УНИВЕРЗИТЕТ У НИШУ

ПРАВНИ ФАКУЛТЕТ

Компјутерска крађа

(мастер рад)

МЕНТОР:

Проф. др Дарко Димовски

СТУДЕНТ:

Александра Трифуновић

број индекса: М 007/20-УП

Ниш, 2022. године

Садржај

УВОД

Компјутерски криминал је посебан вид компјутерског криминалитета, који је тешко дефинисати због његове феноменолошке разноврсности, и који као такав нема опште усвојену дефиницију, јер представља новији облик криминалног деловања, који се протеком времена све више усавршава, односно развијају се разне нове методе у деловању и начину понашања (modus operandi), јер иако обухвата постојеће облике криминала које чине људи, овде је специфичност у томе што се као средство и/или циљ извршења кривичног дела јавља компјутер, те га је из тог разлога тешко дефинисати јединственим и прецизним појмовним одређењем.[1]

Компјутерски криминалитет је облик криминалног понашања, код кога се коришћење компјутерске технологије и информатичких система испољава као начин извршења кривичног дела или се компјутер употребљава као средство и/или циљ извршења, чиме се у кривично-правном смислу остварује нека релевантна последица. [2]

Компјутерски криминалитет односи се на злоупотребе које тичу угрожавања интегритета, доступности или поверљивости рачунарских мрежа, телекомуникационих система и са њима повезаних података или се односе на употребу таквих мрежа и система за извршење традиционалних кривичних дела. То је свеукупност различитих облика, видова и форми испољавања противправних понашања управљених против безбедности рачунарских података, информационих и компјутерских система у целини или њихових појединих делова на различите начине и различитим средствима у намери да себи или другоме прибави каква корист (имовинске или неимовинске природе) или да се другоме нанесе каква штета.[3]

[1]Мегатренд Универзитет, Факултет за право, јавну управу и безбедност – ФДУА – Право и нове технологије, Београд Лутовац С., Рачић.J.– Компјутерски криминалитет као савремени облик криминалитета - Стручни чланак, 2021.године,, одобрен 15.09.2021.године, стр.284.
[2] Ibid.
[3]М. Павловић., Д. Тошић. - Кривичноправна заштита безбедности рачунарских података - стручни рад, 2017. године. Вол.8.бр. 1, стр.44.

Неке од основних карактеристика или обележја компјутерског криминалитета јесу:

- специфичан начин и вршење кривичног дела - уз помоћ или посредством компјутера,
- друштвено опасна, противправна понашања за која закон прописује кривичне санкције,
- посебан објекат заштите – безбедност рачунарских података или информационог система у целини или појединог сегмента,
- као и намера учиниоца да себи или другоме на овај начин прибави какву корист (имовинску или неимовинску) или другоме нанесе какву штету.[4]

Иако се компјутерски криминалитет реализује помоћу компјутера, он може имати облик било ког од традиционалних видова криминалитета (крађе, утаје, проневере...), те се компјутерска технологија може злоупотребљавати на разне начине, али најчешћи појавни облици компјутерског криминалитета су противправно коришћење услуга, неовлашћено прибављање информација уз помоћ компјутера, компјутерски тероризам, компјутерске крађе, компјутерске преваре, компјутерске саботаже, неовлашћено преправљање или уништење информација садржаних у компјутеру као и онемогућавање или отежавање приступа таквих информација овлашћеним корисницима, неовлашћена употреба компјутерског времена или услуга и др. [5]

У овом раду детаљније ћемо се бавити компјутерском крађом, као једним од појавних облика компјутерског криминалитета, где ће најпре укратко бити изложена проблематика око дефинисања појма компјутерске крађе, врсте компјутерске крађе, затим ће бити изложени релевантни домаћи законски прописи, међународне конвенције и директиве које дају законодавни оквир и дефинишу стандарде у супротстављању компјутерској крађи, идентификацији и заштити жртава компјутерске крађе, а ради критичког сагледавања свих предности и мана постојећег/непостојећег законодавног

[4]Д. Јовашевић, (коаутор Т. Хашимбеговић), Кривичноправна заштита безбедности рачунарских података – реферат поднет на саветовању: ''Злоупотребе информационих технологија'' – ЦД Зборник радова, Тара, 2004. године, стр. 3.
[5]ДрВ. Николић - Ристановић, Др С. Костантиновић– Вулић, Криминологија, издавачко-графичко предузеће „Прометеј", Београд 2018, стр.175-176.

оквира, као и идеја у ком смеру би постојећи/непостојећи оквир требало да се развија како би се правни систем што боље и ефикасније суочио и стао на пут оваквом проблему, који из године у годину, напредује и развија се упоредо са информационим технологијама.

Предмет

Предмет истраживања при изради завршног – мастер рада на тему „Компјутерска крађа“ представља пре свега уочавање глобалног проблема компјутерског криминалитета, као и компјутерске крађе, као једног од најзначајнијих појавних облика компјутерског криминалитета, затим сагледавање правног оквира на националном и међународном нивоу, свеукупност различитих метода у деловању, начину испољавања противправних понашања управљених против безбедности рачунарских података, информационих и компјутерских система, као и резултати истраживања и анализе резултата, кроз упоређивање статистичких података и примера у пракси, који се тичу ове појаве.

Значај

Значај истраживања на тему „Компјутерска крађа“ огледа се у томе што је сама Компјутеркса крађа новији облик криминалног деловања који се протеком времена све више усавршава, односно развијају се разне нове методе у деловању и начину понашања (modus operandi), јер иако обухвата постојеће облике криминала које чине људи, овде је специфичност у томе што се као средство и/или циљ извршења кривичног дела јавља компјутер, а имајући у виду технолошки напредак, као и ажурирање и надоградњу рачунарских система и рачунарске мреже, с тога је непоходно да се новонастале ситуације и иновативне околности, регулишу/санкционишу кроз законску легислативу.

Циљ

Циљ истраживања је указивање на то да је овој теми потребно посветити много више пажње, с обзиром да законодавство, како међународно, тако и национално, не иду у корак са временом, у конкретном случају. Имајући у виду брзину којом се развијају информационе технологије, као и информатичка знања, чија злоупотреба неретко доводи до пораста компјутерског криминалитета, где се као један од појавних облика најчешће

јавља компјутерска крађа (где је циљ и/или средство извршења дела компјутер), од изразите је важности указати на чињеницу да је потребно вредно радити на сузбијању овог облика компјутерског криминалитета, како би се овакав вид компјутерског криминалитета, у време када је компјутерска технологија на врхунцу, на адекватан начин, уврстио у важеће међународно и национално законодавство и развили адекватни системи заштите.

I ПОЈАМ КОМПЈУТЕРСКЕ КРАЂЕ

Компјутерска крађа јесте један од појавних облика компјутерског криминалитета, али као такав није појмовно одређен и прецизно дефинисан. Основно обележје овог дела је противправно одузимање туђе покретне ствари (било да је реч о стварима у физичком облику или подацима и датотекама у преносивом облику).[6] Како у конкретном случају постоји разлика у погледу објекта који се овим делом присваја, веома је тешко одредити прецизну дефиницију појма компјутерске крађе.

Појам компјутерске крађе, поред крађе која се изводи тако што се отуђују рачунари и рачунарска опрема, подразумева и крађу идентитета, крађу рачунарских података, крађу кодова, лозинки, идентификационих бројева, као и разноврсне робе. Мрежно окружење и интернет пружају велике могућности за крађу пословних и других тајни, софтвера и ауторских дела, али и за крађу личних тајни и и њихово коришћење за крађу новца и друге нападе на личности. У порасту је број крађе података са личних рачунара или мобилних уређаја, као и велике базе података које располажу милионским записима о личностима, а све ради, углавном, финансијских злоупотреба од стране извршиоца дела, ради даље продаје на црном тржишту или уцењивањем компанија и организација које чувају податке.[7]

Веома су разноврсни и променљиви облици у којима се појављује ово дело, као и начини њихове реализације. Компјутерска крађа има висок обим појављивања у оквиру компјутерског криминалитета. У основи постоје два начина реализације овог дела:

– класичан, који подразумева физички улазак у просторије и одношење објекта, који се присваја и други

– логички упад у рачунарски систем и условно речено „одношење" објеката који се присвајају.[8]

[6]С. Петровић, Компјутерски криминал, Министарство унутрашњих послова Републике Србије- Уредништво часописа „Безбедност" и „Полицајац", Београд, 2000, стр. 118.
[7]А.Ђукић, Безбедност - Крађа идентитета-облици, карактеристике и распрострањеност, Интердисциплинарни научни часопис Војно дело, бр.3, 2017, стр. 100.
[8]С. Петровић, 2000. оп.цит., стр. 118-119.

У том смислу у области компјутерског криминалитета, можемо издвојити типичне облике крађе и направити класификацију у зависности од објекта који се овим делом присваја:

- крађа рачунара и рачунарских компоненти (персоналних рачунара, монитора, штампача, дискова, меморијских чипова, процесора...),
- крађа података,
- крађа лозинки, кодова, идентификационих бројева ...[9]

Најопаснојом врстом компјутерске крађе, сматра се крађа идентитета, услед чега на овај начин углавном долази до задирања и продирања у индивидуалну приватност и интегритет комерцијалних трансакција. На овај начин се купују разне ствари, добијају кредити од банака, набављају лажне исправе и сл. Експанзијом електронске трговине, процењује се да ће доћи до повећања ове врсте крађе. [10]

Како се у раду разматра компјутерска крађа као посебан облик компјутерског криминалитета, посебну пажњу ћемо посветити крађи идентитета, као најопаснијом врстом компјутерске крађе, а затим се осврнути и на остале појавне облике компјутерске крађе.

1. КРАЂА ИДЕНТИТЕТА

Иако постоје различите дефиниције крађе идентитета као облика компјутерске крађе, сви битни елементи обухваћени су следећим одређењем - „Крађа идентитета (identity theft) је форма криминала у којој неко користи туђи идентитет да би извршио криминалну радњу.[11] То је посебан облик компјутерске крађе који обједињава нелегално прибављање поверљивих личних података за једно или више лица и њихово коришћење за извршење нових кривичних дела. Нелегално прибављање података о личности обавља се без знања особе која је жртва, а притом се присваја њено име и други лични подаци.[12]

[9]Ibid, стр. 119.
[10]Д. Димовски, Компјутерски криминал – Зборник радова Правног факултета у Нишу, Правни факултер, Центар за публикације, 2010.годин , стр. 205.
[11] С. Петровић, Компјутерски криминал, Војноиздавачи завод, Београд, 2004, стр.133.
[12] А.Ђукић, оп.цит., стр. 101.

Крађа идентитета се састоји у неовлашћеном коришћењу личних података који су постали јавно доступни, а који се односе на датум рођења, број телефона, тренутно пребивалиште, занимање, пријатељи, личне фотографије. Реч је о злоупотреби личних података који се налазе у виртуелном простору. У случајевима крађе идентитета на интернету, од корисника рачунара, путем лажних порука електронске поште или разноразних веб сајтова, сазнају се лични и финансијски подаци. Приликом крађе идентитета неко лице лажно се представља као друго лице у намери прибављања противправне имовинске користи или друге личне користи. Крађа идентитета почиње са присвајањем личних података о неком лицу, које се врши без знања и пристанка тог лица, путем обмањивања, крађе или преваре, а наставља се употребом прикупљених података за извршење кривичних дела која су у највећем броју случајева везана за стицање противправне имовинске користи лицима која злоупотребљавају украдени идентитет.[13]

Под општим појмом крађе идентитета могу се подразумевати различити модели и појавни облици крађе података о личности и велики број метода и поступака њихове употребе при извршењу нових криминалних радњи, различити профили жртава, садржаји и вредности штете које се наносе жртвама и друге специфичности. Крађа података обично има свој крајњи циљ, који се постиже извршењем новог кривичног дела, чије последице могу да буду материјалне и нематеријалне природе. Крајњи циљеви поред финансијских и политичких, могу да буду уцене, тероризам и сл. Зато се крађа идентитета може посматрати у ужем и ширем смислу[14]:

- у ужем смислу то је нелегалан поступак прибављања података о једној или више личности,
- у ширем смислу, поред прибављања података о личностима, крађа идентитета обухвата њихову употребу или продају на црном тржишту, уступање другим лицима и даље коришћење за извршење других криминалних радњи.[15]

Појмом крађе идентитета бавиле су се и најутицајније међународне организације, које су покушавале да је кроз своје стратешке документе дефинишу и регулишу. Крађа

[13] В.Николић – Ристановић, Др С. Костантиновић – Вулић.оп,цит., стр.112-113.
[14] А.Ђукић, оп.цит., стр. 101.
[15] Cifas, ,,Identity Fraud", https://www.cifas.org.uk/identity_fraud

идентитета је на 12. Конгресу УН у вези с превенцијом криминала и кривичног правосуђа, а који је одржан 2010.године, дефинисана као злоупотреба личних података другог лица, са намером вршења преваре. ОЕБС је установио да постоји крађа идентитета када једно лице прибавља, пребацује, поседује или користи личне податке физичког или правног лица на недозвољен начин, у намери да изврши превару или почини неко друго кривично дело. Извршиоци користе различите методе, како би нечији идентитет преузели и прибавили податке о тој особи. Неке од метода које се користе јесу следеће: слање електронских порука чија садржина обмањује жртву, активирање вируса и других злонамерних програма, упућивање на интернет сајтове са лажном садржином, који су осмишљени за обмањивање корисника, са намером да на истом оставе своје личне податке и сл. Када се на неки од наведених начина дође до примене нечијих личних података, такви подаци се злоупотребљавају на различите начине, од којих су најчешћи отварање лажних рачуна, злоупотреба постојећих банковних рачуна, бесправно коришћење одређених државних сервиса, служби и докумената, преваре у вези здравственог осигурања и сл. Савет Европе је 2007.године припремио платформу за израду јединствене, универзалне легислативе која се односи на крађу идентитета, а која је дефинисана као „крађа или преузимање постојећег идентитета (идентификационих обележја лица или значајног дела истих) са или без пристанка лица чија су и без обзира да ли је власник жив или је преминуо". [16]

Код крађе идентитета издвајају се три облика кроз које се манифестује: најважнији јесте modus operandi, односно начин извршења дела, затим мета напада и мотивација извршиоца дела. Најчешћи начини извршења дела у конкретном случају јесу, коришћење интернет претраживача и система за дељење датотека, напади хакера као и напади методама социјалног инжењеринга. Мета напада су подаци о идентификационим бројевима (нпр. јмбг, ЛБО број и сл.), бр. личних докумената (бр. личне карте, пасоша, кредитне или платне картице), корисничка имена и шифре на различитим интернет налозима. Мотивација за извршење дела је различита, али не и мање важна: она је најчешће усмерена ка стицању материјалне добити, прикривање нечијег правог идентитета или као припремна радња за извршење неког другог кривичног дела. [17]

[16]В.Николић – Ристановић, Др С. Костантиновић – Вулић.оп,цит., стр.114-115.
[17] Ibid.

Идентитет се краде коришћењем туђе личне карте, возачке дозволе, јмбг или сличних персоналних података којима се може извршити кривично дело на штету или у име жртве. То ствара и додатне проблеме за жртву, јер може да јој наруши углед, чак и онда када је учинилац ухваћен, а и у отклањању последица жртва троши много времена и новца. Ова крађа може се обавити крађом новчаника или торбице са документима, коришћењем техничких средстава за појединачне крађе идентитета, али и крађом података са рачунара или мобилних уређаја, са и без коришћења мрежног окружења.[18]

Појавни облици крађе идентитета, посматрани у ужем смислу и према локацији смештаја информација о личности и коришћењем средствима и техникама за њихово нелегално прибављање могу се разврстати на три широке групе:

- крађа идентитета класичним методама изван информационог и комуникационог система,
- крађа идентитета са личних рачунара и мобилних уређаја у мрежном окружењу,
- крађа идентитета из информационих и комуникационих система.[19]

У конкретном случају ћемо се више позабавити крађом идентитета са личних рачунара и мобилних уређаја у мрежном окружењу и крађом идентитета из информационих и комуникационих система.

С обзиром на велике разлике међу државама у степену економског развоја и различитости у културним, образовним и другим областима живота, коришћење мрежа и интернета је веома разнолико. Тако нпр. у Шведској, Холандији и Данској, интернет сваког дана користи око 90% испитаника, док у Румунији, Португалу, Грчкој и Бугарској, интернет користи повремено око 55% испитаника, а остали испитаници никад нису приступили интернету. На нивоу свих држава ЕУ интернет користи око 76% испитаника (од тога 63% сваког дана), док 24% испитаника никад није користило или нема приступ интернету. [20]

[18] А. Ђукић, оп.цит., стр. 101.
[19] Ibid, стр. 102.
[20] Ibid, стр. 103.

Графикон 1. Учесталост коришћења интернета у земљама ЕУ

Употреба компјутера и интернета у Србији је такође у сталном порасту, како на нивоу појединаца, тако и на нивоу државе. Од укупног броја корисника, интернет сваког или скоро сваког дана користи преко 3.070.000 лица (85% популације), а најчешће се читају онлајн новине, часописи (77,4%), траже информације о роби и услугама (71,3%) и учешће у друштвеним мрежама (75,6% популације), за разлику од 2015. године, где је интернет био коришћен углавном за приступ друштвеним мрежама, данас преко 1.510.000 грађана (око 42% интернет популације) користи интернет за приступ органима јавне управе, преко 1.450.000 лица (38% интернет популације), куповало је робу/услуге путем интернета у последњих годину дана, а интернет банкарство користи око 20% интернет популације или 760.000 грађана Србије.[21]

[21]Ibid, стр. 104.

Графикон 2. Намена коришћења интернета у Србији данас

На основу ових резултата може се закључити да се велики број појединаца који користе интернет понаша веома неопрезно или боље речено, неодговорно. У последњих пар година, већина је путем интернета учинила доступним личне податке (име, датум рођења, подаци из личне карте и др., (чак 56% интернет популације).[22]

Интернет као глобална мрежа пружа много погодности, али су зато и сви учесници и актери у том систему уједно и потенцијалне мете напада ради крађе личних података, новца са рачуна или пословних информација.

За крађу идентитета са личних рачунара који су у систему интернета, развијен је велики број метода и њихово прецизно раздвајање практично је немогуће, али се могу издвојити два основна:

1) фишинг (phishing) са подврстама вишинг (vishing) и смишинг (smishing) и

[22]РЗС Употреба информационокомуникационих технологија у Србији, (2016), 12-19. http://webrzs.stat.gov.rs/WebSite/respository/documents/00/02/25/89ICT2016s.pdf

2) примена малвера (malwer) са подврстом фарминг (pharming).[23]

Због опасности и могућих штета, као и начина и методе поступања криминалаца, посебно се мора размотрити примена фамилије малциозног софтвера под називом ransomver (ransomwaer), при чему се злонамерни софтвер инсталира на рачунар жртве, а његовим активирањем се онемогућава нормалан рад рачунара, а жртва се уцењује да откупи шифру којом ће елиминисати негативан утицај инсталираног малвера. Овакав поступак је делотворнији уколико се примењује на велике информационе и комуникационе системе ради уцене.[24]

Сваки од ових начина (метода) има своје препознатљиве карактеристике, али им је заједнички циљ – присвајање туђег новца или испољавање другог негативног утицаја на жртву (уцена, компромитовање и др.)

