, хакер се може представити спамом као непосредни руководилац и од вас тражити да отворите документ који је стигао уз мејл, у коме се налази малициозни софтвер.

Спам се може провалити помоћу заглавља мејла. Заглавље мејла садржи информације како је тај мејл путовао од једног до другог мејл сервера и на основу тога се може закључити да ли је мејл спам или није. Програми за пријем и слање мејлова не приказују заглавље мејла, већ се до заглавља мејла долази избором кроз мените за сваки мејл посебно. Некада распоред ставки може да сигнализира да мејл није стигао са имејл адресе са које пише да је послат или да није стигао на регуларан начин.

Закон о оглашавању Републике Србије у члану 5 прописује следеће: "Порука која представља огласну поруку мора бити препознатљива. Ако се огласна порука појављује заједно са другом поруком, односно обавештењем, која нема огласну природу, огласна порука мора бити јасно означена. Забрањено је оглашавање усмеренео на подсвет, као и препоручивање производа и услуга током емисија које нису намењене оглашавању и други облици скривеног оглашавања."[91]

великог значаја у доказивању да мејл није спам, и може да заобиђе реч Нигерија која је у потпуно другачијем контексту употребљена у датој електронској пошти.

[90] Плескоњић Д., Мачек Н., Ђорђевић Б., Царић М., *Сигурност рачунарских мрежа* Виша електронска школа, Београд, 2006. година

[91] Закон о оглашавању Републике Србије „Службени гласник РС", бр. 79/2005 і 83/2014, члан 5.

У 2015. години забележен је пад појаве спам мејлова у интернет саобраћају. Те године САД и Русија су биле највећи извори спама, затим Кина, Вијетнам, Немачка, Украјина.[92]

4.3.1. Случајеви спам превара

- **Случај Miss Wumi Abdul**

Постоје случајеви када извршиоци преваре користе ауторитет усамљене удовице која је пре свега атрактивна, млада и која жели да се повеже са профилима тзв. електронских жигола којима ће дати шансу да је шармирају и који ће на тај начин доказати да су џентламени. Од њих удовица захтева да јој примаоци мејла пруже помоћ пошто се представља као незаштићена млада девојка, отвара душу и објашњава каква је тужна судбина задесила њу и њену породицу. У поруци наводи да јој се срећа осмехнула што је пронашла особу од поверења и жели да пренесе свој новац на рачун потенцијалне мете и то у земљи у којој жртва живи и да јој на тај начин жртва учини веома велику услугу. Као знак захвалности нуди жртви 15% од укупне суме новца која се преноси. Након сваке следеће поруке имагинарна девојка жели да пробуди сажаљење код саговорника и сваки пут му све више прича да је коначно вратила веру у људе и да је срећна и то све захваљујући жртви која је пристала да јој помогне. У овој врсти Нигеријске преваре извршилац се представља као млада девојка, чак има и припремљење слике које доказују њену атрактивност и зато бира оне мете за које сматра да би урадили све за такву девојку, а неке мете извршиоци су чак навели заљубе у њу и на тај начин врло лако реализовали свој циљ крађе новца од лаковерних мушкараца.[93]

- **Случај Mr. Wong Du**

Велико интересовање може изазвати када кориснику интернета стигне порука са насловом "партнерство". Тешко је одолети знатижељи да се отвори мејл и прочита предлог господина Винга Дуа. Винг Ду је радио као банкарски службеник у Северној Кореји и радио је са рачунима особа које раде у влади дате државе и открио је да се на тим рачунима налазе велике суме новца, истовремено је открио и рачун који је

[92] Proportion of spam in email traffic, https://securelist.com/analysis/quarterly-spam-reports/71759/spam-and-phishing-in-q2-of- 2015/, приступила 25.09.2018. године.
[93] *Wumi Abdul Nigerian Scam,* http://www.hoax-slayer.com/wumi-abdul-scam.shtml, приступила 12.08.2019. године

припадао некадашњем председнику Парк Чунг Хију, који је био на власти све до 1979. године. Он наводи да је председник преминуо и да за толико година нико није долазио да подигне новац са тог рачуна и да жели да се тај новац пренесе на рачун жртве ове преваре како би жртва и банкарски службеник поделили новац на равне части, с тим што ће жртва да уплати новац на име трошкова преноса овог новца.[94] Жртва може лако поверовати у истинитост ове преваре, с обзиром на то да је стварно постојао тај председник и даје велика вероватноћа да је у тој банци имао рачун и да се на њему налазила толика сума новца.

- **Случај charity distribution**

У овом случају се као предмет преваре користи хумани гест од стране особе која је тешко болесна. Наиме, господин Питер Атах се јавља у нади да ће наћи особу која ће му помоћи да 15 милиона долара проследи хуманитарним организацијама. Он измишља потресну причу наводног пошиљалаца, ради се о особи која има 55 година, из јужне Африке, а живи у Нигерији, иначе се ради о председнику нафтне компаније, некада ожењеног и оца двоје деце. Нажалост, чланови његове породице су доживели саобраћајну несрећу и погинули пре 6 година. Због посвећености послу, није пуно био са својом породицом, па због гриже савести, он жели да помогне другима. Међутим, он се тренутно налази у болници, због тешке болести и остало му је још пар месеци живота. Последња жеља му је да уложи новац у добротворне сврхе. Он нема поверења у своје пријатеље и рођаке, па због тога моли поштеног примаоца да му помогне око реализације. При том, наводи, да је прималац слободан да узме одређену суму новца за себе.[95]

4.4. Преваре са наградама

Преваре са наградама постоје деценијама и специфичне су јер имају добру рекламу која манипулише грађанима и грађани изнова и изнова учествују у оваквим преварама као жртве. Најчешће је реч о играма на срећу које имају велики утицај на становништво и путем интернета. Постоје бројне лутрије као и начини за освајање

[94] *Mr. Wong Du Nigerian Scam,* http://www.hoax-slayer.com/wong-du-scam.shtml, приступила 12.08.2019. године
[95] *Charity Distribution Nigerian Scam,* http://www.hoax-slayer.com/peter-attah-scam.shtml, приступила 12.08.2019. године

примамљиве новчане награде. Иако некад не изгледају уверљиво, постоје појединци који ће се упустити у освајање обећане награде.

Игре на срећу су дефинисане Законом о играма на срећу. Под играма на срећу подразумевају се игре које учесницима пружају могућност добитка, уз наплату, у новцу, стварима, услугама или правима, при чему тај добитак или губитак не зависе од знања и вештине учесника у игри већ од случаја или неког извесног догађаја.[96] Треба разграничити шта не спада у категорију игара на срећу. Па је у истом члану овог закона дефинисано да се играма на срећу не сматрају оне игре које се могу приредити пред јавношћу, игре у којима се такмичи у знању и вештини из различитих области, при чему крајњи резултат зависи искључиво од постигнутих резултата из задате области.

Свака лутријска превара започиње тако што се шаље обавештење путем имејла, поште, телефонским позивом, а понекад то обавештење са собом укључује и поруку да је прималац поруке победио и да је освојио велику суму новца. Обично се примаоцу поруке каже да је његова имејл адреса насумично изабрана, да је субјекат изабран као добитник награде зато што је дугогодишњи корисник услуга дотичне компаније која је послала обавештења као и то да се ово примљено обавештење чува у тајности и да се контактира "агент за потраживања". Када мета преваре контактира наводног агента, онда се од превареног тражи да плати накнадне обраде или трошкове преноса како би добитници могли извршити исплату освојеног новца, међутим преваранти никада не изврше исплату новца који је освојен на лутрији. Како би преваранти деловали уверљивије они користе имена легитимних лутријских организација или других легитимних компанија, али то не значи да су на било који начин легитимне организације укључене у овај вид преваре.[97] Циљ преваранта је да наведе жртву да уплати што већу суму новца за потребе трошкова и да на крају када прикупе жељени новац обавесте превареног да је награда одложена или да постоје технички проблеми и да ће исплата да се изврши чим буде могућа, али се то никада не догоди. Након саопштења да је жртва освојила награду, постављају се питања као што су: "Да ли сте некада добијли овакву награду?" или "Како се осећате када сте победили?". Затим се прикупљају подаци особе која је мета преваре као што су адреса, имејл адреса, број телефона и на крају му је послато име особе којој се треба јавити ради преузимања награде. Оно што је занимљиво, преваранти не траже шифру платне картице јер до тога долазе тако што убаце вирус у рачунар корисника док жртва даје своје личне податке.

[96]Члан 2, Закон о играма на срећу, „Службени гласник РС“ бр 84/2004 и 85/2005
[97] *Преваре са наградама,* https://en.wikipedia.org/wiki/Lottery_scam, приступила 03.10.2019.год.

