УНИВЕРЗИТЕТ СВ. КЛИМЕНТ ОХРИДСКИ- БИТОЛА

ФАКУЛТЕТ ЗА БЕЗБЕДНОСТ – СКОПЈЕ

Бојан Димитриевски

КРИМИНАЛИСТИЧКИ И КРИМИНОЛОШКИ КАРАКТЕРИСТИКИ НА КОМПЈУТЕРСКИТЕ ИЗМАМИ ВО РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

(магистерска теза)

Скопје, 2024

Ментор:

Проф. д-р Светлана Николоска
редовен професор на Факултетот за безбедност - Скопје Универзитет „Св. Климент Охридски“ - Битола

Членови на комисија:

1. Проф. д-р Цветко Андреески
редовен професор на Факултетот за безбедност – Скопје Универзитет „Св. Климент Охридски“ - Битола

2. Проф. д-р Миодраг Лабовиќ
редовен професор на Факултетот за безбедност – Скопје Универзитет „Св. Климент Охридски“ - Битола

Датум на одбраната: _____

Датум на промоцијата: _____

Наука на која што се стекнува магистеристерското звање:
Безбедност и финансиска контрола

Апстракт

Во последните децении, и посебно во последните неколку години, компјутерската технологија и Интернетот се развиваат со огромна брзина. Тие навлегуваат во секој дел на општеството и претставуваат средство за забава и исполнување на слободното време, но поважно – средство за извршување на работните обврски, начин на заработка итн. Во секој случај, придобивките од нив се огромни и многу значајни. Сепак, секое добро нешто има и своја темна страна. Па така, во последните години сме сведоци на голем број личности и претпријатија што биле жртви на компјутерски измами. Ваквите измами носат огромни материјални штети, но и штети по психичкото здравје на поединецот, како и штети за целокупното општество. Затоа, превенцијата и сузбивањето на компјутерските измами е од клучно значење за да имаме функционално општество.

Компјутерските измами се карактеризираат со повеќе манифестни облици и начини на извршување, а се дефинирани како вид компјутерски криминал т.е. измами кои се извршуваат со цел да се стекне противправна материјална корист за себе или за друг, со тоа што во заблуда не се доведува лице туку споменатa заблуда се однесува на компјутер што се користи за остварување на измами во кривично-правна смисла. Компјутерот или Интернетот, се извор, предмет, средство, цел или простор на кривичното дело. Компјутерските измами се распространети не само во Република Северна Македонија туку и на светско ниво, па затоа надлежните институции преземаат мерки за нивно сузбивање и превенирање.

Во овој труд ќе се направи осврт на криминалистичките и криминолошките карактеристики на компјутерските измами во Република Северна Македонија, а воедно ќе се осврнеме и на мерките што институциите во Република Северна Македонија ги преземаат против ваквиот вид криминалитет. Со тоа ќе ја покренеме свесноста за важноста на ваквите мерки, со цел да се оствари оптимално функционирање на целокупното општество.

Клучни зборови: компјутерски измами, информатика, карактеристики превенција, сузбивање

Abstract

In recent decades, and especially in the last few years, computer technology and the Internet have been developing at a tremendous speed. They penetrate into every part of society and represent a means of entertainment and fulfillment of free time, but more importantly – a means of performing work duties, a way of earning money, etc. In any case, their benefits are huge and very significant. However, every good thing has its dark side. So, in recent years we have witnessed a large number of individuals and companies that have been victims of computer fraud. Such frauds bring enormous material damages, but also damages to the psychological health of the individual, as well as damages to the entire society. Therefore, the prevention and suppression of computer fraud is of crucial importance in order to have a functioning society.

Computer fraud is characterized by several manifest forms and methods of execution, and is defined as a type of computer crime, i.e. frauds that are carried out with the aim of obtaining an illegal material benefit for oneself or for another, by not misleading a person, but the said deception refers to a computer that is used to commit frauds in the criminal-legal sense. The computer or the Internet is the source, object, means, target or space of the crime. Computer frauds are widespread not only in RSM but also at the world level, so the competent institutions take measures to suppress and prevent them.

This paper will review the criminal and criminological characteristics of computer fraud in the RSM, and we will also refer to the measures that the institutions in the RSM take against this type of crime. With that, we will raise awareness of the importance of such measures, in order to achieve optimal functioning of the entire society.

Keywords: ***computer fraud, informatics, characteristics, prevention, suppression***

СОДРЖИНА

ВОВЕД.....8

ТЕОРЕТСКО-ХИПОТЕТСКА РАМКА.....11

1.Формулација на проблемот на истражување.....11
2. Предмет на истражување.....15
2.1. Појмовно – категоријален апарат..... 18
2.2. Операционализација на проблемот.....21
2.3. Временска рамка на истражувањето.....21
2.4. Дисциплинарно определување.....22
3. Цел на истражувањето.....22
4. Хипотетска рамка.....24
4.1. Општа хипотеза.....24
4.2. Помошни хипотези.....24
5. Методи и техники на истражување.....25
6. Научна и општествена оправданост на истражувањето.....26

ОСНОВИ НА КОМПЈУТЕРСКИОТ ИМОТЕН КРИМИНАЛИТЕТ.....27

1. Компјутерски имотен криминалитет.....27
2. Анализа на препораки од Конвенција за компјутерски криминалитет.....30
3. Појавни облици на компјутерски измами.....32
4. Облици и форми на компјутерски измами.....35
5. Кривично-правна регулираност на компјутерските измами во Република Северна Македонија.....38
6. Анализа на криминални ситуации со компјутерски измами.....40

6.1. Компарација на криминализацијата на компјутерската измама во земјите во регионот.....44
6.2. Земји од Европската Унија.....51

КРИМИНАЛИСТИЧКИ КАРАКТЕРИСТИКИ И КРИМИНАЛИСТИЧКО ИСТРАЖУВАЊЕ НА КОМПЈУТЕРСКИТЕ ИЗМАМИ.....56

1. Криминалистички карактеристики на компјутерските измами.....56
1.1. Компјутерот како средство и објект на криминален напад кај компјутерските измами.....57
1.2. Начини на извршување на компјутерската измама.....58
1.3. Време и период на извршување на компјутерската измама.....60
1.4. Место и простор на извршување.....61
1.5. Организираност на сторителите.....61
1.6. Личноста на сторител.....62
1.7. Личност на жртвата и придонес на жртвата за нејзина виктимизација.....63
2. Криминалистичко истражување на компјутерските измами.....65
2.1 Компјутерска форензика и електронски доказ.....65
3. Последици од компјутерските измами.....69

КРИМИНОЛОШКИ КАРАКТЕРИСТИКИ НА КОМПЈУТЕРСКА ИЗМАМА (ОБЕМ, ДИНАМИКА И СТРУКТУРА).....70

НАДЛЕЖНОСТИ ЗА КРИМИНАЛИСТИЧКО ИСТРАЖУВАЊЕ НА КОМПЈУТЕРСКИТЕ ИЗМАМИ.....77
1. Координација и соработка.....77

ПРЕВЕНЦИЈА ОД КОМПЈУТЕРСКИ ИЗМАМИ.....80
1. Креирање на безбедна лозинка.....82
2. Превенција при онлајн-банкарство и трговија.....83

3. Превенција на phishing.....84
4. Сегашни и идни предизвици.....85
5. Обуки за компјутерска безбедност.....87

ЕМПИРИСКО – АНКЕТНО ИСТРАЖУВАЊЕ.....88
1. Интервју (СВР Скопје).....88
2. Интервју (Анализа на граѓани).....91
3. Дискусија за резултатите од емпириско-анкетното истражување.....96

ЗАКЛУЧОК.....98
ЛИТЕРАТУРА.....103

ВОВЕД

Компјутерскиот криминалитет е вид криминалитет кој се појавува преку различни појавни облици и форми кои врз основа на нивните криминалистички карактеристики се категоризираат во повеќе подгрупи од кои позначајна е групацијата на имотен компјутерски криминалитет. Кај оваа групација на криминалитет значајно е тоа дека како средства на извршување се компјутерските уреди, а нивното извршување се овозможува со користење на компјутерските мрежи и системи. Како посебно кривично дело во македонското казнено законодавство е инкриминирано „Компјутерска измама“ во Главата 23 на Кривични дела против имотот. Главната движечка сила т.е. мотивот е стекнување на имотна корист која е во директна зависност од начинот на извршување, но и времето на криминално делување и организираноста на сторителите.

Во криминолошката литература постои сфаќање дека комјутерскиот криминалитет е дел од имотниот криминалитет. Но, постојат и сфаќања дека се работи за самостоен облик на криминалитет, но и дека тој е дел од организираниот криминалитет. Современата автоматизација на деловното работење со примена на компјутерската техника во областа на стопанството создава поволни можности за финансиски манипулации и незаконски финансиски трансакции врз основа на што се создаваат можности за присвојување на високи финансиски (парични) средства.

Во рамките на овој труд ќе биде изработена анализа на состојбите од досега пријавените сторители на кривичното дело компјутерска измама, а исто така ќе биде направена анализа на начините на извршување, видот и висината на штетите како и на организираноста на сторителите.

Европската Унија континуирано презема активности во областа на сајбер безбедноста и борбата против компјутерскиот криминал. Се чини дека е препорачливо да се вратиме во 1990 – тите, кога беа усвоени првите необврзувачки правни акти за регулирање на овие прашања. Тие побараа имплементација на соодветни мерки, со посочување на конкретни решенија или предлози за нацрт – законските акти, како и развој на стратегии и акциски планови за подобрување на безбедноста во онлајн – просторот. Рамковната одлука на Советот 2005/222/ЈХА од 24 февруари 2005 година за напади врз

информациски системи беше првиот обврзувачки правен инструмент на ЕУ чија цел беше борба против компјутерскиот криминал. Во принцип, документот вклучуваше дефиниции за најрелевантните концепти („информациски систем“, „компјутерски податоци“, „правно лице“ и слично) и ги обврза земјите – членки да го разгледаат нелегалниот пристап до информатичките системи и незаконското мешање во системот како казниви дела. Беше упатено и на одговорноста на правните лица, јурисдикцијата и воспоставувањето мрежа на точки за контакт кои одржуваат 24 – часовна услуга, достапна 7 дена во неделата, за да се олесни размената на информации за напади врз информациски системи. Ограниченият број на кривични дела дефинирани во Рамковната одлука 2005/222, заедно со потребата да се препознаат новите закани, како и намерата да се приспособат регулативите кон новите иницијативи на ЕУ во областа на сајбер безбедноста и да се дополнат за да се дојде до сеопфатното регулирање на оваа тема, на крајот доведе до одлука за развој на нов правен инструмент за компјутерски криминал. Работата на новата регулатива се совпадна со усвојувањето на Договорот од Лисабон, кој овозможи да се користи директивата за регулирање на прашањата за компјутерскиот криминал. (Radoniewicz: 2022)

Според статистиките направени во Холандија, во 2022 се регистрирани 2,2 милиони жртви на компјутерски криминал. Во 2022 година, 15 % од холандското население на возраст од 15 и повеќе години посочиле дека биле жртви на една или повеќе форми на онлајн криминал. Ова одговара на 2,2 милиони луѓе. Повеќето биле жртви на измами, потоа следат хакирање, онлајн закани и вознемирување. Дваесет проценти (официјално) го пријавиле инцидентот во полиција. Статистиката на Холандија (CBS) известила за овој проблем ова врз основа на резултатите од истражувањето за сајбер безбедноста и сајбер криминалот. Истражувањето е спроведено помеѓу август и октомври 2022 година меѓу повеќе од 32 илјади луѓе на возраст од 15 и повеќе години. Во 2022 година, 8 % од населението на возраст од 15 и повеќе години биле жртви на онлајн измами, особено на измама при онлајн пазарување (6 %), 5 % доживеале хакирање, додека 4 % се соочиле со закани и вознемирување преку Интернет. Младите луѓе биле најчести жртви на вториот облик. Помеѓу 15 до 24 – годишниците, секој петти изјавил дека се соочил со закани преку Интернет, малтретирање, следење или срам, т.е. форма на сексуално престапно однесување каде што се дистрибуираат голи фотографии или видеа од жртвата или се закануваат дека ќе бидат дистрибуирани.

За 37 % од жртвите на сајбер криминал, инцидентот во 2022 година довел до помала доверба во другите луѓе, а како резултат на тоа, 30 % се чувствувале или се чувствуваат помалку безбедни. Проблеми со спиењето, депресивни симптоми, симптоми на анксиозност и преживување на инцидентот одново и одново биле споменати од 7 до 8 % од жртвите. Ако ги набљудуваме специфичните форми на онлајн криминал, последните поплаки биле пријавени од жртви на онлајн закани и вознемирување повеќе од двојно почесто од жртвите на другите онлајн злосторства. Над половина од жртвите на компјутерски криминал го пријавиле некаде: во полиција, професионални социјални работници, членови на семејството, роднини или пријатели. Удел од 21 % пријавиле што им се случило во полиција. Речиси сите пријавувања за компјутерски криминал во полиција резултираа со официјален полициски извештај (19 %). Најчесто наведената причина за непријавување на инцидентот во полиција (и поднесување пријава) е тоа што на жртвата не ѝ паднало на памет или жртвата не го сметала за важно, а некои мислеле дека пријавувањето би било бесполезно. (https://www.cbs.nl/en-gb/news/2023/19/2-2-million-cybercrime-victims-in-2022)

Компјутерските измами не се непознати за повеќето држави во регионот и светот, а Република Северна Македонија исто така не е поштедена од нив. Станува збор за кривично дело што доведува до многу опасности за жртвите, кои се однесуваат на претрпена материјална штета, но и психичка штета која се манифестира со страв и недоверба. Како најкористени и најпопуларни облици се фишинг, инженеринг и фарминг. Надлежните институции во регионот и светот преземаат соодветни мерки за нивна превенција и санкционирање, како што е случај и во Република Северна Македонија. Сепак е неопходно и понатаму ова кривично дело да се истражува во континуитет со цел да се следат состојбите и опасностите во Република Северна Македонија. Во врска со ова можеме да се повикаме на претходни истражувања и трудови од оваа област, на пример: Сулејманов (2003), Ачкоски (2012), Грујиќ (2018), Николоска (2013) и други.

Воедно, важно е да се нагласи дека МВР е надлежно за откривање, расветлување, докажување и превенција на компјутерскиот криминалитет. Поради тоа, ќе бидат наведени и штетите или стекнатата противправна имотна корист од компјутерски измами, кои се објавени во извештаите на МВР и се однесуваат за последните пет години, што ќе биде, воедно, и временската рамка на истражувањето.

Ќе биде направена и анализа на состојбите од досега пријавените сторители на кривичното дело „Компјутерска измама“ и ќе се анализираат начините на извршување, видот, висината на штетите и најчестите причини на извршување на кривичното дело, како и организираноста на сторителите.

ТЕОРЕТСКО – ХИПОТЕТСКА РАМКА

ФОРМУЛАЦИЈА НА ПРОБЛЕМОТ НА ИСТРАЖУВАЊЕ

Со напредувањето на технологијата, општеството добива многубројни нови придобивки. Една од нив е развојот на информатичката технологија, која го наоѓа своето место во сите сфери на општественото функционирање. Олеснувањата и придобивките од развојот на информатичката технологија се многубројни, но сето тоа не е без ризици и опасности. Имено, развојот на оваа технологија носи и нови проблеми и предизвици што претходно му биле непознати на општеството, на пример, компјутерските измами.

Секојдневното користење на компјутерите и Интернетот стана неизоставен дел од современиот начин на живот. Денес тие се неразделен дел како од приватниот така и од професионалниот живот на повеќето поединци, но и алатка без која не може да се замисли ниту еден работен ден во институциите и во претпријатијата. Компјутерите и Интернетот станаа потреба како во секојдневниот живот и комуникација, така и во деловниот свет за организација, раководење и комуникација помеѓу деловните субјекти во земјата и странство. Како што информатичката технологија претставува голема придобивка или трета индустриска револуција, така и истата се злоупотребува од страна на поедници и групи кои ги искористуваат своите знаења и вештини за криминогени цели со цел стекнување на финансиска корист на побрз начин, со постоење на голема можност нивните криминални актвности да не бидат откриени и санкционирани. Глобалната комуникациска мрежа создава огромни можности за криминални однесувања при што компјутерот се јавува во улога на средство за извршување на криминална активност или претставува објект на напад на вештите криминалци.

Криминалците ги усовршуваат своите знаења и вештини, но и поголемите можности кои ги даваат компјутерските мрежи и системи континуирано се насочени кон стекнување на вештини во насока на злоупотреба на Интернетот и можностите за брза комуникација, но и злоупотреби кои се овозможени со креирање на нови алатки и злоупотреба на постојните.

Глобалниот виртуелен свет стана погодно место за работење и приватна комуникација и како таков е погоден амбиент за многу луѓе, а со самото тоа во текот на деведесетите години од минатиот век стана многу интересен и за криминалците. Вештите сторители на кривични дела од областа на компјутерскиот криминалитет (или како што уште се нарекува „високотехнолошки криминал“), вешто го искористија Интернетот кој стана „учител на вештини“ за криминалците од другите области и тоа во целиот свет. Ваквата врска на Интернетот и криминалот оформи два типа на високотехнолошки криминал и тоа: напад на мрежа и користење на мрежата како средство и место на извршување за другите криминални активности. Меѓународната соработка помеѓу криминалците е многу олеснета благодарение на Интернетот. Со проширени граници на делување во своите различни појавни облици, високотехнолошкиот криминал денеска поставува нови предизвици со кои се загрозуваат граѓаните, колективната безбедност, како и економската стабилност на многу држави. (Urošević V. i Uljanov S.: 2010).