Фишинг (пецање) јесте појам који се односи на преваре ради добијања података од лица коме су ти подаци познати. При чему се обично користи фактор хитности на који жртва треба да реагује, а први корак је слање е-поште као мамца. Типична фишинг порука изгледа као да је послата од неке важне институције (банке, поште, трговинске компаније, пензионог фонда итд.). Фишинг је метод који шаље једну поруку хиљадама прималаца, од којих ће већина активирати поруку, а многи и дати тражене податке.[25]

Вишинг и смишинг су верзије технике пецања, где се уместо е-поште користе технике социјалног инжењеринга (манипулације), код вишинга и мобилни телефон или текстуалне поруке код смишинга, али са истом опасношћу и истим последицама као и код фишинга.[26]

Малвери (малциозни софтвер) који се примењује у фази прикупљања и злоупотребе података, поред фишинга, најраспрострањенију су начин крађе идентитета. Малвери или злонамерни софтвери су програми који су убачени у рачунар жртве без њеног знања са циљем да ометају рад рачунара или прикупљају тражене податке. Према начину рада

[23] А. Ђукић, оп.цит., стр. 105.
[24] Ibid.
[25] „Sajber hronika", Informacija, 16.06.2016. http://www.informacija.rs/Sajber-hronika/Kralj-spama-koji-kompromitovao-pola-miliona-Facebook-naloga-osudjen-na-2-5-godina-zatvora.html:
[26] А. Ђукић, оп.цит., стр. 106.

злонамерног софтвера, то могу бити: вируси, тројанци, шпијунски софтвер, фарминг и друге врсте, које се међусобно преплићу и не искључују, а заједничко им је да нанесу штету жртви.[27]

За недозвољену финансијску трансакцију и превару, коришћењем малвера, процес се може приказати у три корака:

- ***Зараза рачунара жртве –*** Дистрибуција малциозног софтвера на рачунар жртве може се обавити лажираном и од стране жртве прихватљивом е-поруком, оглашавањем, коришћењем безбедносне рањивости у претраживачима или другом корисничком софтверу и слично, где се учитава код који води до малвера.[28]
- ***Прикупљање података битних за новчану трансакцију (креденцијала – коросничка имена и лозинке)*** обавља се: снимањем екрана или тастатуре, праћењем куцања на тастатури, праћење времена пријављивања према банци, преусмеравањем интернет претраживача крајњем кориснику на злонамерни рачунар или већ страницу, коришћењем алата за даљински приступ и др.[29]
- ***Извршење неовлашћене трансакције*** - Ако преварант поседује креденцијале жртве, он може обавити трансфер новца на било који рачун, а ако их не поседује може применити аутоматизовани малвер који ће и новац током трансакције између крајњег корисника и финансијске институције преусмерити на другу локацију. Један од поступака познат је као фарминг где се легитимни веб сајтови преусмеравају на нове локације. Не користе се преваре да корисник сам да властите податке, већ злонамерни код који се инсталира на рачунар жртве или на сервер у рачунарском систему. Инсталирани код преусмерава информације које се се шаљу преко мреже са праве на лажну адресу, без пристанка и знања корисника. На овај начин наноси се штета жртви електронског банкарства и плаћања рачуна, па се новац преусмерава на банковне рачуне који служе за крађу новца.[30]

[27] Ibid.
[28] Ibid.
[29] Ibid.
[30] Ibid.

Крађа новца од банке и њених клијената коришћењем украденог идентитета корисника интернета, такође је учестала појава и има следећи сценарио у пет корака:

1. Проналажење већег броја корисника интернета који плаћају рачуне преко интернета, за шта се користе лако доступне е-адресе и добро осмишљене е-поруке, чијим отварањем се инсталира злонамерни софтвер и осигурава приступ рачунару жртве.[31]
2. Куповина специјализованог софтвера (exploit kits) на црном тржишту, потребног ради инсталирања специјалних банкарских тројанаца у рачунар жртве. Овакав софтвер се стално развија и усавршава и на црном тржишту му је цена од неколико стотина до преко хиљаду долара.[32]
3. Инсталирање софтвера са банкарским тројанцима у рачунар жртве посредством мреже и раније инсталираног злонамерног софтвера.[33]
4. Када се рачунар жртве, који је под контролом криминалаца, користи за електронско банкарство, а криминалци нису познати креденцијали жртве, подаци које шаље жртва усмеравају се на лажни сервер – техника напада са рачунаром посредником или методом ,,човек у средини" (man in the middle – MITM). Док је корисник уверен да је платио рачун, новац је преусмерен и укњижен на неком рачуну који је отворен за крађу или што је чешћи случај новац се упућује на већ постојеће легалне рачуне уз пристанак и за провизију власника рачуна (money mules – муле за пренос новца). Власници рачуна за пренос новца регрутују се посредством интернета ради обављања послова са примамљивим називима радних места, као што су ,,финансијски менаџер" или ,,менаџер за пренос новца", а послове обављају радећи код куће за уговорени хонорар.[34]

[31] Ibid, стр. 107.
[32] ,,Моćни hakerski alati-exploit kits", Informacija, 14.02.2011.
http://www.informacija.rs/Virus/Mocni-hakerski-alati-exploit-kits.html
[33] А. Ђукић, оп.цит., стр. 107.
[34] Europol, ,,Europe-wide ation targets monez mule schemes", Eurojust Web, 01.03.2016.
http:/www.eurojust.europa.eu/press/pressreleases/pages/2016-03-01.aspx:
Prema objavi Europola od 01.03.2016. u vremenu od 22 do 26.02.2016. Europol, pravosudni i drugi organi više država EU, ali i nečlanica (Moldavija i druge), udružilo je snage u akciji protiv ,,novčanih mula", a kao rezultat operacije bilo je identifikovanje skoro 700 lica ta prenos novca, uhapšeno 81 lice, a otkriveni su i sprečeni značajni finansijski gubici i otkriveni preko 900 žrtava nedozvoljenih transakcija.

Ова лица обично не знају порекло новца и уверена су да раде легалан посао и за легалну фирму, а у ствари су саучесници у извршењу кривичног дела.[35]

Са свог легалног рачуна уз минималну надокнаду „финансијски менаџер" брзо пребацује новац на рачуне лопова, чиме је дело и окончано.[36]

Без обзира на начин на који је неовлашћено приступљено рачунару крајњег корисника, хакерисање е-поште сматра се за један од најефикаснијих пролаза у рачунарски простор корисника интернета и омогућава веома разноврсне нападе. Када се злонамерна порука испоручи рањивом рачунару, тада је испоручен и злонамерни код, а он може да на рачунару прикривено инсталира тројанце (злонамерни софтвер), да усади црве (софтвер који умножава сам себе, преноси се кроз мрежу и преузима контролу над функцијама рачунара), да злоупотреби целокупни систем или да покрене прилоге е-поште, што значи да може све.[37]

Информационо-комункациони систем јесте организациона структура, која је организована на начин да обухвата: комуникационе мреже, електронске уређаје или групе међусобно повезаних уређаја, а све у циљу аутоматске обраде података коришћењем рачунарских програма, података који се обрађују, претражују или преносе помоћу уређаја и мрежа.[38]

Неовлашћено прикупљање података из базе податаке (или збирки података) представља насилни упад у рачунарски систем, где у том случају нису угрожени само подаци о личности, већ и целокупно пословање рачунарског система. Овај поступак је истоветан са насилним упадом у туђе објекте, а познат је под појмом хакерисање или хакинг (hacking – човеков ум против рачунара), иако сам појам може означити и позитивне поступке, како би се рачунар искористио на најбољи начин.[39]

---

[35]Cifras, „Money Mules" more likely to be aged under 30", 08.12.2016. https://www.cifas.org.uk/press_centre/monez-mules: U prvih devet meseci 2016. U V. Britaniji je 73.503 individualnih bankovnih računa korišćeno za nelegalne transakcije novca, 39,4% imalaca legalnih računa su mlađi od 31 godine, dok su imaoci računa u dobi od 31 do 50 godina, zastupljeni sa 3%.

[36] А. Ђукић, оп.цит., стр. 108.

[37] S. Meklur, Dz. Šambri, Dz. Kurtc, Хакерске тајне: заштита мрежних система, превод Д. Смиљанић, М. Шуњур, Београд, 2006, стр. 558.

[38] А. Ђукић, оп.цит., стр. 109.

[39] Ibid, стр. 109.

Ако се жели груба подела начина крађе туђих података из информационо-комуникационог система, што хакинг као метод и јесте, разликују се два основа облика реализације овог дела.[40]

- Прибављање потребних информација за упад у туђи рачунарски систем (садржаји база података, интернет адресе, телефонски бројеви, параметри за идентификацију и сл.). Начин и методе прибављања информација су веома различити, а користе се за претраживање електронске и друге поште, новина и других публикација, прислушкивање, испитивање методе социјалног инжењеринга, подмићивање, крађе и сл. За добијање потребних информација неретко се користе запослени у рачунарским центрима, који својом непажњом, незнањем или са намером, доприносе лакшем упаду нападача у систем. На основу познатих информација упад у туђи рачунарски систем је знатно олакшан, а поступак безбеднији по нападача.[41]
- Тежи начин, али никако мање опасан, захтева велико стручно знање, стрпљив и дуготрајан рад нападача, као и квалитетнију опрему и софтвер. Метод се заснива на постепеном приступу систему преко софтверских баријера и других система заштите по принципу „покушај, погреши, нађи и отклони грешку и поново покушај".[42]

Када се једном нађе у систему, нападач може додатно да користи слабости система и оствари привилеговани приступ до свих потребних података и датотека. Карактеристике хакинга су да је то добро планиран, недозвољен и насилан приступ, да је базиран на високом професионланом знању нападача и да је притом нападач по правилу, безбедно удаљен од места упада у рачунарски систем. Крађа података личности на овај начин има за последицу много украдених података који се могу користити за разна кривична дела и нанети физичким лицима и привредним друштвима велике штете.[43]

[40] С. Петровић, 2004, оп.цит., стр. 196-197.
[41] А. Ђукић, оп.цит., стр. 109.
[42] Ibid.
[43] „Najveća krađa u istoriji" – Telegraf, 06.08.2014
.http://www.telegraf.rs/hi-tech/internet/1181038-najveca-kradja-podataka;

Због наведених могућности и евидентних претњи, откривених крађа идентитета и на основу њих реализованих разних превара, првенствено банкарских, 2/3 корисника интернета у ЕУ изражава забринутост за личне податке који се чувају код државних органа. Више од половине грађана ЕУ забринуто је за своје банкарске картице и могућности да буду жртве крађа и превара. То се поткрепљује податком да је током 2004.године, у земљама ЕУ забележен нагли пораст броја покушаја инсталирања злонамерних софтвера или приступа рачунару посредством е-поште или телефона и то на 47% активних рачунара.[44]

Напади на личне рачунаре, где су као облици најзаступљенији малвери (тројанци, црви), спам и фишинг напади, показују тенденцију повећања, како по броју напада, тако и по нарастању броја различитих злонамерних софтвера који се примењују. У току 2015. године, према извештају лабораторије Касперски откривено је 2.961.727 штетних инсталационих пакета малвера, 884.774 нових злонамерних мобилних програма (троструко повећање у односу на 2014.) и 7.030 мобилних балканских тројанаца.[45]

Број нових малвера стално расте, тако да је у периоду од 2003. до 2013.године, откривено око 200.000, 2014.године, око 300.000, а 2015.године, око 900.000, новог малициозног кода.

Карактеристике нових малвера су такве да крајњи корнисник није у стању да их елиминише, извршиоци користе разне методе за њихово скривање, а у употреби су малвери који криминалцима дају потпуну контролу над зараженим рачунаром.[46]

Током 2015.године, у свету је регистровано око 147 милинона фишинг напада (напада на који су се активирали антифишинг системи, па се може претпоставити да их је било знатно више). Од тог броја највише напада претрпеле су Русија (17,8%) и САД (15,2%). Према циљу, фишинг напади су највише били усмерени на онлајн финансијске институције (банке, системи плаћања и онлајн продавнице).[47]

---

[44] European Commision, Ciber security report 2014;
Употреба информационо-комунникационих технологија у РС, 2014, стр.19.
http://webzs.stat.gov.rs/WebSite/repository/documents/00/01/50/47/ICT2014s.pdf
[45]A. Ivanov i dr., Overall statistics for 2015., u Kaspersky Security Bulletin 2015. (Securelist,15.12.2015.), https://securelist.com/files/2015/12/KSB_2015_statistics_FINAL_EN.pdf
[46] А. Ђукић, оп.цит., стр. 110.
[47] Ibid.

На повећани обим угрожености података о личности указују и следећи подаци из 2015. године:

- регистровано је 1.966.324 обавештења о покушајима инфекција личних рачунара, злонамерним софтвером ради крађе новца, преко онлајн приступа банковним рачунима,

- на 753.684 личних рачунара откривен је ransomver, а 179.209 рачунара је било мета шифровања овим софтвером,

- 34,2 % корисника рачунара је било током године изложено најмање једном веб нападу,

- за нападе је коришћено 6.563.145 различитих рачунара.[48]

На светском нивоу током 2015. године, откривено је 1.505 упада у базе података, што је за око 8% више, него претходне 2014.године.[49] Нападе су у великом броју организовали актуелни или бивши запослени у фирми (око 65% свих напада).

Процена је да су током 2015. године, били угрожени подаци за око милијарду људи, а само у 21-ом нападу („мега напади'") било је угрожено 814, 5 милиона података о личности, поред којих се као веома успешни напади могу сврстати и 55 напада, који су, сваки појединачно, угорзили преко милион података о личности. Као последица спољних хакерских напада, компромитовано је око 2/3 од укупног броја компромитованих података, али је велики број података, неконтролисно „исцурио" због немара или намере запослених.[50]

Ако се разматрају путеви којима се неовлашћено приступа подацима о личностима или другим вредним информацијама, највећи број напада на базе података изведен је хакерским нападима посредством интернета (46%), затим преко крађе докумената (14%), губитка због немара или намерно (8%), посредством е-порука (7%), итд. По областима рада најугроженије су компаније које се баве високом технологијом (29%), образовне установе (20%), а затим здравство, банкарски сектор, трговином и саобраћај.[51]

---

[48] A. Ivanov i dr, оп.цит.

[49] Infowatch, „global data leakage report 2015.", 2016.
http://infowatch.com/report2015.
InfoWatch je firma „Kaskerski Lab" sa sedištem u Rusiji i bavi se informacionom bezbednošću i zaštitom preduzeća.

[50] Ibid.
Oko 191 milion podataka o biračima sad dospelo je na internet zbog grešaka u bazi podataka.

[51] Blic, „Panamski papiri", 09.05.2016.
http://www.blic.rs/vesti/svet/panamski-papiri-dokumenti-na-internetu4-adrese-iz-srbije/ejht9e;

Спољним нападима највише су угрожене компаније које се баве виском технологијом, трговином и саобраћајем, а унутрашњим нападима највише су угрожени лични подаци у банкама, осигурању и здравству. Уопштено, државне институције су претрпеле око 17% од укупно 1.505 напада, пословне организације око 73%, а остале институције и организације, укључујући и међународне организације – око 10% напада. Карактеристике крађе података 2015.године, у свету је да је највећи број података отуђен у релативно малом броју напада (у 55 великих и 21 мега напада), где је компромитовано близу милијарду личних података. Најновији подаци показују да се једним хакерским нападом могу присвојити и подаци о знатно већем броју лица, па чак и преко милијарду корисничких налога. [52]

Према броју напада којима су биле изложене базе података на територијама држава, предњаче САД са 859 напада, затим Русија (118), В. Британија (112), Канада (38), Немачка (38), Аусралија (27), а следе их Јапан, Индија, Јужна Кореја и Аустрија.[53]

2. КРАЂА РАЧУНАРА И РАЧУНАРСКИХ КОМПОНЕНТИ
(персоналних рачунара, монитора, штампача, дискова, дискета, меморијских чипова, процесора и др.)

Крађа компјутерске опреме, постаје за компјутерску индустрију претња која сваке године односи више милијарди долара, због чега ову појаву многи сматрају епидемијом. При чему се процењује да ће се овај проблем драстично повећати у будућности, јер су људи свесни вредности компјутера и његових компоненти, а с обзиром на њихов напредак и вредност, временом су постали најновије трајно потрошачко добро, које је циљ лопова. Раније су то били колор телевизори, затим видео рекордери, па радио за кола, а сада су то компјутери. Уз то прилике су веће, па су и искушења већа.[54]

Овај облик крађе је у порасту посебно што су меморијске картице, дискови, микропроцесори, флеш меморије, лаки за крађу, (за њихово изузимање из компјутера

[52] Blic, „Najveci hakerski napad u istoriji", 15.12.2016. http://www.blic.rs/vesti/svet/najveci-hakerski-napad-u-istoriji-hakovani-podaci-vise-od-milijardu-korisnika-jahua/ohixjej7:
kompanija yahoo, objavila je avgusta 2013. Godine da je hakovano vise od milijardu naloga korisnika te kompanije. Ukradeni su korisnički podaci koji sadrže imena i mail adrese, brojeve telefona, datume rodjenja, bezbedonosna pitanja i odgovore, koji se koriste za potvrdu identiteta naloga. Ovo hakovanje otkriveno je posle 3,5 godina,
[53] InfoWatch, „Global data leakage report 2015", 2016., http://infowatch.com/report2015,
[54] С. Петровић, 2000., оп.цит., стр. 119.

потребно је пар минута), лако се транспортују, јер су мали и непроналажљиви, а веома су вредни и слободно се могу продавати на отвореном тржишту.[55]

Потражња за њима је рапидно растућа, нарочито захваљујући све снажнијим перформансама персоналних рачунара, у првом реду процесора и меморијских модула. Што се тиче процесора, њихова снага и брзина никада нису довољни, па ће крађа компонената наставити и даље да храни и значајно проширује црно тржиште овом врстом робе.[56]

Постоје извештаји да многе компјутеризоване компаније верују да су њихови персонални рачунари снабдевени са довољно меморије. Међутим, након обављене ПС контроле установљено је да се из многих машина систематичнно уклоњене меморијске картице и капацитет меморије преполовљен. Корисници нису приметили недостатак меморије, али је већина осетила да мрежа функционише споро. Много меморије је украдено од стране особља које је тиме побољшало перформансе својих кућних рачунара или су је препродали на улици.[57]

Слична ситуација је и са процесорима, свака нова верзија било ког софтвера, у чему опет предњачи Microsoft Windows, испоставља захтеве за знатно снажнијим процесорима, од оних који су могли радити са претходном верзијом тог софтвера. Како је фреквенција појављивања нових софтвера и нових верзија старих софтвера прилично висока, драматично се увећава потреба за све снажнијим процесорима.

Murphy J. је истакао још 1995. године, да је тада улична вредност Pentium процесора била четири пута већа од вредности дроге или хероина, те да ако се украде један Pentium процесор, може се остварити приход од 30 до 40 хиљаде доларе годишње. С тим у вези, уместо да краду велике компјутере, криминалци су схватили да могу само да га отворе и извуку процесор и меморијске картице, вредни више стотина долара, који се могу продавати отворено, користећи огласе у средствима јавних информисања, јер поседовање и продаја компјутерских компоненти није инкриминисано као кривично дело.[58]

[55] Ibid.
[56] Ibid.
[57] J. Murphy, RAM RAIDERS, Computer Weekly, June, 1995, str. 2.
[58] Ibid.