Затим преваранти чекају да се некада изврши плаћање картицом преко интернета и након тога приступе шифри или пин-у дате картице. Веома је важно да се појединац сам заштити од оваквих превара. Никада не сме да дозволи да изврши плаћање да би му се уручила одређена награда и то уколико ни сам корисник није учествовао лично у таквим играма на срећу или није корисник услуга компаније која нуди награду. Корисници не смеју да дозволе да се предају похлепи, увек морају бити сумњичави и опрезни када се ради о идеалним понудама и брзим испорукама, јер све то звучи превише добро да би било истинито, што и преварантима јесте циљ, да пласирају идеалну причу која ће привући што већи број корисника.[98]

4.4.1.Случајеви преваре са наградама

- **Случај фејсбук наградне игре**

Што се фејсбук наградне игре тиче, превара почиње када мејл шаље Фејсбук у којем се срећни "добитник" обавештава да је он победник "Међународне онлајн лутрије" за дату годину и да је освојио одређену суму новца. Наводно је добитник насумично изабран и потребно је да он контактира "одељење за исплате" ради преузимања награде. Они који поверују у такве тврдње и обрате се одељењу за исплате, обавештавају се да морају да уплате одговарајући износ за постојеће трошкове преноса, пореза, осигурања и сл. Осим тога што жртва преваре може остати без новца, она такође даје своје личне и финансијске податке које предаје криминалцима наводно да би доказала свој идентитет, а касније ти подаци могу бити искоришћени за крађу идентитета.[99]

- **Случај Google наградне игре**

Google наградне игре су карактеристичне по томе што се корисницима шаљу обавештења да је мејл пристига од самог Google-а. Овде се долази до злоупотребе преводилачког сервира ове мреже. Али, на крају крајева, коришћење преводилачког онлајн сервиса у таквим мејловима легитимине лутријске организације и компаније то

[98] *Преваре са наградама*, https://www.informacija.rs/Drustvene-mreze/Facebook-ova-online-lutrija-ne-postoji-cuvajte-se-prevara.html, приступила 03.10.2019.год.

[99] Један од познатијих случајева Фејсбук наградне игре је када је 65-годишњи држављанин Јужне Кореје заједно са својом ћерком отпутовао у Јужну Африку да преузме милионе које је освојио на једној од оваквих лутрија. Заправо се догодило да су били киднаповани од стране нигеријске банде онда када су дошли у Јужну Африку, а починиоци су од супруге превареног тражили откуп. На крају се све завршило без већих проблема, спашена су лица која су била отета, али је ово касније показало широј јавности каквим се ризицима излажемо верујући свако и свему на интерету.

никада не би дозволиле, па самим тим врло је лако утврдити да је реч о превари, ипак велики проценат од укупних корисника ове глобалне мреже поверовало је и у овакву врсту наградне игре, без обзира што не изгледају истинито. Проблем ових превара је што криминалци користе познате компаније, тј позивају се на њих приликом слања недозвољених мејлова. Углавном се ради о *McDonald's, Coca-Cola, Yahoo, BMW* компанијама и о другим познатим организацијама. Све те компаније не могу да спрече да се њихов углед и назив злоупотребљавају, а жртвама такве поруке, где се оне спомињу, уливају велико поверење и лако их је преварити.[100]

- **Случај Eu commonwealth lottery promotions**

Самим тим што постоји захтев да се контактира извесни господин Маршал Елис из Нигерије, који користи јавни бесплатни сервис live.com, довољно је да укаже да је реч о превари. Такође, организатори игара на срећу никада не остварују контакт слањем мејла на њихове личне имејл адресе, комуникација треба бити остварена с пословних адреса. Још занимљивије је да се ради о европској лутрији, па се због тога поставља питање: "Зашто је Елис становник Нигерије?" Термини као што су да је баш ваша имејл адреса одабрана или да је ваша адреса победила су знаци који одају преваранте.

На основу свега, може се закључити да се наградне игре овог типа често користе, да им је карактеристично то да су добитници насумично изабрани, да се изискује да уплате одређену суму новца на име административних трошкова и да када уплате одређени износ, преваранти никада не изврше исплату обећане награде актуелне лутрије која се наводи у мејлу.[101]

Према подацима Kaspersky Лабораторије, поруке као што су ове чине више од 3% свих спам мејл поруке месечно, што значи да се ради о хиљадама порука.

4.5.Преваре са злонамерним апликацијама

Преваре са злонамерним апликацијама или програмима подразумевају преваре новијег доба и основна карактеристика јесте да користе дате апликације да би добили жељене информације које су пре свега поверљиве као што су бројеви рачуна и пин-

[100] *Наградна игра,* https://www.dostop.si/lazne-nagradne-igre-kako-jih-prepoznati-in-se-jim-izogniti/ , приступила 27.05.2020. год

[101]Congratulations, you've won! The reality behind online lotteries. https://securelist.com/analysis/publications/36450/congratulations-youve-won-the-reality-behind-online-lotteries/, приступила 15.10.2019. године.

кодови. Ова превара се разликује од нигеријских и лутријских превара по томе што се овде не тражи директно новац који се правда разним трошковима, већ су усмерене на стицање материјалне користи и то уз помоћ поверљивих података од којих је извршилац дошао, а све то захваљујући употреби злонамерних апликација.[102]

Глобални проблем данашњице јесу тзв. фишери и спамери. Фишери могу да контактирају огроман број корисника уз минималан ризик да буду идентификовани и то зато што користе савремену технику за слање масовних порука електронске поште. Ова група превара се може поделити на фишинг (*Phishing)* и фарминг (*Pharming*). Представљају моделе крађе поверљивих података и то користећи лажне веб сајтове, а пре свега сајтове финансијског садржаја где се од жртве захтева да унесе број свог рачуна или пин- код.

Фишинг (*Phishing)* представља криминалну радњу која користи технике социјалног инжињеринга. То је вид преваре помоћу које нападачи долазе до важних информација које се односе на детаље о кредитним картицама и лозинке. Изводи се помоћу електронске поште или система тренутних порука.[103]

Фарминг (*Pharming*) је напад који за циљ има преусмеравање *HTPP* захтева корисника на лажне или злонамерне апликације уместо на оригиналне. Крајњи резултат јесте да преварена особа остависвоје основне податке који су пре свега осетљиви на веб страници нападача који је ту своју страницу лажно представио као да је легитимна.[104]

Фарминг се разликује од фишинга у томе што нападач не мора да наводи корисника да притисне хипервезу у електронској поруци, чак и ако корисник тачно зада веб адресу у адресно поље читача. Тада преварант може да преусмери корисника ка злонамерној веб локацији. Код фарминга је, заправо, добољно само да жртва отвори дату страницу да би се у рачунар убацио злонамерни програм који ће да краде информације. Постоје бројне мере заштите од ових модела превара али треба напоменути да апсолутна заштита не постоји![105]

Ова превара почиње тако што се корисницима шаљу поруке које су написане у таквој форми да делују као да су послате од стране банака или неке друге легитимне финансијске институције и да на основу такве поруке жртву наведу да унесу своје

---

[102] *Преваре са злонамерним апликацијама, https://support.microsoft.com/hr-ba/help/17228/windows-protect-my-pc-from-viruses* , приступила 27.05.2020. год.

[103] *Фишинг, https://www.it-klinika.rs/blog/sta-je-phishing-email-i-kako-se-odbraniti* , приступила 27.05.2020. год.

[104] *Фарминг, https://sr.wikipedia.org/sr-el/%D0%A4%D0%B0%D1%80%D0%BC%D0%B8%D0%BD%D0%B3* , приступила 27.05.2020. год.

[105] Др Косановић Мирко, *Интернет ризици,* Висока техничка школа струковних студија, Ниш, 2017.год.

поверљиве податке У поруци се наводи да је прималац поруке потрошио знатну количину новца и да ће му због тога бити укинута картица уколико се не јави финансијској институцији или банци код које има картицу. У случају да се не јави у поруци се такође наводи да ће му се наплаћивати одређена камата на износ који чак прималац поруке највероватније ни не дугује. У поруци се такође налази и сајт који прималац мора да посети. Обично се ради о сајту дате организације и жртви преваре се налаже да посети дати сајт ради заштите својих поверљивих информација од нејасно наведених претњи.

Када жртва уђе у предложени сајт односно када отвори линк који се налази у поруци, тада следи повезивање са сајтом који садржи злонамерну апликацију и који личи као да је оригиналан с намером да што лакше превари жртву. Када жртва не сумњајући у аутентичност веб странице, остави своје поверљиве информације, нападач их затим узима и користи за крађу идентитета да би извршио противправне финансијске трансакције. Резултат тога јесте велики финансијски губитак прималаца такве поруке, а чак постоје и тежи случајеви када жртва може изгубити и свој лични електронски идентитет који се може искористити у криминалне сврхе онда када извршилац преузме поверљиве информације.[106]

4.5.1. Случајеви преваре са злонамерним апликацијама

- **Случај верификација Твитера**

Особама које користе Твитер дата је могућност верификације налога. Ипак, предметни налог је успешно опонашао Твитеров званични налог "Verified Account", па је због тога корисник морао да попуни образац са одређеним информацијима као што су имејл адреса, корисничко име, број пратилаца, лозинка и да наведе зашто жели да верификује налог. Уколико корисник жели да верификује свог налог, мора да плати надокнаду и да унесе број платне картице, датум истека, име, адресу становања, број телефона и имејл налог на који ће примити потврду. На тај начин преваранти су могли да украду налоге и информације о платним картицама. Неопрезни корисници који су пратили упутства нису ни приметили да сајт за плаћање није имао сигурну везу. Неискуство корисника се показало на тај начин што Твитер не прихвата захтеве за

[106] Живанка Миладиновић, *оп. цит., докторска дисертација,* Београд, 2016, стр. 117

верификацију налога иако је налог прихватљив за верификацију, међутим и поред тога корисници су успешно бити преварени.[107]

- **Случај- Твитер верификација плавим бецом**

Утицајним људима и компанијама Твитер даје могућност да верификују свој налог плавим бецом и тиме се пратиоцима профила потврђује аутентичност налога. Твитер не прихвата верификацију профила плавим бецом обичних корисника, како би се спречила злоупотреба имена познатих личности и брендова. Због немогућности имања плавог беца код обичних корисника, преваранти су смислили нову превару са злонамерним апликацијама. Преваранти су направили лажни веб сајт на коме заинтересовани могу да добију плави бец без обзира да ли су познати или не. На тој страници корисник Твитера треба да унесе корисничко име и лозинку. Затим се ти подаци шаљу криминалцима, док су жртве усмерене на званичну Твитерову страну са најчешће постављеним питањима у вези са верификовањем налога.[108]