Корисниците на компјутери во денешно време имаат сè поразвиена свест за потребата од основна безбедност на Интернет. Сепак, темпото на технолошки промени ќе продолжи, а приспособливоста на сајбер - криминалците ќе биде чекор пред останатите и ќе го отежнува имплементирањето на законите. Така, изреката што звучи како клише „мисли глобално, дејствувај локално“, е многу релевантна во контролата на компјутерскиот криминал. (Andriansyah A. 2023)

Во криминолошката литература се посветува внимание на проучување на нови појавни облици и форми на криминалитет каде компјутерот се јавува како главно средство на извршување, а компјутерските мрежи и системи сè повеќе се објект на криминален напад. Во првите дефиниции за компјутерски криминалитет како средство за извршување на кривични дела е компјутерот, а компјутерските системи и мрежи се објект на заштита. Се потенцира употребата на компјутерот при вршења на измами, затајувања или злоупотреби при што целта е присвојување на пари или услуги или вршење на политичка

или деловна манипулација која вклучува и дејствија насочени кон компјутерот. (Bequai A., 1978). Според истражувањата на Константиновиќ Вилиќ и Николиќ Ристановиќ компјутерскиот криминалитет по својот карактер е најблиску до имотниот криминалитет.

Македонскиот криминолог и поранешен судија Сулејманов (Сулејманов З., 2008) во својата книга „Криминологија“ потенцира дека: „Под компјутерски криминалитет се подразбира секое дејствие во кое компјутерот е средство и цел за извршување на кривично дело”. Како појавни облици на компјутерски криминалитет се наведени повеќе криминални поведенија кои се или треба да бидат инкриминирани во националните законодавства, а тоа се: приод во компјутерски систем; компјутерска измама; компјутерски фалсификат; компјутерска шпионажа и саботажа и кражби на време од компјутерски системи.

Како дел од имотниот компјутерски криминалитет се компјутерските измами кои се инкриминирани како посебно кривично дело во Глава 23 Кривични дела против имотот во Членот 251 б, а за првпат ова кривично дело е инкриминирано во 2004 година (Кривичен законик на РМ, Сл. весник на РМ бр. 19/04), како резултат на препораките од Конвенцијата за компјутерски криминалитет од 2001 година.

Република Северна Македонија, како држава што забрзано ги следи трендовите во напредокот на технологијата и глобализацијата, за жал не остана имуна на компјутерските измами. Тоа и се подразбира, бидејќи една држава не постои во изолација, туку е во постојан контакт со глобалните случувања, како позитивни така и негативни. За расветлување на компјутерските измами е надлежен Секторот за компјутерски криминал и дигитална форензика при Министерството за внатрешни работи на Република Северна Македонија.

Компјутерските измами се посебно кривично дело кое има свои криминалистички карактеристики кои треба да се истражуваат и врз основа на добиените сознанија да се креираат тактики и техники за нивно откривање, расветлување и обезбедување на докази кои се прифатливи за правосудните органи во насока на водење на кривични постапки и санкционирање на сторителите.

Од воведувањето на „Компјутерска измама“ како посебно кривично дело, македонската криминалистичка практика бележи повеќе начини на извршување, организираност на сторителите и специфичности околу криминалистичкото истражување

кое е најважно од аспект дека преку процесот на расветлување се добиваат и сознанија за специфичните криминалистички карактеристики и давање одговор на т.н. „златните прашања на криминалистиката“ односно деветте криминалистички прашања клучни за целосно расветлување на криминалните ситуации и покренување на обвинение против сторителите и понатамошна успешна кривична постапка.

Анализата на статистичките податоци релевантни во светски рамки, покажува дека дигиталната технологија и компјутерскиот криминал се одлики на модерниот живот, и тие станаа широко распространети во речиси сите сфери на животот. Околу 60 % од светското население се интернет корисници и глобалното усвојување на дигитални технологии брзо се зголемува. Користењето на интернет на глобално ниво се зголеми за приближно 7 % во текот на една година (од јануари 2020 до јануари 2021), а особено зголемување се должи и на пандемијата на корона вирусот. Според последните податоци, до март 2023 година има повеќе од пет милијарди корисници на Интернет. Тоа доведе до еволуција на криминалното однесување, зголемувајќи ја инциденцата и на компјутерските измами (Andriansyah A.; 2023).

За илустрација, според истражувањата на Internet Crime Complaint Center (IC3) во Соединетите Американски Држави, штетата од компјутерски измами во 2006 година изнесувала 198 милиони долари, во 2007 година е достигнат износ од 239 милиони долари, а во 2008 година тој износ е 264 милиони долари, при што компјутерот се јавува како средство или објект на криминален напад. (The Latest Cybercrime Statistics On The Internet, Tech Watch, http://www.techwatch.co.uk/2008/04/04/the-latest- cybercrime-statistics/)

Според Bratić (Bratić; 2023), во најчестите сајбер напади се вбројуваат: социјален инженеринг, фишинг, преземање податоци во „помин“, „man in the middle“, напад со отфрлено УСБ и малициозен софтвер. Во својот прирачник тој ги опишува наведените напади кои имаат елементи на компјутерска измама и наведува дека поединците можат да се идентификуваат на различни начини, а идентитетите се содржат во документи како возачки дозволи, картички за осигурување, изводи итн. Се подразбира дека лозинките, банкарски податоци и лични податоци не смеат да се споделуваат на Интернет или со други лица. Како заштита од кражба на податоци и нивна злоупотреба, авторот напоменува дека корисно е да се создаваат сложени лозинки, повеќе пати да проверат пред

да се кликнеме на одреден линк, да се користат безбедни wifi- мрежи, VPN, да се исклучува Bluetooth и сл.

Компјутерските измами, посебно нивните криминалистички карактеристики е предизвик да се истражуваат и да се добијат сознанија за тоа кои се најчестите начини на извршување од страна на сторителите (modus operandi), истражување на просторот и на криминално делување (radius operandi) и организираноста на сторителите како и добивање на сознанија за времето на извршување (tempus operandi), посебно времето на криминално делување на сторителите до моментот на нивното откривање и преземање мерки за обезбедување на докази. За компјутерските измами битни се електронските докази и специфичностите во постапката на нивно обезбедување и чување и нивното приспособување за да бидат прифатливи за правосудството.

2. ПРЕДМЕТ НА ИСТРАЖУВАЊЕ

Предметот на истражување на овој магистерски труд се криминалистичките карактеристики на компјутерската измама во Република Северна Македонија и тоа начинот на извршување (modus operandi), времето и периодот на извршување (tempus operandi), средствата на извршување (instrumentum operandi), просторот и местото на извршување (radius i locus operandi), како и организираноста на сторителите. Имено, предметот ќе биде насочен кон теоретско проучување на кривичното дело „Компјутерска измама“ во Република Северна Македонија од аспект на кривично правната инкриминираност (битието на делото). Ќе се направи анализа на кривично правната инкриминираност на исти и слични кривични дела и компарација со неколку кривични законодавства на држави од опкружувањето и земји членки на Европската Унија, посебно да се добијат сознанија за хармонизацијата на ова кривично дело со другите законодавства, бидејќи тоа е потребно од аспект на меѓународната правна помош и соработка во процесот на откривање и расветлување на криминалните ситуации од меѓународен карактер во кои се инволвирани и сторители од нашата држава, или криминалното делување е насочено спрема правни и физички лица на кои им е нанесена штета. Во истражувањето ќе се опфати и анализа на повеќе практични примери од македонската криминалистичка

практика. Во насока на продлабочен увид во оваа честа, но многу опасна криминална појава на денешното време, особено внимание ќе посветиме на опишување на нејзините криминалистички карактеристики.

Компјутерската измама е инкриминирана со кривично дело „Компјутерска измама“, во Членот 251 - б од Кривичниот законик на Република Северна Македонија, во кој се пропишува дека „тој што со намера за себе или за друг да прибави противправна имотна корист со внесување во компјутер или информатички систем невистинити податоци, со невнесување на вистинити податоци, со менување, бришење или прикривање на компјутерски податоци, со фалсификување на електронски потпис или на друг начин ќе предизвика невистинит резултат при електронската обработка и преносот на податоците, ќе се казни со парична казна или со затвор до три години. Ако сторителот прибавил поголема имотна корист, ќе се казни со затвор од три месеци до пет години. Ако сторителот прибавил значителна имотна корист, ќе се казни со затвор од една до десет години. Тој што делото од став 1 ќе го стори само со намера да оштети друг, ќе се казни со парична казна или со затвор до една година. Ако со делото од став 4 е предизвикана поголема штета, сторителот ќе се казни со затвор од три месеци до три години. Тој што неовластено изработува, набавува, продава, држи или прави достапни на друг посебни направи, средства, компјутерски програми или компјутерски податоци наменети за извршување на делото од став 1, ќе се казни со парична казна или со затвор до една година. Обидот за делото од ставовите 1 и 4 е казнив. Ако делото од овој член го стори правно лице, ќе се казни со парична казна. Посебните направи, средства, компјутерски програми или податоци наменети за извршување на делото ќе се одземат. За делото од став 4 гонењето се презема по приватна тужба. Терминот компјутерска измама, всушност, е подреден поим што спаѓа во доменот на компјутерскиот (сајбер) криминал т. е. група криминални активности, што вклучуваат компјутери, мрежи или Интернет.

Од големо значење е наведувањето на начините на извршување на компјутерските измами. Во овој труд ќе се водиме, главно, според класификацијата на Зврлевски и соработниците (2014). Начините на извршување ќе бидат детално објаснети и поткрепени со соодветни примери.

Во магистерскиот труд ќе се спроведе детално истражување во врска со условите што треба да бидат исполнети за да може да се констатира дека е извршена компјутерска

измама. Воедно, ќе се посвети внимание и на тоа какви последици по општеството носи кривичното дело компјутерска измама и зошто е од особено големо значење да се имплементираат оперативни активности за да се превенираат и да се спречат компјутерските измами. Трудот ќе се фокусира, пред се, на карактеристиките на компјутерските измами во Република Северна Македонија.

Посебен осврт ќе се направи и на активностите што надлежните органи ги имплементираат за спречување на компјутерските измами, но и за справување со веќе извршените кривични дела од овој вид. За оваа цел, покрај научна и стручна литература ќе се направи и анализа на Извештаите на Министерството за внатрешни органи како директно надлежен државен орган за сузбивање на компјутерскиот криминалитет во соработка и координација со јавното обвинителство.

Компјутерските измами се посебни кривични дела со бројни манифестни појавни облици кои се поврзани со начинот на извршување, односно кои техники и алатки се користат за доведување во заблуда на оштетените, корисници на Интернет, чии податоци се злоупотребуваат и врз основа на воспоставените шеми на сторителите истите успеваат да се стекнат со одредена имотна и финансиска корист.

Компјутерската измама се врши со намера за да се стекне противправна имотна корист за себе или за друг, со тоа што за разлика од класичната измама кога друго лице се доведува во заблуда да стори нешто на сопствена штета, а во туѓа корист, кај компјутерските измами заблудата се однесува на компјутерот во кој се внесуваат неточни податоци, или се пропушта да се внесат вистинити податоци. Во одредени случаи се наведува ситуација за внесување на вистинити податоци врз основа на порака со измамничка цел, а врз основа на внесените податоци, криминалците пристапуваат до други бази на податоци и ги злоупотребуваат. Најбројни се компјутерските измами во финансиското работење, осигурувањето и деловното работење, при што се создаваат ситуации или се користат алатки за пресретнување на деловни податоци и креирање на лажен деловен однос и пренасочување на финансиски средства со финансиски трансакции на друго физичко или правно лице.

Предмет на теоретско проучување ќе бидат појавните облици и форми на компјутерски измами кои се манифестирале во домашната и странската криминалистичка практика, посебно измамите кои се многу познати во научната и стручната литература, но

и истражување на новите појавни облици и форми кои се разликуваат според начинот на извршување.

Покрај начините на извршување, предмет на проучување и истражување ќе бидат битните криминалистички карактеристики на ова кривично дело врз основа на кои се издвојува од останатите имотни компјутерски кривични дела.

2.1. Појмовно – категоријален апарат

Компјутерска измама – Најрашириот облик на компјутерски криминал, подвид на компјутерскиот криминал, кои се извршува за да се стекне противправна корист за себе или за некое друго лице, со тоа што во заблуда не се доведува и одржува некое лице туку заблудата се однесува на внесување на невистинити податоци во компјутер, или пак намерно се испушта внесување на точните податоци (Ачкоски, 2012).

Компјутерски криминал[1] – „Компјутерскиот криминал е вид на криминал при кој кривичното дело е овозможено или вклучува употреба на електронски комуникации или информациски системи, вклучувајќи го кој било компјутерски уред, Интернет или и двете заедно (Goni; 2012).

„Компјутерскиот криминал не може да се опише само со една дефиниција, туку најдобро може да се опише како збир од дејства, кои се базираат на објектот на прекршок или на начинот на извршување што влијае на компјутерските податоци или системи“ (Sabillon; 2016)

Кривично дело – Противправно дело што со закон е определено како кривично дело и чии обележја се одредени со закон. Законодавецот прогласува одредено поведение како кривично дело, затоа што станува збор за општествено опасно поведение на човекот. Кривичното дело се карактеризира со следните елементи: дејствие, предвиденост во законот, противправност, вина и казнивост (Кошевалиска 2013).

[1] Во литературата на англиски јазик, овој термин е познат и како сајбер криминал (cyber crime). Терминот е навлезен и во македонскиот јазик. Бидејќи станува збор за синоними, а за да се постигне поголема јасност за читателот, во овој труд ќе се користи само називот компјутерски криминал.

Криминалистичко истражување – Поимот криминалистичко истражување (crime analysis) се однесува на општиот концепт и на дисциплината што се практикува од страна на полициската заедница. Се употребува и терминот criminal analysis за да се опише една комплетна дисциплина што се однесува на престапници, жртви и места. Станува збор за операционализација, истражување на криминален проблем што се одликува со сложена природа, па поради тоа и неговото расветлување бара сложена постапка, која вклучува повеќе законски мерки, дејствија и криминалистички методи. Воедно, вклучени се и повеќе државни органи што поседуваат законска надлежност за истражување на кривичните дела (Николоска 2013) .

Компјутерски систем - Под поимот на компјутерски систем се подразбира секој уред или група на уреди кои се меѓусебно поврзани и со кои се врши автоматска обработка на податоци. (Кривичен законик на РМ, Сл.весник на РМ 07/08)

Компјутерски податоци – Во информатиката, податоците се информации што се преведени во форма која е ефикасна за пренесување или обработка. (https://www.techtarget.com/searchdatamanagement/definition/data)

Криминалистички карактеристики – Општо е прифатено дека суштинските состојки на секое кривично дело се (1) доброволно дело или пропуштање (actus reus), придружено со (2) одредена состојба на умот (mens rea). Акт може да биде каков било вид на доброволно човечко однесување. На пример, движењата при епилептичен напад не се чинови, ниту движењата што ги прави сомнабулист пред да се разбуди, дури и ако резултираат со смрт на друго лице. Кривичната одговорност за резултатот, исто така, бара направената штета да е предизвикана од обвинетиот. Тестот за причинско-последична врска помеѓу однесувањето и резултатот е дека настанот не би се случил на ист начин без директно учество на сторителот. (https://www.britannica.com/topic/criminal-law/The-elements-of-crime). Исто така, во криминолошката литература, криминалистички карактеристики се начинот на извршување (modus operandi), времето и периодот на извршување (tempus operandi), средствата на извршување (instrumentum operandi),

просторот и местото на извршување (radius i locus operandi) и организираноста на сторителите.

Компјутерска форензика – Компјутерската форензика се занимава со собирање на дигитални докази од местото на компјутерското злосторство. Постојат три вида на форензика која се однесува на компјутерски системи и електронски докази. Првиот вид е традиционалната компјутерска форензика која претставува собирање на дигитални докази од компјутер, диск или од уред кој вклучува компјутер или се смета дека може да создаде или да преработи електронски (дигитални) податоци. Вториот вид на компјутерска форензика е сајбер – форензиката или мрежната форензика. Таа опфаќа собирање докази кои покажуваат дека одредени дигитални податоци преминале преку некој медиум меѓу две точки во мрежата. Третиот вид е форензичката анализа на софтвер која се занимава со идентификување на авторот, на дел од софтверскиот код од самиот код (Николоска 2013).

Дигитален (електронски) доказ – Според меѓународната дефиниција во областа на форензичките науки, дигитален доказ е секоја информација во дигитален облик која има доказна вредност и која е приспособена или пренесена во таков облик. Овој поим вклучува компјутерски складирани или генерирани доказни информации, дигитализирани видео или аудио доказни сигнали, сигнали од дигитален мобилен телефон, информации на дигитални факс машини и сигнали од други дигитални уреди (Николоска 2013).