Посебно индикативна је чињеница на коју указују полицијски извори, да су силиконски чипови били монета у трговини дрогом.[59]

Наиме, уочено је да је својевремено, међународна акција рестрикције циркулисања кеша, усмерила картеле дроге да прихвате да се за дрогу може плаћати и микрочиповима, јер се они могу отворено преностити по целом свету, а потражња за њима значи да се они могу лакше конвертовати у кеш, него чекови од 100 долара, јер су доларски чекови, за разлику од чипова носили серијске бројеве, на основу чега их је било далеко лакше пратити и контолисати.[60]

Јединица за високотехнолошки криминал у саставу FBI истраживала је крађу чипова у Сан Франциску, као и у Хјустону, Бостону, Фениксу и Лос Анђелесу. Иако није устаљена пракса неколико случајева крађе је ипак обелодањено. Dalas Semi Conductor INC у Тексасу, коришћењем прикривених надзорних камера, открио је да запослени краду чипове и продају их на црном тржишту.[61]

Крађа рачунара и рачунарских компоненти је актуелна још од 1993.године, када је у Вашингтону само вредност украдених чипова износила око 40 милиона долара, што је установила AMA (American Electronics Association), а силиконска долина у Калифорнији је била технички коридор у којем се највише крала висока технологија.[62]

Boyle Bill наводи да је Scotland Yard (полицијска служба) још 1995. године значајан део своје активности усмерио на крађу компјутера и његових компоненти у Великој Британији, а за ту сврху је формирана и посебна група под називом Joint Action Group. Задатак групе био је да промовише добру праксу заштите и укључи програм превенције од криминала, као и планове за хватање лопова. Група је иницирала да је крађа хардвера криминална активност која се најбрже увећава у Великој Британији, посебно као резултат недостатка чипова, високе цене микропроцесора и захтева за компјутерском меморијом, што потврђују и информација да су у Великој Британији још 1994.године осигуравајуће

[59] Ibid, стр. 32.
[60] С. Петровић, 2000, оп.цит., стр. 121.
[61] B. Violino., HIGH-TECH THIEVES, Information week, may 29.1995, стр. 529.
[62] Ibid, стр. 14.

фирме исплатиле више од 200 милиона фунти на име обештећења клијената због крађе компјутера.[63]

Intel, један од водећих светских произвођача компјутерских чипова, укључио се у борбу против ове врсте криминала још пре две деценије, штампајући серијске бројеве на чиповима, стварајући на тај начин услове за праћење производа, што омогућава и FBI-u спровођење „стинг" операције – операција убода (операција осмишљена да ухвати особу која је покушала да почини злочин). С друге стране осигуравајуће компаније покривају своје губитке настале крађом, али своје трошкове надокнађују повећањем премија, чиме врше притисак на целу индустрију, али и на кориснике да побољшају заштиту.[64]

Крађа рачунара и његових компоненти датира још из 90-их година, нарочито крађа чипова и процесора, што потврђују и подаци да су постојали гангови који су своју криминалну делатност усмеравали на крађу чипова и процесора, до те мере, да су напади приликом крађе били брутални, нарочито у силиконској долини у Калифорнији, да су приликом крађе, чланови гангова користили ватрено и хладно оружје, често наносећи лаке и/или тешке телесне повреде, које су неретко као последицу имале смртни исход. Тако је полиција још 1994. године, спречила напад ганга који је планирао да нападне и убије возача камона, који је транспортовао чипове, а затим украде камион са компјутерским чиповима. У Италији су припадници ганга коришћењем кратежа и аутоматског оружја, претукли чувара у једној малој фабрици персоналних рачунара, и украли чипове у вредности од 2.3 милиона фунти.[65]

Из једне фабрике у В. Британији украдени су компјутерски чипови у вредности од 3.5 милиона долара. Из једне новинске агенције украдена је компјутерска опрема у вредности од 308.000 долара, а једна наоружана група, користећи сузавац и скраћене сачмаре, украла је из једне фабрике у јужном делу Лондона компјутерску опрему, у вредности од 230.000 долара.[66]

[63] Ibid, стр.529.
[64] С. Петровић, 2000, оп.цит., стр. 123.
[65] J. Murphy, оп.цит., стр. 32.
[66] С. Петровић, 2000, оп.цит., стр. 124.

Интересантан је податак да је у нашој земљи, 2015. године, из зграде Народне скупштине, украдено чак 20 компјутера, што су органи власти открили сасвим случајно у току ванредног пописа.[67] Олакшавајућа околност је што је реч о рачунарима који још увек нису били у употреби, с обзиром да су украдени из магацина, те се у њима нису налазили никакви важни подаци, који би могли да нанесу штету како држави, тако и њеним грађанима.

3. КРАЂА ПОДАТАКА

Крађа података постала је веома актуелна са развојем информационо-комуникационих технологија, што је узроковало да се тим и таквим подацима тргује на црном тржишту, а подаци којима се највише тргује јесу они који се односне на ,,пословне тајне". Како је развој технологије проширио могућности и отворио нове путеве трговцима ,,црним подацима" (како се још називају на црном тржишту) на интернету су се развили сервиси система електронских огласних табли, а које су намењене за незакониту продају и трампу података. Овакви сервиси су у функцији, не више од 3 месеца, након чега се ,,гасе", односно мења се интернет адреса, као и сви подаци који се тичу њих, што умањује могућност њиховог откривања.[68]

Такође, у великој мери користе се и интернетови сервиси за дискусионе групе (USENET), као и предности технологије заштите интернета, укључујући бесплатне криптолошке алгоритме са јавним кључевима и анонимне remailer програме, што омогућава сигурно прикривање продаје или трговине украденим подацима широм света. Ништа се не преноси у отвореном облику, а стране које комуницирају ни не знају ко је ко. Представници федералних истражних органа САД процењују да лопови годишње украду податке вредне више од 10 милијарди долара и при томе, они признају да до сада воде изгубљену битку.[69]

Оно што виртуелни простор на интернету издаваја јесте анонимност која олакшава продају нелегално добијених информација, чак и ако је извршилац крађе неко ко не поседује стручно знање из ове области. Анонимност је кључна у овом случају, јер ако је неко сигуран

[67] https://www.kurir.rs/vesti/politika/1689006/skupstina-puna-lopova-ukrali-20-kompjutera-i-televizor
[68] Ibid, стр. 124-125.
[69] Ibid, стр. 125.

да ће остати анониман, он ће се пре осмелити на крађу података, јер је пракса показала да је веома тешко доћи до извршиоца у конкретним случајевима.

Крађа пословних тајни, наравно није нова, али интернет и други онлајн сервиси дају информационим торбарима да купе, продаје или трампе податке. Зато у времену у коме информација постаје кључ пословног успеха, заштита података, посебно пословних тајни, неспорно је да је веома значајна.

Друга велика претња долази од растућег броја информационих брокера, који користе онлајн комуникације да би посредовали између купаца и продаваца на црном тржишту података. Многи од њих су бивши припадници тајних служби, који тесно сарађују са хакерима у илегалној трговини подацима.[70]

У једном случају, агенти бивше Источне Немачке украли су податке о пословним активностима 3.000 западноамеричких фирми. Метод је био веома једноставан. Подаци су били смештени онлајн на time-sharing раунару фирме, која је изнајмљивала рачунарске услуге. Агенти су отворили рачун код ове компаније под именом измишљене фирме. Уз мало експериментисања и неколико добро промишљених питања постављених службеницима, агенти су били у могућности да приступе жељеним подацима.[71]

4. КРАЂА ЛОЗИНКИ, КОДОВА И ИДЕНТИФИКАЦИОНИХ БРОЈЕВА

Крађу лозинки, кодова и идентификационих бројева можемо у конкретној ситуацији упоредити са крађом кључева, јер су лозинке, кодови и идентификациони бројеви тзв. логички кључеви који омогућавају улазак у „забрањене зоне" у којима је могуће извршити неку илегалну активност.[72]

Ова врста компјутерске крађе детаљније је образложена кроз део текста који се тиче крађе идентитета, као појавног облика компјутерске крађе, јер у погледу начина на који се иста испољава, кад су у питању лозинке и кодови, метода који се примењују, као и мотива и циљева за вршење овог облика компјутерске крађе, ситуација је идентична.

[70] C. Wilder, B. Violino, ONLINE THEFT, InformationWeek August 28, 1995, no. 542, str. 30.
[71] С. Петровић, 2000, оп.цит., стр. 126.
[72] Ibid.

II КАРАКТЕРИСТИКЕ ИЗВРШИОЦА КОМПЈУТЕРСКЕ КРАЂЕ

С обзиром на бројне мотиве извршења компјутерске крађе, као и појавних облика кроз које се компјутерска крађа испољава, не може се говорити о јединственом профилу извршиоца. Међутим, може се говорити о подели извршиоца у три групе:

1. Аматери, којима припадају извршиоци који иначе имају легално занимање, али ова категорија, није јединствена већ се у оквиру ње може говорити о трима категоријама:
   - Слаби и подложни појединци - делају у оквиру ове области зато што је систем контроле слаб, знају да је вероватноћа за њихово откривање веома мала, те не воде рачуна о последицама, у супротном, тешко да би предузимали било какве радње које могу да се доведу у везу са компјутерском крађом,
   - Фрустрирани појединци – најчешће је реч о извршиоцима, који су изреволтирани поступцима људи из њихове околине, те дају себи за право да се свете и "преваспитавју", тиме што врше компјутерске крађе,
   - Људи са пороком - на овакве извршиоце утичу социопатолошке појаве, као што су алкохолизам, коцкање и наркоманија, које утичу на одређене појединце да се одају вршењу кривичних дела из ове области.[73]
2. Професионални криминалци – реч је о извршиоцима, којима је бављење криминалом редовна активност, која може да се подведе под њихово „занимање". Развојем информационих технологија, проширили су се и могућности њиховог деловања, односно како технологија напредује, њима је све лакше и једноставније да пробијају системе заштите и делају. Професионални криминалци се према степену организације могу поделити на:
   - Индивидуалне криминалце – они врше компјутерске крађе самостално, а циљ им је у већини случајева стицање имовинске користи. Њихово криминално понашање је локалног карактера, а криминални потенцијал мали, али за њихове потребе задовољавајући,

[73] Д. Димовски, оп.цит., стр. 208.

- Организоване групе – јесу групе, које чини неколико чланова са заједничким интересима, који су углавном материјални и појединачни. Последице њиховог деловања су такође локалног карактера, али се у погледу потенцијала истичу у односу на индивидуалце,
- Криминалне организације – су највиши организациони облик криминалаца, односно организација, која се издваја у погледу своје структуре, где је дисциплина и хијерархија оно што их одликује, веома су међусобно одани и лојани једни другима, а углавном нису фокусирани само на једну криминалну област, већ поред компјутерске крађе, врше и дела из других области под окриљем криминала.[74]

3. Хакери – су лица, која уз помоћ свог рачунарског знања, упадају у туђе компјутерске системе, у случају компјутерске крађе, углавном ради крађе података. Одликује их жеља и потреба да улазе у компјутерске системе, уз помоћ свог знања. Реч је о особама, које су искључене из реалног живота и живе у неком свом свету, где им је једина сатисфакција контакт са рачунарима и продирање у туђе рачунаре и системе, ради прикупљања података у конкретном случају. Много је забележених случајева продирања у компјутерске системе влада различитих држава и међународних организација. Углавном се ради о професионалним програмерима или информатичарима, који су високо образовани, али неретко у оквиру ове групе можемо сврстати и оне који се хакерисањем баве из хобија, а знања из ове области су стекли, бавећи се компјутерима из чисте радозналости.[75]

Истраживања су показала да су углавном у 100% случајева хакери особе мушког пола, веома интелигентни и склони истраживачком и логичком размишљању и увек такмичарски расположени. Не поштују људе који не знају ништа о компјутерима и виде себе као ауторитете над компјутером.[76]

[74] С. Константиновић Вилић, В. Николић Ристановић, М. Костић, Криминологија, Пеликан принт, Ниш, 2009., стр. 14.
[75] Д. Димовски, оп.цит., стр. 209-210.
[76] Истраживање је спровео A. J Smit, Опширније видети: С. Петровић, стр. 274.

III КОМПЈУТЕРСКА КРАЂА У ПРАВНИМ ОКВИРИМА

Право споро реагује на развој нове технологије, те с изузетком телефона и писаће машине, технолошка револуција из прошлог века није много утицала на право. Право се бавило уопште технологијом стварајући нова правила у ваздушном саобраћају, у вези са генетским инжињерингом и сл.[77]

Међутим, постоји међународна и национална легислатива, која уређује област компјутерског криминалитета, али која је веома оскудна што се тиче појмовног дефинисања и одређивања компјутерске крађе, као једног од најчешћих појавних облика компјутерског криминалитета.

У наставку рада биће пружена листа оваквих прописа релевантних са аспекта заштите, остваривања права и подршке потенцијалним жртвама компјутерског криминалитета, уз посебан осврт на прописе који се баве овом материјом у оквиру националног законодавства.

1. МЕЂУНАРОДНИ АСПЕКТ КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА-КОМПЈУТЕРСКЕ КРАЂЕ

На међународном плану, неопходно је постићи сарадњу, како бисмо се проблему компјутерског криминалитета супротставили на адекватан начин. Како је компјутерски криминалитет област која завређује пажњу целе међународне заједнице, не само једне државе, дошло је до доношења међународних правила која регулишу ову област, те су временом потписане и ратификоване одређене конвенције.

Прва иницијатива за борбу портив високотехнолошког криминала покренута је од стране Операционог комитета америчког Сената у фебруару 1977. године, где се први пут предлаже развој легислативе која се тиче компјутерског криминала. [78]

Европска унија била је иницијатор за борбу против вискотехнолошког криминала на међународном нивоу. Период од 1998. до 2002.године, био је веома значајан за Европску

[77] П. Димитријевић, Право информационе технологије, InternetLaw, Sven, Ниш, 2011, стр. 54.
[78]М. Лепојевић –Ковачевић, Б, Лепојић, Међународни стандарди у супротстављању компјутерском криминалу и њихова примена у Србији, Зборник IKSI, 1-2/2007-Б, стр. 272.

унију, која је донела бројне документе у циљу формирања правног оквира за регулисање и заштиту од високотехнолошког криминала, безбеднијег сајбер простора као и успостављања боље међународне кооперације.[79]

Хронолошки посматрано, један од првих докумената који се односи на ову проблематику, за подручје Европе, донет је 17. маја 1991. године, а реч је од Директиви Савета Европске заједнице о правној заштити компјутерских програма, којом су државе чланице Европске заједнице биле обавезане на њену примену од 01. јануара 1993. године.[80] Директива је објављена у Службеном листу Европске заједнице бр. Л 122/42 од 17. маја 1991. године. [81]

Уједињене нације су на Осмом конгресу за спречавање криминала, одржаном у Хавани 1990.године, донеле посебну Резолуцују у којој је констатована потреба за инкриминисањем различитих злоупотреба. Иста је била од значаја државама чланицама за успостављање и реализацију мера у овој области. Ову резолуцију прихватила је Генерална скупштине УН.[82]

Такође, још 1985.године, ОЕБС је сугерисао државама чланицама да инкриминишу различите злоупотребе везане за уношење, мењање или брисање података или програма ради остваривања криминалних циљева. [83]

Као не мање важно, треба напоменути да је Савет Европе 1989. године, предузео иницијативу у погледу борбе против високотехнолошког криминала и донео Препоруку Р(89)9, којом се захтева од држава чланица да инкриминишу дела која се налазе на посебној тзв. „минималној листи". Препоруком је дата могућност државама чланицама да уведу у своја законодавства кривична дела са тзв. "опционе листе". [84]

Затим је донета Конвенција о високотехнолошком криминалу, потврђена 23. новембра 2001. године у Будимпешти, коју је Република Србија ратификовала 19. марта

[79] М. Лепојевић - Ковачевић, Б. Лепојевић, , оп.цит, стр. 272.
[80] С. Лутовац, Ј. Рачић – оп.цит. стр. 284.
[81]Директива Савета Европске заједнице о правној заштити компјутерских програма- објављена у Служебеном листу Европске заједнице бр. Л 122/42 од 17. маја 1991. године.
[82]Д.Димовски, оп.цит. стр. 198.
[83] Ibid.
[84] Ibid.

2009. године, коју ћемо детаљеније образложити у даљем тексту, с обзиром да је реч о најзначајнијем документу у области високотехнолошког криминала.

1.1. Међународна конвенција о високотехнолошком криминалу

Међународна конвенција о високотехнолошком криминалу јесте најзначајнији документ у овој области, који је донет од стране Савета Еворпе и носи назив Конвенција о високотехнолошком криминалу.[85]

Конвенција о високотехнолошком криминалу је једини и први мултилатерални уговор који регулише сарадњу у истрази и оптужењу у вези кривичних дела високотехнолошког криминала. [86]

У преамбули исте наглашено је да државе чланице Савета Европе, као и друге државе потписнице имају циљ спровођења заједничке политике у борби против овог глобалног проблема.[87] Наведена конвенција састоји се из четири дела/поглавља.

Прво поглавље конвенције односи се на дефинисање основних термина, као што су рачунарски систем, рачунарски податак, давалац услуге, податак о саобраћају.[88]

Друго поглавље говори о мерама које је потребно предузети на националном нивоу, у циљу доношења законске регулативе која ће покрити кривична дела из области компјутерског криминала. У овом делу су дефинисани облици компјутерског криминала које је потребно законски регулисати, а они се деле на четири групе дела.[89]

- дела против поверљивости, целовитости и доступности рачунарских података и система – њих чине незаконити приступ, пресретање, ометање система, ометање података, злоупотреба уређаја,
- дела у вези са рачунарима – код њих су фалсификовање и крађе најтипичнији облици напада,

[85]Ibid.
[86]Ibid, стр. 199.
[87]С. Лутовац , Ј. Рачић, оп.цит стр. 284.
[88] М. Ковачевић-Лепојевић, Б. Лепојевић, - оп.цит. стр. 276.
[89] Ibid.

- дела везана за садржаје – дечија порнографија је најчешћи садржај који се појављује у овој групи, обухватајући посредовање, дистрибуцију, трансмисију, чување или чињење доступним расположивим ових материјала, њихова производња ради дистрибуције и обрада у компјутерском систему,
- дела везана за кршење ауторских и сродних права, која обухватају репродуковање и дистрибуцију заштићених дела (законима о интелектуалној својини и ауторском праву) где се као средство извршења јављају компјутерски системи.[90]

У овом делу Конвенције, дата је препорука националним законодавствима да дефинишу одговарајуће процедуре у циљу адекватног кривичног поступка при процесуирању ових кривичних дела. Такође се тражи да се дефинишу надлежна тела на одређеним деловима своје територије, у чију ће надлежност бити процесуирање кривичних дела из области компјутерског криминала. [91]

Треће поглавље односи се на међународну сарадњу, где се поред општих принципа међународне сарадње у овој кривичној материји, дефинишу и принципи екстрадиције починилаца, генерални принципи међународне сарадње као и принципи међусобне сарадње у одсуству адекватних међународних уговора. У овом делу наглашена је обавеза државе потписнице да обезбеди одговарајуће тело доступно 24 часа, 7 дана у недељи, за контакт и сарадњу по питању компјутерског криминала са сличним телима у другим државама.[92]

Последњим, четвртим поглављем, одређене су завршне одредбе наведене конвенције, а које се тичу четири аспекта конвенције: датума отварања за потпис, начина ступања на снагу, потенцијалних земаља потписница и др.[93]

[90]Ibid, стр. 276.
[91]Ibid, стр. 277.
[92]Ibid.
[93]Ibid.