- **Случај- апликације које нуде могућност сазнања ко посећује профил**

Једна од апликација која је привукла бројне жртве је она која омогућује кориснику Фејсбука да открије ко најчешће посећује њихов профил. Доказано је да је ово најуспешнији метод за крађу корисничких имена и лозинки корисника. Ова апликација се може активирати на следеће начине:

- Може се преузети софтвер који прикрива малвер који ће кориснику слати обавештење сваки пут када је Фејсбук налог посећен, као и ко га је посетио. Када се кликне на дугме ”*Download*”, преузеће се и тројанац Infostealer који краде информације са зараженог рачунара.
- Може се уписати корисничко име и лозинка за Фејсбук налог.[109]

[107] *Верификација твитера, https://www.informacija.rs/Drustvene-mreze/Fiseri-kradu-podatke-korisnika-uz-pomoc-laznog-Twitter-profila-za-verifikaciju.html* , приступила 27.05.2020. год.
[108] *Плави бец, https://verificationhandbook.com/book_cr/chapter3.php* , приступила 27.05.2020. год.
[109] *Ко вам гледа профил, https://www.index.hr/magazin/clanak/ako-ste-isli-vidjeti-tko-vas-gleda-na-facebooku-profil-vam-je-u-opasnosti/918312.aspx* , приступила 27.05.2020. год.

4.6. Преваре из области електронског банкарства

Електронско банкарство подразумева један ефикасан систем једноставног плаћања. Реч је о могућности пристуоа банци независно од њеног радног времена и то путем интернета. Клијенти могу да врше плаћање и трансфере новца с рачуна на рачун, могу имати увид у евиденцију трансакција, да наручују чекове, мењају своје податке и плаћају комуналије. Данашња технологија је толико напредовала, да свака банка нуди е-банкинг услуге које могу да користе њени клијенти. Овај систем плаћања и трансфера има своје предности јер се њиме избегава чекање у редовима, плаћања провизије и многе друге ситуације које клијентима могу одузимати време, али поред тога свесни смо да коришћење електронског банкарства доноси и низ опасности.

Прве онлајн банке појавиле су се крајем 1990-их и одмах су постале изазов за сајбер криминалце. С обзиром на то да банке имају веоме добре безбедносне системе, сајбер криминалци су знали да је веома тешко напасти саме банке, па су зато као мету напада узели саме клијенте.

Постоје два начина како приступити е-банкинг сервису:

- Може се приступити преко личног рачунара на који је инсталиран софтвер помоћу кога се може приступити серверу.
- Може се приступити са било ког рачунара тако што ће се конектовати на интернету, где се налази апликација намењена е-банкинг услугама.

Постоје 4 корака како би се успешно извела е-банкинг превара.

Први корак је проналажење жртве. Један од најбољих начина да се дође до већег броја људи и нежељена пошта. Социјалне мреже представљају погодно тло за налажење жртве. Одерећене апликације као што су апликације везане за гледање снимака представљају увод у е-банкинг превару. Уколико жртва несвесно кликне на злонамерни линк у фишинг мејлу или можда сурфује интернетом, тада жртвин рачунар може бити заражен вирусом.

Други корак подразумева куповину exploit kit пакета на интернету. Грешка корисника рачунара је та што своје инсталиране програме не ажурирају редовно, што представља добру ствар за пљачкаше, и омогућава потпуну контролу над њима. Потребно је само повезати спам мејл или апликацију са exploit kit-ом

Трећи корак подразумева инсталацију малвера који ће обезбедити могућност крађе поверљивих података који се односе на електронско банкарство.

Постоје одређени тројанци за е-банкинг преваре као што су:

Зеус се користи за крађу података налога корисника е-банкинга и онлајн трговине. Постоји велики број верзија и код малвера Зевса је био продаван и за 10.000 долара.[110]

TSPY:BANKER.NJH је тројанац који може да препозна када корисник укуца било који од УРЛ-ова банака које су његови циљеви. Може затворити тренутно отворени прозор браузера, уколико се ради о Google Chrome-у, може приказати грешку и да отвори нови лажни прозор Chrome-а. Корисник ово не може приметити.[111]

Путем СМС порука се такође може извести е-банкинг превара, користи се малвер ZitMo. Ова врста превара је заступљена у Кини, такође и у Европи, поготово у Румунији и Немачкој.[112]

Четври корак наступа када је остваре инфекција малвером. Корисник иначе није свестан да постоји малвер који чека да се жртва пријави на свој е-банкинг налог.

Након што се корисник е-банкинга улогује, систем нападач иницира на рачунару зараженом вирусом трансакције трансфера новца. Кориснику се појави лажни прозор за поновну идентификацију. Он верује да је уплатио неки налог, међутим, новац намењен плаћању рачуна је завршио негде другде. Овај процес се понавља увек када се корисник пријављује на свој е-банкинг налог.

Како преваранте не би открили, они користе неколико различитих имена домена и сервера. Уколико се открију, они брзо и лако замене своју инфраструктуру, чиме се обезбеђује интегритет њихове инфраструктуре за нападе, као и континуитет њиховог рада и токови нелегалног новца.[113]

Четври корак је последња ствар коју треба да уради пљачкаш банке. Када прибави неопходне информације, изврши нелегалне финансијске трансакције, нападач се сусреће са проблемом пребацивања новца украденог електронским путем у властиту земљу. Потребно је наћи посредника из исте земље одакле је жртва, посредник често није свестан да учествује у криминалној радњи.

---

[110] *Тројанац Зевс,* http://www.informacija.rs/Vesti/Bankarski-Trojanac-Zeus-se-prodaje-na-Facebook-u.html , приступила 10.11.2019. год .

[111] *Тројанац* TSPY:BANKER.NJH, http://www.informacija.rs/Sajber-hronika/Lordfenix-Prica-o-uspehu-20-ogodisnjeg-hakera-koji-prodaje-svoje-bankarske-trojance.html, приступила 10.11.2019. год.

[112] Стручњаци упозоравају "Банкарски" тројанци и ransomware за Андроид у порасту, http://www.informacija.rs/Mobilni-telefoni/Strucnjaci-upozoravaju-Bankarski-Trojanci-i-ransomware-za-Android-u-porastu.html, приступила 10.11.2019. год.

[113]Случај "Eurograbber": Како је малвер украо 36 милиона евра са банковних рачуна европских корисника http://www.informacija.rs/Vesti/Slucaj-Eurograbber-Kako-je-malver-ukrao-36-miliona-evra-sa-bankovnih-racuna-evropskih-korisnika.html, приступила 10.11.2019. год.

4.6.1. Случајеви преваре из области електронског банкарства

- **Случај- група Анунак из Русије**

Ова група је почела тако што је вршила напад на малопродаје у САД, Аустралији и Европи, њихов главни циљ је био да инфицира ПОС терминале[114] малверима, уз чију помоћ би прикупљали податке о платним картицама током трансакција. Напад је, на почетку, био организован на 16 фирми, од којих су се 12 налазиле у САД. Крађа информација је потврђена у три случаја. Такође, група Анунак је компромитовала компјутере у америчким PR медијским организацијама, како би стекли предност у трговању на берзи. Између осталог, ова група је успела да приступи на више од 50 руских банака и 5 платних система, док су две од тих институција изгубиле лиценцу за обављање банкарских послова. Најуспешнија година за ову групу била је 2014. година, успели да украду око 25 милиона долара до данас.[115]

- **Случај- Либанска клопка**

Механизам "либанске клопке" састоји се од пластичног кућишта у коме се стављају картице тзв скимера и специјно прерађене флеш меромије, која чува податке о великом броју картица. Ову врсту преваре је покушао бугарски држављанин А.С. (38), који је ухваћен на граничном прелазу Градина када је покушао да унесе "либанску клопку".[116] Пре него што је измишљена "либанска клопка", коришћене су траке из ВХС касета, које су биле савијене у облику латиничног слова У, дужине 15цм, та трака се убацивала у отвор за картице. Превара су обављали тако што су чекали да неко дође са картицом коју би трака задржала, преваранти би притекли у помоћ, уз образложење да је и њему банкомат прогутао картицу. Онда би од корисника тражио да поново укуца ПИН код, који би запамтили и након тога подигли новац.[117]

---

[114] ПОС терминал (Point Of Sale) представља врсту терминала помоћу ког се може плаћати роба и услуга. Опремљен је софтвером за процесирање трансакција платним картицама и користи се у услужним и трговачким радњама.

[115] *Руски хакери украли 25 милиона долара од банака и са банкомата,* http://www.informacija.rs/Vesti/Ruski-hakeri-ukrali-25-miliona-dolara-od-banaka-i-sa-bankomata.html, приступила 24.05.2020. године

[116] *Либанска клопка, https://www.blic.rs/vesti/hronika/libanska-klopka-bugarin-uhapsen-sa-spravom-za-pljackanje-zrtva-nista-ne-primeti-dok/zkvtjn9, приступила 24.05.2020. године*

[117] *Либанска клопка, https://noizz.rs/noizz-news/libanska-klopka-prevara-na-bankomatu-od-koje-svi-strepe/bqq2hlq, приступила 24.05.2020. године*

- **Случај- фотографско памћење**

Јусуке Танигучи (34) је успео да запамти податке са кредитне картице, од 1.300 клијената у продавници где је радио, а затим користио те податке са картице за себе. Он је имао фотографско памћење и успео је да у једном тренутку запамти 16- цифрени број картице, име власника, датум истека и сигурносни код. Након што је полиција извршила претрес и ухапсила наведену особу, пронађена је свеска у којој су се налазила имена и бројеви кредитних картица које је он украо.[118]

III ПОСЛЕДИЦЕ КОМПЈУТЕРСКЕ ПРЕВАРЕ

Последице компјутерске преваре могу се поделити на следећи начин:

- Материјалне (финансијске) последице,
- Нематеријалне последице,
- Комбиноване последице.