ЕВРОПОЛ – Организација на Европската Унија надлежна за спроведување на законот, која работи со криминалистичко-разузнавачки информации. (https://mvr.gov.mk/page/europol)

2.2. Операционализација на проблемот

Операционализацијата на предметот на истражување ќе се врши најпрво преку теоретско проучување на домашна и странска научна и стручна литература од областа на компјутерскиот криминалитет, но и криминологијата и криминалистиката. Ќе се посвети внимание на анализа на дефинираност на поимот на компјутерска измама и значајните компоненти во дефинираноста. Посебно ќе се посвети внимание на проучување на поголем број на појавни облици и форми на компјутерските измами, посебно нивните специфичности од аспект на начинот на извршување, но и времето, просторот и местото на криминалното делување и местото на настанување на криминалната последица. Сторителите на овој криминал или компјутерските измамници се посебна категорија на сторители кои покрај личните компоненти имаат и значајна компонента на знаења и вештини за користење на компјутерската технологија и нејзините можности, во насока на злоупотреба во смисла на доведување во заблуда на правни и физички лица преку електронска комуникација и наведување да сторат одредени чекори кои ќе бидат искористени во нивна штета, а во корист на измаманиците. Посебно внимание ќе се посвети на анализа на случаите од домашната криминалистичка практика преку анализа на случаи, но и анализа на случаи кои имаат меѓународен карактер, а има инволвирано сторители од нашата држава, или штетата е нанесена на правни и физички лица. Посебно ќе се направи анализа на извршените кривични дела и пријавените сторители како и видот и висината на противправната имотна корист или нанесената штета.

Покрај тоа, ќе биде ставен акцент на соработката помеѓу институциите, како и на овластувањата на релевантниот Сектор од Министерството за внатрешни работи на Република Северна Македонија, на спроведените активности за откривање, расветлување и обезбедување докази во врска со извршените компјутерски измами на територијата на Република Северна Македонија.

2.3. Временска рамка на истражувањето

Временската рамка на истражувањето во овој труд ќе биде ограничена, во голема мера, на последните пет години т.е. од 2018 до 2023 година. На овој начин се постапува

поради потребата од добивање на што е можно поактуелни резултати т.е. резултати што се релевантни за актуелниот временски период. Освен тоа, повеќе податоци и студии укажуваат на тоа дека компјутерските измами се зачестуваат со изминувањето на годините, па затоа и материјалот за истражување, како и примерите, ќе бидат пообемни.

2.4. Дисциплинарно определување

Во овој магистерски труд ќе се истражува на дисциплинарно сеопфатен начин, затоа што предметот на истражување опфаќа неколку области и науки. Компјутерската измама е составен дел од:

Правото, кое опфаќа збир на правни норми што ги пропишува државата, и чие непочитување таа ги казнува т.е. ги санкционира.

Кривичното право, кое понекогаш се нарекува и казнено право, поставува прописи за условите под кои компјутерската измама преставува кривично дело. Од друга страна, дел од кривичното процесно право се објаснувањата за надлежностите на органите за постапување по компјутерската измама. Тука се предвидени мерките и дејствијата на предистражната постапка.

Криминалистиката, која е наука што пронаоѓа, проучува и усовршува практично засновани научни методи и средства, кои се најпогодни за да се да се открие и разјасни кривичното дело компјутерска измама, да се открие сторителот и да се приведе кон кривична санкција, но и да се обезбедат сите докази заради утврдување на објективната вистина и да се спречи извршувањето идни кривични дела.

Криминологијата, која ги проучува појавните облици и форми на компјутерски измами.

3. ЦЕЛ НА ИСТРАЖУВАЊЕТО

Главната цел на овој магистерски труд е, со користење на научно-истражувачките методи употребени во емпириското истражување, да се даде научна дескрипција и објаснување за безбедноста на компјутерските системи, опасностите со кои тие се соочуваат генерално за оштетувањето и неовластеното навлегување во компјутерските

системи. Со анализирањето на овие кривични дела ќе се препознаат недостатоците, пропустите и слабостите на информатичкото општество генерално и конкретно за компјутерските системи, но и за мерките на заштита на сите оние кои имаат директен или индиректен пристап до компјутерските системи. Со тоа ќе се создаде квалитетна платформа за подобрување на информатичката безбедност во информатичкото општество во Република Северна Македонија.

Како резултат на тоа, неопходно е да се иницира примена на соодветни криминалистички мерки (оперативно-тактички и форензичко-технички мерки и активности и истражни дејствија) за успешно откривање и докажување на ова кривично дело, обезбедување на физички и дигитални докази кои ќе бидат употребени во кривичната постапка со цел откривање и пронаоѓање на сторителите за да може судот да носи мериторни пресуди.

Практични цели и задачи на научно истражувачката работа се навремена идентификација и детекција на оштетувањета и неовластеното навлегување во компјутерските системи и зголемување на информатичката безбедност. Освен тоа, ќе ги проучиме индикаторите за зачестеност на ова кривично дело во Република Северна Македонија, во кои појавни облици се појавува ова кривично дело како и начините на оперативно истражување. Во овој труд ќе се проучат и законските, криминалистичките и превентивните мерки за заштита (Стандардна оперативна процедура за компјутерски криминал при Министерството за внатрешни работи на Република Македонија , Кривичен законик, Закон за кривична постапка, Закон за полиција и Закон за внатрешни работи со конкретна примена на одредбите кои се однесуваат за ова кривично дело).

Исто така, ќе ги афирмираме и позитивните искуства (врз основа на компаративен метод) за регулираноста на оваа област во соседните и други европски земји, во однос на информатичката безбедност и справување со ризиците и нивна контрола, оштетувањето и неовластеното навлегување во компјутерските системи, како и нивно откривање и докажување и превентивните мерки кои се преземаат заради заштита. Ќе обрнеме внимание и на ризиците, заканите и опасностите врз информатичката безбедност.

Преку истражувањето треба да се дојде до конкретни решенија и предлози за поголема информатичка безбедност на компјутерските системи и поефикасно откривање и докажување на оштетувањето и неовластеното навлегување во компјутерските системи.

4. ХИПОТЕТСКА РАМКА

За успешно реализирање на предметот и целите на истражување неопходно е поставувањето на хипотетска рамка, која воедно ќе даде и соодветна научна поткрепа на тезата. Имајќи ги предвид претходно поставените предмет и цели на истражувањето, поради потребата истражувањето да добие конкретна насока, дефинирани се една општа хипотеза и пет помошни хипотези, кои за време на истражувањето ќе се тестираат и ќе се истражуваат. Како автор на трудот, ќе се обидам да ги докажам и да ги оправдам поставените хипотези. Во заклучокот на овој труд ќе се содржи соодветна оценка за тоа дали добиените резултати ги оправдуваат или ги отфрлаат претходно поставените хипотези.

Главната хипотеза е: „Компјутерските измами се имотни кривични дела кои се издвојуваат од класичната измама и од останатите компјутерски кривични дела по специфичните начини на извршување, односно способноста на измамниците во делот на манипулација со компјутерските податоци и стекнување на високи криминални приноси кои се поврзани со временскиот период на криминалното делување и умешноста во електронската комуникација со „жртвите“ и наведување за нивен придонес во криминалната реализација на сторителите.“

Помошна хипотеза 1: Компјутерските измами се вршат заради остварување на финансиска добивка како противправна имотна корист.

Помошна хипотеза 2: Органите на Република Северна Македонија прават напори за справување со компјутерските измами, преку преземање на соодветни оперативни активности, превентивни дејства и слично.

Помошна хипотеза 3: Покрај напорите и преземените активности за сузбивање на компјутерските измами од страна на органите на Република Северна Македонија, потребно е и зголемување на граѓанската свест за овој вид криминал. Граѓаните на Република Северна Македонија треба да бидат информирани за тоа како самостојно да

умеат да се заштитат од компјутерските измами, и да ги превенираат уште пред да се случат.

Помошна хипотеза 4: Компјутерските измами предизвикуваат сериозни импликации и штети во приватниот и професионалниот живот на жртвите. Преку извршување на кривичното дело компјутерска измама, се остварува значителна матријална штета, која бележи значителен пораст низ годините.

Помошна хипотеза 5: Со зголемување на соработката на органите на Република Северна Македонија со надлежните органи од странските држави, може да се спречи и да се намали штетата од компјутерските измами.

5. МЕТОДИ И ТЕХНИКИ НА ИСТРАЖУВАЊЕ

Темата на магистерскиот труд детално ќе биде елаборирана во неколку теоретско-истражувачки фази што се достапни на онлајн научните бази како Google Scholar, Research Gate, Ebsco Host и други, а коишто опраќаат неколку фази, и тоа: фаза на пребарување, фаза на селектирање и фаза на обработка на претходни теоретски истражувања. Преку применувањето на горенаведените фази, ќе се спроведе научен преглед на литературата од областа на компјутерските измами и на претходно спроведените истражувања од оваа област.

Секако, важен дел од трудот ќе биде и применувањето на научно-истражувачки методи (квалитативни и квантитативни). Од општите научни методи, основен метод ќе биде методот на анализа на содржина т.е. аналитичко-синтетички метод, кој ќе се користи во текот на изработката на целиот научен труд за да се усогласат и воедначат главите и јасно да се презентираат прашањата коишто ќе бидат тема во секоја од главите поединечно.

Со примената на дескриптивниот метод детално ќе биде опишан предметот на истражување поткрепувајќи го со релевантни примарни и секундарни истражувања. Со компаративниот метод ќе биде извршен компаративен преглед во врска со темата на магистерскиот труд, но и за претставување на оперативните активности за превенција од компјутерски измами, коишто се применуваат во дел од државите што ќе бидат опфатени

во истражувањето. Станува збор за споредување на состојбата во Република Северна Македонија, некои од земјите од регионот и земјите-членки на Европската Унија, врз основа на правната регулатива и други меѓународни акти за оштетувањето и неовластеното навлегување во компјутерските системи и методиката на криминалистичко истражување и докажување, споредба со искуството од меѓународните полициски институции и тела кои што се задолжени генерално за сузбивање на компјутерскиот криминалитет и користењето на апликативен софтвер за информатичка безбедност во Република Северна Македонија и во регионот.

6. НАУЧНА И ОПШТЕСТВЕНА ОПРАВДАНОСТ НА ИСТРАЖУВАЊЕТО

Се очекува дека резултатите од спроведеното истражување ќе бидат значајни од научна гледна точка. Прво, во Република Северна Македонија се забележува, особено во последните неколку години, сè поголема зачестеност на компјутерските измами. Притоа, во Република Северна Македонија досега се спроведени само мал број на научни истражувања на оваа тема. Следствено на тоа, со изработката на ова истражување, ќе се добие научен труд со суштински значајна тема, кој ќе придонесе како недоволно истражувана тема на нашите простори. Второ, поставените задачи на истражувањето не само што целат кон теоретско претставување, туку се обидуваат да дадат и имплементативен преглед на актуелната состојба и да создадат услови за генерирање за идно, поефикасно справување со компјутерскиот криминал од кое сите засегнати страни ќе имаат придобивки, а пред се и најважно ќе се зголеми безбедноста и стабилноста во државата. Трето, засегнатите страни ќе добијат научни материјали како развиените земји ги надминуваат случаите на компјутерски измами и кон оперативни активности низ годините се покажале како најефикасни. Дополнително, ограничувањата коишто ќе произлезат од ова истражување ќе послужат како основа, идеја и можност за спроведување на понатамошни, уште подлабоки научни истражувања од областа со кои ќе се направи значителен исчекор во областа на истражување.

Обработката на темата е значајна од општествена гледна точка поради тоа што компјутерските измами се суштински и сериозен проблем којшто поттикнува кражба и

злоупотреба на лични информации и материјални средства, а тоа значително го влошува квалитетот на животот, приватноста на поединците и функционирањето на претпријатијата. Добиените резултати од истражувањето ќе покажат како преку имплементирање на оперативните активности ќе се влијае на начин да се надмине оваа состојба односно, ќе се влијае преку превенција на кривичното дело да се надмине ризикот од кражба на информации и средства и повредата на приватноста. Се предлага поголема ангажираност и внимателност од страна на надлежните органи на Република Северна Македонија при процесот на превенција и справување со компјутерските измами. Меѓутоа, и поединците имаат не помала одговорност, имено, да постапуваат внимателно за време на користење на Интернетот и споделувањето на своите лични податоци.

ОСНОВИ НА КОМПЈУТЕРСКИОТ ИМОТЕН КРИМИНАЛИТЕТ

1. КОМПЈУТЕРСКИ ИМОТЕН КРИМИНАЛИТЕТ

Различни автори го дефинираат компјутерскиот криминалитет преку различни дефиниции, но се чини дека сите дефиниции споделуваат заедничка поента. Според Сулејманов (2003), компјутерскиот криминалитет содржи елементи на имотен криминалитет. Воедно, овој автор нагласува дека во денешно време се среќаваат повеќе видови инкриминации кои претставуваат заштита од компјутерски криминалитет, како на пример приод во компјутерски систем, компјутерска измама, компјутерски фалсификат, компјутерска шпионажа и саботажа и кражби на време од компјутерски системи. Со наведените криминални појави се опфатени манипулациите со податоци, (употреба на неисправни и нецелосни податоци, неовластено употребување на податоци и неовластено влијание врз текот на обработката на податоците), манипулации со програми (неисправно обликување на програми) и манипулации од типот на стопанската шпионажа, каде посебно се става акцент на неовластеното оддавање на деловна тајна.

Станува збор за престап кој се смета за специфично компјутерски инцидент и кој на извршителот може да му донесе корист од значителни размери, додека, пак, на сопственикот на компјутерскиот систем може да му нанесе значителна и сериозна штета.

Всушност, станува збор за неовластено употребување на службени компјутери за приватни цели. Во сферата на компутерскиот криминал, покрај облиците на загрозување на човековите слободи и права, со секој изминат ден се зголемува опасноста од користење на компутерските системи за остварување материјална корист или предизвикување штета, која може да биде непосредна или посредна. Според тоа, во првиот случај може да се работи за корист или штета предизвикана со користењето на информациите или податоците, или со нивно бришење или уништување во самиот систем, преку бришење на програми и слично. Во вториот случај системот се користи за внесување или менување на податоци што предизвикуваат натамошни штетни располагања со имотот од страна на трети лица (на пример, зголемувањето на износот на депозитот на банковната сметка на сторителот). По својата природа, делата што влегуваат во поимот на компјутерски криминал се по своето објективно битие блиски на оштетувањето туѓи предмети и измамата, со која ги поврзува и идентичната намера за прибавување противправна имотна корист или оштетување на друг (Камбовски 2003).

Николоска (2013) ги анализира дефинииите на Дон Паркер, според кој, компјутерскиот криминалитет претставува злоупотреба на компјутерот преку секоја активност што е поврзана со користење компјутерска технологија во која жртвата може да има загуба или веќе претрпела загуба, а сторителот дејствува со цел да добие корист за себе, или пак, би можел да добие корист. Николоска (2013) ја истакнува и дефиницијата на Бого Брвар, според кој се работи за кривични дела кај кои компјутерот е средство, предмет или објект, а за чие извршување е неопходно познавање од областа на компјутерите и информатиката. Димовски (2010) го дефинира компјутерскиот криминалитет како општествено опасна појава за чие остварување сторителот користи компјутерско знаење и технологија, со преземање на компјутерскиот систем во најширока смисла (хардвер, софтвер, нивно единство; еден компјутер или компјутерска мрежа), кој се користи како алатка или како предмет на криминална активност, напад или и двете. Некои теоретичари го користат и терминот „сајбер криминал“.

Според Божиновски (2018), глобалните компјутерски мрежи ги зголемуваат шансите за создавање на нови облици на криминал. Па така, во последните години забележуваме појава на посебни, софистицирани, продорни, технички потковани, бескрупулозни, понекогаш одмаздољубиви поединци на кои човек многу тешко може да

им се спротистави, а нивното сопирање е уште покомплицирано. Често, нивната цел е стекнување на публицитет и популарност, на пример, со тоа што лесно се движат низ виртуелниот сајбер простор, кој одлично го владеат и им е добро познат, па се чувствуваат како да се дома. Тоа ги зголемува проблемите при нивното идентификување. Активностите им се олеснети благодарение на огромниот простор и широката достапност на Интернетот. Последиците од електронскиот криминал или од т.н. вируси, црви или тројанци се големи. Божиновски (2018) наведува дека во Австрија во 2003 година електронскиот криминал предизвикал штета од 3,5 милиони долари, а вирусите, тројанците и црвите 2 милиони долари. Во Велика Британија, пак, во 2003 година електронскиот криминал предизвикал штета од 128 милиони фунти, а вирусите, тројанците и црвите 27,8 милиони фунти.

Компјутерските измами не се непознати за повеќето држави во регионот и светот, а Република Северна Македонија исто така не е поштедена од нив. Надлежните институции во регионот и светот преземаат соодветни мерки за нивна превенција и санкционирање, како што е случај и во Република Северна Македонија. Меѓутоа, од држава до држава постојат одредени разлики.