1.1.1. Допунски протокол уз Конвенцију о високотехнолошком криминалу

Допунски протокол уз конвенцију и високотехнолошком криминалу сачињен је 28. јануара 2003. године у Стразбуру и односи се на инкриминацију кривичних дела против расизма и ксенофобије извршених преко компјутерских система.[94]

Оснивањем Комитета стручњака за криминал у сајбер простору, Савет Европе био је иницијатор 1996. године, за усвајање ових докумената. Задатак поменутог Комитета била је анализа кривичних дела која се могу извршити путем телекомуникационих мрежа, првенствено Интернета, да би се на основу налаза сачинио нацрт међународне конвенције.[95]

Република Србија ратификовала је 19. маја 2009. године, Конвенцију о високотехнолошком криминалу, заједно са додатним протоколом уз Конвенцију о високотехнолошком криминалу.[96]

Поред наведене конвенције и допунског протокола, донети су следећи акти који су од значаја за компјутерски криминал*:*

• Директива 2013/40/ЕУ Европског парламента и Савета ЕУ о нападима на информационе системе и замени Оквирне одлуке Савета 2005/222/ЈХА;

• Безбедносна агенда Европске уније за период од 2015. до 2020. године;

• Стратегија сајбер безбедности Европске уније из 2013. године – „Отворен, безбедан и заштићен сајбер простор", и

• ИОЦТА (2017) – Процена претње од Интернет организованог криминала.[97]

[94]Ibid.
[95]РС-Министарство унутрашњих послова -Управа за полицијско образовање-Висока школа унутрашњихпословау сарадњи саХанс Зајдел фондацијом – Зборник радова -Међународна научностручна конференција, Сузбијање криминала иевропске интеграције, с освртом нависокотехнолошки криминал, Лакташи, 28–30. марта 2012. Године, стр.4.
[96]С. Лутовац и Ј.Рачић -оп.цит, стр. 284.
[97]Ibid.

2. КРИВИЧНО-ПРАВНА ЗАШТИТА КОМПЈУТЕРСКЕ КРАЂЕ У ЗЕМЉАМА БИВШЕ ЈУГОСЛАВИЈЕ

Ради адекватног сагледавања ове теме, осврнућу се и на законску нормативу компјутерске крађе у земљама бивше Југославије, међу којима су поред Србије још и Словенија, Хрватска, Северна Македонија, Босна и Херцеговина и Црна Гора

1. Република Словенија

Кривични закон Републике Словеније („Сл. Гласник Републике Словеније", бр. 95/04- званични консолидовани текст, и 55/08 – КЗ -1)[98] не прописује компјутерску крађу као издвојено кривично дело, као ни њене појавне облике, нити садржи посебну главу кривичних дела која се односе на област компјутерског криминалитета.

Кривична дела која се односе непосредно на компјутерски криминалитет у овом закону су кривично дело из чл. 225. Неоправдани улазак у информациони систем,[99] глава XXXIII Кривична дела против имовине и кривично дело из чл. 242. Упад у информациони систем,[100] глава XXIV Кривична дела портив привреде.

С обзиром да овако слаб систем нормирања дела из области компјутерске крађе, у погледу процесуирања извршиоца дела која се тичу компјутерске крађе, конкретно крађе података, поред наведених кривичних дела која су у непосреној вези са компјутерским криминалитетом, могу се у зависности од случаја и околности, применити и дело из чл. 151. Неовлашћено објављивање приватних докумената,[101] дело из чл. 154. Злоупотреба личних података[102] – глава XXVI Кривична дела против људских права и слобода, а у појединим случајевима и кривична дела из члана 236. Преваре у трансакцијама хартија од вредности[103]

[98] „Сл. Гласник Републике Словеније", бр. 95/04- званични консолидовани текст, и 55/08 – КЗ -1,
[99] чл. 225. Кривични закон Републике Словеније, („Сл. Гласник Републике Словеније", бр. 95/04- званични консолидовани текст, и 55/08 – КЗ -1),
[100] чл. 242. Кривични закон Републике Словеније, оп. цит.,
[101] чл. 151. Кривични закон Републике Словеније, оп. цит.,
[102] чл. 154. Кривични закон Републике Словеније, оп. цит.,
[103] чл. 236. Кривични закон Републике Словеније, оп. цит.,

– глава XXIV Кривична дела против привреде и чл. 217. Превара[104] – глава XXIII Кривична дела против имовине.

У погледу крађе рачунара и рачунарске опреме примењују се одредбе чл. 211. Крађа[105] и чл. 212. Тешка (Велика) крађа,[106] глава Кривична дела против имовине.

2. Република Хрватска

У кривично законодавство Републике Хрватске уврштена су кривична дела из области компјутерског криминалитета у глави XXV, под називом Кривична дела против рачунарских система, програма и података и то следећа кривична дела:[107]

- чл. 266. Неовлашћени приступ,[108]
- чл. 267. Ометање рада рачунарског система,[109]
- чл. 268. Оштећење рачунарских података, [110]
- чл. 269. Неовлашћено пресретање рачунарских података, [111]
- чл. 270. Рачунарска саботажа, [112]
- чл. 271. Рачунарска превара, [113]
- чл. 272. Злоупотреба направа, [114]
- чл.273. Тешка казнена дела против рачунарских система, програма и података.[115]

У Хрватском кривичном законодавству компјутерска крађа није прописана као посебно кривично дело, али сам анализом Кривичног (Казненог) закона Републике Хрватске, приметила да је приступљено са већом пажњом, него у другим земљама бивше

[104] чл. 217. Кривични закон Републике Словеније, оп. цит.,
[105] чл. 211. Кривични закон Републике Словеније, оп. цит.,
[106] чл. 212. Кривични закон Републике Словеније, оп. цит.,
[107] Казнени закон ХР (НН 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21),
[108] чл. 266. Казнени закон ХР (НН 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21),
[109] чл. 267. Казнени закон ХР, оп. цит.,
[110] чл. 268. Казнени закон ХР, оп. цит.,
[111] чл. 269. Казнени закон ХР, оп. цит.,
[112] чл. 270. Казнени закон ХР, оп. цит.,
[113] чл. 271. Казнени закон ХР, оп. цит.,
[114] чл. 272. Казнени закон ХР, оп. цит.,
[115] чл. 273. Казнени закон ХР, оп. цит.,

Југославије, приликом инкриминисања кривичних дела из области компјутерског криминалитета у законодавство Републике Хрватске, јер од прописаних кривичних дела из главе XXV, на случај комјутерске крађе, једино се не могу применити кривична дела из члана 272. Злоупотреба направа[116] и 267. Ометање рада рачунарског система. [117]

Поред примене ових кривичних дела на компјутерску крађу, осврнућемо се и на друга кривична дела која су у посредној вези са компјутерским криминалитетом, иако не спадају под кривична дела из области компјутерског криминалитета, а која се као таква неретко примењују на компјутерску крађу, у зависности од случаја до случаја.

Када је реч о компјутерској крађу података, поред претходно наведених кривичних дела из области компјутерског криминала, иста се може довести у вези и са кривичним делом против безбедности сигурносног промета, чл. 244а. Недозвољено поседовање безготовинског система плаћања,[118] кривичним делима против приватности, чл. 146. Неовлашћена употреба личних података[119] и чл. 142. Повреда тајности писама и других пошиљки. [120]

На крађу рачунара и рачунарске опреме, извесно је да се примењују одредбе чл. 228. и 229. односно Крађа[121] и Тешка крађа,[122] из главе XXIII Кривична дела против имовине.

3.Република Северна Македонија

Законодавство Републике Северне Македоније у погледу компјутерског криминалитета и конкретно компјутерске крађе, као и њених појавних облика је веома недефинисано. Северена Македонија у свом кривичном законику (Кривичен законик, „Службен весник на Република Македонија" број 80/99, број 4/2002 година, број 43/2003, број 19/2004, број 81/2005, број 60/06, број 73/06, број 7/08, број 139/08, број 114/09, број 51/11, број 135/11 , 185/11, број 142/12, број 166/12, број 55/13, број 82/13, број 14/14, број

[116] чл. 272. Казнени закон ХР, оп. цит.,
[117] чл. 267. Казнени закон ХР, оп. цит.,
[118] чл. 244а. Казнени закон ХР, оп. цит.,
[119] чл. 146. Казнени закон ХР, оп. цит.,
[120] чл. 142. Казнени закон ХР, оп. цит.,
[121] чл. 228. Казнени закон ХР, оп. цит.,
[122] чл. 229. Казнени закон ХР, оп. цит.,

27/14, број 28/14, број 115/14 и број 132/14) нема посебну главу која уређује област компјутерског криминалитета, нити издвојено кривично дело компјутерска крађа, већ се дела из ове области процесуирају кроз друге врсте кривичних дела.[123]

Република Северна Македонија је у глави која се односи на кривична дела против имовине, регулисала као посебна кривична дела поједина противправна понашања која се односе на компјутерски криминалитет:

- члан 251. Оштећење и неовлашћен приступ рачунарском систему,[124]
- члан 251-а. Израда и увођење рачунарских вируса,[125]
- члан 251б. Компјутерска превара;[126]

Из наведеног закључујемо да је компјутерска крађа у законодавству Републике Северне Македоније, регулисана кроз друга кривична дела која се доведе у непосредну или посредну везу са компјутерским криминалитетом, из разлога, јер компјутерска крађа, није регулисана као посебно кривично дело у овом законодавству, те је с тога, као алтернатива за овакву врсту дела, предвиђена већ постојећа нормативa, у зависности од случаја до случаја.

С обзиром на овакво нормативно уређење компјутерског криминалитета извесно је да се на компјутерску крађу рачунара и рачунарских компоненти, у кривичном законодавству Републике Македоније, примењују се одредбе члана 235.[127] и члана 236[128]. Кривичног законика, а којима су уређена кривична дела Крађа и Тешка крађа, те се с тим у вези, противправна понашања које се тичу компјутерске крађе рачунара и рачунарских

[123], „Службен весник на Република Македонија" број 80/99, број 4/2002 година, број 43/2003, број 19/2004, број 81/2005, број 60/06, број 73/06, број 7/08, број 139/08, број 114/09, број 51/11, број 135/11 , 185/11, број 142/12, број 166/12, број 55/13, број 82/13, број 14/14, број 27/14, број 28/14, број 115/14 и број 132/14,

[124] чл. 251. Кривичен законик, „Службен весник на Република Македонија" број 80/99, број 4/2002 година, број 43/2003, број 19/2004, број 81/2005, број 60/06, број 73/06, број 7/08, број 139/08, број 114/09, број 51/11, број 135/11, 185/11, број 142/12, број 166/12, број 55/13, број 82/13, број 14/14, број 27/14, број 28/14, број 115/14 и број 132/14,

[125] чл. 251а. Кривичен законик, оп. цит.,

[126] чл. 251б. Кривичен законик, оп.цит.,

[127] чл. 235. Кривичен законик, оп.цит.,

[128] чл. 236. Кривичен законик, оп.цит.,

података, подоводе под наведена кривична дела против имовине Кривичног законика Републике Македоније.

У погледу компјутерске крађе идентитета и других личних и пословних података, у зависности од околности случаја могу се примењивати и одредбе члана 149. Кривичног законика, којима је уређено кривично дело Злоупотреба личних података[129], одредбе члана 147. Повреда тајности писма и других пошиљки[130], из главе Кривична дела против слободе и људских и грађанских права, као и кривична дела из члана 251. Оштећење и неовлашћен приступ рачунарском систему[131] и члана 251б. Компјутерска превара[132].

Иако Северна Македонија, нема баш најадекватанији кривични систем заштите када је у погледу компјутерска крађа, оно што је занимљиво, јесте чињеница да се од 2018. године, у Прилепу у Северној Македонији ради на пројекту изградње **Business Continuity and Disaster Recovery Data Center,** односно објекта, под називом „Бетонски прстен" за чување података у Прилепу, а који ће обезбедити континуитет IT пословања министарства унутрашњих послова. Основни циљ овог и оваквог пројекта је да се обезбеди заштита опреме, као и свих информација/података, софтвера, од крађе, а којима се користи министарство унутрашњих послова Северне Македоније. Основна функција овог објекта је да обезбеди сигуран смештај компјутера, складишта, мрежних уређаја, енергију за њихово одржавање, као и повезаност са другим уређајима унутар и изван њега. [133]

Сервер соба пројектована је као соба у соби и обезбеђује највиши ниво физичке заштите, а самим тим спречава и ризике. Уграђени системи, обезбеђују свеобухватну заштиту и као такви мултифункционалну безбедност бекап и сервер система мрежних компјутера и система комуникације. Пројекат и изградњу овог објекта финансира Европска унија.[134]

[129] чл. 149. Кривичен законик, оп.цит.,
[130] чл. 147. Кривичен законик, оп.цит.,
[131] чл. 251. Кривичен законик, оп.цит.,
[132] чл. 251б. Кривичен законик, оп.цит.,
[133]https://www.gradnja.rs/wp-content/uploads/2020/08/Business-Continuity-Disaster-Recovery-Data-Center-1X2STUDIO-05.jpg
[134] Ibid.

Иако је овај и овакав пројекат идејно лепо осмишљен, са циљем да се заштите како подаци грађана, којима располаже Министарство унутрашњих послова, тако и интерно - комуникациони системи овог државног органа, остаје нејасно да ли ће у оквиру овако осмишљене и организоване процедуре електронске заштите података у самом објекту, постојати и системи, помоћу којих ће Министарство унутрашњих послова моћи да предупреди криминалне радње из области компјутерске крађе података и у другим државним органима, као и оне које су усмерене на комуникационе системе личних рачунара грађана.

4. Босна и Херцеговина

У Босни и Херцеговини кривична дела из области компјутерског криминала регулисана су ентитетским законодавством – Кривичним законом Федерације Босне и Херцеговине и Кривичним законом Републике Српске.

Федерација БиХ

У Кривичном закону ФБиХ („Сл. новине ФБиХ", бр. 36/2003, 21/2004 – испр., 69/2004, 18/2005. 42/210, 56/2014, 76/2014, 46/2016 и 75/2017)[135] глава XXXII посвећена је кривичним делима против система за електронску обраду података, иако ни у овом случају компјутерска крађа није регулисана као посебно кривично дело. У кривична дела против система за електронску обраду података, спадају:

- чл. 393. Оштећење рачунарских података и програма,[136]

- чл. 394. Компјутерски фалсификат,[137]

- чл. 395. Компјутерска превара,[138]

- чл. 396. Сметње у раду система и мрежа електронске обраде података,[139]

- чл. 397. Неовлашћен приступ заштићеном систему и мрежи електронске обраде података, [140]

- чл. 398. Компјутерска саботажа;[141]

Уколико обратимо пажњу на сва кривича дела из главе XXXII, можемо да приметимо да су иста посвећена искључиво радњама које се односе на компјутерски криминалитет, али компјутерска крађа није регуслисана као посебно кривично делу ни у овом случају.

Када је реч о компјутерској крађи рачунара и рачунарских компоненти, на противправна понашања, која су усмерена на крађу рачунара и рачунарске опреме, и у овом случају је извесно да се премињују одредбе члана 286 Крађа[142] и 287. Тешка крађа,[143] из

[135] "Службене новине Федерације БиХ", бр. 36/2003, 21/2004 – испр., 69/2004, 18/2005. 42/210, 56/2014, 76/2014, 46/2016 и 75/2017,
[136] чл. 393.Кривични закон ФБиХ, ("Службене новине Федерације БиХ", бр. 36/2003, 21/2004 – испр., 69/2004, 18/2005. 42/210, 56/2014, 76/2014, 46/2016 и 75/2017),
[137] чл. 394. Кривични закон ФБиХ, оп. цит.,
[138] чл. 395. Кривични закон ФБиХ, оп. цит.,
[139] чл. 396. Кривични закон ФБиХ, оп. цит.,
[140] чл. 397. Кривични закон ФБиХ, оп. цит.,
[141] чл. 394. Кривични закон ФБиХ, оп. цит.,
[142] чл. 286. Кривични закон ФБиХ, оп. цит.,
[143] чл. 287. Кривични закон ФБиХ, оп. цит.,

главе XXV - Кривична дела против имовине, Кривичног закона ФБиХ, у зависности од околности случаја.

Када је реч о крађи идентитета и других личних и пословних података, поред кривичних дела против система за електронску обраду података, а који се односе искључиво на област компјутерског криминалитета, могу се у конкретном случају примењивати и одредбе Кривичног законика којима су нормирана друга кривична дела, а у завинсоти од околности случају то могу да буду: кривична дела из члана 186. Повреда тајности писма и друге пошиљке,[144] кривично дело из члана 193. Недозвољено кроишћене личних података,[145] из главе XVII -Кривична дела против слободе и права човека и грађана и др.

Република Српска

У кривичном закону Републике Српске ("Сл. Гласник РС, бр. 64/2017, 104/2018 – одлука УС, 15/2021 и 89/2021)[146] такође, глава XXXII, односи се на кривична дела против безбедности компјутерских података, где су предвиђена следећа кривична дела из области компјутерског криминалитеа:

- чл. 407. Оштећење компјутерских података и програма,[147]
- чл. 408. Компјутерске саботаже,[148]
- чл. 409. Израда и уношење компјутерских вируса,[149]
- чл. 410. Компјутерска превара,[150]
- чл. 411. Неовлашћени приступ заштићеном компјутеру, компјутерској мрежи, телекомуникационој мрежи и електронској обради података,[151]

[144] чл. 186. Кривични закон ФБиХ, оп. цит.,
[145] чл. 193. Кривични закон ФБиХ, оп. цит.,
[146] "Сл. Гласник РС, бр. 64/2017, 104/2018 – одлука УС, 15/2021 и 89/2021,
[147] чл. 407. Кривични закон Републике Српске ("Сл. Гласник РС, бр. 64/2017, 104/2018 – одлука УС, 15/2021 и 89/2021),
[148] чл. 408. Кривични закон Републике, оп.цит.,
[149] чл. 409. Кривични закон Републике, оп.цит.,
[150] чл. 410. Кривични закон Републике, оп.цит.,
[151] чл. 411. Кривични закон Републике, оп.цит.,

- чл. 412. Спречавање и ограничавање јавној компјутерској мрежи,[152]
- чл. 413. Неовлашћено коришћење компјутера и компјутерске мреже.[153]

Ни у Кривичном закону Републике Српске компјутерска крађа није предвиђена као посебно кривично дело, нити неки од њених појавних облика, те у том случају на компјутерску крађу, у зависности од околности, могу применити кривична дела из главе XXXII, против безбедности компјутерских података и то чл. 410. Компјутерска превара, чл. 411. Неовлашћени приступ заштићеном компјутеру, компјутерској мрежи и електронској обради података и чл. 413. Неовлашћено коришћење компјутера или компјутерске мреже, такође, у неким случајевима, могу се применити и одредбе овог закона, којима су регулисана друга кривична дела, која не подпадају под област компјутерског криминалитета, а то су кривично дело Повреда тајности писма или других пошиљки из чл. 153. као и Неовлашћено коришћење личних података из чл. 157.