1. Материјалне последице

Материјалне последице могу настати када учинилац врши превару како би стекао противправну имовинску корист, за себе или неког другог или је не стекне али објективно причини материјалну штету. Самим развојем технологије постоји све већи број идеја појединаца како стићи до што већег материјалног добитка, без обзира на противправни начин стицања. Разлози за вршење компјутерских превара су многобројни као на пример лоша економска ситуација, незапосленост, добар живот без много рада и труда итд.[119]

Штета која наступа услед вршења компјутерских превара је огромна, чак надмашује износ који се може добити вршењем класичних кривичних дела и може се мерити стотинама милиона долара. Углавном је реч о штети која је тешко сагледива и много већа него што се сматра у првом тренутку.

[118] *Електронско банкарство,* https://zanimljivostidana.com/zanimljivosti/prodavac-zapamtio-i-ukrao-kreditne-kartice-preko-1-300-ljudi.html, приступила 24.05.2020. године

[119] Обезбеђење доказа у криминалистичкој обради кривичног дела привредног криминалитета, Виша школа унутрашњих послова, Београд Земун, 2002, стр. 135

На основу извештаја компаније за рачунарску безбедност Symantec која је произвођач антивирусног софтвера Norton, више од две трећине одраслих у свету користи интернет, прецизније 69% је било жртва сајбер криминала уопште. Истраживање компаније наводи да је 2011. године сајбер криминалом било погођено око 430 милиона људи, финансијска штета је износила 14 милијарди долара, што доводи до закључка да нпр. трговина дрогом има знатно мањи износ прихода у односу на сајбер криминал.[120] Подаци из јула 2013. године на основу анализе америчког Центра за стратешке и међународне студије и компаније McAfee показале су годишњи губитак светске економије од сајбер криминала у износу од 500 милијарди долара.[121]

Светске силе као што су САД, Кина, Јапан и Немачка имају годишњи губитак у износу од око 200 милијарди долара када је у питању сајбер криминал. Различита истраживања су показала да око 40 милиона становника САД је бар једном у животу била жртва преваре, при чему су им украдени лични подаци, у Турској око 54 милиона становника, у Немачкој око 16 милиона, док је у Кини више од 20 милиона становника било жртва преваре.[122]

Што се тиче повратка новца који је украден од стране компјутерских превараната, на основу истраживања које је спровео Kaspersky Lab, 41% жртава превара никада није повратило свој новац, 45% је успело да поврати, док је 14% успело само део новца да поврати.[123]

2. Нематеријалне последице

Нематеријалне последице подразумевају неовлашћено откривање туђих тајни или неко друго индискретно понашање које се односи на компјутерско узнемиравање или прогањање, без постојања материјалне користи. Компјутерско узнемиравање може бити директно или индиректно. Под директним узнемиравањем се подразумева претња или поруке застрашујућег садржаја које су послате жртви путем мејла, слање заражених порука или компјутерских вируса. Под индиректним узнемиравањем се подразумева ширење неистине о жртви на интернет форумима, слање поруке другим

[120] У САД је било више од 74 милиона жртава сајбер криминала, уз директне финансијске губитке од 32 милијарде долара.
[121] Koliko svetsku ekonomiju košta sajber kriminal, http://www.informacija.rs/Vesti/Koliko-svetskuekonomiju-kosta-sajber-kriminal.html , приступила 03.05.2020. године
[122] *Top 20 Countres Found to Have the Most Cybercrime,* http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/ , приступила 03.05.2020. године
[123] Koliko svetsku ekonomiju košta sajber kriminal, http://www.informacija.rs/Vesti/Koliko-svetskuekonomiju-kosta-sajber-kriminal.html , приступила 03.05.2020. године.

корисницима интернета у име жртве.[124] Када је у реч о прогањању, подразумева се конвенционално прогањање, узнемиравање у неконвенционалном сајбер простору, које се врши посредством информационих технологија. Сличност између сајбер прогањања и конвенционалног прогањања је у континуираном узнемиравању и изазивању страха код жртве.[125]

Индикатори психолошког злостављања у сајбер простору су: лажно представљање, обмањивање и недозвољено саопштавање, оговарање или клеветање, вређање, узнемиравање и прогањање, искључивање односно прогонство. Као средства комуникације која се користе како би се испољило психолошко злостављање у сајбер простору могу бити текстуалне поруке, електронске поруке, инстант поруке, сајтови за социјално умрежавање, блогови, веб сајтови итд.

Сајбер прогањање представља скуп поступака у оквиру којих појединац или група путем комуникационо-информационе технологије узнемирава једну особу или више појединаца. Под тим понашањем се подразумевају претње, лажне оптужбе...[126]

Када је у питању психолошко злостављање познато је да није реч о новој појави, али се као нова појава може посматрати у сајбер простору које је настало развојем информационих технологија и интернет глобализацијом. Последице психолошког злостављања се не манифестују само на појединца већ на целокупно друштво.[127] Путем психолошког злостављања испољавају се сва негативна понашања према другим лицима од стране злостављача, помоћу електронске технологије, која се може користити у било које време и у сваком простору, према сваком физичком лицу које користи електронску технологију.[128]

[124] Ellison, L., Akdeniz, Y. (1998), Cyber-stalking: the Regulation of Harassment onthe Internet,"Criminal Law Review", December Special Edition: Crime, Criminal Justice and the Internet, p. 29–48.
[125] Bocilj, P. (2003), Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet, "First Monday", vol. 8, no. 10, http://firstmonday.org/issues/issue8_10/bocij/index.html , приступила 03.05.2020. године
[126] Bocilj, P., McFarlane, L. (2002), Online harassment: towards a definition of cyber stalking, „Prison Service Journal", (139), p. 31–8.
[127] Б. Поповић-Ћитић, Вршњачко насиље у сајбер простору „Темида", ISSN: 1450-6637, vol. 12, no. 3. стр. 43–62, 2009, DOI: 10.2298/TEM0903043P.
[128] Baum, K., Catalano, S., Rand, M., Rose, K., Stalking victimization in the United States, Washington, DC: Bureau of justice report, US Department of justice, 2009, http://www.ojp.usdoj.gov/bjs/abstract/svus.htm, последњи пут приступили 12.04.2016.године.

Истраживања у многим државама у свету показала су огромне последице психолошког злостављања у сајбер простору, пре свега над школском популацијом (cyberbullying).

У Јужној Кореји спроведено је истраживање у коме је учествовало 5.000 студената, резултати истраживања су показала да је чак 36% студената било жртва сајбер малтретирања у 2012. години и да су се због тога осећали усамљено, беспомоћно и мање вредно.[129]

Што се тиче пријављивања неког од облика сајбер малтретирања, на основу истраживања APA Media Psychology Division резултати су да само једна од четири жртве школског узраста пријављује малтретирање. Током 2012. године у САД чак 850.000 ученика и студената су били жртве злостављања. Злостављачи су у стању да открију жртвине личне податке на веб сајту, па на основу тих података злостављач објављује информације у жртвино име, што доводи жртву у стање које изазива тешке последице путем страха, поремећаја у спавању или исхрани итд.[130]

Истраживање о прогањању у САД у 2006. години дошло је до следећих резултата: на основу идентификације 3.424.100 жртава прогањања, 83% жртава трпеле су узнемираваең путем мејла, док је 35% случајева трпело узнемиравање путем инстант порука. У Великој Британији 79% је било узнемиравано путем мејла, док путем инстант порука 13%, собе за чет су коришћене у 8% случајева, интерактивни сајтови су коришћени у 2% случајева. 82% учиниоца су били мушког пола, просечног узраста од 24 године. 52% жртве су биле женског пола, просечне старости 32 године.[131]

3.Комбиноване последице

Комбиноване последице подразумевају рушење нечијег угледа, а истовремено настанак финансијске штете. Поред тога што чињењем кривичног дела произилази финансијска штета, код жртве кривичног дела јављају се страх, нервоза, бес, осећај личне несигурности.

---

[129] D'Ovidio, R., Doyle, R., A study on cyber stalking: Understanding investigative hurdles, FBI Law Enforcement Bulletin, ISSN 0014-5688, vol. 73, no. 3, p. 10–17, 2003, http://www.fbi.gov/publications.htm , приступила 06.05.2020. године.

[130] Kowalski, R. M., Limber, S. P., Agatston, P. W., Cyber Bullying: Bullying in the Digital Age, John Wiley & Sons, ISBN: 978-14443-21-88-3, 2010.

[131] D'Ovidio, R., Doyle, R.(2003), A study on cyber stalking: understanding investigative hurdles, „FBI Law Enforcement Bulletin", 73 (3), p 10–17, www.fbi.gov/publications , приступила 06.05.2020. године

Комбиноване последице могу представљати уцене о приватним инфомацијама до којих се може доћи употребом тзв. полицијског малвера. Често је епилог тих случајева трагичан, што се може видети следећим примерима.