Компјутерските измами се вбројуваат во имотните кривични дела бидејќи преку нив извршителот остварува противправна имотна корист. Како што нагласува Сулејманов (2003), во имотниот криминалитет т.е. во кривичните дела против имотот спаѓаат сите дела што се насочени против имотот, а со чија помош нивниот сторител настојува за себе или за друго лице да прибави одредена материјална корист или пак некому да му причини материјална штета. Од друга страна, Сулејманов (2013) ги дефинира измамите како кривични дела против имотот и имотните права и интереси, и тие се состојат од доведување или одржување во заблуда на одредено лице, преку лажно прикажување или прикривање на околностите . Ова лице се доведува или се одржува во заблуда така што е наведено нешто да стори или да не стори на штета на својот или на туѓ имот. Ако ја споредиме дефиницијата на компјутерските измами со оваа дефиниција, станува јасно дека тие можат да се сметаат за имотен криминалитет.

Според Кајзер, во зависност од засегнатото правно добро можат да се разликуваат три вида компјутерски злоупотреби, и тоа:

1. Компјутерски повреди на личноста, особено на приватната сфера на граѓанинот;

2. Компјутерски деликти против индивидуалните или социјални правни добра;

3. Компјутерски имотен криминалитет во потесна смисла (Милковска 2012)

Бидејќи компјутерскиот криминал и компјутерските измами се област која заслужува внимание не само на една земја, туку и на целата меѓународна заедница, беа донесени меѓународни правила кои ја регулираа оваа област. Обединетите Нации, на Осмиот конгрес за превенција на криминалот, одржан во Хавана во 1990 година, донесе посебна Резолуција во која е констатирана потребата од криминализирање на разни злоупотреби. Со неа, земјите-членки добиваат обврска да воспостават систем на мерки за спречување на разни злоупотреби. Оваа Резолуција беше прифатена од Генералното собрание на ОН (Димовски 2010).

На 11 септември 1995 година, Советот на Европа ја усвои Препораката за дефинирање на компјутерскиот криминал, и го дефинираше како напад поврзан со информатичка технологија – кое било однесување за чија истрага, истражните органи мора да се здобијат со информација т.е. доказ, носител на доказна информација што е обработена или пренесена преку компјутерски систем или преку друг систем на автоматска обработка на податоците. Воедно Генералното собрание на ООН има донесено и неколку резолуции што се занимаваат со информатичката безбедност, и има назначено петнаесет члена на Експертската група за проучување на прашањето за информатичката безбедност (Николоска 2013).

2. АНАЛИЗА НА ПРЕПОРАКИ ОД КОНВЕНЦИЈА ЗА КОМПЈУТЕРСКИ КРИМИНАЛИТЕТ

Еден од најважните меѓународни документи во врска со компјутерскиот криминал е Конвенцијата за компјутерски криминал на Советот на Европа (ETC 185), која произлезе од потребата да се воедначат и да се систематизираат материјалните и процесните норми од областа на компјутерсиот криминал и електронските докази на глобално ниво. Претходно постоеле обиди да се дефинираат материјалните норми за регулирање на меѓународно правната соработка, но тие не биле толку успешни како Конвенцијата. Овој документ, со својата сеопфатност, флексибилност и можност за лесно инкорпорирање во националните законодавства, иако првично наменет за државите во Европа, стана

препознатлив механизам за едноставно и олеснето комуницирање помеѓу сите држави во светот. Како продолжение на Конвенцијата за компјутерски криминал, подоцна се надоврзуваат и Конвенцијата за заштита на личните права при автоматизиран процес на обработка на личните податоци со амандманите и Дополнителниот Протокол за авторизиран проток на лични подотоци надвор од државата, Дополнителен Протокол на Конвенцијата за компјутерски криминал за заштита од расизам и ксенофобија, Конвенција за заштита на децата од сексуална експлоатација и сексуално злоставување и Директивите на ЕУ. Конвенцијата беше усвоена од страна на Советот на Европа во Будимпешта на 23.11.2001 година. Истата била составена на англиски и на француски јазик, при што двата текста се со еднаква автентичност и во единствен примерок биле депонирани во архивата на Советот на Европа. Генералниот секретар на Советот на Европа испратил заверени примероци до секоја од државите земји-членки на Советот на Европа, но и до државите што не се членки, а што учествувале во изготвувањето на Конвенцијата, како и до секоја држава што била поканета да пристапи кон Конвенцијата. Вкупно 58 држави ја потпишале Конвенцијата, од кои 28 со ратификација. Нашата држава ја потпиша Конвенцијата на 23.11.2001 година, ја ратификуваше на 15.09.2004 година, а стапи во сила на 01.01.2005 година.

Конвенцијата се состои од преамбула, 4 глави и 48 члена. Во глава I се даваат дефиниции на најзначајните поими, како што се компјутерски систем, компјутерски податоци, провајдер на услуги и преносни податоци. Во глава II се наведени мерките што треба да се преземат на национално ниво, а во глава III станува збор за меѓународната соработка. На крај, во глава IV се илустрирани завршните одредби.

Содржината на Конвенцијата вклучува материјални, процесни норми, како и норми за меѓународна соработка. Одредбите од областа на материјалното право се однесуваат на: недозволен пристап, недозволено пресретнување, упад во податоци, упад во систем, злоупотреба на уред, фалсификување поврзано со компјутер, измама поврзана со компјутер, дела поврзани со детска порнографија, дела поврзани со повреда на авторски и други сродни права. За овој труд е најзначаен Член 8, во кој се даваат препораки во врска со „измама поврзана со компјутер“. Во Конвенцијата е наведено дека „Секоја Страна ќе усвои такви законодавни и други мерки кои се неопходни со домашното право да се

инкриминираат односно предвидат како кривични дела, кога со умисла и противправно се преземаат дејствија со кои се предизвикува намалување на имотот на друго лице преку

а) внесување, менување, бришење или прикривање на компјутерски податоци;

б) упад (вмешување) во функционирањето на одреден компјутерски систем;

со измамничка или друга нечесна намера да се стекне противправна имотна корист за себе или за друг.

Препораките од оваа конвенција наоѓаат примена и во Република Северна Македонија. Вака дефинирани одредби се внесени и во македонското материјално законодавство и тоа во делот на општите одредби каде што се дефинирани основните поими за овој вид на криминал, како и специфични конкретни кривични дела.

3. ПОЈАВНИ ОБЛИЦИ НА КОМПЈУТЕРСКИ ИЗМАМИ

Во рамките на погоре наведената дефиниција за компјутерски криминалитет на Сулејманов (2003), компјутерската измама е еден вид на инкриминација од областа на компјутерскиот криминалитет. Повторно станува збор за поим за кој постојат повеќе дефиниции, но и одредени тешкотии за негово прецизно дефинирање. Како посебен појавен облик на компјутерски криминалитет повеќето научници и истражувачи ги дефинираат компјутерските измами како посебен облик на компјутерски криминалитет кој се издвојува од класичната измама според криминалистичките карактеристики, каде основно средство на извршување е компјутерот, а начинот на извршување е поврзан со користење на можностите и алатките за компјутерска комуникација, но и средства и шеми за пресретнување на компјутерски податоци кои подоцна се искористуваат во креирање на специфични облици на компјутерски измами.

Компјутерските измами, според Ачкоски (2012) се посебен вид на компјутерски криминал, кај кои станува збор за измами се кои се извршуваат со намера за стекнување на противправна материјална корист за себе или пак, за друго лице. Специфичноста кај нив се состои во тоа што во заблуда не се доведува или одржува некое лице како кај обичните измами и како кај материјалните кривични дела со кои се предизвикува штета, туку заблудата се однесува на компјутер во кој се внесуваат лажни податоци, или намерно

се испушта внесувањето на вистинити податоци, или компјутерот се користи за остварување на измами во кривично правна смисла на кој било друг начин.

Како посебен криминален облик, компјутерската измама е дефинирана во документ[2] на Советот на Европа како „внесување, менување, бришење или прикривање на компјутерски податоци или компјутерски програми, или на друг начин влијание на процесот на обработка на компјутерските податоци, кои предизвикуваат стекнување на противправна имотна корист“. Компјутерските измами може да се вршат на повеќе начини и компјутерските делинквенти во тој поглед се многу инвентивни и креативни, а компјутерот за измамниците претставува удобно средство за да го лишат човековиот мозок од способноста да прави разлика помеѓу тоа што е замислено (имагинарно) и тоа што е реално (вистинско), со што се манифестира како совршена жртва.

Масовноста на компјутерските измами се зголеми со развојот на компјутерските системи и нивното масовно прифаќање во општеството. Компјутерската измама стана уште почеста со компјутеризацијата на финансиските институции, кои воедно претставувале и првите цели на ваквите измами. На пример, во 1995 година, со помош на компјутерска измама е извршено ограбување на најстарата банка на Англија. Во 1996, инженерската компанија Омега изгубила повеќе од 10 милиони долари преку компјутерска измама на незадоволен вработен. Во 2001 година, две вработени во Cisco извршите кражба на 8 милиони долари преку наплата на трансакции, продажба на акции со опција за наплата преку компјутерска измама. Наведените податоци од не толку далечното минато ја потврдуваат претпоставката дека со текот на годините, компјутерската измама би можела да стане сè позастапена, а со тоа да предизвика и поголема штета. Како информатичките експерти така и органите за борба против криминалот предвидуваат дека компјутерскиот криминал ќе стане помасовен во иднина (Николоска 2013).

Основата на компјутерската измама се состои во доведување во заблуда со внесување на неточни податоци во компјутер или со пропуштање на внесување на точни податоци, или користење на компјутерот на кој било кој друг начин за остварување на измама во кривично – правна смисла. На таков начин со внесување, односно невнесување на податоци се влијае на резултатот на електронската обработка на податоците и нивниот

[2] Конвенција за компјутерски криминал (Совет на Европа), (ETC 185)

пренос, со намера да се стекне противправна имотна корист, или да се нанесе штета. Компјутерските измамници ги злоупотребуваат оние карактеристики кои придонесуваат за порастот на електронската трговија: анонимност, дистанцираност помеѓу продавачот и купувачот. Заедно со сето тоа, измамниците ја користат предноста што измамата преку Интернет не бара пристап до некој систем за исплата и што дигиталниот пазар е сеуште недоволно уреден, за измамниците претставува скоро идеално со услови за компјутерска измама. (https://kriminalist.rpg-board.net/t15-topic)

Компјутерската измама преставува модификација на „нормалната/обичната“ измама и треба да се третира на сличен начин. Компјутерската измама е создадена за да се пополни празнината во кривичното право во сѐ подигитализираниот и автоматизиран свет. Онаму каде што човекот може да биде жртва на измама, компјутерската измама со создавањето на овој нов факт ја поистоветува манипулацијата со операција за обработка на податоци со измама. Онаму каде што машината го заменува човекот, манипулацијата со податоци ја заменува измамата. Тука не е потребен посебен чин на измама. Потребни се само дејствија кои, доколку се направат на некое лице, би предизвикале грешка кај тоа лице. Во центарот на компјутерската измама се наоѓа операцијата за обработка на податоци. Тоа се сите автоматизирани процеси во кои се постигнуваат посакуваните резултати од работата со снимање на податоци и нивно поврзување со програми. Класичен пример е отклучување на мобилен телефон. Кога се внесува PIN-от, тоа се податоци кои се внесуваат во електронски работен процес. Програмата што го блокира пристапот до мобилниот телефон „знае“ дека може да го отвори пристапот само кога ќе ја внесете оваа комбинација од броеви. Програмата ги обработува податоците и води до работниот резултат „Овозможување употреба на мобилен телефон“.

Според Николоска (2013), измамата, која во својата суштина го содржи лажното прикажување на фактите или пак, прикривањето на фактите, може да биде извршена на многубројни класични начини, но преку користењето на информатичката технологија, автоматизацијата на класичните методи или со создавањето на нови методи, овој криминал го зголемува својот квалитет и квантитет. Најтипични се компјутерските измами поврзани со државната управа, комуникациите, услугите, осигурувањето, инвестициите, бизнисот и довербата.

4. ОБЛИЦИ И ФОРМИ НА КОМПЈУТЕРСКИ ИЗМАМИ

Основната разлика помеѓу компјутерската измама и класичната измама се состои во тоа што при компјутерска измама, измамата и штетата се предизвикани со помош на употреба на компјутери или информациски системи, додека кај класичната измама не се користат такви технички помагала. Меѓутоа, и во едниот и во другиот случај, целта на сторителот е да стекне финансиска предност за себе или за трето лице преку измама на жртвата и на таков начин да предизвика финансиска штета (https://www.juraforum.de/lexikon/computerbetrug).

Според Николоска (2013), компјутерската измама се разликува од класичната измама затоа што сторителот и извршителот не се познаваат лично, не остваруваат физичка комуникација и не постои елементот на доведување во заблуда со помош на лажно претставување или со лажна презентација на одредени факти. Тоа што е специфично е фактот што помеѓу нив не постои физички контакт, дури е можно жртвата воопшто да не знае дека е жртва, а сторителот ги употребува своите вештини и збирот од можности што ги дава масовната комуникација и размената на податоци преку Интернет. За очекување е компјутерската измама да стане масовно кривично дело, и тоа најмногу со фалсификувањето на електронскиот потпис во деловната комуникација во економскиот и правниот сектор, иако тоа не е толку застапено (сè уште) во Република Северна Македонија. Сепак, кај ова кривично дело е задолжително да се докаже намерата и умислата на сторителот со цел стекнување противправна имотна корист.

Од друга страна, термините компјутерска измама и интернет измама често се користат како синоними[3], со тоа што компјутерската измама, која се нарекува уште и интернет измама, преставува кој било вид измама или шема шема што користи една или повеќе компоненти на интернетот, како на пример, виртуелни мрежи за разговор, e-mail, форуми, или веб-страни, со чија помош се претставуваат лажни трансакции, или за пренос на средствата за измама на финансиските институции или на други поврзани со шема. Од друга страна, некои автори ги разграничуваат овие термини. На пример,

[3] Заради остварување на поголема концизност, во рамките на овој труд, компјутерската измама и интернет измамата ќе се користат како синоними.

Матијашевиќ и др. (2012) нагласуваат дека интернет измамата се однесува на секоја измама при чие извршување лице кое има намера да прибави противправна имотна корист за себе и за други, користи една или повеќе компоненти на Интернет, како што се виртуелни простории за разговор, веб-страници, електронска пошта итн, со цел да се создадат услови за лажно прикажување или прикривање на факти кои би го довеле човекот во заблуда или би се задржале во неа, така што тоа лице би направило нешто на штета на својот или туѓ имот, на пример. извршувајќи некоја финансиска трансакција или префрлувајќи некои податоци на финансиска институција која е цел на нападот. Интернет измамата го мами, пред сè, лицето. Таа не е секогаш и нужно компјутерска измама, бидејќи некои интернет измами одговараат на класични измами кои го користат Интернетот како средство за извршување без никакво посебно влијание врз електронската обработка на податоците или работењето на компјутерот (т.е. измамени се луѓето). За разлика од ова, компјутерската измама го измамува компјутерот и електронската обработка доведува до погрешен резултат со да се добие противправна имотна корист, а тоа е differentia specifica на овие два поима. (Jelena Matijašević, Žaklina Spalević, Svetlana Ignjatijević; 2012).

Зврлевски и соработниците (2014) набројуваат неколку вида компјутерски измами т.е. начини на нивно извршување:

– Инвестициски шеми: Во овој случај, Интернетот се користи за да се даде финансиска поддршка за користење на Интернет за давање финансиска поддршка за високи технички шеми (на пр. сајтови за виртуелен шопинг или провајдери на нови сервиси)

– Шеми за кредитни картички: Употреба на незаконски добиени детали на кредитни картички за купување на производи со висока вредност преку Интернет.

– Можности за бизнис/шеми за работа од дома: Преку Интернет се рекламираат бизнис можности за користење на Интернет, а жртвата плаќа однапред за информацијата или производот за работа.

– „Нигериска измама“ (т.н. Измами 419): Западно-африкански измами со променет начин на достава. Во денешно време, наместо писмо или факс, се праќа електронска порака. Останатиот пристап е ист и постои потенцијално голема можност за спамирање. Овој вид измама е најпозната компјутерска измама во криминалистичката литература и

најчесто започнува со писмо и електронска порака која е осмислена на таков начин, за да изгледа како намерно да е испратена на примачот на пораката. Измамата се врши со помош на лажна порака за добитници на игра на среќа, лажни пораки поврзани со добротворни прилози, пораки со „љубовни и деловни понуди“, хуманитарни акции, наследство на имот на починати лица – подалечни роднини и сл. извршувањето на „Нигериската измама“ најчесто започнува со убедување на „жртвата“ да учествува во поделба на одредени финансиски фондови, со убедување за однапред да се уплати одреден паричен износ, кој е далеку понизок од износот за кој се ветува дека ќе се добие од фондот, односно од испраќачот на пораката. Сторителите на ваквите измами најчесто користат лажни податоци и кражба на идентитет, а при претставувањето користат лажни фотографии за да бидат поубедливи. (Urošević; 2009) На пример, жртвата добива e - mail од наводниот син на починатиот Нигериец, шеф на државата, кој е наследник на милиони долари, скриени во сметки низ светот. Личноста што ја чита електронската пошта е доведена во заблуда да поверува дека е добитник на пари на среќа. Меѓутоа, за возврат, од жртвата се бара надомест за адвокат за неколку илјади долари, за да се поврди дека парите се сигурни. Жртвите испраќаат пари за адвокатски услуги, но никогаш не добиваат пари. Со цел да ги намамат жртвите, сторителите секојдневно испраќаат пораки со кои ветуваат високи суми пари ако се изврши определена работа, но под услов претходно да им се достават податоци за жртвите за да ја исплатат таканаречената договорена „заработувачка“. (Николоска 2013)

– Интернет банкарство: Оваа измама се извршува преку копирање на веб страната на некоја банка. Малку се менува веб адресата, се обезбедуваат линкови до легални банкарски сервиси и само еден или два линкови се за големи инвестиции кои бараат трансфер на значителни суми со цел да се осигура вклучување во вистински неверојатна можност за инвестиции.