У случајевима физичке крађе рачунара и рачунарске опреме, примењују се кривична дела из главе XX, чл. 224. Крађа и чл. 226. Тешка крађа.

Босна и Херцеговина је 09.09.2022. године, претрпела можда један од највећих хакерских напада у последњих пар деценија, када су хакери напали институције у БиХ. Злонамерним вирусима, нападнути су сервери парламента БиХ, услед чега су били закључани сви подаци који су тамо чувани. Нападнути су још и представништво Бих и Веће министра. Запослени у седишту законодавне и извршне власти, више од две недеље нису могли да приступе подацима и да регуларно обављају свој посао.[154]

Како нападачи још увек нису идентификовани, а БиХ више од две недеље уз помоћ својих најбољих хакера, није могла да отклони последице напада, јасно је да је систем заштите од компјутерског криминалитета на државном нивоу веома слаб, те да је потребно и неопходно предузети одређене кораке у погледу заштите од компјутерске крађе.

[152] чл. 412. Кривични закон Републике, оп.цит.,
[153] чл. 413. Кривични закон Републике, оп.цит.,
[154]https://www.021.rs/story/Info/Region-i-svet/317762/Hakeri-napali-institucije-u-BiH-zaposleni-bez-pristupa-racunarima.html

5. Република Црна Гора

У Црној Гори су присутна сва кривична дела из области високотехнолошког криминала. Међу којима су највише присутна кривична дела из области крађа идентитета, рачунарских превара, крађа е-маил налога...

Процењује се да је штета причињена вршењем ових кривичних дела у Црној Гори у претходних неколико година преко 1.500.000 еура, што је само причињена штета пријављена од стране црногорских фирми и грађана. Сумња се да је стварна причињена штета много већа од званичне.[155]

Примена легислатива ЕУ из области компјутерског криминала у законодавству Црне Горе

Како је растао број корисника интернета у Црној Гори, тако су прилагођавани и црногорски закони везани за кривична дела „високотехнолошког криминала“. Тако су већ 2004. године у Кривични законик имплементирана кривична дела из области рачунарског криминала. Како се тренд кривичних дела мењао, тако су се вршиле измене и допуне Кривичног законика. Већ 2014. године законом су обухваћена сва кривична дела из области високотехнолошког криминала која су у потпуности усклађена са легислативом Европске уније, али компјутерскра крађа није предвиђена као издвојено кривично дело. [156]

Кривичним закоником 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)[157] у глави XXVIII прописана су следећа кривична дела против безбедности рачунарских података:

[155]https://www.portalanalitika.me/clanak/224774--sajber-kriminal-u-crnoj-gori-krada-indentiteta-ucjene-djecja-pornografija
[156] Ibid.
[157]„ 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,

- чл. 349. Оштећење рачунарских података и програма,[158]
- чл. 350. Ометање рачунарског система,[159]
- чл. 351. Прављење и уношење рачунарских вируса,[160]
- чл. 352. Рачунарска превара,[161]
- чл. 353. Неовлашћени приступ рачунарском систему, [162]
- чл. 354. Злоупотреба уређаја и програма. [163]

И у овом случају, као што можемо да видмо, компјутерска крађа није предвиђена као посебно кривично дело, иако је наводно реч о свим кривичним делима из области високотехнолошког криминала, те се иста доводи у везу са појединим побројаним кривичним делима против безбедности рачуарских података, као и другим прописаним кривичним делима против имовине, слобода и права човека и грађана, а у неким сличајевима и против платног промета и привредног пословања.

На компјутерску крађу података, у зависности од околности случају, у оквиру кривичног законодавства Црне Горе, могу се применити одредбе чл. 352. и 353. Кривичног законика, односно кривична дела Рачунарска превара[164] и Неовлашћени приступ рачунарском систему,[165] из главе XXVIII Кривична дела против безбедности рачунарских података, као и кривична дела из чл. 172. Повреда тајности писама и других пошиљки[166] и чл. 176. Неовлашћено прикупљање и коришћење личних података,[167] из главе XXV Кривична дела против слобода и права човека и грађана, а у појединим случајевима када се дело доводи у везу са платним прометом, кредитним картицама и картицама за безготовинско плаћање, онда се примењује кривично дело из чл. 260. Фалсификовање и

[158] чл. 349. 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),
[159] чл. 350. Кривични законик Црне Горе, оп. цит.,
[160] чл. 351. Кривични законик Црне Горе, оп. цит.,
[161] чл. 352. Кривични законик Црне Горе, оп. цит.,
[162] чл. 353. Кривични законик Црне Горе, оп. цит.,
[163] чл. 354. Кривични законик Црне Горе, оп. цит.,
[164] чл. 352. Кривични законик Црне Горе, оп. цит.,
[165] чл. 353. Кривични законик Црне Горе, оп. цит.,
[166] чл. 172. Кривични законик Црне Горе, оп. цит.,
[167] чл. 176. Кривични законик Црне Горе, оп. цит.,

злоупотреба платиних картица и картица за безготовинско плаћање.[168] Такође, није искључена ни примена чл. 244., односно кривично дело Превара.

У погледу крађе рачунара и рачунарске опрема, извесно је да се примењују одредбе члана 239. и 240., односно Крађа[169] и Тешка крађа[170] из главе XXIV Кривична дела против имовине, а у зависности од околности случаја.

Институције и надлежност за борбу против високотехнолошког криминала

Држава Црна Гора је ишла у складу са новим трендовима из области информационо-комуникационих технологија и формирала Министарство за информационо друштво у оквиру којег је формиран CIRT тим (CERT – Computer Emergency Response Team) који је задужен за кординацију и помоћ државним органима како би се смањио ризик од рачунарских инцидената, као и подизање свести о сабјер претњама и сајбер безбедности. У свету тренутно постоје више од 250 CIRT тимова.[171]

Такође, у МУП-у Црне Горе у Управи полиције, 2015. Године, формирана је Јединица за борбу против високотехнолошког криминала, која се налази у склопу Одсека за борбу против организованог криминала и корупције.[172]

3. НАЦИОНАЛНИ ПРАВНИ ОКВИР

Осим побројаних међународних аката, који се баве проблемом компјутерског криминалитета, након ратификације конвенције о високотехнолошком криминалитету, на домаћем плану је извршена регулација законодавног система, који се односи на област компјутерског криминала.

С тим у вези, у даљем тексту осврнућемо се на законску регулативу, која уређује област компјутерског криминалитета или је у блиској вези са истим.

---

[168] чл. 260. Кривични законик Црне Горе, оп. цит.,
[169] чл. 239. Кривични законик Црне Горе, оп. цит.,
[170] чл. 240. Кривични законик Црне Горе, оп. цит.,
[171] https://www.portalanalitika.me/clanak/224774--sajber-kriminal-u-crnoj-gori-krada-indentiteta-ucjene-djecja-pornografija, оп. цит.,
[172] Ibid.

С обзиром да компјутерска крађа није појмовно и јасно одређена, нити као таква на директан начин инкриминисана у домаће законодавство, приликом осврта на национални правни оквир који се тиче компјутерског криминалитета, уједно ћемо обрадити и компјутерску крађу као најчешћи појам компјутерског криминалитета и образложити како и на који начин се она инкриминипе кроз нацинално законодавство, након ратификације Конвенције о високотехнолошком криминалу.

Након ратификовања Конвенције о високотехнолошком криминалу Република Србија се овом облику криминалитета супротставља применом следећих закона:

•Кривичним закоником,[173]
•Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала,[174]
•Законом о кривичном поступку,[175]
•Закон о електронским комуникацијама,[176]
•Закон о информационој безбедности,[177]
•Закон о организацији и надлежности државних органа у сузбијању организованог криминала, тероризма и корупције,[178] и
•Закон о спречавању прања новца и финансирања тероризма.[179]

1.2.Кривичноправна заштита

Кривични законик и Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, јесу најзначајнији у погледу националне регулативе која се тиче компјутерског криминалитета, те ћу се њима посветити са већом пажњном, гледано са кривично-правног аспекта компјутерског криминалитета, односно компјутерске крађе.

[173]„Сл. гласник РС“, бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019
[174]„Сл. гласник РС“, бр. 61/2005 и 104/2009
[175]„Сл. гласник РС“, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 - одлука УС и 62/2021 - одлука УС
[176]„Сл. гласник РС“, бр. 44/2010, 60/2013 - одлука УС, 62/2014 и 95/2018 - др. закон
[177] „Сл. гласник РС“, бр. 6/2016, 94/2017 и 77/2019
[178]„Сл. гласник РС“, бр. 94/2016 и 87/2018 - др. закон
[179]„Сл. гласник РС“, бр. 113/2017, 91/2019 и 153/2020

1.2.1. Кривични законик

Последњих година у Србији коришћење компјутерске технике достигло је велике размере. Основани су велики информациони системи у органима управе, органима унутрашњих послова, заводима за статистику, здравствевним установама, универзитетима, факултетима, те је то један од основних разлога због чега је неопходна кривичноправна заштита од компјутерског криминалитета.

Након доношења Закона о потврђивању конвенције о високотехнолошком криминалу, који је у службеном гласнику РС, објављен 19. Марта 2009. године, под бројем 19 и ратификовања Конвенције о високотехнолошком криминалу, кривично-правна заштита од компјутерског криминалитета остварена је предвиђањем кривичних дела против безбедности рачунарских података у глави XXVII Кривичног законика Републике Србије, а то су следећа кривична дела[180]:

• Оштећење рачунарских података и програма[181];
• Рачунарска саботажа[182];
• Прибављање и уношење рачунарских вируса[183];
• Рачунарска превара[184];
• Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података[185];
• Спречавање и ограничавање приступа јавној рачунарској мрежи[186];
• Неовлашћено коришћење рачунара или рачунарске мреже[187], и
• Прибављање, набављање и давање другом средстава за извршење кривичнихдела против безбедности рачунарских података.[188]

[180]Кривични законик РС, глава XXVII- члан 298-304а.
[181]члан 298. Кривичног законика РС,
[182]члан 299. Кривичног законика РС, оп.цит.
[183]члан 300. Кривичног законика РС, оп.цит
[184]члан 301. Кривичног законика РС, оп.цит
[185]Члан 302. Кривичног законика РС, оп.цит
[186]Члан 303. Кривичног законика РС, оп.цит
[187]Члан 304. Кривичног законика РС, оп.цит
[188]Чл. 304а. Кривичног законика РС, оп.цит

Када су у питању кривичне санкције, прописана је примена казне затвора или новчане казне у зависности од тежине учињеног дела.[189]

Компјутерска крађа није посебно предвиђена у нашем законодавству као посебно кривично дело, као ни други типични облици крађе који се јављају под окриљем компјутерске крађе (као што су крађа података, крађа идентитета, крађа рачунара и рачунарских компоненти и сл....)

Један од најзначајнијих облика компјутерске крађе, као што смо већ напоменули јесте крађа идентитета, те ћемо за исту, као и за друге појавне облике компјутерске крађе, образложити како су регулисани националном легислативом.

1.2.2. Законска регулатива крађе идентитета

У важећем кривичном законодавству Србије није посебно предвиђено кривично дело крађа идентитета. Уколико дође до крађе идентитета, примењују се одредбе Кривичног законика које се односе на рачунарску превару (чл. 301), неовлашћен приступ рачунарским мрежама (чл.302), превару (чл. 208), фалсификовање и злоупотребу платних картица (чл. 255 ст. 4), неовлашћена употреба туђег пословног имена и друге посебне ознаке робе или услуга (чл. 233).[190] Иста законска регулатива, односи се и на крађу друге врсте података, као што су лозинке, бројеви рачуна, платних картица, кодови.

1.2.3. Законска регулатива крађе рачунара и рачунарске опреме

Што се тиче крађе рачунара и рачунарске опреме, као појавног облика компјутерске крађе, који улази под окриље компјутерског криминалитета, иста, као ни крађа идентитета, није посебно предвиђено кривично дело.

Имајући у виду судску праксу, која и није баш многобројна, као и одредбе Кривичног законика које се тичу кривичних дела против безбедности рачунарских података, долазимо до закључка да у случајевима крађе рачунара или рачунарске опреме, исте се подводе под

[189] С. Лутовац , Ј.Рачић, оп.цит, стр. 284.
[190] Ibid, стр. 116.

кривична дела Крађа из члана 203. или Тешка крађа из члана 204. Кривичног законика, у зависности од околности случаја.[191]

Крађа и тешка крађа, спадају у кривична дела против имовине из главе XXI Кривичног законика и прописане су чланом 203. и чланом 204.поменутог законика.[192]

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

Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала уређује се образовање, организација, надлежност и овлашћења посебних организационих јединица државних органа, ради откривања, кривичног гоњења и суђења за кривична дела против безбедности рачунарских података одређена Кривичним закоником, кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења кривичног дела јављају рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, као и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 2000 или настала материјална штета прелази износ од 1.000.000 динара, кривична дела против полних слобода и права човека и грађана, полне слободе, јавног реда и мира и уставног уређења и безбедности Републике Србије, која због начина извршења употребљених средстава могу се сматрати кривичним делима високотехнолошког криминала. [193]

Овај закон дефинише високотехнолошки криминал као вршење кривичних дела, код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику.[194]

---

[191] Чл. 203., чл. 204. Кривичног законика „Сл. гласник РС",б р. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019;
[192] Чл. 203., чл.204. Кривичног законика, оп.цит.
[193]М. Павловић, Д. Тошић оп.цит, стр. 49.
[194]чл. 2.Закон о организацији и надлежности државних органа за борбу противвисокотехнолошкогкриминала „Сл. Гласник РС" “, бр. 61/2005 и 104/2009;

Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала, а за поступање кад су у питању кривична дела из области високотехнолошког криминала, надлежно је Више јавно тужилаштво у Београду и то за целу територију Републике Србије, у оквиру кога је оформљено посебно одељење за борбу против високотехнолошког криминала. Републички јавни тужилац из редова заменика јавних тужилаца, бира и поставља посебног тужиоца (уз његову писмену сагласност) који руководи радом овог тужилаштва. Поред свих општих услова за избор за заменика вишег јавног тужиоца, у овом случају предност имају заменици јавних тужиоца, који поседују посебна знања из области информатичких технологија. Посебни тужилац се у случају када дође до сазнања да се у једном кривичном предмету ради о кривичним делима предвиђеним овим законом, обраћа се у писменој форми Републичком јавном тужиоцу захтевајући да ме се пренесе или повери надлежност. [195]

Поред посебног јавног тужилаштва овим законом предвиђа се и образовање службе за борбу против високотехнолошког криминала у оквиру министарства надлежног за унутрашње послове, ради обављања послова органа унутрашњих послова у вези са кривичним делима одређеним овим законом. [196] Она је у ствари формирана као Одељење за борбу против високотехнлошког криминала у оквиру Службе за борбу против организованог криминала (СБПОК). То значи да је служба систематизована у Управи криминалистичке полиције Дирекције полиције, тј. у седишту Министарства унутрашњих послова. У организационом смислу, Одељење за борбу против високотехнолошког криминала чини више организационих јединица. Старешину службе поставља и разрешава министар унутрашњих послова по прибављеном мишљењу посебног тужиоца. Исто тако, законом је предвиђена обавеза министра унутрашњих послова да ближе уреди рад Одељења за борбу против високотехнолошког криминала, одговарајућим подзаконским актом, а у складу са Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала. Одељење за борбу против високотехнолошког криминала је по природи ствари упућено на сарадњу са другим организационим целинама Службе за сузбијање организованог криминала, посебно са Одсеком за прикупљање и обраду дигиталних доказа у оквиру Службе за специјалне истражне методе, али и са осталим

[195]М. Павловић , Д. Тошић, оп.цит.стр. 49-50.
[196]Ibid, стр, 50.

организационим јединицама Управе криминалистичке полиције у Дирекцији полиције. Исто важи и за одговарајућу сарадњу са службама безбедности у Србији (BIA, VBA), али и за одговарајућу сарадњу са појединим службама страних земаља, као што је британска служба за сузбијање организованог криминала (SOCA), у оквиру које делује Национална јединица за борбу против високотехнолошког криминала (NHTCU) са седиштем у Лондону. Одељење за борбу против високотехнолошког криминала развијало је свестрану сарадњу и са Националним централним бироом Интерпола Београд, будући да високотехнолошки криминал представља један од најчешће коришћених облика прекограничног (транснационалног) криминала.[197]

Суд надлежан за поступање код ових кривичних дела у првом степену је Виши суд у Београду, а у другом Апелациони суд у Београду. У оквиру Вишег суда у Београду, образовано је одељење за борбу против високотехнолошког криминала. Судије у овом Одељењу распоређују се из реда судија тог суда уз њихову сагласност, а распоређује их председник Вишег суда у Београду. Као и код тужиоца и код судија, предност имају судије које поседују посебна знања из области информатичких технологија.[198]

III СТРАТЕГИЈА ЗА БОРБУ ПРОТИВ КОМПЈУТЕРСКОГ КРИМИНАЛА

Оно што бих издвојила као значајно, а везано за конкретну тему и сам високотехнолошки криминал уопште, јесте пројекат CyberCrime@IPA, реч је о заједничком пројекту Европске уније и Савета Европе о регионалној сарадњи у борби против компјутерског криминала (а у оквиру кога се као један од најзначајних појавних облика јавља и компјутерска крађа), учесници овог пројекта били су поред Србије и Албанија, Босна и Херцеговина, Хрватска, Црна Гора, Македонија и Турска, чији су представници (министри и високи функционери који представљају министарство унутрашњих послова и безбедности, министарство правде и државна тужилаштва земаља и подручја која учествују у пројекту) на конференцији у Дубровнику у Хрватској 15. фебруара 2013. године усвојили Декларацију о стратешким приоритетима борбе против високотехнолошког криминала.[199]

[197]Ibid.
[198]Ibid.
[199]Cybercrime@IPA – Заједнички пројекат ЕУ и ЕС за регионалну сарадњу у борби противвисокотехнолошког криминала – Стратешки приоритети сарадње у борби против високотехнолошког криминала,

Иако су представници земаља учесница овог пројекта усвојили наведену декларацију још 2013. године, стратешки приоритети за борбу против високотехнолошког криминала, који су наведени у поменутој декларацији нису у потпуности реализовани, а ради адекватне заштите од компјутерског криминалитета, не треба никако стављати по страни том приликом одређене приоритете, јер су исти од енормног значаја за адекватну заштиту од компјутерског криминалитета, који је у експанзији последњих пар година, због незаустављивог напретка информационо-комуникационих система.