Један од примера је седамнаестогишњак Џозеф Едвардс који је обесио када је добио лажни мејл од стране полиције где се наводило да је користио нелегалне веб сајтове и да због тога мора да плати 100 фунти како се не би покренуо судски поступак. Едвардс је боловао од аутизма што је допринело томе да поверује да је тај мејл истинит. Након што је извршио самоубиство, истрага је показала да је његов лаптоп заражен малвером који је закључао уређај уцењујући Едвардса путем Ukash-а[132]. Како би спречио полицију да учини даље кораке у вези "непристојних" слика које су се налазиле на његовом рачунару и како би спречио сазнање његове породице о томе, он је одузео себи живот.[133]

IV НАДЛЕЖНОСТ ДРЖАВНИХ ОРГАНА У БОРБИ ПРОТИВ КОМПЈУТЕРСКЕ ПРЕВАРЕ У РЕПУБЛИЦИ СРБИЈИ

1. Посебно одељење за борбу против високотехнолошког криминала Вишег јавног тужилаштва у Београду

За откривање високотехнолошког криминалитета, уједно и за откривање компјутерске преваре надлежно је Више јавно тужилаштво у Београди за територију Републике Србије. Формирано је посебно одељење, односно посебно тужилаштво за борбу против високотехнолошког криминала у Вишем јавном тужилаштву.

Радом Посебног тужилаштва руководи Посебни тужилац за високотехнолошки криминал. Као посебан тужилац може се изабрати републички јавни тужилац из реда заменика јавних тужилаца. Реч је о лицу које испуњава услове за избор заменика вишег јавног тужиоца, уз постојање писмене сагласности лица које се поставља. Предност има

[132] Сервис који отежава да се открије идентитет криминалца који користе како би изнудили новац од корисника.
[133] Još jedno samoubistvo zbog „policijskog" malvera. http://www.informacija.rs/Sajber-hronika/Josjedno-samoubistvo-zbog-policijskog-malvera.html , приступила 06.05.2020. године.

лице са посебним знањем из области информатичке технологије.[134] Поред руководиоца у Посебном тужилаштву су ангажована и два заменика Вишег јавног тужиоца коју су специјализована за ову област, такође и два тужилачка саветника са административним особљем.[135]

2. Служба за борбу против високотехнолошког криминала у оквиру МУП-а

Како би се полиција борила против најновијих технологија, потребно је да буду високообучени и технолошки опремљени савременим средствима. У оквиру МУП-а постоји Посебна служба, која је почела са радом у априлу 2008. године.

Закон о оснивању и надлежности државних органа за борбу против високотехнолошког криминала, у члану 9 регулише рад ове Службе на следећи начин: "Ради обављања послова органа унутрашњих послова у вези са кривичним делима из члана 3. овог закона, образује се у оквиру министарства надлежног за унутрашње послове служба за борбу против високотехнолошког криминала."[136] Ова служба поступа по захтеву посебног тужиоца, у складу са законом. Дужност овог органа је да открије високотехнолошки криминала, такође, може бити ангажован у претходном кривичном поступку, уколико треба да се изврши увиђај. У 2008. години поднето је 35 кривичних пријава, одузета су 53 рачунара и 49.000 оптичких дискова. Углавном се ради о кривичном делу из члана 199 КЗ, међутим, у последње време се повећао број кривичних дела рачунарска превара и злоупотреба платних картица.[137]

У оквиру ове службе, од 2001. године (када је регистрован први случај у Интерполу) па до 2010. године, формирано је 256 досијеа, у којима се налазе појединии или групни случајеви високотехнолошког криминала.[138]

---

[134] Закон о организацији и надлежности државних органа у борби против високотехнолошког криминала ("Сл.гласник РС", бр.61/2005 и 104/2009), члан 4.

[135] *Посебно тужилаштво за борбу против високотехнолошког криминала Вишег јавног тужилаштва у Београду, http://www.beograd.vtk.jt.rs/,* приступила 27.05.2020. год.

[136] Закон о организацији и надлежности државних органа у борби против високотехнолошког криминала (Сл.гласник РС") бр. 61/2005 и 104/2009, члан 9.

[137] Удружење јавних тужилаца и заменика јавних тужилаца, Сузбијање високотехнолошког криминала, АТС, Београд, 2010, стр. 231.

[138]Уљанов, С., Урошевић, В., Ивановић, З., Високотехнолошки криминал из угла међународне сарадње криминалистичке полиције, зборник радова са међународног научно-стручног скупа "Међународна и национална сарадња и координација у супростављању криминалитету", вол.3, бр.1, стр. 530-541, Интернационална асоцијација криминалитета, Бања Лука, 2010, стр. 537

3. Надлежност и организација судова у случајевима сајбер криминала

У трећем делу Закона о организицији и надлежности државних органа у борби против високотехнолошког криминала прописана је надлежност суда у предметима ове врста криминалитета. У члану 10. је наведено: "За поступање у предметима кривичних дела из члана 3. овог закона надлежан је Виши суд у Београду, за територију Републике Србије." [139] Док је у другостепеном поступку надлежан Апелациони суд у Београду. Судије у овом Одељењу су распоређене од стране председника Вишег суда из реда судија тог суда, уз постојање њихове сагласности.[140] Судије су распоређене на две године, с тим што постоји могућност да се период од две године продужи одлуком председника Вишег суда, уз постојање писмене сагласности од стране лица које се ту распоређује.

Пракса посебног Већа за борбу против високотехнолошког криминала говори да је највећи број кривичних дела која су заступљена код нас свакако кривично дело интелектуалне својине, где је објект заштите ауторско дело. Када је реч о осталим делима из области високотехнолошког криминала, најзаступљенији облици су превара (члан 208КЗ), у којој се као средство за извршење дела јавља рачунар, рачунарска превара, рачунарска саботажа и неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података.[141]

[139] Закон о организацији и надлежности државних органа у борби против високотехнолшког криминала ("Сл. гласник РС", бр. 61/2005 и 103/2009), члан 3.

[140] Постоји могућност да се распореди и судија другог суда.

[141] Удружење јавних тужилаца и заменика јавних тужилаца, Сузбијање високотехнолошког криминала, АТС, Београд, 2010, стр. 237.

V ПОСЕБНИ ДЕО- ИСТРАЖИВАЊЕ: "Компјутерска превара у Републици Србији у периоду од 2014. године 2018. године"

Коришћење интернета како на глобалном нивоу, тако и у Републици Србији је у константном порасту. На основу статистичких података, у 2007. години у Републици Србији је регистровано да је интернет користило 1.270.000. корисника, док је у 2017. години тај број био у порасту, укупно 4.705.141. корисника. Што значи да је у том временском периоду број корисника интернета увећан чак за 370%, а уједно је увећан и ризик да се рачунарска превара појави у што бројнијем облику.[142]

1. Предмет и циљ истраживања

Орган који је најактивнији у борби против компјутерске преваре је свакако Посебно одељење за борбу против високотехнолошког криминала Вишег јавног тужилаштва у Београду, те су за потребу истраживања у оквиру овог мастер рада коришћени подаци које поседује претходно наведено тужилаштво. Предмет истраживања је број кривичних пријава, број оптужница и број донетих пресуда за кривична дела компјутерске преваре, као и да ли су пријављене особе биле мушког или женског пола. С обзиром да је реч о кривичном делу новијег датума, може се рећи да кривично дело компјутерска превара није толико заступљено у Републици Србији у односу на друга кривична дела која регулише Кривични законик РС. Такође, за потребу истраживања коришћени су подаци које поседује Републички завод за статистику.

2. Просторни и временски оквир истраживања

Просторни оквир истраживања се односи на територију Републике Србије, с тим што аутономна покрајина Косово и Метохија није обухваћена. Временски оквир истраживања је период од 2014-2018. године

3. Методе и хипотезе истраживања

Основна метода која је коришћена ради спровођења истраживања је метода анализе података који су прибављени од стране Посебног одељења за борбу против високотехнолошког криминала Вишег јавног тужилаштва у Београду и метода анализе података преузетих од стране Републичког завода за статистику Републике Србије.

---

[142] *Републички завод за статистику,* https://www.stat.gov.rs/vesti/20190920-godisnje-istrazivanje-o-ikt/?a=27&s , приступила 26.05.2020. године

Спроведеним истраживањем наведене су следеће хипотезе:

- Највећи проценат извршиоца кривичног дела компјутерске преваре су мушкарци.
- Највећи проценат извршиоца кривичног дела компјутерске преваре су пунолетна лица.
- Код малолетних лица је забележено да су највећи проценат извршиоца кривичног дела компјутерске преваре девојчице.
- Хронолошки посматрано, присутан је тренд раста броја кривичног дела компјутерска превара.
- Мали је проценат решених кривичних дела компјутерске преваре.

Посебном одељењу за високотехнолошки криминал Вишег јавног тужилаштва у Београду је упућен захтев у коме је затражен увид у податке о заступљености компјутерске преваре у Републици Србији, тачније о броју кривичних пријава, броју поднетих оптужница, донетих пресуда, као и о старосној, образовној, полној структури и о радном статусу за период од 2014. до 2018. године. У захтеву је наведен број кривичних пријава, број поднетих оптужница и број пресуда, као и број донетих пресуда у односу на мушки и женски пол.