– Катастрофални повици за доброволни измами: На пример, повеќето веб страни кои бараат помош за жртвите од цунамито на Далечниот Исток се лажни;

– „Herbal Viagra“: Во полето на алтернативните онлајн медицински третмани со кои се спамираат корисниците, поголемиот дел на производи немаат позитивни ефекти (ако воопшто се изврши нивна достава) или се опасни по човековото здравје;

– „Руски невести“: Веб страни кои нудат контакти со убави жени од источна Европа и евтини посети во земјите од поранешниот Советски Сојуз;

– Добивки на лотарија: Барање за исплата на добивки од лотарија или помош за освојување на победа. Најчесто, станува збор за странски лотарии.

– „Phishing“: Терминот phishing е сложенка што ја користи првата буква P од зборот password (анг. лозинка) и fishing (анг. риболов). Го опишува стекнувањето податоци за лажни веб-страници, измамничка е-пошта и малициозен софтвер. Притоа, не се доаѓа само до лозинките, туку и до сите други податоци за дигиталниот идентитет. (Stammer 2012). Електронската пошта личи како да е од добро познат извор (на пример банка или интернет сервис провајдер) со која се бара да се потврдат личните податоци. Во поопасната варијанта на фишинг, жртвата е упатена на локација, и посетувајќи ја, предизвикува инфекција со малициозен софтвер. Само со кликнување на линкот во пораката, постои ризик од зараза на компјутерот со вирус (пр. тројански коњ). Тој ги регистрира податоците и ги препраќа го сторителите, и тие понатаму ќе ги употребат за криминални цели (https://www.justiz.bayern.de/media/images/behoerden-und-gerichte/sicher_surfen.pdf).

5. КРИВИЧНО-ПРАВНА РЕГУЛИРАНОСТ НА КОМПЈУТЕРСКИТЕ ИЗМАМИ ВО РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

Со донесувањето на Кривичниот законик на Република Македонија во 1996 година, се предвидеа типични инкриминации како компјутерски кривични дела, но исто така и во одредени класични инкриминации се воведоа одредби за можноста од извршување со компјутер или во случај на нападната компјутерска мрежа или компјутерски систем. Од друга страна, измените и дополнувањата на Кривичниот законик на РМ од 2004 година внесоа значајни промени со изменување на содржината и дополнување на инкриминациите, а исто така се креирани и нови инкриминации.

Од воведувањето на кривичното дело „Компјутерска измама“ од 2004 година е изминат период од скоро две децении, што го прави овој проблем актуелен за теоретско проучување и добивање на истражувачки сознанија како за криминалистичките карактеристики, така и за откриените кривични дела и санкционираните сторители, но и

сознанија за видот и висината на криминалната корист или нанесената штета со ова кривично дело во Република Северна Македонија.

Потоа, со измените на Кривичниот законик од 2008 година, македонското материјално казнено законодавство ги имплементира препораките од Конвенцијата за компјутерски криминал со тоа што, прво се постави дефиниција на најважните поими што се употребуваат во процесот на инкриминирање на нови кривични дела и при измените и дополнувањата на веќе постоечките кривични дела. Исто така, во согласност со измените и дополнувањата на Кривичниот законик од 2009 година се донесуваат збир од квалитативни промени во казненото законодавство, и тоа најмногу преку воведувањето на правни норми што се однесуваат на попрецизно определување на одговорноста на правните лица, делот на конфиксација на имот, редефинирање на економските казнени дела, како и редефинирање на компјутерските кривични дела. Посебно се дефинирани и значајните норми што се користат во инкриминациите на кривични дела од претходно споменатите групации. Ова е многу значајно во водењето на постапките за откривање, расветлување, докажување и превенција на компјутерскиот криминал, најмногу поради тоа што не е можно да се работи на криминални случаи и расветлување и докажување на криминал, ако во времето на извршување на ваквите дејствија, истите дејствија не биле предвидени како кривични дела.

Компјутерската измама, како што беше споменато во претходните поглавја, е подвид на компјутерскиот криминал. Од друга страна, компјутерскиот криминал како таков е инкриминиран во Кривичниот Законик, во кој се наведени и материјалните одредби. (Зврлевски и сор. 2014).

Од спроведените истражувања во нашата држава, според Николоска и Ѓошева, за периодот 2007 – 2017 година, за сторено кривично дело „Компјутерска измама“ по Член 251 б пријавени се вкупно 17 сторители, од кои 14 се обвинети и истите се осудени. (Николоска и Ѓошева; 2019).

Зачестеноста на пријавите за компјутерски измами е официјално потврдена и според податоците објавени на официјалниот сајт на Министерството за внатрешни работи на Република Северна Македонија, каде што е наведено дека ваквите пријави доаѓаат од страна на правни и физички лица кои се македонски државјани и се однесуваат на сомненија за измами извршени преку Интернет. Најчесто, жртви се македонски граѓани

и правни лица, а наведени се поактуелни начини на извршување на кривичното дело компјутерска измама.

6. АНАЛИЗА НА КРИМИНАЛНИ СИТУАЦИИ СО КОМПЈУТЕРСКИ ИЗМАМИ

Во продолжение ќе наведеме неколку примери за извршување на компјутерска измама на територијата на Република Северна Македонија.

Пример 1: *Според Секторот за внатрешни работи СВР Струмица, е објавена информација дека „Во јули 2021 година е откриен случај со меѓународна полициска соработка за криминална ситуација во која осомничени лица во повеке наврати извршиле неовластен упад во електронската комуникација помеѓу правен субјект од Радовиш и правен субјект од Лондон и со менување и прекривање, односно пренасочување на компјутерски податоци доставиле лажни фактури на кои извршиле промена на сметката на која требало субјектот од Радовиш да изврши уплата. Врз основа на вака изготвени лажни фактури правниот субјект од Радовиш извршил 4 уплати на различни сметки во банки во Велика Британија, за кои преку меѓународна правна помош е утврдено дека се сопственост на четворицата осомничени од Велика Британија. Со стореното дело осомничените се стекнале со противправна имотна корист во висина од 15.006.000 денари (244.000 евра), на штета на правниот субјект од Радовиш*“ (aktor.mk/chetvorica-britanci-so-komjuterski-izmami-zakrpile-firma-od- radovish-so-244-iljadi-evra---eve-kako-se-fateni-od-mvr)

Од аспект на криминалистичките карактеристики, според начинот на извршување станува збор за неовластен упад во електронска комуникација, достава на лажни фактури и промена на сметката со менување, прекривање и пренасочување на компјутерски податоци. Извршен е во јули 2021, со помош на компјутери, од страна на правен субјект (четворца осомничени), а за простор и место на извршување се сметаат Република Северна Македонија и Велика Британија.

Пример 1	
Начин на извршување	Неовластен упад во електронска комуникација, достава

	на лажни фактури и промена на сметката со менување, прекривање и пренасочување на компјутерски податоци,
Време и период на извршување	јули 2021
Средства на извршување	компјутери
Простор и место на извршување	Република Северна Македонија, Велика Британија
Организираност на сторителите	група од четворица осомничени (правен субјект)

Пример 2: *Во јануари 2023, кривична пријава за компјутерска измама поднесе и ОВР Гевгелија. Станува збор за четириесет годишник, кој со компјутерска измама проневерил над 20.000 евра. За И.Т.(40) од Богданци постоело основано сомнение за сторено кривично дело „оштетување и неовластено навлегување во компјутерски систем''. И.Т. од Богданци на 29.11.2022, користејќи програма преземена од интернет, навлегол во персонален компјутер на правно лице од Скопје – претставништво во Гевгелија и направил долг во висина од 1.249.000 денари*. (https://gevgelijanet.com/2023/01/27/).

Пример 2	
Начин на извршување	Оштетување и неовластено навлегување во компјутерски систем,
Време и период на извршување	ноември 2022
Средства на извршување	компјутери, програма преземена од интернет
Простор и место на извршување	Богданци, Гевгелија, Скопје
Организираност на сторителите	еден извршител

Пример 3: *Секторот за внатрешни работи Тетово до Основното јавно обвинителство Тетово поднесе кривична пријава против правно лице со седиште во тетовско Селце Кеч, А.М.(22) од истото село и А.С.(36) од тетовско Милетино. Против правниот субјект поради основи на сомнение за сторени три кривични дела „компјутерска измама", „злоупотреба на лични податоци" и „лажно претставување", А.М. поради основи на сомнение дека ги сторил трите споменати кривични дела и А.С. поради сомнение дека сторил кривично дело „несовесно работење во службата".*

А.С. се сомничи дека како вработен во општина Тетово во текот на 2021 година креирал е-маил адреса и му ја предал на А.М., кој е сопственик и управител на правниот субјект, без согласност и знаење на неговиот претпоставен во општина Тетово. Оваа службена е-адреса А.М. потоа ја користел за директен контакт со повеќе социјални мрежи, лажно претставувајќи се дека е началник на Отсек за превенција на сајбер криминал за подрачјето на Тетово и користејќи лажна легитимација со лажен број, електронската адреса ја користел за затворање профили и кориснички имиња, а правниот субјект, пак, лажно се претставувал како државна агенција за сабјер криминал (https://mk.tv21.tv/krivichna-prijava-za-kompjuterska-izmama-lazhno-pretstavuvane/)

Анализата на овој случај покажува дека овде има специфични карактеристики т.е. станува збор за повеќе извршени кривични дека во една криминална ситуација или стек на кривинични дела. На пример, покрај компјутерска измама забележуваме и злоупотреба на службена положба, лажно претставување итн.

Пример 3	
Начин на извршување	Креирање на службена е-маил адреса без знаење на претпоставениот, која е користена за лажно претставување на социјални мрежи и за затворање на профили и кориснички имиња,
Време и период на извршување	2023
Средства на извршување	компјутери, службена e-mail адреса, лажна легитимација со лажен број
Простор и место на извршување	Селце, Милетино, Тетово
Организираност на сторителите	организирани извршители преку правен субјект

Пример 4: *Секторот за компјутерски криминал и дигитална форензика при МВР до надлежното ОЈО поднесе кривична пријава против М.Ш. (53) и А.Ш. (49) поради постоење основано сомнение за сторено кривично дело – "компјутерска измама" по чл.251-б од КЗ на Република Северна Македонија. Имено, пријавените со цел да се стекнат со противправна имотна корист формирале Фондација "Допир" и креирале веб*

страна https://bidihumansega.mk/ која активно работела на собирање средства за помош на деца со посебни потреби и ретки болести.

Од страна на Секторот за компјутерски криминал и дигитална форензика, утврдено е дека регистрант на веб страната https://bidihumansega.mk/ е лицето М.Ш., кој и воедно е претседател на Фондацијата.

Во рамки на спроведената истрага, Секторот за компјутерски криминал и дигитална форензика изврши низа проверки, меѓу другото и околу тоа дали лицата, односно корисниците на веб страната за кои се собираат донации, евидираат во системот на Министерството за внатрешни работи и притоа констатирано е дека поголемиот дел од корисниците не постојат, односно креирани се измислени, лажни, фиктивни профили преку кои веб страницата собирала донации и парични средства. Притоа утврдено е и дека заклучно со 27.03.2019 година преку веб страната https://bidihumansega.mk/ собрани биле 3.531.199 денари.

По направената анализа на банкарските сметки констатирано е дека од собраните парични средства, пријавените вршеле повлекување на парични средства за сопствени потреби. На 27-ми овој месец, а по претходно обезбедена судска Наредба за претрес, издадена од Основен суд Скопје I Скопје, извршен е претрес на деловни простории во стан во Скопје, при што беа пронајдени голем број на докази кои укажуваат дека лицата М.Ш. и А.Ш. свесно вршеле внесување на невистинити податоци и фотографии од деца кои биле предмет за собирање на парични средства по основ на донации и со тоа довеле во заблуда голем број на граѓани и правни лица кои донирале парични средства. Со Наредба од Судија за претходна постапка од Основен Суд Скопје I – Скопје, паричните средства од фондацијата се замрзнати.

Начинот на извршување вклучува креирање на фондација, веб-страна и лажни профили, преку кои се собирале донации и парични средства. Во 2019 година, со помош на компјутер т.е. креирање на веб-страна, на територијата на Република Северна Македонија, лицата М.Ш. формирале фондација и свесно вршеле внесување на невистинити податоци и фотографии од деца кои биле предмет за собирање на парични средства по основ на донации, доведувајќи во заблуда голем број на граѓани и правни лица.

Пример 4	
Начин на извршување	Креирање на фондација, веб-страна и лажни профили, преку кои се собирале донации и парични средства
Време и период на извршување	2019
Средства на извршување	компјутер, веб-страна
Простор и место на извршување	Република Северна Македонија
Организираност на сторителите	Лицата М.Ш. и А.Ш. (кои биле и во роднинска врска) формирале фондација и свесно вршеле внесување на невистинити податоци и фотографии од деца кои биле предмет за собирање на парични средства по основ на донации, доведувајќи во заблуда голем број на граѓани и правни лица

6.1. Компарација на криминализацијата на компјутерската измама во земјите во регионот

Во продолжение ќе разгледаме како е регулирана компјутерската измама во земјите од регионот, претставено преку примерите на Србија и Албанија. Измамата и компјутерската измама се криминализирани во кривичното законодавство на Република Србија. Кривичното дело измама (чл. 208 од КЗ) го прави тој што со намера да прибави противправна парична корист за себе или за друг, некого ќе доведе во заблуда со лажно прикажување или прикривање факти или го држи во заблуда и притоа го поттикнува да направи нешто на штета на својот или туѓ имот прави или не прави. Сторителот на ова кривично дело ќе се казни со затвор од шест месеци до пет години и парична казна. Тој што ова дело ќе го стори само со намера да повреди друг, ќе се казни со затвор до шест месеци и парична казна. Овде зборуваме за привилегирана форма на кривично дело за кое е предвидена поблага казна во однос на основната форма. Доколку е прибавена дел од имотната корист или е причинета штета во износ поголем од четиристотини и педесет илјади динари, сторителот ќе се казни со затвор од една до осум години и парична казна. Доколку е прибавена дел од имотната корист или е причинета штета во износ поголем од

милион и петстотини илјади динари, сторителот ќе се казни со затвор од две до десет години и парична казна. Во овој случај, висината на незаконски стекнатата имотна корист е квалификациона околност. Од друга страна, кривичното дело компјутерска измама (чл. 301 од Кривичниот законик) го прави тој што внесува неточни информации, не внесува точни информации или на друг начин прикрива или лажно презентира информации и на тој начин влијае на резултатот од електронската обработка. и преносот на податоци со намера да се даде, добива противправна имотна корист од друг и на тој начин предизвикува друга штета на имотот (Мирић 2018).

На страницата на Министерството за внатрешни работи на Република Србија, во врска со компјутерските измами е наведено дека високотехнолошкиот криминал вклучува кривични дела против безбедноста на компјутерските податоци, и тоа:

- Оштетување на компјутерски податоци и програми;
- Компјутерска саботажа;
- Креирање и воведување на компјутерски вируси;
- Компјутерска измама;
- Неовластен пристап до заштитен компјутер, компјутерска мрежа и електронска обработка на податоци;
- Спречување и ограничување на пристапот до јавна компјутерска мрежа и
- Неовластено користење на компјутер или компјутерска мрежа.