Како не би дошло до забуне, овај и овакав пројекат, који се односи на високотехнолошки криминалитет, истичем у овом раду као значајан из разлога, јер без постављања општих приоритета у погледу компјутерског криминалитета, не можемо ни компјутерску крађу обрадити на адекватан начин, с обзиром да иста спада под област компјутерског криминалитета, те је врло важно успоставити јасне опште циљеве и приорите, на којима ће радити како земље учеснице у овом пројекту, тако и друге земље које се безуспешно боре са овом врстом криминала деценијама уназад, а након чега би требало посебну пажњу посветити сваком од појавних облика компјутерског криминалитета појединачно, међу којима је и компјутерска крађа, јер компјутерска крађа није прописана као посебно кривично дело, нити један од њених појавних облика, како у међународној легислативи, тако и у националној. С тим у вези врло је важно обратити пажњу на у даљем тексту изложене приоритете, јер напомињем, без темељнијег уређења компјутетског криминлитета не можемо издвојити компјутерску крађу засебно, јер се иста тренутно испољава кроз кривична дела која се односе на област компјутерског криминалитета, а без икаквог конкретног одређења да се таква дела примењују и односе и на компјутерску крађу, те за сада компјутерску крађу, морамо посматрати кроз одредбе којима су дефинисана друга кривична дела из области компјутерског криминалитета (као и друга дела која нису у непосредној вези са компјутерским криминалитетом, нити спадају под кривична дела против безбедности рачунарских података) али не и сама компјутерска крађа. Како би се дошло до стадијума појединачне обраде и посвећености појавним облицима компјутерског криминалитета (у конкретном случају компјутерске крађе) адекватне заштите како од стране државе, тако и система заштите који ће бити обезбеђени

https://rm.coe.int/16802f6a41

и загарантовани сваком појединцу, приликом употребе комуникационо-информационих технологија, веома је важно фокусирати се првобитно на оне опште циљеве и приоритете.

С тим у вези, одлучила сам да већи део текста поменуте стратегије за борбу против виоскотехнолошког криминала презентујем кроз текст овог рада, јер сматрам да приоритете дефинисане овим пројектом, односно мере које би владе држава учесница овог пројекта требале предузети, јесу неопходне у циљу борбе против високотехнолошког криминала и саме компјутерске крађе (из претходно објашњених разлога), те да их је потребно реализовати у што краћем року, како би државе учеснице пројекта, па и наша земља, имале адекватан систем заштите за борбу против, превасходно компјутерске крађе, па и самог компјутерског криминалитета у општем смислу.

Стратешки приоритети које је требало реализовати од стране земља учесница овог пројекта, јесу следећи:

1. Стратешки приоритет: политике и стратегије у области високотехнолошког криминала[200]

Будући да информациона и комуникациона технологија трансформише друштва, безбедност ИКТ постала је приоритет политика многих влада. То се одражава у усвајању стратегија безбедности рачунарских система с првенственим фокусом на заштиту критичне информационе инфраструктуре. Владе стога треба да размотре припрему посебних стратегија борбе против високотехнолошког криминала или да унапреде компоненте везане за високотехнолошки криминал у оквиру стратегија односно политика безбедности рачунарских система.

Надлежни органи треба да размотре следеће мере:

- Усвојити политике односно стратегије борбе против високотехнолошког криминала с циљем осигурања делотворне реакције кривичног правосуђа на кривична дела против рачунара и помоћу рачунара као и било које кривично дело које укључује електронске доказе. Као елементе таквих политика

[200] Ibid.

односно стратегија размотрити превентивне мере, законодавство, специјализоване јединице за спровођење закона и тужилаштва, међуагенцијску сарадњу, обуку органа за спровођење закона и правосуђа, сарадњу јавног и приватног сектора, делотворну међународну сарадњу, финансијске истраге и спречавање превара.

- Успоставити платформе на интернету за подношење пријава од стране јавности о високотехнолошком криминалу. То би требало да обезбеди боље разумевање претњи и трендова високотехнолошког криминала и да олакша деловање кривичног правосуђа. Такве платформе могу да се користе и за информисање јавности и упозорења о претњама.

- Подизати свест и промовисати превентивне мере на свим нивоима.

- Укључити се у сарадњу јавног и приватног сектора, укључујући нарочито сарадњу између органа за спровођење закона и пружаоца интернет услуга.

- Укључити се у највећем могућем степену у међународну сарадњу. То обухвата пуно коришћење постојећих билатералних, мултилатералних и регионалних споразума, нарочито Будимпештанске конвенције о високотехнолошком криминалу. Треба спровести мере и обуку за убрзање међународне правне помоћи. Владе (потписнице Конвенције и посматрачи) треба да активно учествују у раду Комитета Конвенције о високотехнолошком криминалу и треба да се укључе у сарадњу са Европским центром за борбу против високотехнолошког криминала и другим иницијативама Европске уније.

- Редовно оцењивати делотворност реакције кривичног правосуђа на високотехнолошки криминал и водити статистику. Такве анализе би помогле да се утврди и побољша успешност деловања кривичног правосуђа и да се ефикасно распоређују ресурси.

2. Стратешки приоритет: Потпун и делотворан правни основ за деловање кривичног правосуђа[201]

Усвајање потпуног и делотворног законодавства које испуњава захтеве у погледу људских права и владавине права треба да буде стратешки приоритет.

Надлежни органи треба да размотре следеће мере:

- Додатно побољшати одредбе процесног права о приступу органа за спровођење закона електронским доказима.

- Оценити делотворност законодавства. Треба водити статистичке податке о предметима који се истражују, гоне и по којима је донета пресуда и треба документовати примењене процедуре.

- Постарати се да овлашћења органа за спровођење закона подлежу условима и заштитним механизмима у складу са чланом 15. Будимпештанске конвенције. То треба да обухвати судски надзор интрузивних овлашћења, али и поштовање начела сразмерности и нужности.

- Оснажити законодавство о заштити података у складу са међународним и европским стандардима. То ће олакшати прекогранично дељење података и за потребе спровођења закона.

- Прилагодити законодавство о финансијској истрази, одузимању имовине проистекле из кривичног дела и о прању новца и финансирању тероризма интернет окружењу. Правила и прописи нарочито треба да предвиде брзу домаћу и међународну размену информација.

[201] Ibid.

3.Стратешки приоритет: Специјализоване јединице за борбу против високотехнолошког криминала[202]

Високотехнолошки криминал и електронски докази захтевају специјализовану реакцију кривичних правосудних органа. Органи за спровођење закона и тужилаштва треба да буду у стању да истражују и гоне кривична дела против рачунарских података и система, кривична дела помоћу рачунара, као и електронске доказе у вези са било којим кривичним делом. Битно је схватити да се технологија мења из дана у дан и да се стално повећава радно оптерећење јединица за борбу против високотехнолошког криминала и форензичких јединица. Прибављање ресурса (особља, опреме, софтвера) и одржавање специјализованих вештина и прилагођавање таквих јединица новонастајућим условима представља непрекидан изазов. Непрекидно јачање специјализованих јединица за борбу против високотехнолошког криминала треба да буде стратешки приоритет.

Надлежни органи треба да размотре следеће мере:

- Основати – где то још није учињено – специјализоване јединице за борбу против високотехнолошког криминала у оквиру кримииналистичке полиције. Тачна организација и функције треба да буду резултат пажљиве анализе потреба и да се заснивају на закону.

- Унапредити специјализацију тужилаца. Размотрити оснивање специјализованих јединица тужилаштва или, као другу могућност, групе специјализованих тужилаца да усмеравају или помажу другим тужиоцима у случајевима који укључују високотехнолошки криминал и електронске доказе.

- Редовно преиспитивати функције и обезбеђивање ресурса специјализованих јединица. То треба да омогући прилагођавања, а тако и одговоре на нове изазове и све веће захтеве.

[202] Ibid.

- Олакшати сарадњу и размену добрих пракси између специјализованих јединица на регионалном и међународном нивоу.

- Побољшати процедуре за истраге високотехнолошког криминала и поступање са електронским доказима. Испитати и размотрити имплементацију националних и међународних стандарда и добрих пракси по том питању. Размотрити коришћење „ водича о електронским доказима“ који је израђен у оквиру пројекта Cybercrime@IPA.

4. Стратешки приоритет: обука органа за спровођење закона[203]

Имплементацију домаће стратегије обуке органа за спровођење закона. Циљ треба да буде да се обезбеди да органи за спровођење закона имају вештине и компетенције неопходне да истражују високотехнолошки криминал, обезбеђују електронске доказе, врше рачунарску форензичку анализу за кривичне поступке, помажу другим органима и доприносе безбедности мреже. Улагање у такву обуку је оправдано с обзиром на ослањање друштва на информационе технологије и с тим повезане реизике.

Органи за спровођење закона треба да буду у стању не само да истражују кривична дела против и помоћу рачунарских система већ и да поступају са електронским доказима у вези са било којом врстом кривичног дела. Са експоненцијалним растом коришћења информационих технологија у друштву, у једнакој мери су порасли и изазови за органе за спровођење закона. Сви службеници органа за спровођење закона – од органа који први реагују до високоспецијализованих рачунарских форензичких истражитеља – треба да буду оспособљени да поступају са високотехнолошким криминалом и електронским доказима свако на свом нивоу. Идентификовани су, али још нису потпуно имплементирани елементи стратегија обуке органа за спровођење закона.

Имплементација одрживих стратегија обуке за обучавање службеника за спровођење закона наодговарајућем нивоу треба да буде стратешки приоритет.

[203] Ibid.

Надлежни органи треба да размотре следеће мере:

- Укључити правила и протоколе о поступању са електронским доказима на свим нивоима националне обуке. Важно је препознати да електронски докази утичу на све криминалне активности и да потребу за обуком за препознавање електронских доказа и поступање с њима имају сви службеници органа за спровођење закона који оперативно поступају, а не само они у специјализованим јединицама. Та обука би могла да буде базирана на „ водичу о електронским доказима“ који је израђен у оквиру пројекта Cybercrime@IPA.

- Размотрити увођење индивидуалних планова обуке за специјализоване истражитеље. Промене у технологији и начину на који починиоци кривичних дела злоупотребљавају ту технологију значе да постоји потреба за одговарајућим бројем високообученог особља које је компететно и способно да спроводи истраге и/или испитивања дигиталних доказа на највишем нивоу.

- Размотрити имплементацију процедура да би се обезбедило да се максимално искористи улагање у обуку о високотехнолошком криминалу. Обука о високотехнолошком криминалу и рачунарској форензици веома је скупа. Како би обезбедиле да се улагање адекватно исплати, земље треба да се постарају да се чланови особља поставе и задрже на положајима који одражавају ниво знања и вештина које они поседују. У том циљу, стратегије обуке и стратегије управљања људским ресурсима треба да буду комплементарне.

5. Стратешки приоритет: Обука правосудних органа[204]

Пошто, поред кривичних дела против и помоћу рачунара, све већи број других врста кривичних дела укључује доказе на рачунарским системима или другим уређајима за чување података, на крају све судије и тужиоци треба да буду спремни да поступају са

[204] Ibid.

електронским доказима. У земљама и подручјима који учествују у пројекту Cybercrime@IPA учињен је напредак у смислу да су припремљени модули за обуку, да су обучени инструктори и да су одржани основни и напредни пилот курсеви. Поред тога, оснива се Регионални пилот центар за обуку правосудних органа о високотехнолошком криминалу и судским доказима. Та достигнућа треба институционализовати.

Оспособљавање свих судија и тужилаца да врше гоњење и пресуђују у области високотехнолошког криминала и користе електронске доказе у кривичним поступцима треба да остане стратешки приоритет.

Надлежни органи треба да размотре следеће мере:

- Интегрисати обуку правосудних органа о високотехнолошком криминалу и електронским доказима у редовне програме. Домаће институције за обуку судија и тужилаца треба да интегришу основне и напредне модуле обуке о високотехнолошком криминалу и електронским доказима у своје редовне програме обуке за почетну обуку и обуку уз рад.

- Јачати Регионални пилот центар за обуку правосудних органа основан у Загребу у Хрватској. Домаће институције за обуку правосудних органа из региона треба да сарађују са Регионалним пилот центром за обуку правосудних органа ради ажурирања материјала за курс, документовања и ширења добрих пракси и пружања регионалне обуке.

- Увести мере како би се обезбедило да обука правосудних органа о високотехнолошком криминалу и електронским доказима буде обавезна. Током пројекта је било очигледно да је обука за судије и тужиоце добровољна у већини области пројекта. То је довело до многих случајева у којима су учесници похађали обуку само веома кратко време током курсева и нису имали пуну корист од обуке која је пружена.

- Увести евиденцију обуке за појединачне судије и тужиоце. Како би се обезбедило да се обука која се пружа судијама и тужиоцима искористи на

најбољи начин, препоручљиво је да се води евиденција о целој обуци коју добијају појединци како би се прикупили информације о потребама за даљом специјализованом обуком и обезбедило да буду обучени прави људи и да се њихове вештине искористе на одговарајући начин.

6. Стратешки приоритет: Финансијске истраге и спречавање и сузбијање превара и прања новца на интернету[205]

Највећи део криминала који укључује интернет и друге информационе технологије усмерен је на остваривање економске добити путем различитих врста превара и других облика привредног и тешког криминала. Тако се стварају и циркулишу на интернету велики износи користи проистекле из кривичног дела.

Стога финансијске истраге које су усмерене на тражење, трајно и привремено одузимање имовине проистекле из кривичног дела и мере за спречавање превара и за спречавање и сузбијање прања новца на интернету треба да постану стратешки приоритет.

Владе треба да размотре следеће мере:

- Успоставити платформу на интернету за подношење пријава од стране јавности о превари на интернету и о високотехнолошком криминалу уопште. Коришћење стандардизованих образаца пријава омогућиће бољу анализу претњи и трендова, криминалних послова и организација, као и уобичајених модела новчаних токова и прања новца. То ће олакшати мере кривичних правосудних органа и финансијских обавештајних служби за гоњење починилаца кривичних дела и трајно и привремено одузимање имовине проистекле из кривичног дела. Платформа треба да врши и превентивне функције (подизање свести и образовање јавности, упозорења о претњама, инструменти и савети). Што су домаће платформе усклађеније с платформама других земаља и подручја, то ће се више олакшати регионалне и међународне анализе и деловање.

[205] Ibid.

- Промовисати проактивне паралелне финансијске истраге приликом истраге високотехнолошког криминала или кривичних дела која укључују информационе технологије/интернет. То захтева повећану међуагенцијску сарадњу између органа надлежних за борбу против високотехнолошког криминала и за финансијске истраге као и финансијских обавештајних служби. Такву међуагенцијску сарадњу може олакшати заједничка обука.

- Направити поуздане форуме (домаће и регионалне) за размену информација између јавног и приватног сектора о претњама рачунарским системима у вези са финансијским сектором. Домаћи форуми треба да буду на располагању кључним заинтересованим странама (као што су представници финансијског сектора, пружаоци интернет услуга, јединице за борбу против високотехнолошког криминала, финансијске обавештајне службе, тимови за реаговање на рачунарске безбедносне инциденте).

- Успоставити правни оквир за привремено и трајно одузимање имовине проистекле из кривичног дела и дигиталних средстава, као и за спречавање прања новца преко интернета. То треба да обухвати дигитална средства као што је е-новац и виртуелне валуте. Правила, прописи и процедуре за спречавање прања новца треба да се примењују и на системе за плаћање преко интернета.

7. Стратешки приоритет: Сарадња између органа за спровођење закона и пружалаца интернет услуга[206]

Сарадња између органа за спровођење закона и пружалаца интернет услуга (ИСП) и других лица из приватног сектора битна је за заштиту права корисника интернета и за њихову заштиту од криминала. Делотворне истраге високотехнолошког криминала често нису могуће без сарадње ИСП. Међутим, таква сарадња треба да узме у обзир различите улоге органа за спровођење закона и ИСП, као и права корисника на приватност.

[206] Ibid.

Унапређена сарадња органа за спровођење закона и ИСП и размена информација између јавног и приватног сектора у складу са прописима о заштити података треба да постане стратешки приоритет.

Владе треба да размотре следеће мере:

- Установити јасна правила и процедуре на домаћем нивоу за приступ органа за спровођење закона подацима које поседују ИСП и друга лица из приватног сектора у складу са прописима о заштити података. Јасан правни основ у складу са одредбама процесног права и заштитним механизмима и условима Будимпештанске конвенције о високотехнолошком криминалу помоћи ће да се испуне захтеви у погледу људских права и владавине права.

- Неговати културу сарадње између органа за спровођење закона и ИСП. У том погледу основни инструмент су меморандуми о разумевању између органа за спровођење закона и пружалаца интернет услуга. Регионална координација таквих МОР олакшала би способност органа за спровођење закона да спроводе истраге преко регионалних граница на основу сазнања да су у другим земљама и подручјима усвојени слични стандарди.

- Олакшати размену информација између јавног и приватног сектора преко граница. Лица из приватног сектора поседују велике количине података о рачунарским безбедносним инцидентима. Прекогранична размена таквих података помогла би унапређењу безбедности информационе инфраструктуре, као и истрази починилаца кривичних дела. Владе треба да размотре законодавство и закључивање споразума који омогућавају размену информација између јавног и приватног сектора и да подстичу развијање смерница за олакшавање размене информација унутар и преко граница, укључујући процесне, техничке и правне заштитне механизме и заштитне механизме у смислу заштите података.

8. Стратешки приоритет: Ефикаснија регионална и међународна сарадња[207]

Високотехнолошки криминал и електронски докази по природи су транснационални, те стога захтевају ефикасну међународну сарадњу. Потребно је неодложно деловање да се обезбеде електронски докази у иностраним јурисдикцијама и да се обезбеди обелодањивање таквих доказа. Међутим, неефикасност међународне сарадње, нарочито међународне правне помоћи, и даље се сматра једном од главних препрека које спречавају делотворну акцију против високотехнолошког криминала.

Стварање ефикасније међународне сарадње по питању високотехнолошког криминала и електронских доказа треба да буде стратешки приоритет.

Владе треба да размотре следеће мере:

- Искористити могућности Будимпештанске конвенције о високотехнолошком криминалу и других билатералних, регионалних и међународних споразума о сарадњи у кривичним стварима.

- Обезбедити обуку и размену најбољих пракси. Органи надлежни за сарадњу полицијских и правосудних органа треба да се укључе у домаћу, регионалну и међународну обуку и размену најбољих пракси. То треба да олакша сарадњу засновану на поверењу.

- Оценити делотворност међународне сарадње. Министарства правде и унутрашњих послова и тужилаштва треба да прикупљају статистичке податке о захтевима за међународну сарадњу у вези са високотехнолошким криминалом и електронским доказима, укључујући врсту захтева за помоћ, благовременост одговора и коришћене процедуре. То треба да помогне да се идентификују добре праксе и уклоне препреке за сарадњу.

- Ојачати делотворност контакт тачака доступних 24 сата дневно, 7 дана у недељи. Такве контакст тачке успостављене су у свим земљама и подручјима

[207] Ibid.

у складу са чланом 35. Будимпештанске конвенције, али треба да се унапреди њихова улога и можда треба да постану проактивније и потпуно функционалне.

- Редовно прикупљати статистичке податке о контакт тачкама доступним 24 сата дневно, 7 дана у недељи, и другим облицима међународне сарадње и преиспитивати њихову делотворност.