4. Резултати истраживања

Према подацима Посебног одељења за борбу против високотехнолошког криминала у периоду од 2014. до 2018. године забележено је да је стопа криминала на територији Републике Србије у порасту. У периоду од 2014. године до 2018. године, посебном одељењу за борбу против високотехнолошког криминала поднете су кричивне пријаве компјутерске преваре против укупно 75 лица, што се оптужница тиче, поднето је 14, а када су у питању пресуде, број пресуда које су донете у овом периоду износи 7, од којих је шест пресуда донето у односу на оптужене мушког пола и једна пресуда која је донета у односу на особу женског пола.

1.1. Број пријава, оптужба и песуда

Период:	Кривична пријава	Оптужба	Пресуда
2014-2018	75	14	7

1.2. Број пресуда у односу на мушки и женски пол

Пол:	Пресуда
Мушки пол	6
Женски пол	1

Републички завод за статистику садржи податке који су везани за компјутерску превару, односно податке о пунолетним и малолетним учиниоцима ове врсте кривичног дела у Републици Србији. У оквиру статистичких података приказани су бројеви пријаве, оптужбе и пресуде. Конкретно, у овом истраживању приказани су подаци у временском периоду од 2014. до 2018. године.

1.1. Табела: Пунолетни учиниоци, период 2014-2018

Година	2014	2015	2016	2017	2018
Пријава	1	1	5	11	2
Оптужба	0	1	3	10	13
Пресуда	0	0	1	7	0

Према републичком заводу за статистику број пријава кривичног дела компјутерске преваре чији су починиоци пунолетне особе је у периоду од 2014. до 2018. је износио 20 пријава надлежним судским органима и у истом периоду подигнуто је 27 оптужница против пунолетних починиоца. Година са највећим бројем пријава компјутерске преваре је 2017. година са укупно 11 пријава, док је 2016. пријављено 5 случајева, а 2018. свега два. Најмање пријављених случајева је забележено 2014. и 2015., по једна пријава за сваку годину. Највише оптужница против пунолетних учиниоца кривичног дела компјутерске преваре подигнуто је 2018. године, Републички завод за статистику бележи 13 оптужница, док је годину дана раније број оптужница износио 10. У периоду који је претходио 2017. години, а са почетком од 2014. године, према Републичком заводу за статистику број отужница је занемрљив у односу на 2017. и 2018. годину и износи укупно 4, од чега су 2016. подигнуте три оптужнице, а 2014. ниједна. Однос подигнутих оптужница и пресуда је у великој диспропорцији, па је тако у периоду од 2014. до 2018. године донето 8 правоснажних пресуда против пунолетних починиоца кривичног дела компјутерске преваре, а највећи број пресуда је донето 2017. године, укупно 7, док је 2016. донета само једна пресуда. Што се тиче преосталих година које

се односе на период овог истраживања, није било донетих пресуда против пунолетних учиниоца кривичног дела компјутерске преваре.

1.1. Пунолетни учиниоци, период 2014-2018

Година	2014	2015	2016	2017	2018
Мушки пол	1	1	4	11	2
Женски пол	0	0	1	0	0

Када је полна структура пунолетних учиниоца кривичног дела компјутерске преваре у питању, у периоду од 2014. до 2018., на који се односи ово истраживње, према Републичком заводу за статистику забележена је једна особа женског пола као учиниоц кривичног дела и то 2016. године, док пре и после 2016. године, а у оквиру периода на које се истраживање односи, није забележен ниједан учиниоц женског пола. Насупрот учиниоцима женског пола, највећи број мушких учиниоца кривичног дела компјутерска превара је забележен 2017. године када је према Републичком заводу за статистику износио 11 пунолетних мушких учиниоца. Укупан број учиниоца за преостали период на који се односи ово истраживње је осам и то 2016. четири, 2018. два, док је у 2014. и 2015. години забележен по један учиниоц мушког пола.

1.1. Малолетни учиниоци, период 2014-2018

Година	2014	2015	2016	2017	2018
Пријава	3	0	0	0	0
Оптужба	0	0	0	0	0
Пресуда	0	0	0	0	0

Што се малолетних учиниоца кривичног дела компјутерске преваре тиче, према Републичком заводу за статистику забележене су само три пријаве 2014. године, док у периоду до 2018. није забележена ниједна пријава. Насупрот три пријаве за цеолокупан период од 2014. до 2018. Републички завод за статистику наводи да у истом периоду није подигнута ниједна оптужница нити је било правосудних прсуда надлежног суда.

1.1. Малолетни учиниоци, период 2014-2018

Година	2014	2015	2016	2017	2018
Мушки пол	0	0	0	0	0
Женски пол	3	0	0	0	0

Републички завод за статистику наводи податак, да су 2014. године забележена три малолетна лица женског пола као учиниоци компјутерске преваре, док у периоду до 2018. није забележен ниједан случај. Што се малолетних учиниоца компјутерске преваре мушког пола тиче, Завод за статистику наводи податак да од 2014. до 2018. није забележен ниједан такав случај.[143] Републички завод за статистику као и Више јавно тужилаштво за сајбер криминал, коме сам се обратила писмом позивајући се на Закон о приступу информацијама од јавног значаја, не воде евиденцију пријављених, оптужених и осуђених лица по старосној, полној и образовној структури, као ни по радноправном статусу лица.

[143] Републички завод за статистику као и Више јавно тужилаштво за сајбер криминал, коме сам се обратила писмом позивајући се на Закон о приступу информацијама од јавног значаја, не воде евиденцију пријављених, оптужених и осуђених лица по старосној, полној и образовној структури, као ни по радноправном статусу лица.

ЗАКЉУЧАК

Глобалне рачунарске мреже су створиле могућност за нове облике криминала. Интернет представља идеално скровиште за извршење различитих врста кривичних дела. Компјутерске преваре су једна од највећих претњи у сајбер простору. Није потребно посебно знање из области информационих технологија, па је због тога лако извршити превару. Ранији облици превара, као што су Нигеријска превара, полако ишчезавају, њих мењају новији облици превара, који на софистициран начин преузимају контролу над зараженим рачунаром.

Једини начин да се одбранимо, односно да не наседнемо на преваре које вребају на сваком нашем кораку приликом боравка на интернету јесте коришћење здравог разума. Без рационалног понашања и свести о опасностима које сајбер простор носи, сваки безбедносни програм биће узалудан.

На основу претходног изнетог у овом раду, може се закључити да су технолошке иновације створиле могућности за појаву нових облика криминала чије је место деловања сајбер простор а извршиоци користе рачунаре и рачунарске системе као средство за извршавање својих криминалних радњи. Важно је нагласити да је савремено друштво постало зависно од коришћења информационо- комуникационе технологије и да се више него икада пре изложено различитим облицима компјутерског криминала који данас актуелни у сајбер простору. Свесни смо данас да смо сви ми корисници интернета и да је он толико незаштићен и рањив да га све то чини погодним тлом и скровиштем за сајбер криминалце који уз помоћ њега врше компјутерске противзаконите радње различитих модела. Једна од највећих претњи у сајбер простору која је све учесталија јесу компјутерске преваре за чије извршење није неопходна сложена организација ни много времена већ се овај вид компјутерског криминала извршава једноставно, у веома кратком временском периоду и у тајности, да преварени није ни свестан да је постао жртва компјутерског преваранта. Данас смо упознати са ризицима и опасностима које су проузроковале компјутерске преваре. Постоји велики број жртава који су се сусрели са различитим видовима превара, пре свега мислећи на оне најбројније као што је „нигеријска превара“ или класичне спам преваре, а у данашње време корисницима рачунарских система и мрежа прете знатно софистицираније модели компјутерских превара који врло лако могу да заразе рачунаре и да на тај начин украду личне и финансијске податке корисника. Није овде реч само о преварама у виду инфицирања рачунара и крађе личних података, ту се

криминалне радње не завршавају , јер је данас актуелно да се лични подаци до којих је криминалац дошао, продају на црним тржиштима а затим се даље користе у противправне сврхе. Колико год се сусретали са различитим видовима превара путем интернета, знамо и сами да ћемо изнова користити услуге које нам нуде глобалне рачунарске мреже јер без тога не можемо да функционишемо. То је зато што су рачунар, рачунарски системи и мреже постали саставни и нераскидиви део човековог живота. Једини начин да се смањи број жртава и кривичних дела компјутерског криминала јесте да се он регулише путем закона и јачањем свести у друштву а пре свега у оквиру млађе популације о томе колико је опасан сајбер простори и које су то адекватне мере које сваки појединац 70 може предузети да би се на време спасио да не падне у руке сајбер криминална, односно да његови подаци не буду украдени и злоупотребљени. Држава је ,поред појединца као корисника рачунара, та која мора да делије превентивно и репресивно у области сузбијања сајбер криминала. У пракси се више јавља констатација да је боље на време спречити превару, тј. док до преваре није дошло јер сајбер криминалци и преваранти користе се најновијим методама да прикрију своје трагове онда када већ изврше кривично дело. Зато је неопходно да се ревидирају постојећи и усвајају нови прописи и закони који ће да регулишу борбу против компјутерског криминала и који ће допринети што бољој заштити корисника информационо- комуникационе технологије. Од великог је значаја да се постојећи закони промене и прошире новим одредбама јер и сами смо свесни чињенице да је сајбер криминал склон виталности и може да се мутира врло брзо због чега и представља озбиљан безбедносни проблем. Многе државе нису у стању да се изборе са овим обликом криминала јер борба против њега изискује велике финансијске издатке из државног буџета па зато многе државе осећају страх да се упусте у борбу са оваквим феноменом. На крају свега овога није држава та која нас може спасити од свих ових опасности који вребају у сајбер простору, него смо то ми сами, односно наш здрав разум и свесност о опасностима које сајбер простор носи са собом. Потребно је да деца у основним школама схвате да рачунар није игра, да омладина не одаје лако своје личне податке, да не користи непроверене сајтове, да се не упуштају у конверзацију с непознатим особама и да не верују у различите приче о новчаним добицима, пословним понудама које им пристижу на емајл јер ће их бити све више и имаће упечатљиву сржј која ће лако преварити примаоца таквих порука.