Покрај горенаведените кривични дела, во оваа област спаѓаат и кривичните дела против интелектуалната сопственост, сопственоста и правниот сообраќај, каде што компјутерите, компјутерските мрежи, компјутерските податоци, како и нивните производи во материјална или електронска форма се јавуваат како предмети или средства за извршување на кривични дела. Согласно оваа законска дефиниција, областа на високотехнолошкиот криминал опфаќа и кривични дела каде што компјутерите и компјутерските мрежи се јавуваат како средство за извршување на кривичното дело измама, злоупотреба на платежни картички на Интернет, злоупотреба во областа на електронската трговија и банкарство, злоупотреба на деца за порнографски цели на Интернет (т.н. детска порнографија), говор на омраза на Интернет (ширење национална, расна, верска омраза и нетрпеливост итн.) Најчестите форми на извршување криминални дејствија на Интернет се компјутерска измама поврзана со аукциски интернет-страници

(електронски продавници), компромитирање и злоупотреба на платежни картички, „нигериски“ измами и DDoS напади. (http://www.mup.gov.rs/wps/portal/sr/gradjani/saveti/)

Во Република Албанија, компјутерската измама исто така се вбројува во имотниот криминал. Според Членот 143/б од Кривичниот законик на Република Албанија, компјутерската измама претставува внесување, менување, бришење или отстранување на компјутерски податоци или мешање во работата на компјутерски систем, со цел да обезбеди за себеси или за трети лица, со помош на измама, нелегална економска корист или предизвикување на губење на имотот на трето лице. Компјутерската измама се казнува со затвор, во траење од шест месеци до шест години. Кога ова кривично дело се извршува во соработка, на штета на повеќе лица, или кога донело тешки материјални последици, се казнува со затвор од пет до петнаесет години (https://akshi.gov.al/wp-content/uploads/2020/11/LEGJISLACIONIMBIKRIMINKIBERNETIK.pdf)

Во Република Бугарија, во дигиталната ера, компјутерската измама станува се поважна. Според чл. 263а од Кривичниот законик, во овој случај, физичкото лице не е цел на измамата, а измамникот е машина. Казната, како и во класичната измама, е парична казна или затвор до 5 години. Прекршителот влијае на исходот од процесот на обработка на податоци. Законот споменува 4 начини на дејствување, имено: неправилно програмирање, употреба на неточни или нецелосни податоци, неовластена употреба на податоци и друго неовластено влијание врз процесот на обработка на податоците. (https://www.bg-anwalt.de/bg/infoteka/nakazatelnopravo/izmama_komputyrna_izmama_i_nepravomerno_izpolzvane_na_uslugi.html)

Компјутерската измама е инкримирана и во Република Хрватска, и тоа во член 271 од Кривичниот законик. Таму стои дека тој што со цел да прибави противправна имотна корист за себе или за друг, внесува, менува, брише, оштетува, прави компјутерски податоци неупотребливи или недостапни или го попречува работењето на компјутерски систем и на тој начин предизвикува штета на друг, ќе се казни со затвор од шест месеци до пет години.

Ако со кривичното дело од ставот (1) на овој член е направена значителна штета или е прибавена значителна корист, сторителот ќе се казни со затвор од една до осум години (https://zakonipropisi.com/hr/zakon/kazneni-zakon/271-clanak-racunalna-prijevara)

Анализата на кривичното законодавство на Босна и Херцеговина укажува дека кривичното законодавство на Босна и Херцеговина обезбедува кривична правна заштита на компјутерските системи и електронските системи за обработка на податоци со цел да се постигне нивна непречена употреба од од сопственикот или овластен корисник. Исто така, кривичното законодавство на Босна и Херцеговина го казнува секое лице кое користи компјутери како средство за извршување на криминални дејствија: детска порнографија, перење пари, тероризам и други криминални дела поврзани со активности на Интернет. Затоа, со пропишување на кривични дела со кои се заштитуваат компјутерските системи и податоци, се создаде основа за кривично гонење, со тоа што ефективноста на кривичното гонење зависи од многу услови, а пред се од јасноста на нормите содржани во кривичното дело (Плех 2019).

Бидејќи веќе дојдовме до констатацијата дека компјутерските измами не се случуваат во изолација, можеме со голема веројатност да претпоставиме дека тие се значаен проблем и за земјите од регионот. Во ова поглавје ќе ги разгледаме карактеристиките на компјутерските измами од пет земји од регионот, а потоа ќе наведеме два случаи: Еден од Србија, и еден од Албанија. Потоа ќе извршиме споредба со случаите од Република Северна Македонија.

Пример 1: *Во февруари 2023, Српското обвинителство за високотехнолошки криминал (ВТК) го започна вториот дел од меѓународната акција „Infinity“ во врска со финансиски измами на интернет, а досега се уапсени 16 осомничени за компјутерска измама, соопштено е во Белград. Првиот дел од акцијата е спроведен во јануари. Направен е претрес на повеќе локации и добиени се значајни податоци и докази, а со анализата на овие податоци е утврдено основано сомнение дека вработени во најмалку две фирми во изминатите неколку години оштетиле повеќе од 127.000 граѓани на други земји во вкупен износ кој надминува седум милијарди долари, а точната сума сè уште се утврдува. Уапсените во вториот дел од акцијата се обвинети дека измамиле најмалку 200 странски државјани во вкупен износ над 20 милиони американски долари, повикувајќи се на измамнички финансиски трансакции на Интернет. Акцијата е иницирана со Eurojust, агенцијата на Европската Унија за соработка во кривичното правосудство и командата на Федералната полиција на Австралија, а Специјалното обвинителство на*

Србија наведува дека се претресени 16 локации во Белград и низ Србија. Покрај 16-те уапсени за компјутерска измама, перење пари и криминален заговор, досега се запленети повеќе од 130.000 евра во готовина, неколку сметки со криптовалути и неколку автомобили, а во тек се и имотни проверки. Специјалното обвинителство за високотехнолошки криминал ги предупреди граѓаните на Србија и странските државјани кои живеат и работат во Србија да бидат особено внимателни при понудите за вработување во таканаречените „кол-центри“, кои наводно ги едуцираат и советуваат клиентите на кој било финансиски пазар, вклучително и тргувањето со крипто валути. Таквите активности се строго регулирани со Законот за пазар на капитал и активностите на Комисијата за хартии од вредност, која ги издава потребните дозволи (https://netpress.com.mk/srbi-a-apse-a-poradi-me-unarodna-izmama-na-internet-vredna-mili-ardi-dolari/)

Анализата покажа дека станува збор за внимателно организирана измама, при што начинот на извршување се состои од измамнички финансиски трансакции на Интернет, со помош на компјутери и други електронски уреди. Периодот на извршување е 2023, а просторот и местото се Белград и други локации низ Србија. Сторителите се соработници од исти фирми.

Пример 1	
Начин на извршување	измамнички финансиски трансакции на Интернет
Време и период на извршување	2023
Средства на извршување	компјутери и други електронски уреди
Простор и место на извршување	Белград и други локации низ Србија, со штети нанесени на граѓани од други земји
Организираност на сторителите	соработници од исти фирми

Пример 2: *Во јули 2023, албанската полиција објави нови детали за нападот на групата која се занимавала со компјутерска измама. Од 14 лица под истрага, 5 се оставени во затвор, 4 во домашен притвор и по пет други се прогласени за трага. Тие телефонски измамиле италијански државјани и според истрагата оваа измама изнесува 4,7 милиони евра. Во акцијата на терен, запленети се разновидна компјутерска опрема,*

мобилни уреди, УСБ и друга опрема за производство на биткоини, откриени при проверките извршени во повеќе станови. Албанските обвинители заедно со италијанските специјалци на прес-конференцијата рекоа дека истрагите за онлајн измами се тешки и затоа побараа континуирана соработка за напад на оваа раширена појава. Претставникот на италијанската полиција изјави дека станува збор за тешки истраги, бидејќи криптовалутите се користат за да се сокријат приходите од незаконски активности, а истрагата е во тек.

Според начинот на извршување станува збор за телефонска измама, во која учествувала организирана група на сторители од вкупно 14 лица. Во 2023 година, со помош на компјутери, мобилни телефони и УСБ, измамата се одвивала на просторот на Албанија и Италија.

Пример 2	
Начин на извршување	телефонска измама
Време и период на извршување	2023
Средства на извршување	компјутери, мобилни уреди, УСБ
Простор и место на извршување	Албанија, Италија
Организираност на сторителите	организирана група од 14 лица

Споредувајќи ги примерите за компјутерски измами од Република Северна Македонија со примерите од земјите од регионот, набљудуваме неколку сличности. Во врска со начините на извршување, забележуваме дека во примерите од земјите од регионот, станува збор за измамнички финансиски трансакции на Интернет (Србија) и телефонска измама (Албанија). Од средствата, најчесто се користат компјутери и мобилни уреди, а сторителите најчесто се организираат во групи или делуваат преку иста фирма.

Во примерите од Република Северна Македонија наведени во извештаите на МВР, забележуваме дека најчесто се случуваат оштетување и неовластено навлегување во компјутерски систем и компјутерска измама, со помош на претходно украдени платежни картички при купување на интернет и плаќање на сметки преку интернет (e-commerce) и со неовластено навлегување во компјутерски системи со промена на содржина на веб

страниците на правни лица (2018 година). Во 2019 година, компјутерските измами се се значително покомплексни, а кај интернет измамите најчести се лажните огласи за купопродажба на интернет портали и пресретнување на e-mail комуникација помеѓу приватни фирми со цел нивна измама, насочување и плаќање на друга банкарска сметка. Во текот на 2020 година, измамите се направени со измама при електронска уплата за изнајмување на стан, подигнати парични средства од кредитни картички на правно лице и со пресретнување на email комуникација помеѓу приватни фирми со цел нивна измама, насочување и плаќање на друга банкарска сметка. Во 2021, најпрепознатлив е случајот на четирите унгарски државјани со привремен престој во Велика Британија, кои од август до декември 2020 година извршувале повеќекратен неовластен упад во електронската комуникација помеѓу правен субјект од Република Северна Македонија и странско правно лице од Лондон, при што со менување и прикривање и пренасочување на компјутерските податоци доставиле лажни фактури со што ги довеле во заблуда правните субјекти, поради што биле извршени четири уплати на различни сметки во банки во Велика Британија. Исто така, вработен во единица на локална самоуправа извршил неовластено навлегување, менување и внесување на лажни податоци во финансовата картица на даночен обврзник, додека останатите кривични дела се извршени преку измама на лица при уплата на сретства за изнајмување на стан, уплата на сретства за стекнување ваучер со криптовалути и уплата на парични средства кон лица од Р. Турција по основ на наводна добивка на награда. Во 2022, карактеристичен е случајот во кој бугарски државјанин, преку испраќање на електронски пораки од странски повикувачки број довел во заблуда лице преку ветување за стекнување на наследство. Исто така, регистриран е случај во кој шалтерски работник од АД Македонска Пошта при наплата на сметки од странки истите не ги евидентирал во системот, односно внесувал податоци од друг корисник со кое вршел препечатување на претходно уплатени сметки, а паричните средства ги задржувал за себе. Едно кривично дело е извршено и од страна на вработен во правно лице кој извршил бришење на компјутерски податоци.

Од другите наведени примери за Република Северна Македонија, можеме да ги забележиме следните начини на извршување: неовластен упад во електронска комуникација, достава на лажни фактури и промена на сметката со менување, прекривање и пренасочување на компјутерски податоци, оштетување и неовластено навлегување во

компјутерски систем, создавање на службена e-mail адреса за измамнички цели, како и креирање на фондација, веб-страна и лажни профили за собирање на донации и парични средства.

Забележуваме сличности во средствата за извршување на измамите: компјутери што се користат за нелегални трансакции, креирање на измамнички веб-страни итн, како и мобилни уреди за извршување на телефонски измами. И во Република Северна Македонија, сторителите поретко делуваат сами, а многу почесто во организирани групи, на пример, соработувајќи како дел од иста фирма, формирајќи фондации и слично.

Во врска со просторот и местото на извршување на кривичното дело, во претходните поглавја беше наведено дека местото на извршување на компјутерската измама најчесто е во тесна врска со локацијата на компјутерот од којшто криминално се дејствува, иако последиците можат да се забележат дури и на другиот крај од светот. Ова се потврди и во примерите од Република Северна Македонија: На пример, во извештајот на МРВ од 2018 година е истакнато дека „и понатаму е присутен трендот на нелегално преземање и посредување во деловната комуникација преку електронска пошта помеѓу македонски и странски компании, при што е вршено пренасочување на банкарските трансакции“. Исто така, примерот бр.1 од Република Северна Македонија забележуваме дека просторот и местото на извршување се Северна Македонија, но и Велика Британија. Во примерот од Република Србија, кривичното дело се одвивало во Белград и други локации низ Србија, со штети нанесени на граѓани од други земји.

6.2. Земји од Европската Унија

Со оглед на тоа што компјутерските измами последниве години се зачестена криминална појава која има меѓународен карактер, земјите-членки на Европската Унија не се одминати од неа. Имено, околу три четвртини од жителите во Европската Унија често користат интернет, па затоа се привлечна цел за сајбер криминалците. Со цел да се избегнат ваквите појави, во април 2012 година, Европската комисија предложи формирање на Центар за борба против компјутерскиот криминал како дел од Европол. Овој предлог беше одобрен од Советот во резолуцијата во јуни 2012 година, а со

реализација се започна на 1 јули 2012 година (https://www.bmi.gv.at/magazinfiles/2012/11_12/files/europol_cybercrime.pdf).

Според податоците на ЕВРОПОЛ за начинот на извршување на овие криминални активности, се издвојуваат неколку вида компјутерски измами што полицијата најчесто ги забележала во случаите на кои работела. Првата е наречена „романтична измама“, во која, вообичаено, измамникот им приоѓа на поединци преку апликации за пронаоѓање сродни души или, пак, преку социјалните медиуми. Притоа почнува како романса и додворување, сè додека не се стекне доволно доверба за да се отвори прашањето за инвестирање. Кога доаѓа до тој момент, измаменото лице најчесто останува „покусо“ за неколку илјади евра, а љубовта е користена само како емотивна заблуда за оштетениот. Вториот вид случаи на измами се наречени „пријателски измамник“, при што измамниците најчесто отвораат профили како вашите пријатели и комуницираат со вас. Бидејќи вие немате никаков сомнеж дека не комуницирате со вашиот пријател, многу лесно станувате дел од измамничка инвестициска шема, во која ќе загубите многу пари. „Шанса за бизнис“ е третата најатрактивна измама за криминалците. Измамникот ѝ се обраќа на потенцијалната жртва нудејќи ѝ неповторливи шанси за криптоинвестиции. Ја убедува жртвата дека треба да инвестира врз база на лажно успешни и профитабилни компании. Во многу случаи, жртвата на крајот сфаќа дека не може да ги повлече инвестираните пари и дека е измамена. Не секоја реклама е вистинска и токму затоа многу е важно да не се наседнува на сите реклами што ги гледате на социјалните мрежи. Во првиот миг кога некоја примамлива реклама ќе ви го привлече вниманието да кликнете на неа, вие ги испраќате вашите лични податоци, по што добивате повик од измамник, кој ќе ве убеди да инвестирате.
(https://novamakedonija.com.mk/category/multimedija/galerija/)

Пример 1: *Во јануари 2023 во Република Бугарија е спроведена голема акција против бугарска банка за криптовалути. Инспекторите тврдат дека 94 милијарди долари промет поминал преку платформата NEXO, која е поврзана со поранешен пратеник. Над 300 обвинители и специјални полицајци биле вклучени во проверката за тоа дали постоеле податоци за перење пари и даночни кривични дела. Во изминатите месеци, криптобанката имаше проблеми и во САД за работа без лиценца, но не и во*

Бугарија. За еден од главните клиенти на криптобанката во Бугарија се наведува дека финансирал терористички акти. Пребарани се повеќе од 15 адреси поврзани со криптобанката. Платформата била вклучена во трговија со криптовалути на берзи во Британија, Швајцарија, САД и офшор дестинации. Како што изјави портпаролката на главниот обвинител, Сијка Милева, предмет на истражување се активностите на организирана криминална група, и тоа перење пари, даночни кривични дела, кривични дела поврзани со банкарство без потребна лиценца и компјутерска измама, а за последните пет години преку платформата поминале повеќе од 94 милијарди долари промет. Компанијата развивала шема за привлекување на странски државјани да инвестираат во биткоини за многу високи каматни стапки.

Светослав Василев од Одделот за компјутерски криминал при Министерството за внатрешни работи изјави дека се откриени над 3,6 милиони трансакции од и до крипто берзата Nexo. Коосновач и управен партнер на Нексо е поранешниот пратеник во Реформскиот блок, Антони Тренчев. Меѓу оние кои биле на разговор во Обвиителството се директорот на Нексо, Коста Канчев и финансискиот директор Калин Методиев. Нексо објави неколку пораки на Твитер, без да им прецизира на своите следбеници дека се кривично гонети. Компанијата Нексо објави соопштение во кое се вели дека се уште не им се претставени официјални документи кои недвосмислено би укажувале против нив (https://fokus.mk/golema-aktsija-protiv-bugarska-banka-za-kriptovaluti/).

Од извршената анализа, можеме да заклучиме дека според начинот на извршување, станува збор за компјутерска измама преку криптобанка. Имено, во 2022 година, со помош на компјутери како средства за извршување на измамата, организирана група преку фондацијата NEXO во Бугарија, Британија, Швајцарија, САД и офшор дестинации, учествувала во оваа компјутерска измама.

Пример 1	
Начин на извршување	измама преку криптобанка
Време и период на извршување	2022

Средства на извршување	компјутери
Простор и место на извршување	Бугарија, Британија, Швајцарија, САД и офшор дестинации
Организираност на сторителите	организирана група преку фондацијата NEXO

Пример 2: *Во јули 2023 година е откриен случај на компјутерска измама во Нирнберг, каде измамници ограбија десетици луѓе со помош на лажни СМС-пораки и на тој начин украдоа милионски суми. Окружниот суд Нирнберг-Фурт ги осуди петте мажи на затворски казни за компјутерска измама. Друг обвинет доби условна казна за помагање и поттикнување на измамата, изјави портпаролката на судот. Шестминатa обвинети на возраст од 20 до 30 години пред судот ги признаа наводите и со тоа го скратија процесот. Бидејќи четворица од обвинетите биле на возраст меѓу 18 и 21 година за време на делото, судењето се одржа пред совет за малолетници. На четворицата им е изречена малолетничка притвор од четири години до една година и девет месеци. Двајцата постари обвинети се осудени на три години и шест месеци затвор и две години условно.*

Обвинетите испратиле лажни СМС-пораки до повеќе од 400 лица, лажејќи дека тоа се пораки од нивните банки. Кога примателите потоа ги открија своите податоци за пристап за онлајн банкарство, тогаш обвинетите ги ограбиле сметките на засегнатите. Според обвинението, тие биле успешни во повеќе од 360 случаи. Причинетата штета со делата во периодот од април 2021 до март 2022 година изнесува околу 1,4 милиони евра. Во некои случаи, банката забележала измама или сметката била блокирана навреме.