Иако су земље учеснице овог пројекта усвојиле стратегију за борбу против високотехнолошког криминала још 2013. године, од тада се ни у једној од тих земаља за период од скоро 10 година, није много тога променило.

Земље које су усвојиле Декларацију за бробу против високотехнолошког криминала, показале су заинтересованост за даљи напредак по питању компјутерског криминалитета, али реализација предвиђених стратешких приоритета развија се спорим темпом. С обзиром да су информационо-комуникациони системи напредовали за период од 10 године енормном брзином, а да за то време земље стагнирају у погледу спровођења предвиђених приоритета и циљева у погледу борбе са високотехнолошким криминалом, долазимо до закључка да не само да не идемо у корак са развојем информационих система, већ увелико каснимо.

Као помак у овој области Влада Републике Србије је 2018. године, донела стратегију за борбу против високотехнолошког криминалитета за период од 2018-2023. године. Стратегија представља наставак и проширење активности којима је циљ јачање ефикасности свих субјеката у области сузбијања високотехнолошког криминала у Републици Србији. Посебно је усмерена на наставак усклађивања законодавства с међународним стандардима, даље унапређење капацитета носилаца борбе против високотехнолошког криминала, унапређење превентивног и проактивног приступа друштва у сузбијању свих облика криминала у тој области, унапређење интересорне

сарадње у друштву, као и сарадње Републике Србије на регионалном и међународном нивоу у области високотехнолошког криминала.[208]

Поменута Стратегија Владе за борбу против високотехнлошког криминала, донета је 2018. године, а за период од 2018-2023.године, како до сада нисмо имали конкретну дефиницију компјутерске крађе у нашем законодавству, као ни издвојено дело компјутерске крађе у кривичном законику, иако су у глави XXV уређена кривична дела која се тичу компјутерског криминалитета и где се нека од њих могу применити на компјутерску крађу, у зависности од околности случаја, видећемо да ли ће РС до краја 2023. године, предузети неке мере по питању темељнијег регулисања компјутерске крађе и њених појавних облика, као и да ли ће је као такву уврстити у кривично законодавство, и предузети друге неопходне мере, у погледу откривања извршиоца ове врсте компјутерског криминалитета и система заштите, који би предупредили да уопште и дође до настанка овакве врсте кривичних дела. Због тога је у погледу компјутерске крађе, релизација оваквих стратегија, веома значајна.

IV РАЗЈАШЊЕЊЕ И ДОКАЗИВАЊЕ КОМПЈУТЕРСКЕ КРАЂЕ

Комплексност разјашњења и доказивања компјутерског криминала, у конкретном случају компјутерске крађе може бити веома велика. Како је предузимање појединих опретивно-тактичких и истражних радњи у криминалистичкој обради условљено конкретном оперативном ситуацијом, односно њеним објективним, субјективним и другим елементима, потребно је указати да се подручје могућег одвијања компјутерског криминала, односно компјутерске крађе, може поделити на три типична сегмента, који у значајној мери опредељују оперативну ситуацију:[209]

- Мрежа рачунарских система (глобална рачунарска мрежа), која покрива шира географска подручја и повезује више рачунарских система, са бројним терминалима, персоналним рачунарима и интерним и екстерним коринисцима, [210]

[208] "Службени гласник РС", број 71 од 25. септембра 2018. – СТРАТЕГИЈУ за борбу против високотехнолошког криминала за период 2019–2023. године,
[209] С. Петровић, 2000. оп.цит., стр.307.
[210] Ibid..

- Локална рачунарска мрежа, која покрива ужи географски простор (најчешће један или неколико објеката, са одређеним бројем терминала, персоналних рачунара и, углавном, интерних корисника,[211]
- Ограничен број персоналних радних станица и интерних корисника, који могу, али не морају бити повезани у мини локалне мреже, а оне зависно од примењеног облика огранизације, могу покривати неколико просторија, један спрат или вертикалу објекта.[212]

Разјашњење компјутерског криминалитета и саме компјутерске крађе у првом подручју (глобалне рачунарске мреже и бројни интерни и екстерни корисници), због броја и сложености техничких и логичких веза, броја потенцијалних извршилаца и њихове распрострањености на широком географском подручју, представља енорман задатак који се мора водити као пројекат са компетентним стручњацима за свако појединo подручје, јер једино се тако на прави начин може осмислити, организовати, синхронизовати и водити једна овако сложена акција. При томе, учинилац може бити било ко и било где, укључујући и иностранство, а тежина учињеног кривичног дела може бити екстремно велика. [213]

У другом подручју (локалне рачунарске мреже), проблем је нешто једноставнији, али још увек довољно сложен да би постојала изразита потреба за организованом и професионалном криминалистичком обрадом. Извршилац ће вероватно бити унутар организације, но његово откривање може ипак бити врло тешко.[214]

Трећи сегмент представља посебан проблем. Због широког распростирања јефтиних персоналних рачунара, са употребом софтвера, који су далеко од тога да се могу сматрати заштићеним, проблем се везује уз број и шаренило оперативних система, програмских језика и разноразних апликација. Док поједина кривична дела у оваквом амбијенту могу бити од релативно малог значаја, њихова фреквенција може бити забрињавајућа. [215]

Због свега овога, представници надлежног државног органа би на пријаву оваквог деликта, који за њих предствља основану сумњу да је извршено кривично дело, морали

[211] Ibid.
[212] Ibid.
[213] Ibid.
[214] Ibid, стр.308.
[215] Ibid.

реаговати, пре свега у складу са криминалистичким начелима брзине и оперативности, како би се спречили информациони дефицит, могућност уништења материјалних трагова и припремање ефикасне лажне одбране. При томе, њихова основна обавеза би била да у преткривичном поступку утврде чињенично стање и да прикупе и сачувају доказе потребне за покретање кривичног гоњења једног или више учинилаца кривичног дела. [216]

Закључак је јасан, нова времена траже и нову врсту полицајаца способних да проналазе доказе у рачунарима, рачунарским мрежама, магнетним медијима и софтверским пакетима. Они морају бити добро припремљени да би се успешно могли супротставити компјутерској крађи и самом компјутерском криминалитету и криминалцима који га извршавају. [217]

Ово утолико пре што криминалци ове врсте, као и сви други корисници, теже да максимално искористе предности нове технологије и усаврше све илегалне активности. Нажалост њихове акције далеко превазилазе могућности полиције да ефикасно одговоре на овај изазов. [218]

Из наведених разлога, разјашњење проблема компјутерске крађе и самог компјутерског криминалитета, који је у суштини мултидисциплинарни проблем, мора се радити тимски, при чему ће бити неопходно да у тиму, поред криминалистичких стручњака, буду укључени зависно од конкретног случаја и стручњаци, за поједине области информатике. [219]

Основна структура тима, са потребним знањем за истраживање ове врсте злоупотреба приказана је у наредној табели:[220]

[216] Ibid, стр. 309.
[217] Ibid, стр. 311.
[218] Ibid.
[219] Ibid.
[220] Ibid.

	Компјутер	Контрола	Истрага
Специјалисти	70%	15%	15%
Контролори	10%	75%	15%
Оперативни радници	10%	10%	80%

Табела 1. Структура тима са потребним знање за истраживање компјутерских злоупотреба

Ова сарадња би морала почети још у фази примања пријава од стране жртве. Пријаву би морао примити или специјализовани оперативац (са криминалистичким и информатичким знањем) или класичан оперативац у присуству информатичара. Ово због тога што оваква врста пријаве не би се смела узимати на устаљен начин, већ у оквиру детаљног разговора са оштећеним, уз максимално разјашњење евентуално присутних нејасноћа, при чему би свакако требало узети у обзир и све оно што је оштећени припремио у усменој или писменој форми, а посебно у циљу што прецизнијег и потпунијег уобличавања пријаве, његове претпоставке у односу на извршено дело и потенцијалног учиниоца. [221]

После примања пријаве оперативни радник и информатичар би морали одмах заједнички изанализирати прва сазнања, проценити ситуацију и уобличити могуће верзије чињеничног стања. У оквиру постављања верзија требало би планирати и све неопходно оперативно-тактичке и истражне радње, које би се морале обавити да би се проверили наводи пријаве и дошло до доказа о (не)постојању дела и учиниоца. У фази планирања разјашњавања ове врсте компјутерског криминалитета, свакако треба предвидети и формирање тима за реализацију планираног задатка. [222]

Тим би требало да чине: руководилац тима са општом одговорношћу, оперативни радници упућени у криминалистичку обраду и процедуре за руковање доказним материјалима, руководилац информатичке службе и зависно од конкретног случаја, стручњаци за финансије и рачуноводство, као и информатичари разних профила (специјалисти за хардвер, за системски и апликативни софтвер, стручњаци за комуникације,

[221] Ibid, стр. 312.
[222] Ibid.

оператери на систему и др.). Према потреби у екипу могу бити укључена и униформисана службена лица.[223]

Чланови тима би требали, између осталог, заједнички да разјасне евентуално присутне недоумице везане за потпуно разумевање и правних и техничких апстракта решавања проблема и утврде јасне спецификације доказа, који ће се прикупљати, имајући у виду чињеницу да вероватно неће бити могуће надокнадити оно што се пропусти. Посебно треба избегавати занемаривање одређених процедура или доказа потребних да би се доказни материјал на суду био прихваћен. Овакав приступ ће елиминисати каснију конфузију и могућу дисквалификацију материјала. Уз све ово, било би веома корисно да сви чланови тима у одређеној мери разумеју правну и информатичку терминологију и технологије и криминалистичке и аутоматске обраде података. [224]

Такође је веома важно да план садржи и разумну процену времена потребну за извођење целокупне ситуације. При томе треба бити великодушан у процени, посебно ако се планира преузимање рачунарског центра уз обустављање његових редовних функција. Процена времена ће бити неопходна како би се корисници упозорили на време током којег им систем неће бити на располагању и како би на бази тога могли предузети одговарајуће мере у циљу радног прилагођавања новим условима. Одлука о комплетном преузимању рачунарског центра и веома детаљне и прецизне анализе из простог разлога што штета која због тога може настати може увелико превазићи штету изазвану криминалним делом које се истражује. [225]

У оквиру припремних радњи свакако би требало обезбедити и неопходне носиоце података, па се тим мора благвремено снабдети довољним бројем дискова и трака за копирање доказног материјала. Такође ће бити неопходан и адекватан прибор за обележавање тог материјала. [226]

Примену оперативно-тактичких радњи и мера и истражних радњи, које подразумевају излазак на лице места и његово обезбеђење, вршење увиђаја, прикупљање

[223] Ibid.
[224] Ibid, стр. 312-313.
[225] Ibid, стр. 313.
[226] Ibid.

обавештења, претрес, реконструкцију и вештачење, привремено одузимање предмета, испитивање окривљеног и саслушање сведока, присмотру, праћење и легитимисање, потребна лишења слободе и др., би требало спроводити по познатим криминалистичким начелима уз обавезно прилагођавање специфичностима трагова и предмета компјутрске крађе и компјутерског криминалитета уопште, водећи строго рачуна о процесним одредбама, како се не би довела у питање релевантност пронађених трагова и предмета.[227]

С тим у вези, иако је РС напредовала на овом пољу и донела Закон којим ближе уређује организацију и надлежност државних органа у борби против високотехнолошког криминала, још увек има простора за даљи рад, нарочито у погледу запослених у служби за борбу против високотехнолошког криминала, њихове обучености, знања, као и способности и свих потребних материјалних средстава за брзо реаговање, у што краћем периоду од тренутка пријаве извршења дела.

Важно је у тимовима у Служби за борбу против високотехнолошког криминала, имати строго обучена лица, не у физичком смислу, већ у интелектуалном, а везано за област информационих технологија, тако да држава треба да размотри опцију, да у органима МУП-а, запосли или повећа број запослених IT стручњака или информатичара, а који ће искористити своје знање из ове области, тако што ће моћи адекватно да реагује у одређеном временском интервалу, где још увек постоји шанса за откривање извршиоца кривичног дела.

Такође, напомињем да закон организацији и надлежности државних органа за борбу против виоскотехнолошког криминалитета, предвиђа да тужиоци и судије, у оквиру посебних одељења морају имати информатичка знања, како би могли да обављају своју функцију у складу са материјално-процесним законодавством, те је у том случају неопходно, организовати семинаре, курсеве или школе права из ове области, како би надлежни органи за ову врсту криминала, стекли потребно знање за поступање или постојеће унапредили, имајући у виду чињеницу којом се брзином развијају информационе технологије. Требало би најмање једном у 6 месеци или годину дана, упућивати запослене у надлежним органима на усавршавање у овој области, а нарочито треба водити рачуна о

[227] Ibid.

томе ко ће им и на који начин преносити знање. Таква врста усавршавања не треба да се ослања само на тумачење постојећих законских норми, као и на примену истих, већ и на презентациони приказ како се врше оваква дела, на шта је најзначајније обратити пажњу, који је временски рок деловања након извршења дела како би се дошло до неких материјалних доказа итд...

V СТАТИСТИКА ПРИЈАВЉЕНИХ КРИВИЧНИХ ДЕЛА ИЗ ОБЛАСТИ КОМПЈУТЕРСКОГ КРИМИНАЛА/КОМПЈУТЕРСКЕ КРАЂЕ У РС

Високотехнолошки криминал је у сталном порасту у Србији, тако да је држава била принуђена да због нарастајућег броја криминалних дела повезаних са високотехнолошким криминлом и у складу са потписаном Конвенцијом о високотехнолошком криминалу, предузме одговарајуће мере ради ради побољшања ефекта борбе против овог облика криминала.

Према Закону о организацији и надлежности државних органа за борбу против високотехнолошког криминала из 2005. године, формирана су 2006. године, посебна одељења за борбу портив високотехнолошког криминала у оквиру Републичког јавног тужилашва, МУП-а и Вишег суда у Београду.

У посебном одељењу – Посебно тужилаштво за борбу портив високотехолошког криминала од њеног оснивања до 2015.године, број уписаних предмета у току године је у сталном порасту, почевши од 179 предмета у 2007. години, до 2074 предмета у 2015. години, према графикону 3.

Графикон 3 – Преглед броја уписаних предмета у Посебном тужилаштву за борбу против високотехнолошког криминала за период од 2007-2015.године – извор: А.Ђукић, Безбедност-Крађа идентитета - облици, карактеристике и распрострањеност, стр. 114.

На основу броја уписаних предмета по годинама и уз претпоставку да се овакав тренд настави, са вероватноћом се може очекивати да ће се до краја 2030. године, овај број повећати чак десетоструко, ако не и више.

Због нарастања броја криминалних дела у овој области и недовољне садашње кадровске попуне посебног јавног тужилаштва (тужилац, два заменика тужиоца и три помоћника тужиоца), а ради јачања капацитета органа, предвиђено је да се ово одељење кадровски ојача са још два заменика тужиоца и још два помоћника тужиоца.[228]

Из структуре кривичних дела према подацима за четворогодишњи период од 2012-2015.године, **<u>од укупно 766 поднетих кривичних пријава, само 125 пријава (16,3%) поднето је за кривична дела из главе XXVI КЗ (кривична дела против безбедности</u>**

[228] А. Ђукић, оп.цит., стр. 115.

рачунарских података), остале пријаве (83,7%), поднета су за кривична дела из других подручја КЗ, у којима је коришћен рачунар или рачунарска мрежа.

Како наш кривични закон не познаје компјутерску крађу, као ни њене појавне облике као посебна кривична дела, у конкретном случају, а у зависности од околности, примењују се одредбе којима су регулисана кривична дела против безбедности рачунарских података (глава XXVI КЗ-а), и то углавном, кривична дела Неовлашћен приступ рачунарским мрежама (чл. 302.) и Рачунарска превара (чл. 301) , као и друга дела које нормира КЗ, а које не спадају у кривична дела против безбедности рачунарских података. У зависности од ситуације, то могу да буде Превара (чл. 208), Фалсификовање и злоупотребу платних картица (чл. 255 ст. 4), Неовлашћена употреба туђег пословног имена и друге посебне ознаке робе или услуга (чл. 233). А када је реч о физичкој крађу рачунара и рачунарске опреме, примењују се кривична дела Крађа (чл. 203.) и Тешка крађа (чл. 204).

За кривична дела директно повезана са безбедношћу рачуанрских података (глава XXVI КЗ-а), највећи број пријава поднет је за неовлашћен приступ рачунарским мрежама (чл.302 КЗ-а) и за компјутерске преваре (чл. 301 КЗ-а) – око 83,2%[229], што нас наводи на закључак да су под ова кривична дела подведена и дела из области компјутерске крађе, тачније, крађе идентитета, крађе података, лозинки и кодова, јер наш КЗ не познаје посебно ове врсте кривичних дела.

Ако се упореди број извршилаца кривичних дела са бројем кривичних дела, може се закључити да су дела која су процесуирана због коришћења рачунарске технике, извршили појединци.

[229] Ibid, стр. 116.

ЗАКЉУЧАК

Компјутерска крађа, представља глобални проблем који не заобилази ни једну државу и који је врло распрострањен последњих година због енормног напретка комуникационо-информационих технологија. Има транснационални карактер, што нужно имплицира да је за сузбијање овог проблема неопходна добра међудржавна сарадња, нарочито због специфичности кроз које се огледа овај облик компјутерског криминалитета, а једна од њих је управо могућност извршења дела појединих облика компјутерске крађе, уколико је извршлац у једној држави, а жртва у другој, што у том случају, значи, да извршилац предузима радњу извршња дела из једне земље, место извршења дела може да буде у другој земљи, последица дела у трећој, а да жртва дела, буде у некој четвртој земљи, те је с тога неопходно, пре свега озбиљније и детаљније се посветити овом облику криминалитета на међународном плану.

На међународном, али и на националном плану јесу усвојени акти који представљају инструмент за „борбу“ против високотехнолошког криминала. Међународни и национални инструменти инкриминишу поједина кривична дела из области високотехнолошког криминала, уређују ближу међународну сарадњу, али недовољно, с обзиром на брзину којом се развијају информационе технологије и на доступност исте широком кругу људи у свим деловима света.

Иако држава улаже напоре у борби против компјутерског криминалитета, још увек та заштита није задовољавајућа, нарочито у погледа компјутерске крађе, као посебног облика компјутерског криминала, а која је распрострањена и више него што можемо да претпоставимо, из разлога постојања високе тамне бројке, која не само да би требало да забрињава законодавце, већ и остале државне органе, грађане, па и саме медије, који би требало да искористе свој публицитет да упозоре грађане како и на који начин могу сами да се заштите, а да претходно прибаве информације у погледу начина и могућности заштите од компјутерске крађе и да уколико такви системи не постоје или нису поузадни и адекватни, о томе, обавесте грађане и уједно упозоре државне органе на пропусте који могу да доведу до екстремних последица, што је веома важно, с обзиром на тренутну националну легислативу, која је у погледу конкретно компјутерске крађе врло неодређена, а компјутерска крађа као посебно кривично дело нерегулисана.

Оно што је интересантно и што је немогуће не приметити, јесте чињеница, да је последњих пар година у Србији коришћење компјутерске технике достигло велике размере.