Литература

1) Б. Поповић-Ћитић, Вршњачко насиље у сајбер простору „Темида”, ISSN: 1450-6637, vol. 12, no. 3. стр. 43-62, 2009, DOI: 10.2298/TEM0903043P.
2) В. Водинелић, *Методика откривања, доказивања и разјашњавања рачунарског криминалитета,* Приручник, 4/1990
3) В. Полић, *Компаративна анализа компјутерског криминала у законодавствима Републике Србије и неких страних земаља*, Универзитет Сингидунум
4) В. Спасић, *Актуелна питања у области сајбер криминала (чланак)*, Билтен судске праксе Врховног суда Републике Србије, број 1/2006, Београд
5) В. Урошевић, З. Ивановић, С. Уљанов, *Мач у Word wide web-у: Изазови високотехнолошког криминала,* Београд, 2012, Етернал микс
6) В. Урошевић, *"Нигеријска превара у Р. Србији"*, Безбедност- часопис Министарства унутрашњих послова Р. Србије, бр.3/2009, Београд
7) Директива Европског парламента и Савета о чувању података који су добијени или обрађени приликом пружања јавно доступних услуга електронске комуникације или јавних комуникационих мрежа.
8) Д. Јовашевић, *Кривично право-посебни део*, Ниш, 2014, Номос
9) Д. Вулетић, *Одбрана од претњи у сајбер простору* Одбрана, Београд, 2011
10) Д. Плескоњић, Мачек Н., Ђорђевић Б., Царић М., *Сигурност рачунарских мрежа* Виша електронска школа, Београд, 2006. година
11) Ж. Алексић, М. Шкулић, *Криминалистика,* Правни факултет Универзитета у Београду и Јавно предузеће "Службени гласник", Београд, 2007
12) Ж. Миладиновић, *Кривично дело преваре као модел остваривања сајбер криминала, докторска дисертација,* Београд, 2016
13) Ј. Матијашевић, М. Петковић, *Кривична дела против безбедности рачунарских података- анализа противправних решења и значај у контексту сузбијања високотехнолошког криминала,* Зборник радова са међународне научно-стручне конференције "Криминалистичко-форензичка истраживања", Бања Лука
14) Конвенција о високотехнолошком криминалу
15) Л. Комлен Николић, *Сузбијање високотехнолошког криминала",* Удружење јавних тужилаца и заменика јавних тужилаца Србије, Београд, 2010
16) Л. Соковић, др.сц. Анте Орловић, *Облици пријевара у казненом закону,* 2017
17) М. Бабовић, *Хакерска субкултура и компјутерски криминал,* Правни живот-часопис за правну теорију и праксу, бр. 9/2004, Удружење правника Србије, Београд
18) М. Вујаклија, *Лексикон страних речи и израза*, Штампар Макарије, Београд, 2011
19) М. Косановић, *Интернет ризици,* Висока техничка школа струковних студија, Ниш, 2017
20) Обезбеђење доказа у криминалистичкој обради кривичног дела привредног криминалитета, Виша школа унутрашњих послова, Београд-Земун, 2002
21) П. Димитријевић, *Право информационе технологије,* Internet Law, Sven, Ниш, 2011
22) Р. Јерковић, „*Борба против високотехнолошког криминалитета у Србији*“, Телекомуникације- научно стручни часопис Републичке агенције за телекомуникације, бр. 3/2009
23) С. К. Вилић, В. Н. Ристановић, М. Костић, *Криминологија,* Ниш, 2009, Пеликан принт

24) С. Петровић, *Компјутерски криминал*, Војноиздавачки завод, Београд, 2004
25)
26) Стратегија сајбер безбједности Црне Горе *2013-2017,* стр. 12, Подгорица, јул 2013
27) Удружење јавних тужилаца и заменика јавних тужилаца, Сузбијање високотехнолошког криминала, АТС, Београд, 2010
28) Уљанов, С., Урошевић, В., Ивановић, З., Високотехнолошки криминал из угла међународне сарадње криминалистичке полиције, зборник радова са међународног научно-стручног скупа "Међународна и национална сарадња и координација у супростављању криминалитету", вол.3, бр.1, стр. 530-541, Интернационална асоцијација криминалитета, Бања Лука, 2010

Страна литература:

1) Bellour J. C. *Међународна превара*, Избор бр. 1. Загреб, 1981
2) Bocilj, P., McFarlane, L. (2002), Online harassment: towards a definition of cyber stalking, „Prison Service Journal"
3) Buchanan J., Grant A., (2001), *Investigating and Prosecuting Nigerian Fraud, ''U.S. A ttomeys''* Bulletin, vol. 49., no. 06, USA
4) C. S. McQuade, *Encyclopedia of Cybercrime,* London, 2009, Greenwood press.
5) Convention on Cybercrime – Explanatory Report
6) „Council Directive of 14 may 1991 on the Legal Protection of Computer Programs", Directive 91/250/EEC, OJ no L 122/42.
7) Dyrud M., (2005), *I brought You a good news An analysis of Nigerian 419 Letters,* Proceedings of 2005 Annual Association for Business Communications, Convention Association for Business Communication, USA
8) Ellison, L., Akdeniz, Y. (1998), Cyber-stalking: the Regulation of Harassment onthe Internet,"Criminal Law Review", December Special Edition: Crime, Criminal Justice and the Internet
9) J. C. Bellour, *Међународна превара,* Избор бр.1, Загреб, 1981
10) Kowalski, R. M., Limber, S. P., Agatston, P. W., Cyber Bullying: Bullying in the Digital Age, John Wiley & Sons, ISBN: 978-14443-21-88-3, 2010.
11) S. Schjolberg, *The histoy of cybercrime: 1976-2014,* Norderstedt, 2014, Cybercrime research institute
12) Smith R., Holmes M., Kaufmann P., *Nigerian Advance Fee Fraud, Trends and Issues in crime and criminal justice,* Australian Institute of Criminology, Australia, 1999
13) *The International Handbook of Computer Crime,* Chichester, John Wiley and sons

Закони:

1) Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала ("Сл.гласник РС", бр. 61/2005 и 104/2009)
2) Закон о потврђивању Конвенције о високотехнолошком криминалу, "Сл. гласник РС", бр.19
3) Закон о потврђивању додатног Протокола уз Конвенцију 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.)
4) Закон о оглашавању Републике Србије „Службени гласник РС", бр. 79/2005 і 83/2014

5)
6) Закон о играма на срећу, „Службени гласник РС“ бр 84/2004 и 85/2005
7) Кривични законик ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009 i 111/2009)
8) Кривични законик Републике Српске ("Сл.гласник РС", бр.64/2017 и 104/2018-одлука УС)
9) Казнени законик (КЗ-1), „Уредни лист Републике Словеније”, шт. 55/2008, issn 1318-0576, година XVII.
10) Казнени закон, „Народне новине Републике Хрватске”, бр. 110/97, 27/98, 50/00, 129/00, 51/01, 111/031, 190/03, 105/04, 71/06, 110/07, 152/08.
11) Кривични законик Црне Горе, ("Сл.лист РЦГ", бр. 70/2003, 13/2004-испр. и 47/2006 и "Сл.лист ЦГ"бр.40/2008, 25/2010, 32/2011, 64/2011- др.закон 40/2013, 56/2013-испр., 14/2015, 42/2015, 58/2015-др.закон, 44/2017, 49/2018 и 3/2020)
12) Кривични закон Федерације Босне и Херцеговине, ('Сл.новине ФБиХ", бр.36/2003, 21/2004- испр., 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 и 75/2017)
13) Кривичен законик Република Северна Македонија ("Сл.весник на Република Северна Македонија" број 80/99, 4/2002, 43/2003, 19/2004, 81/2005, 60/06, 73/06, 7/08, 139/08, 114/09, 51/11, 135/11, 185/11, 142/12, 166/12, 55/13, 82/13, 14/14, 27/14, 28/14, 115/14, 132/14)

Коришћени сајтови:

1) Адмирал Џејмс Ставридис, https://www.facebook.com/james.stavridis
2) Верификација твитера, https://www.informacija.rs/Drustvene-mreze/Fiseri-kradu-podatke-korisnika-uz-pomoc-laznog-Twitter-profila-za-verifikaciju.html
3) Електронско банкарство, https://zanimljivostidana.com/zanimljivosti/prodavac-zapamtio-i-ukrao-kreditne-kartice-preko-1-300-ljudi.html
4) Još jedno samoubistvo zbog „policijskog" malvera. http://www.informacija.rs/Sajber-hronika/Josjedno-samoubistvo-zbog-policijskog-malvera.html
5) Како се заштити од спама, https://www.informacija.rs/Anti-spam/Sta-je-spam-i-kako-se-zastititi-od-njega.html
6) Крађа идентитета, http://www.telegraph.co.uk/technology/9136029/How-spies-used-Facebook-to-steal-Nato-chiefsdetails.html
7) Крађа идентитета, https://www.novosti.rs/vesti/naslovna/drustvo/aktuelno.290.html:428129-Kradja-identiteta-Pakao-zbog-dvojnika
8) Ко вам гледа профил, https://www.index.hr/magazin/clanak/ako-ste-isli-vidjeti-tko-vas-gleda-na-facebooku-profil-vam-je-u-opasnosti/918312.aspx , приступила 27.05.2020. год.
9) Колико светску економију кошта сајбер криминал, http://www.informacija.rs/Vesti/Koliko-svetskuekonomiju-kosta-sajber-kriminal.html
10) Лажни профили, https://www.medijskapismenost.hr/kako-se-zastititi-od-krade-online-identiteta/
11) Лажни профили, http://rs.n1info.com/Vesti/a192303/Izbegnite-prevaru-na-Internetu.html
12) Либанска клопка, https://www.blic.rs/vesti/hronika/libanska-klopka-bugarin-uhapsen-sa-spravom-za-pljackanje-zrtva-nista-ne-primeti-dok/zkvtjn9
13) Либанска клопка, https://noizz.rs/noizz-news/libanska-klopka-prevara-na-bankomatu-od-koje-svi-strepe/bqq2hlq