Според начинот на извршување, станува збор за измама со испраќање на лажни СМС-пораки и измама преку онлајн банкарство. Во периодот од април 2021 до март 2022, во Нирнберг, Германија, организирана група од шест лица со помош на мобилни телефони биле вклучени во извршување на измамата.

Пример 2	
Начин на извршување	испраќање на лажни СМС-пораки, измама преку онлајн банкарство
Време и период на извршување	април 2021 – март 2022
Средства на извршување	мобилни телефони
Простор и место на извршување	Нирнберг, Германија
Организираност на сторителите	организирана група од шест лица

Споредувајќи ги примерите за компјутерски измами од Република Северна Македонија со примерите од земјите од Европската Унија, можеме да препознаеме голем број на сличности. Средствата на извршување се во голема мера идентични (компјутери и мобилни телефони). Исто така, забележуваме сличности од аспект на организираноста на сторителите: Извршителите на компјутерски измами многу поретко дејствуваат сами, а многу почесто се организирани во групи, на пример, преку фирми или формирање на различни фондации (најчесто измамнички). Тие најчесто имаат одлични познавања од областа на компјутерската технологија и карактерни црти што им овозможуваат да ги измамат жртвите. Истото го забележуваме и во примерите кај земјите од регионот. Периодот и времето на извршување најчесто се со подолго траење т.е. со месеци па дури и години (како што забележуваме во примерот бр. 2). Просторот и местото на извршувањето не мора да се ограничени само на еден град или држава (како што забележуваме во примерот бр. 1) Според тоа, без разлика дали станува збор за Република Северна Македонија, регионот или земјите од Европската Унија, можеме да заклучиме дека кај сторителите на компјутерски измами се забележуваат одредени шеми на дејствување, што понатаму може да помогне за влегување во нивните траги.

КРИМИНАЛИСТИЧКИ КАРАКТЕРИСТИКИ И КРИМИНАЛИСТИЧКО ИСТРАЖУВАЊЕ НА КОМПЈУТЕРСКИТЕ ИЗМАМИ

1. КРИМИНАЛИСТИЧКИ КАРАКТЕРИСТИКИ НА КОМПЈУТЕРСКИТЕ ИЗМАМИ

Компјутерските измами, како што напоменавме во претходните поглавја, се инкриминирани кривични дела со сопствени карактеристики. Како и секое друго кривично дело, и за нивното разоткривање и сузбивање е потребен систематски пристап за нивно проучување, истражување и расветлување. Според Николоска (2013), криминалистичкото истражување претставува систематско проучување на кривичните дела и проблемите што произлегуваат од нарушувањето на редот. Тоа и е од помош на полицијата при казненото делување, намалувањето на кривичното дело и нередот, како и спречување и проценка на криминалот. Тоа означува и набљудување одблизу и истражување. За разлика од класичниот криминалитет, каде што несоборлив доказ е материјалниот доказ што ги носи трагите од сторителот и на жртвата, кај компјутерскиот криминалитет треба да се гради цврст електронски т.е. дигитален доказ со низа од материјали и елементи со кој се гради спој на идеални докази. Станува збор за дигитални траги што се скриени во компјутерскиот систем. Исто така, како доказ се зема и последицата од извршеното кривично дело, на пример, компјутерски фалсификуван документ. На пример, кај ваквиот документ, од клучна важност е кои се мотивите за негово изготвување, кој го порачал и за кого е наменет,

Иако компјутерскиот криминал, а со тоа и компјутерските измами како негов подвид, се од релативно понов датум, сепак тие имаат свои специфики што се однесуваат на сторителот, средството на извршување, местото, времето на извршување и настанатите последици и штети. Сепак, не станува збор за посебна област на криминалитет по објектот на напад на заштитен објект, како што е класичниот, економскиот или политичкиот криминалитет. Тоа што е најспецифично за компјутерскиот криминалитет е компјутерот како средство на извршување или како средство за подготовка и реализација на друго кривично дело т.е. објект на криминален напад. Од клучна важност е истражувањето на компјутерскиот криминал да се одвива во целост, затоа што овие кривични дела можат

понатаму да бидат причина за извршување на други кривични дела, кои не се компјутерски.

1.1 Компјутерот како средство и објект на криминален напад кај компјутерските измами

Компјутерските измами се карактеризираат по тоа што за нивно извршување се потребни специфични средства. Особено е важно тоа што за негово извршување не се користи оружје и физичка сила туку само компјутери.

Од самиот поим *компјутерска измама* можеме да заклучиме дека компјутерот е најосновното средство за извршување на ваквата измама. Функцијата на компјутерот криминалистичко гледиште, како средство за извршување на кривично дело, може да се изрази преку фактот што сторителот се служи со компјутерот за да изврши одредено кривично дело, најчесто измама, кражба или проневера. Станува збор за кривично дело од областа на општиот криминалитет и стопанскиот криминалитет, кои имаат специфичен начин на извршување, имено, со употреба на компјутер, што воедно претставува и основа за нивно диференцирање од традиционалната поделба на криминалитетот и сведување под поимот на компјутерски кривични дела (Николоска, 2013).

Компјутерите се силни алатки, но во погрешни раце тие може да бидат и силно оружје. Со обезбедување на автоматизирани механизми за модификација и манипулација со електронски форми на општествени вредности, како што се програми и податоци кои реперезентираат стоки, пари или информации, во реализација на одредени криминални деликти, компјутерот се јавува како „субјект“ на криминален напад. Во оваа категорија компјутерските процеси се клучни и тие се користат за да овозможат, олеснат и / или да ја забрзаат реализацијата на одредени криминални активности, а компјутерот го креира единствениот амбиент во кој разновидните криминални активности се реално можни. Притоа, сторителот есенцијално вметнува нови програмски инструкции за да манипулира со компјутерските процеси или конвертира легитимни компјутерски процеси за нелегални (криминални цели)“ (Petrović S.; 2001).

За извршување на компјутерските измами најчесто се употребуваат компјутерските вирусите, кои се, несомнено, најпознатото и најкористеното средство. Станува збор за мали програми од неколку килобајти, што се “вгнездуваат” во други фајлови и имаат една

цел, имено, да направат штета на нападнатиот и заразен компјутер, менувајќи ги или бришејќи ги фајловите. Николоска (2013) ги дефинира вирусите како компјутерски програми или друг збир на наредби што се внесени во компјутерот или компјутерската мрежа, кои се направени на тој начин што можат самите себе да се размножуваат и во исто време на делуваат по давањето на програмата или збирот на наредби на програмите или податоците во компјутерот или во компјутерската мрежа. Криминалот со елементи на правење и внесување на компјутерски вируси е кривично дело што се извршува со помош на две дистинктивни казниви поведенија: Прво, правење на компјутерски вируси и второ, внесување на компјутерски вируси. Тие можат да се извршат од страна на едно лице или повеќе лица што прават поделба на улогите. На пример, дел од групата ги прави вирусите а другите сторители ги внесуваат (Николоска 2013).

Компјутерот може да се зарази преку фајлови од Интернет, од електронска пошта, посета на одредени веб страни итн. Најпознатите видови на вируси се следниве: фајл инфектор, присутен програм инфектор, инфектор на секторот за бутирање, комбиниран вирус, дропер, стелт вирус, вирус-следач, полиморфен вирус, мутациски вирус, генетски заснован вирус, логичка бомба, црв и заклопна врата. (Милковска 2012)

Несомнено, најпознатиот компјутерски вирус претставува Тројанецот, кој е програма што кога ќе биде уфрлена во компјутерот, ги праќа сите шифри на мејлот на оној што го уфрлил. Тој му овозможува на сторителот пристап до хард дискот, и со тоа сторителот може да чита, пишува, да менува фајлови и да има пристап до целокупната меморија (Николоска 2013).

1.2 Начини на извршување на компјутерската измама

Повеќе автори пишуваат за начините на извршување на компјутерските измами. Како што може да се заклучи од дефинициите за компјутерските измами, компјутерот е неизоставен дел за нивното извршување. Меѓутоа, компјутерските измами се карактеризираат и со некои специфични начини на извршување. На пример, Влајиќ и соработниците (2022), наведуваат дека станува збор за збир од кривични дела што се извршуваат со помош на користење на Интернетот, компјутерите или некои други електронски уреди, а во поширока смисла на зборот, се работи за криминални дела во кои

компјутерот или пак, Интернетот, се извор, предмет, средство, цел или простор на кривичното дело. Тие додаваат и нови елементи што се во врска со употребата на компјутерската техника како и со употребата на криминалистичката информатика. Николоска (2013) ги наведува следните начини на извршување на компјутерски измами:

- Со внесување на невистинити податоци во компјутер или информатички систем.
- Со невнесување на вистинити податоци
- Со електронски потпис
- На друг начин што има значително влијание врз резултатите на електронската обработка и преносот на податоците.

Компјутерските измами претставуваат најраширен облик на компјутерски криминалитет бидејќи опфаќаат манипулирање со компјутерските електронски програми во делот на софтверот или преку механички пат во делот на хардверот со цел стекнување на противправна имотна корист за себе или за друг или нанесување на штета. Во компјутерот се внесуваат невистинити податоци или се пропушта внесување на вистинити податоци или на било кој друг начин се врши измама. Бројот на манифестни облици на измами и начините на нивна реализација не е можно во потполност да се согледа бидејќи во практиката се јавуваат како примитивни и груби измами, но и измами каде криминалците манифестираат висок степен на знаења и вештини. (Nikolić–Ristanović & Konstantinović-Vilić, https://kriminalistikaibez.wixsite.com/website-1/post/kompjuterski-kriminalitet).

Бројот на облици на измами, како и начинот на нивната реализација е практично неограничен и во пракса се среќаваат од примитивни и „груби“ до измами за кои е користен висок степен на вештина и рафинираност. Но, во шемите за компјутерски измами секогаш се открива некој претходно постар користен облик на измама. Бидејќи во сите шеми на измами регистрирани на интернет се всушност преработени и прилагодени верзии на шеми, со кои некогаш и со векови се „ставани“ во заблуда невнимателни и лесноверни жртви. Компјутерските измами се карактеризираат со многу големо продирање, заради големината на интернетот како пазар, бидејќи брзо се шират со интернетот како медиум со кој се се случува многу брзо, а исто така и заради ниските трошоци за извршување на ваквиот вид на измами. Компјутерските измамници ги

злоупотребуваат карактеристиките на сајбер просторот за кој придонесува и растот на електронската трговија: анонимност, дистанца помеѓу продавачот и купувачот и моменталната трансакција. На тој начин тие ја користат и предноста на фактите дека измамата преку интернет не бара пристап до некој систем за исплата, како за тоа што бара секој друг вид на измама, а сито така и фактот дека дигиталниот пазар е сеуште недоволно уреден при што се создава одредена конфузаија за потрошувачите, што за компјутерските измамници се создаваат скоро идеални услови за компјутерски измами (Ачкоски 2012).

1.3 Време и период на извршување на компјутерската измама

Времето на извршување на компјутерскиот криминалитет (вклучително и компјутерските измами), како што нагласува Николоска (2013) го дава одговорот на клучното прашање, имено, кога се извршува овој вид криминалитет. Сепак, во одредена мера, тоа се разликува од кривичните дела од општиот или економскиот криминалитет. Иако компјутерот локациски се наоѓа на едно место, сепак нападот или последицата од него може да биде на сосема различна локација, дури и на другиот крај од светот. Исто така, вообичаено последицата настанува во моментот кога криминално се делува, но периодот на криминално делување може да биде подолг, а последицата да настане откако ќе измине повеќе време.

За компјутерските измами е карактеристично тоа што, многу често, времето и периодот на извршување е тешко прецизно да се определат. Тоа е така затоа што овој криминал се случува во т.н. виртуелен простор. Генерално, може да се каже дека времето и периодот на извршување се определени од самиот развој на информатичката технологија. Имено, компјутерските измами бележат поголема зачестеност во последнава деценија отколку пред, на пример, педесет години. Како што наведовме во воведот на овој труд, со цел остварување на поголема концизност и актуелност на истражувањето, ќе се фокусираме на периодот од последните пет години.

1.4 Место и простор на извршување

За компјутерските измами е специфично тоа што просторот и местото на извршување се целосно виртуелни т.е. за да се изврши ова кривично дело не е потребно да има физички контакт помеѓу сторителот и жртвата. Тоа на некој начин може да го отежне откривањето на сторителите и расветлувањето на кривичното дело.

Како што нагласува Николоска (2013), местото на извршување на овој вид криминалитет дава одговор на значајното прашање, имено, каде криминално се делува. Може да се каже дека и просторот и местото на извршување, во одредена мера, се разликуваат од традиционалните учења во однос на кривичните дела од општиот или економскиот криминалитет. Местото на извршување на компјутерската измама најчесто е во тесна врска со локацијата на компјутерот од каде што криминално се делува, иако последиците можат да се забележат дури на голема оддалеченост т.е. на друг крај од светот.

1.5 Организираност на сторителите

Сторителите на компјутерски измами вложуваат огромни напори за добро да се организираат меѓусебе, со цел да не бидат лесно санкционирани. Милковска (Милковска; 2012) во својот труд нагласува дека најчесто станува збор за лица со одлично познавање од областа на компјутерската технологија. Интересен факт е дека многу често, сторителите ваквите дела ги извршуваат главно поради желбата да се докажат во информатичката средина, а потоа заради материјална корист. Николоска (2013) истакнува дека не можеме да ги поистоветиме сторителите на компјутерскиот криминал со сторителите на класичниот криминал, бидејќи постојат специфичности што ги прават различни едни од други.

Во видовите извршители спаѓаат хакерите, крекерите и фрикерите. Хакирањето е активност на програмерите за истражување на границите на компјутерите и компјутерската технологија. Овде спаѓаат игри, бизнис апликации, надземни и сателитски комуникациски системи и секаков вид на мрежна работа, до регулирање на работата на огромни финансиски корпорации (Милковска 2012)

Кракирањето (анг. crack, мк. пукнатина) се однесува на намерното влегување во нечиј компјутерски систем без дозвола. Целта е да се избегнат лозинките и лиценците што се неопходни за користење на одредени компјутерски програми или оперативни системи.

Фрикирањето може да се дефинира како навлегување во компјутери и компјутерски системи со цел да се оствари одредена материјална корист. Со други зборови, се работи за навлегување во компјутерски системи на телефонски и интернет провајдери, заради кражба и неограничено користење на нивните услуги (Милковска 2012)

Во врска со поврзаноста на сторителите, важно е да се истакне дека е многу тешко да се влезе во нивната трага, бидејќи најчесто нивните компјутери се извонредно заштитени и влегувањето во трага бара огромен напор. Исто така, во денешно време се почесто се случува, извршителите да се организираат од било кој дел од светот, без да споделат лични контакти, да си ги споделат искуствата и знаењата, со цел полесно да го остварат замисленото, оставајќи малку, па дури и никакви траги зад себе. Како средства за остварување на измамата, извршителите се служат со компјутерски вируси, фајл инфектори, присутни програм инфектори, инфектори за секторот на бутирање, комбинирани вируси, дропери и слично.

1.6 Личноста на сторител

Сторителите на компјутерски криминал или компјутерски измами мораат да имаат соодветни познавања и вештини од областа на компјутерската техника и криминалистичката информатика. Најчесто станува збор за лица на техничката интелигенција чија криминална активност не е едноставно да се открие или да се докаже. Компјутерската техника овозможува вршење на криминал на големи одалечености, бидејќи не е задолжително сторителот да се наоѓа на местото на настанатата последица. Како што нагласува Николоска (2013), истражувањето и анализата на практичните случаи укажуваат на многубројноста на начините на кои може да се изврши компјутерска измама, преку кои всушност може да се види вообичаениот профил на сторителите: голема лукавост, професионално знаење и интелигенција. Единствената нивна цел е стекнување на противправна имотна корист, а често се забележуваат и елементи на

корупција, односно искористување на службената положба за стекнување на имотна корист за себе или за друг.

1.7. Личност на жртвата и придонес на жртвата за нејзина виктимизација

Жртвата игра клучна улога во компјутерската измама, бидејќи чинот на измама на сторителот го поттикнува да располага со својот имот. Ова создава финансиска загуба која е централен дел од компјутерската измама. Жртви може да бидат поединци, фирми или државни институции. Особено со зачестеното користење на компјутерите и Интернетот, се подразбира дека жртва на компјутерска измама може да биде секој од нас.