Основани су информациони системи у органима управе, органима унутрашњих послова, заводима за статистику, здравственим установама, универзитетима, факултетима, што је апсурд, јер је држава оваквим „електронским напретком“ ставила све податке својих грађана који су од нарочитог значаја, условно речено „на тацни“ професионалним хакерима, а без да има адекватно национало законодавство које се тиче компјутерске крађе, која је само делимично индиректно уврштена у кривична дела против безбедности рачунарских података.

Имајући у виду, брзину, којом се развијају и напредују комуникационо-информационе технологије, електронски системи, као и чињицу да све више грађана приступа коришћењу електронских портала и разноразних апликација, које евидентирају како личне, тако и пословне податке, с обзиром да је држава РС достигла тај стадијум и дала себи за право да обавеже грађане да своје личне податке морају изложити ризику да истима приступи неко други, без да имају избора (електронске базе података, потенцирања преласка на електронски приступ и комуникацију са државним органима итд.)

С тим у вези, не смемо занемарити негативну страну, оваквог „електронског напредовања", и оправдавати оваква поступања чињеницом да електронизација чини живот лакшим, само зато што грађани из своје удобне фотеље, могу предузимати одређене радње, како оне које се тичу посла, тако и оне приватног карактера, без да су свесни ризика који наступа у таквим ситуацијама. Веома је важно да сами грађни буду опрезнији и одговорнији, колико је то у њиховој моћи, приликом употребе информационо-комуникационе технологије и да се више интересују за ову тему, ради своје личне безбедности. Док су државни органи у обавези да обезбеде својим грађанима адекватнији систем заштите, не само јер енормном брзином напредују комуникационо-информационе технологије, већ и због чињенице да је држава та, која чини личне податке својих грађана лако доступним извршиоцима ове врсте криминалитета.

С обзиром на такву тренутну ситуацију, неопходно је, макар упознати грађане са ризицима, који могу да настану (уколико своје податке електронски евидентирају), као и са одређеним системима заштите, приликом коришћења интернета и електронских апликација и сајтова.

Осим што би требало да грађани сами буду обазривији приликом коришћења информационо-комуникационих средстава, макар у ситуацијама које су последица њихових личних одлука и држава мора да се побрине за одређени систем заштите, ради безбедности својих грађана, а нарочито из разлога јер је држава иницијатор за електронско функционисање истих са државним органима, а пређутно и са другим институцијама и организацијама.

Грађани РС, као и грађани других земаља које су незаштићене у овој области, нису ни свесни ризика, које са собом носи коришћење информационох технологија.

Без обзира на постојеће међународне и националне акте, који уређују проблем високотехнолошког криминала, закључак је да постоји простор за даљи рад на међународном и националном законодавном плану пратећи потенцијалне ризике и актуелне околности, а све ради адекватне заштите од компјутерске крађе и генерално компјутерског криминалитета.

Литература

- Димитријевић, П., Право информационе технологије, Internet Law, Sven, Ниш, 2011.;
- Димовски Д., Компјутерски криминал – Зборник радова Правног факултета у Нишу, Правни факултер, Центар за публикације, 2010.године, стр. 195-212.;
- Др Николић - Ристановић В., Др Костантиновић– Вулић С., Криминологија, издавачко-графичко предузеће ,,Прометеј", Београд 2018.;
- Јовашевић Д. (коаутор Хашимбеговић Т.), Кривичноправна заштита безбедности рачунарских података – реферат поднет на саветовању: ’’Злоупотребе информационих технологија’’ – ЦД Зборник радова, Тара, 2004. године;
- Лепојевић -Ковачевић М., Лепојевић Б., Међународни стандарди у супротстављању компјутерском криминалу и њихова примена у Србији, Зборник IKSI, 1-2/2007-Б.;
- Мегатренд Универзитет, Факултет за право, јавну управу и безбедност – ФДУА – Право и нове технологије, Београд Лутовац С., Рачић.Ј.– Компјутерски криминалитет као савремени облик криминалитета - Стручни чланак, 2021.године,, одобрен 15.09.2021.године;
- Павловић М., Тошић Д. - Кривичноправна заштита безбедности рачунарских података - стручни рад, 2017. године. Вол.8.бр. 1, стр. 41-53.;
- Петровић С., Компјутерски криминал, Војноиздавачки завод, Београд, 2004;
- РС-Министарство унутрашњих послова -Управа за полицијско образовање-Висока школа унутрашњихпословау сарадњи са Ханс Зајдел фондацијом – Зборник радова -Међународна научностручна конференција, Сузбијање криминала иевропске интеграције,с освртом нависокотехнолошки криминал, Лакташи, 28–30. марта 2012.;
- Ђукић, А. (2017). Безбедност - Крађа идентитета-облици, карактеристике и распрострањеност, Интердисциплинарни научни часопис Војно дело, бр.3;
- Петровић, С. (2000). Компјутерски криминал. Београд: Министарство унутрашњих послова РС - Уредништво часописа ,,Безбедност" и листа ,,Полицајац";
- Meklur, S., Šambri, Dz., Kurtc, Хакерске тајне: заштита мрежних система, превод Смиљанић, Д., Шућур, М., (2006), Београд;
- Violino, B. (1995). HIGH-TECH THIEVES, Information week, pp. 529;
- Murphy, J. (1995). RAM RAIDERS, Computer Weekly, pp. 2 -32.
- Константиновић Вилић, С., Николић Ристановић, В.,. Костић, М. (2009). Криминологија, Ниш: Пеликан принт, стр. 14.
- Wilder, C., Violino, B (1995). ONLINE THEFT, InformationWeek pp. 30
- Cifas, ,,Identity Fraud", https://www.cifas.org.uk/identity_fraud;
- РСЗ Употреба информационокомуникационих технологија у Србији, (2016), 12-19.,
- ,,Sajber hronika", Informacija, 16.06.2016. http://www.informacija.rs/Sajber-hronika/Kralj-spama-koji-kompromitovao-pola-miliona-Facebook-naloga-osudjen-na-2-5-godina-zatvora.html;
- ,,Moćni hakerski alati-exploit kits", Informacija, 14.02.2011. http://www.informacija.rs/Virus/Mocni-hakerski-alati-exploit-kits.html;
- Europol, ,,Europe-wide ation targets monez mule schemes", Eurojust Web, 01.03.2016. http:/www.eurojust.europa.eu/press/pressreleases/pages/2016-03-01.aspx;
- Cifras, ,,Money Mules" more likely to be aged under 30", 08.12.2016. https://www.cifas.org.uk/press_centre/monez- mules;

- Najveća krađa u istoriji" – Telegraf, 06.08.2014. http://www.telegraf.rs/hi-tech/internet/1181038-najveca-kradja-podataka;
- Ivanov i dr., Overall statistics for 2015., u Kaspersky Security Bulletin 2015. (Securelist,15.12.2015.), https://securelist.com/files/2015/12/KSB_2015_statistics_FINAL_EN.pdf;
- Infowatch, ,,global data leakage report 2015.", (2016). http://infowatch.com/report2015;
- Europol, ,,Europe-wide ation targets monez mule schemes", Eurojust Web, 01.03.2016. http:/www.eurojust.europa.eu/press/pressreleases/pages/2016-03-01.aspx;
- Cifras, ,,Money Mules" more likely to be aged under 30", 08.12.2016. https://www.cifas.org.uk/press_centre/monez- mules;
- https://www.gradnja.rs/wp-content/uploads/2020/08/Business-Continuity-Disaster-Recovery-Data-Center-1X2STUDIO-05.jpg;
- https://www.021.rs/story/Info/Region-i-svet/317762/Hakeri-napali-institucije-u-BiH-zaposleni-bez-pristupa-racunarima.html;
- https://www.portalanalitika.me/clanak/224774--sajber-kriminal-u-crnoj-gori-krada-indentiteta-ucjene-djecja-pornografija;

Правни акти

- Директива Савета Европске заједнице о правној заштити компјутерских програма-објављена у Службеном листу Европске заједнице бр. Л 122/42 од 17. маја 1991. године;
- Закон о електронским комуникацијама,,,Сл. гласник РС“, бр. 44/2010, 60/2013 - одлука УС, 62/2014 и 95/2018 - др. закон;
- Закон о информационој безбедности,,,Сл. гласник РС“, бр. 6/2016, 94/2017 и 77/2019;
- Закон о организацији и надлежности државних органа у сузбијању организованог криминала, тероризма и корупције,,,Сл. гласник РС“, бр. 94/2016 и 87/2018 - др. закон;
- Закон о потврђивању конвенције о високотехнолошком криминалу, ,,Сл. Гласник РС", бр. 19/2019;
- Закон о спречавању прања новца и финансирања тероризма, „Сл. гласник РС“, бр. 113/2017, 91/2019 и 153/2020;
- Законом о кривичном поступку, ,,Сл. гласник РС“, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 - одлука УС и 62/2021 - одлука УС;
- Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала,,,Сл. гласник РС“, бр. 61/2005 и 104/2009;
- Кривичним закоником, ,,Сл. гласник РС“, бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019;
- European Commision, Ciber security report (2014);
- Закон о заштити података личности, ,,Сл. Гласник РС', бр. 7/2018;
- Кривични законик, „Службен весник на Република Македонија" број 80/99, број 4/2002 година, број 43/2003, број 19/2004, број 81/2005, број 60/06, број 73/06, број 7/08, број 139/08, број 114/09, број 51/11, број 135/11 , 185/11, број 142/12, број

166/12, број 55/13, број 82/13, број 14/14, број 27/14, број 28/14, број 115/14 и број 132/14;

- Кривични закон, „Службене новине Федерације БиХ", бр. 36/2003, 21/2004 – испр., 69/2004, 18/2005. 42/210, 56/2014, 76/2014, 46/2016 и 75/2017;
- Кривични законик, „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;
- Казнени закон ХР (НН 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21);
- Кривични закон, „Сл. Гласник Републике Словеније", бр. 95/04- званични консолидовани текст, и 55/08 – КЗ -1;
- Cybercrime@IPA – Заједнички пројекат ЕУ и ЕС за регионалну сарадњу у борби противвисокотехнолошког криминала – Стратешки приоритети сарадње у борби против високотехнолошког криминала, https://rm.coe.int/16802f6a41;
- "Службени гласник РС", број 71 од 25. септембра 2018. – СТРАТЕГИЈУ за борбу против високотехнолошког криминала за период 2019–2023. године;

САЖЕТАК

Завршни – мастер рад на тему „Компјутерска крађа", у уводном излагању базира се на феноменолошку разноврсност компјутерског криминалитета, који као такав нема опште усвојену дефиницију, с обзиром да је реч о новијем облику криминалног деловања, а који се протеком времена све више усавршава, тј. развијају се разне нове методе у деловању и начину понашања – modus operandi, те га је из тог разлога тешко дефинисати јединственим и прецизним појмовним одређењем. Како је реч о области која је новијег добра и која је недовољно истражена, па самим тим разне методе у деловању и начину понашање (а које би могле да се сврстају под окриљем овог облика криминалног деловања), нису преточене у законски оквир, од нарочитог је значаја истражити и изанализирати међународни и национални правни оквир компјутерског криминалитета у генералном смислу, јер се кроз исти индиректно прожима и сама компјутерска крађа, која појмовно постоји само у теоријском смислу, али иста као таква није регулисана адекватно ни међународним, а ни национланим законодавством – те је томе посвећено цело једно поглавље мастер рада. Ради безбеднијег сајбер простора, као и успостављања боље међународне кооперације, са циљем да се овако комплексна област што боље уреди, у мастер раду, осврнула сам се и на међународну и националну праксу у области компјутерске крађе, као и на резултате истраживања и анализе резултата, ове опширне, а тако уско обрађене теме. У завршним цртама рада изнела сам своје закључке настале као последице теоријског, али и истраживачког сагледавања теме компјутерска крађа. Предмет истраживања при изради завршног – мастер рада на тему „Компјутерска крађа“ представља пре свега уочавање глобалног проблема компјутерског криминалитета, као и компјутерске крађе, као једног од најзначајнијих појавних облика компјутерског криминалитета, затим сагледавање правног оквира на националном и међународном нивоу, свеукупност различитих метода у деловању, начину испољавања противправних понашања управљених против безбедности рачунарских података, информационих и компјутерских система, као и резултати истраживања и анализе резултата, кроз упоређивање статистичких података и примера у пракси, који се тичу ове појаве. Циљ истраживања је указивање на то да је овој теми потребно посветити много више пажње, с обзиром да законодавство, како међународно, тако и национално, не иду у корак са временом, у конкретном случају. Имајући у виду

брзину којом се развијају информационе технологије, као и информатичка знања, чија злоупотреба неретко доводи до пораста компјутерског криминалитета, где се као један од појавних облика најчешће јавља компјутерска крађа (где је циљ и/или средство извршења дела компјутер), од изразите је важности указати на чињеницу да је потребно вредно радити на сузбијању овог облика компјутерског криминалита, како би се овакав вид компјутерског криминалитета, у време када је компјутерска технологија на врхунцу, на адекватан начин, уврстио у важеће међународно и национално законодавство. При изради завршног – мастер рада на тему „Компјутерска крађа“ и истраживања на ову тему анализирани су и тумачени и случајеви из праксе, како међународне, тако и националне, уз упоредну анализу на које начине су исти уређени у међународној и националној легислативи, као и какав ефекат, тако легислативно уређене, производе, применом метода компаративне квалитативне анализе.

Као крајњи закључак, након истраживања ове теме, оно што бих истакла, као најзначајније, јесте следеће:

- Међународна и национална легислатива, која уређује област компјутерскогкриминалитета је веома оскудна што се тиче појмовног дефинисања и одређивања компјутерске крађе, као једног од најчешће појавних облика компјутерског криминалитета,
- Како је компјутерски криминалитет област која завређује пажњу целе међународне заједнице, не само једне државе, неопходно је постићи сарадњу на међународном плану, како бисмо се проблему компјутерског криминалитета, односно компјутерске крађе, супротставили на адекватан начин,
- Последњих година у Србији коришћење компјутерске технике достигло је велике размере,
- Основани су велики информациони системи у органима управе, органима унутрашњих послова, заводима за статистику, здравствевним установама, универзитетима, факултетима, те је то један од основних разлога због чега је неопходна адекватна кривичноправна заштита од компјутерске крађе и генерално компјутерског криминалитета, јер су лични подаци грађана РС на овај начи постали доступни извршиоцима компјутерског криминалитета (компјутерске крађе)

Кључне речи: крађа, компјутер, неодређеност, подаци, закон, нерегулисаност, заштита, санкција.

Cyber theft

SUMMARY

The final - master's thesis on the topic "Cyber Theft", in the introductory presentation, is based on the phenomenological diversity of computer crime, which as such does not have a generally accepted definition, given that it is a newer form of criminal activity, which is becoming more and more perfected over time. That is various new methods of action and behavior are developing - modus operandi, and for this reason it is difficult to define it with a unique and precise conceptual definition. As this is a relatively new and under-researched area, and therefore various methods of action and behavior (which could be classified under the umbrella of this form of criminal activity) have not been transposed into the legal framework, it is particularly of importance to research and analyze the international and national legal framework of cyber crime in a general sense, because computer theft itself is indirectly permeated through it, which conceptually exists only in a theoretical sense, but as such is not adequately regulated either by international or national legislation - and a whole chapter of the master's thesis is dedicated to it. For the sake of a safer cyber space, as well as the establishment of better international cooperation, with the aim of organizing such a complex area as well as possible, in my master's thesis, I referred to international and national practice in the field of cyber theft, as well as to the results of research and analysis of the results, these extensive, yet narrowly treated topics. In the final lines of the paper, I presented my conclusions, which were the result of a theoretical, but also a research study of the topic of cyber theft. The subject of research during the preparation of the final - master's thesis on the topic "Cyber theft" is first of all the observation of the global problem of cyber crime, as well as cyber theft, as one of the most significant forms of cyber crime, then an overview of the legal framework at the national and international level, the totality of different methods in action, the manner of manifesting illegal behavior directed against the security of computer data, information and computer systems, as well as the results of research and analysis of the results, through comparing statistical data and examples in practice, which concern this phenomenon. The aim of the research is to point out that this topic needs to be given much more attention, given that the legislation, both international and national, does not keep up with the times, in this particular case. Bearing in mind the speed with which information technologies are developing, as well as computer knowledge, the misuse of which often leads to an increase in computer crime, where

cyber theft (where the goal and/or means of execution is a computer) is one of the most common forms of computer crime, from it is important to point out the fact that it is necessary to work diligently to suppress this form of cyber crime, so that this type of cyber crime, at a time when computer technology is at its peak, is adequately included in the valid international and national legislation. During the preparation of the final master's thesis on the topic "Cyber theft" and research on this topic, cases from practice, both international and national, were analyzed and interpreted.

As a final conclusion, after researching this topic, what I would highlight as the most important is the following:

- International and national legislation, which regulates the area of cyber crime, is very scarce as far as the conceptual definition and determination of cyber theft, as one of the most common forms of cyber crime, is concerned.
- As cyber crime is an area that deserves the attention of the entire international community, not just one country, it is necessary to achieve cooperation on the international level, in order to adequately confront the problem of cyber crime, i.e. cyber theft,
- In recent years, the use of computer technology in Serbia has reached large proportions,
- Large information systems have been established in administrative bodies, internal affairs bodies, statistical institutes, health institutions, universities, faculties, and this is one of the main reasons why adequate criminal law protection against cyber theft and cyber crime in general is necessary, because personal data are of RS citizens became available to perpetrators of cyber crime (cyber theft) in this way.

Key words: theft, Computer, vagueness, The data, The law, Irregularity, Protection, Sanction.

БИОГРАФИЈА

Александра Трифуновић, рођена је 25.04.1996. године у Књажевцу. Завршила је „Књажевачку гимназију" у Књажевцу, друштвено-језички смер 2015. године. Основне студије на Правном факултету у Нишу, уписала је школске 2015/2016 године, на коме је дипломирала 15.09. 2020. године, са просечном оценом 8,43. Школске 2020/2021 уписала је мастер студије на Правном факултету у Нишу, смер унутрашњи послови. Била је полазник „Мобилне правне клинике", која је спроведена од стране Правног факултета Универзитета у Нишу. Учествовала је у пројекту „Практични правници" , спроведен од стране Правног факултета Универзитета у Нишу и Савеза студената Правног факултета. Освојила прво место на такмичењу у симулацији суђења са екипом Правног факултета, одржаном на правнијади (Грчка – Кавос), 2018. године. Завршила тренинг „Мониторинг, извештавање и специфичности кривчних поступака за кривична дела са елементима корупције" и учествовала у мониторингу кривичних поступака у оквиру пројекта „Оснаживање студената правних клиника за праћење суђења за корупцију, спроведеном од стране YUCOM-а (Комитета правника за људска права). Тренутно је уписана у именик адвокатских приправника Адвокатске коморе Ниш и обавља приправнички стаж у канцеларији Обрадовић-Барун. Говори енглески језик и служи се немачким и шпанским језиком.

ИЗЈАВА О ИСТОВЕТНОСТИ

ШТАМПАНОГ И ЕЛЕКТРОНСКОГ ОБЛИКА МАСТЕР РАДА

Име и презиме аутора мастер рада: Александра Трифуновић

Наслов мастер рада: Компјутерска крађа

Ментор: Проф. др Дарко Димовски

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 Компјутерска крађа

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: Александра Трифуновић

У Нишу, _____

Потпис аутора

_____