14) Наградна игра, https://www.dostop.si/lazne-nagradne-igre-kako-jih-prepoznati-in-se-jim-izogniti/
15) Нигеријска превара у Републици Србији, http://arhiva.mup.gov.rs/cms/resursi.nsf/Nigerijska_prevara.pdf
16) Наградна игра, https://www.dostop.si/lazne-nagradne-igre-kako-jih-prepoznati-in-se-jim-izogniti/
17) Опрезно са онлине романсама. Дечак због уцене извршио самоубиство после разговора на Скајпу, http://www.informacija.rs/Vesti/Oprezno-sa-online-romansama-Decak-zbog-ucene-izvrsio-samoubistvo-poslerazgovora-na-Skype-u.html
18) Плави бец, https://verificationhandbook.com/book_cr/chapter3.php
19) Преваре са наградама, https://en.wikipedia.org/wiki/Lottery_scam
20) Преваре са наградама, https://www.informacija.rs/Drustvene-mreze/Facebook-ova-online-lutrija-ne-postoji-cuvajte-se-prevara.html
21) Посебно тужилаштво за борбу против високотехнолошког криминала Вишег јавног тужилаштва у Београду, *http://www.beograd.vtk.jt.rs/*
22) Руски хакери украли 25 милиона долара од банака и са банкомата, http://www.informacija.rs/Vesti/Ruski-hakeri-ukrali-25-miliona-dolara-od-banaka-i-sa-bankomata.html
23) Републички завод за статистику, https://www.stat.gov.rs/vesti/20190920-godisnje-istrazivanje-o-ikt/?a=27&s
24) Стратегија за борбу против високотехнолошког криминала, за период 2019-2023, http://arhiva.mup.gov.rs/cms_cir/decaipolicija.nsf/Strategija%20za%20borbu%20protiv%20visokotehnolo%C5%A1kog%20kriminala%20(2019%20-%202023).pdf
25) Службени лист Европске уније, http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32006L0024
26) Спам преваре, https://www.techopedia.com/definition/23763/spamming
27) Стручњаци упозоравају "Банкарски" тројанци и ransomware за Андроид у порасту, http://www.informacija.rs/Mobilni-telefoni/Strucnjaci-upozoravaju-Bankarski-Trojanci-i-ransomware-za-Android-u-porastu.html
28) Тимоти Повел, Флорида, https://www.blic.rs/slobodno-vreme/vesti/hteo-je-nove-zube-i-novog-psa-ali-nije-imao-novca-pa-se-odlucio-na-najbizarniji-korak/4q9xf5k
29) Тројанац Зевс, http://www.informacija.rs/Vesti/Bankarski-Trojanac-Zeus-se-prodaje-na-Facebook-u.html
30) Тројанац TSPY:BANKER.NJH, http://www.informacija.rs/Sajber-hronika/Lordfenix-Prica-o-uspehu-20-ogodisnjeg-hakera-koji-prodaje-svoje-bankarske-trojance.html
31) Фишинг, https://www.it-klinika.rs/blog/sta-je-phishing-email-i-kako-se-odbraniti
32) Фарминг, https://sr.wikipedia.org/sr-el/%D0%A4%D0%B0%D1%80%D0%BC%D0%B8%D0%BD%D0%B3

Страни сајтови:

1) Baum, K., Catalano, S., Rand, M., Rose, K., Stalking victimization in the United States, Washington, DC: Bureau of justice report, US Department of justice, 2009, http://www.ojp.usdoj.gov/bjs/abstract/svus.htm
2) Bocilj, P. (2003), Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet, ”First Monday”, vol. 8, no. 10, http://firstmonday.org/issues/issue8_10/bocij/index.html
3) Council of Europe, Recommendation No. R (89) 9 of the Committee of Ministers to member states on Computer- related crime, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804f1094

4) Charity Distribution Nigerian Scam, http://www.hoax-slayer.com/peter-attah-scam.shtml
5) Congratulations, you've won! The reality behind online lotteries. https://securelist.com/analysis/publications/36450/congratulations-youve-won-the-reality-behind-online-lotteries /
6) D'Ovidio, R., Doyle, R., A study on cyber stalking: Understanding investigative hurdles, FBI Law Enforcement Bulletin, ISSN 0014-5688, vol. 73, no. 3, p. 10–17, 2003, http://www.fbi.gov/publications.htm
7) Mrs Tema Wiliams Nigerian Scam, https://www.hoax-slayer.net/tema-williams-nigerian-scam/
8) Mr. Wong Du Nigerian Scam, http://www.hoax-slayer.com/wong-du-scam.shtml
9) Mother Sarah Alan Rowland Nigerian Scam, http://www.hoax-slayer.com/sarah-alan-rowland-scam.shtml
10) Nigerian spam, https://www.nigerianspam.com/
11) Nigerian Cyber Scammers – LA Times, http://www.latimes.com/la-fg-scammers20oct20-story.html
12) Proportion of spam in email traffic, https://securelist.com/analysis/quarterly-spam-reports/71759/spam-and-phishing-in-q2-of- 2015/
13) S. Schjolberg, *The History of Global Harmoniyation on Cybercrime Legislation- The Road to Geneva*, http://www.cybercrimelaw.net/documents/cybercrime_history.pdf
14) Sgt. Joey Jones Nigerian Scam, http://www.hoax-slayer.com/sgt-joey-jones-scam.shtml
15) "Symantec", https://www.it-klinika.rs/
16) Wumi Abdul Nigerian Scam, http://www.hoax-slayer.com/wumi-abdul-scam.shtml
17) Top 20 Countres Found to Have the Most Cybercrime, http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/

Апстракт

Компјутерска превара

Коришћење рачунара променило је функционисање друштва. Користи од употребе рачунара су бројне, али су исто тако бројне и штетне последице злоупотребе рачунара и рачунарских мрежа настале вршењем недозвољених, противправних радњи. Вршење кривичних дела на интернету, тј. у виртуалном простору одликује се другачијим карактеристикама него вршење обичних кривичних дела. Извршилац на располагању има бројне погодности интернета које му омогућавају да сакрије свој идентитет, прикрије доказе о извршењу кривичног дела и врло често избегне било какав физички контакт са жртвом. Због свега овога, дела која у себи садрже елемент високотехнолошког криминалитета су специфична и захтевају интензивну пажњу појединаца, државе и међународне заједнице. Према најновијим подацима, у тзв. сајбер простору налази се више од милијарду и по људи. Сајбер криминал је глобални проблем, који изискује пуно учешће и сарадњу друштвеног и приватног сектора у свим државама. Кад би само један % од милијарду и по људи имао намеру да коришћењем информационих технологија чини кривична дела, то би створило ситуацију да на светском нивоу имамо 15 милиона потенцијалних преступника.

Кључне речи: високотехнолошки криминалитет, компјутерска превара, Нигеријска превара.

Abstract

Computer fraud

Introduction of computers has changed the way society works. The benefits stemming from computer usage are numerous, but there are also a number of harmful consequences as a result of computers and computer networks' abuses. Committing criminal acts in the virtual space of Internet is characterized by different characteristics than the exercise of common crimes. The perpetrator has at its disposal a number of benefits of the Internet that allow him to conceal his identity, conceals evidence of the commission of the offense and often have no physical contact with the victim. Because of all this, criminal offences with elements of cyber crime are quite specific and require intensive heed of individuals, states and the entire international community. According to the newest data, there are more than billion and a half people in so-called cyberspace. Cyber crime is a global problem which requires full participation and cooperation of public and private sector in all states. If only % of billion and a half of people had the intention to commit crimes by using information technologies, there would be fifteen million of potential criminals.

Key words: high- tech crime, computer fraud, Nigerian fraud.

Биографија

Христина Стевић је рођена 18.05.1993. године у Приштини. Основну школу и Гимназију у Лапљем Селу (смер Природно- математички) је завршила са одличним успехом. Након средње школе, уписала је Правни факултет, на Универзитету у Приштини са привременим седиштем у Косовској Митровици и завршила у децембру 2017. године са просечном оценом 8.4 и тиме стекла звање дипломирани правник. Наредне године је уписала Мастер академске студије права на Правном факултету Универзитета у Нишу. Након завршетка студија успешно обавила стручну праксу у Привременом органу града Приштине и тиме стекла право на полагање државног испита.

ИЗЈАВА О ИСТОВЕТНОСТИ

ШТАМПАНОГ И ЕЛЕКТРОНСКОГ ОБЛИКА МАСТЕР РАДА

Име и презиме аутора мастер рада:
_____

Наслов мастер рада:_____

_____

Ментор: _____

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

_____

_____

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: _____

У Нишу, _____

Потпис аутора

_____