Оттука произлегува прашањето, во кои ситуации треба да се побара правен совет ако постои сомневање дека одредена личност е жррва на извршена компјутерска измама. Одговорот не е секогаш едноставен и еднозначен, но најопшто земено важи следново: Ако сте биле жртва на компјутерска измама или се сомневате дека некој ги злоупотребил вашите податоци, веднаш треба да пријавите во полиција и да се консултирате со адвокат специјализиран за ИТ или кривично право. На овој начин можете да се осигурате дека вашите права се заштитени и дека секоја штета што сте ја претрпеле може да се бара. Адвокатот исто така може да ви помогне во зачувувањето на доказите и комуникацијата со органите за спроведување на законот.

Во моментов веродостојните статистички податоци за жртвите на компјутерскиот криминал се ретки (Cliff and Desilets 2014; Leukfeldt 2017; Lynch 2006), иако статистиката за криминалот е важна за креаторите на политиките. Комисијата на владата на Обединетото Кралство ги наведува следните неколку причини зошто е потребна статистика за криминалот на национално ниво:

1. За да се обезбедат веродостојни квантитативни мерења на криминалните активности и трендови кои ќе му овозможат на парламентот да ја исполни својата демократска функција да бара одговорност од тогашната влада за овој аспект од состојбата на нацијата;

2. За да се информира јавноста, медиумите, академиците и релевантните групи од посебни интереси за состојбата со криминалот во земјата и да обезбеди пристап до податоци кои информираат за поширок дебатни и невладини истражувачки агенди;

3. За да се информираат релевантните аспекти на краткорочната распределба на ресурсите, како во рамките на владата, така и за надворешни поврзани тела - на пр. за полициско работење и поддршка на жртвите;

4. За да се дадат информации за информира управувањето со перформансите и одговорноста на национално ниво на агенции како што е полицијата;

5. За да обезбеди база на докази за долгорочните владини стратешки и политички случувања.

6. За да се примени еден вид на притисок врз создавачите и операторите на ИКТ системи, софтверски апликации итн. да дизајнираат и управуваат со нивните производи на таков начин што ќе ги намалат можностите и провокациите за криминал; и во обезбедувањето веродостојни и валидни податоци кои можат да се користат во анализа на временски серии и проценки на влијанието на превентивните напори (Reep-van den Bergh and Junger 2018).

2. КРИМИНАЛИСТИЧКО ИСТРАЖУВАЊЕ НА КОМПЈУТЕРСКИТЕ ИЗМАМИ

2.1 КОМПЈУТЕРСКА ФОРЕНЗИКА И ЕЛЕКТРОНСКИ ДОКАЗ

Стоилковски и др. (2012) истакнуваат дека, најопшто земено, дигиталната форензичка истрага се дели на две основни категории, и тоа:

- Корпорациска (приватна) дигитална форензичка истрага
- Званична (јавна) дигитална форензична истрага

Истражувањето започнува со предистражна постапка, која е неформална постапка за прибирање на докази, во фаза кога кривичното дело или неговиот сторител се уште не се откриени во целост, а истата ја спроведува полицијата по службена должност или на барање на јавниот обвинител. Таа не е детално законски регулирана и за нејзиното започнување не се носи формално решение. Таа започнува со поднесување на кривична пријава до полиција или друг орган, со информирање на јавниот обвинител за сторено кривично дело за кое се гони по службена должност, при што се спроведуваат извиди од страна на полицијата или таа постапува по упатства на јавниот обвинител или кога е поднесена формална кривична пријава до јавниот обвинител, а тој не може да одлучи по неа без дополнително собирање на потребни известувања. Полицијата е должна да ги преземе сите дејствија за да го открие сторителот и да обезбеди траги и предмети кои можат да послужат како докази и да ги собере сите информации кои би можеле да користат за водење на постапката.

Заради проверка на наводите во кривична пријава или проверка на сознанија за сторено кривично дело, јавниот обвинител може сам да собира известувања, но најчесто издава наредби и насоки на полицијата и другите органи за откривање, бара докази, информации, известувања и податоци и сл. Јавниот обвинител може: да го повика подносителот на пријавата и други лица чии сознанија смета дека може да придонесат за оценка на веродостојноста на наводите во пријавата, да повикува сведоци при што е должен да ги извести за својството во кое ги повикува (https://www.ihr.org.mk/storage/app/media/Publications).

Корпорацискатa истрага се спроведува во рамките на организацијата (корпорацијата) во која се случил комјутерскиот криминален инцидент. Во моментот кога ќе се открие компјутерскиот инцидент, веднаш се започнува со ваквата истрага. Таа се изведува од страна на специјалисти од организацијата и со строго почитување на интерните правила и процедури кои се предвидени за вакви инциденти. Во моментот кога се случува комјутерски инцидент, најзначајно и клучно е многу брзо да се реагира. Во почетната пракса на форензичката истрага на комјутерските докази се покажало дека по откривање на сомнителните податоци, првите седум сена се критични.

Главниот фокус на официјалната корпорациска истрага секогаш е насочен на сведоците и сомнителните. Оптималната комбинација во истрагата на комјутерскиот инцидент е заедничка тимска работа на званичните органи на истрагата одредени од страна на сопственикот на информацискиот систем и ИТ-специјалисти. Секој учесник има своја задача и сите се еднакво важни (Николоска (2013). Предистражната постапка е под раководство на јавниот обвинител, а предвидени се следните истражни мерки или дејствија: претрес, привремено обезбедување и одземање на предмети или имот, привремено одземање на компјутерски податоци, привремено одземање на писма, телеграми и други пратки, постапување со податоци што се банкарска тајна, имот во банкарски сеф, следење на платен промет, попишување на привремено одземени списи, исправи и технички снимки, и вештачење. По корпорацискатa дигитална форензична истрага, следува званичната т.е. јавната форензична истрага. Според Стоилковски и др. (2012), неа ја изведуваат официјалните истражни органи (полициските истражни органи, и специјалното судство за борба против високотехнолошкиот криминал). По наредба на јавниот обвинител, МВР ја спроведува оваа истрага и собира докази како форензична истрага на компјутери или други електронски уреди. Задолжително и неопходно е горенаведените органи да работат усогласено со позитивната законска легислатива, но и да ги почитуваат светските стандардни оперативни процедури за истражување, привремено одземање и испитување на компјутерските системи и другите мрежни уреди, аквизиција на дигиталните податоци/докази независно од оперативната платформа во насока на откривање на валидни дигитални докази. Тоа подразбира дека истражните органи мораат добро да ги познаваат постоечките закони и прописи кои се однесуваат на компјутерскиот криминал, но и добро познавање на стандардните локални процедури за

истражување и утврдување на криминалните активности во областа на компјутерскиот криминал.

Многу значаен дел е и дигиталниот доказ. Станува збор за множество од посредни реални докази, од кои ниеден не смее да се исклучи поради било која причина. Доказите мораат да бидат потполни, меѓусебно да се потполнуваат и да немаат пукнатина за донесување на заклучок, односно за утврдување на цврст доказ.

Ако постојат соодветно дефинирани услови, светската судска практика ги прифаќа компјутерски генерираните и компјутерски меморираните докази. Неопходно е строгото почитување и запазување на овие услови, бидејќи трансформацијата на податоците од серија на кодирани битови во судски доказ е апстрактен процес кој може да предизвика сомнежи кај судиите и поротата и да ги доведе во прашање автентичноста и интегритетот на компјутерски генерираните судски докази. Тоа особено е изразено кај судиите/поротата кои немаат доволно голема едукација од областа на информатичко-комуникациската технологија. Затоа, потребно е да се одредат и доследно да се почитуваат процедурите за ракување и чување, како и прописите за собирање, аквизиција и и анализа на дигиталните докази независно на каков медиум тие се запишани. Апсолутно недозволиво е податоците да се менуваат, да им се нанесува каква било штета или да се манипулира со нив во било кој чекор од истрагата. Собирањето на докази започнува со реконструкција на хипотезата за случајот. Доказите треба да се собираат на местото на случување на криминалната случка, бидејќи тоа може да биде единствен директен контакт со реалните докази. Треба да се работи методично, темелно и внимателно. Користејќи ги заклучоците за случката, потребно е со критички поглед да се вратиме на поставената хипотеза, односно да си поставиме прашање како лично ние би ги прифатиле тие докази ако се наоѓаме на спротивната страна. Потребно е да ги пронајдеме причините за неквалитетниот доказ, односно да утврдиме: зошто доказот не е квалитетен, каде се изгубил некој важен факт, како да се пронајде доказен материјал кој ќе ја пополни празнината, што да направиме ако таков материјал се пронајде, итн. Во оваа фаза од истрагата од иста важност се докажувањето и негирањето на доказот. Карактеристичната заедничка одбрана во сите компјутерски ексцесни ситуации најчесто претставува тезата дека криминалниот акт никогаш не се случил, дека всушност станува збор само за компјутерска аномалија и слично.

Тоа значи дека треба да се да се соберат сите посредни докази од лице место, не само оние докази за кои дигиталните форензичари мислат дека треба да се соберат, туку и се` она што може потенцијално да индицира што навистина се случило. Во процесот на аквизиција генерално е потребно да се снимаат листата на датотеки и логови како докази, дури и ако немаме никаква идеа што навистина се случило. Треба да се има во доказниот материјал секоја датотека која потенцијално може да содржи доказ, пред истата да се изгуби или промени. После иницијалната истрага (без запленување на компјутерот) потребно е да се обрне особено големо внимание на првобитната хипотеза и со тоа дополнително и подетално да се надгради со собраните докази. Голема веројатност постои да е испуштен некој значаен доказ, што претставува добар аргумент компјутерот да се заплени во текот на истрагата, но при тоа мораме да имаме на ум дека тоа не е секогаш лесно. Дигиталниот доказ е посреден доказ. Но, секој од посредните докази, кои заедно го градат доказниот материјал, треба да се третира како директен доказ кој води кон непобитно доказување на криминалното дејание. Сите посредни докази потребно е да се третираат како докази кои директно водат кон непобитно докажување на извршените криминални активности. Дури тогаш почнува изградбата на доказ без пукнатини, односно изградбата на необорив доказ. Сето ова го обработува и истражува компјутерската форензика. Според Стоилковски и др. (2012) алатките за анализа на извршениот електронски криминал можат да се поделат во две групи, и тоа:

1. Алатки за анализа на компримитираниот компјутерски систем во живо,
   - DEFT, Linux базирани сет на алатки компајлирани на CD,
   - HELIX, Linux базирани сет на алатки,
   - COFEE, Microsoft life forensic алатка за обезбедување на податоци/докази од вклучен компјутер
   - FTK, software за правење на image (bit to bit copy) на RAM меморија или целиот file system на хард дискот.
2. Алатки/ софтвер за анализа на компјутер во лабораторија
   - En Case, software за креирање на image и детална анализа на file system на хард дискот.
   - FTK, софтвер за детална анализа на image file,
   - X-way, софтвер за детална анализа на секој бит на хард диск.

3. ПОСЛЕДИЦИ ОД КОМПЈУТЕРСКИ ИЗМАМИ

Како и секое кривично дело, можеме да претпоставиме дека и компјутерските измами оставаат далекусежни и сериозни последици по физичките и правните лица што се нивни жртви. Штетите т.е. последиците можат да се поделат во пет групи. Прво, компјутерските измами оставаат материјални и финансиски штети. Тие настануваат кога сторителот го извршува делото за да стекне противправна имотна корист за себе или за друг, преку искористување на стручното знаење и вештини, но и со тоа што ќе ги злоупотреби финансиските средства што му се доверени за професионално работење. Второ, штетите можат да бидат и од нематеријална природа и да се однесуваат на повредата на половата слобода, половиот морал, повредата на расните или на националните чувства на жртвите. Овде спаѓаат и физичките повреди како и другите видови повреди. Трето, штетите можат да бидат и политички, кога нанесуваат повреди на националните или верските чувства, а тука спаѓаат и штетите нанесени со извршени кривични дела со елементи на компјутерски тероризам. Четврто, штетите можат да се однесуваат на насилство или физичка болка, кои се предизвикуваат преку уцена, изнуда, убиства со употреба на компјутерски системи и слично. Петто, штетата може да биде и комбинирана, со нанесени материјални последици на компјутерските системи, но паралелно со тоа се нанесува и физичка или психичка болка на жртвите (Николоска 2013).

Во една студија за последиците од компјутерскиот криминал објавена од Norton by Symantec „Norton Cybersecurity Insights Report“, се наведува дека 12,7 милиони германци биле жртви на сајбер криминалци минатата година. Пред се, хакерите ја искористуваат негрижата на потрошувачите. Извештајот доаѓа до заклучок дека потрошувачите претрпеле штета од 1,5 милиони американски долари и дека секоја жртва од Германија морала да потроши во просек по 14,8 часа за да ги санира последиците. И покрај негативните искуства, засегнатите имаат тенденција да не го менуваат своето однесување и затоа се подложни на дополнителни напади. Речиси 21.000 потрошувачи ширум светот беа анкетирани за извештајот, вклучително и над 1.000 корисници од Германија.

Студијата се осврнува на последиците од компјутерскиот криминалот и открива дека и покрај зголемената свест за опасностите од интернетот, многу корисници се

занемаруваат во заштитата на нивните лични податоци. Над три четвртини (82 проценти) знаат дека треба активно да ги заштитат своите информации на интернет. Сепак, тие сè уште се подготвени да отвораат линкови или потенцијално заразени прилози во е-пошта од непознати испраќачи. Негрижата на потрошувачите и ризичното однесување на Интернет им олеснуваат на хакерите да успеат во нивните напади со рафинирање на нивните методи и измислување нови измами. Иако измамите со фишинг постојат повеќе од дваесет години, на многу корисници сè уште им е тешко да ја разликуваат лажните мејлови од безбедните. Речиси една четвртина не може да открие напад на фишинг. Бидејќи корисниците продолжуваат да бидат невнимателни со своите податоци, хакерите ги оптимизираат своите тактики и ги прилагодуваат своите измами за да профитираат од негрижата на нивните жртви. Станува сè поважно за потрошувачите соодветно да се заштитат (http://www.itseccity.de/markt/studien/symantec071216.html)

Од наведените видови штети се потврдува претпоставката дека комјутерските измами можат да остават сериозни и далекусежни штети во секој сегмент на општественото фунцкионирање, но и по физичкото и менталното здравје на жртвите.

КРИМИНОЛОШКИ КАРАКТЕРИСТИКИ НА КОМПЈУТЕРСКИТЕ ИЗМАМИ (ОБЕМ, ДИНАМИКА И СТРУКТУРА)

Голем број на компании, служби и институции равиваат систем на заштита, а на ниво на државите се гради систем на кривично – правна заштита со инкриминирање на кривични дела. Меѓутоа, од криминалистичката практика се покажува дека ниту еден систем не е совршен, а криминалците секогаш изнаоѓаат соодветни тактики и техники на деликвентно однесување. Така што, според одредени проценки во Соединетите Американски Држави, просечната штета од компјутерски криминалитет на ниво на година е од сто до триста милиони долари. Како најчести појавни облици на компјутерски криминалитет се диференцираат комјутерските кражби, саботажи, но и компјутерските

измами како најекспонирани имотни компјутерски кривични дела со повеќе начини и шеми на извршување.

Во Република Северна Македонија, компјутерските измами се дел од имотниот криминал и се инкриминирани како посебно кривично дело во Глава 23 Кривични дела против имотот во Членот 251 б, а првпат ова кривично дело е инкриминирано во 2004 година (Кривичен законик на РМ, Сл. весник на РМ бр. 19/04), а како резултат на препораките од Конвенцијата за компјутерски криминалитет од 2001 година.

Македонската криминалистичка практика последниве години бележи повеќе начини на извршување на кривичното дело „Компјутерска измама“, што може да се забележи и од објавите и извештаите на Министерството за внатрешни работи во чии рамки делува и Секторот за компјутерски криминал и дигитална форензика, како и од секојдневните билтени за откриени криминални случаи и од страна на Одделите за компјутерски криминал при Секторите за внатрешни работи на ниво на цела држава. Во продолжение ќе бидат наведени податоци од извештаите на МВР од периодот од последниве пет години:

2018	
Видови и застапеност на компјутерски криминал	Оштетување и неовластено навлегување во компјутерски систем (53) Компјутерска измама (14)
Висина на материјалната штета	11,2 милиони денари
Начини и средства за извршување	Користење на претходно украдени платежни картички при купување на интернет, плаќање на сметки преку интернет (e-commerce), неовластено навлегување во компјутерски системи со промена на содржина на веб страниците на правни лица, нелегално преземање и посредување во деловната комуникација преку електронска пошта

Годишен извештај 2018: Најзастапени кривични дела од компјутерски криминал се оштетување и неовластено навлегување во компјутерски систем (53) и компјутерска измама (14) со кои била предизвикана материјална штета којашто опфаќа 96% од вкупно нанесената материјална штета или 11,2 милиони денари. Делата се извршувани со користење на претходно украдени платежни картички при купување на интернет и плаќање на сметки преку интернет (e-commerce) и со неовластено навлегување во компјутерски системи со промена на содржина на веб страниците на правни лица. И понатаму е присутен трендот на нелегално преземање и посредување во деловната комуникација преку електронска пошта помеѓу македонски и странски компании, при што е вршено пренасочување на банкарските трансакции. При тоа, ваквите активности најчесто се насочени кон малите и средните претпријатија.

2019	
Видови и застапеност на компјутерски криминал	Компјутерски измами (12)
Висина на материјалната штета	36,3 милиони денари
Начини и средства за извршување	Лажни огласи за купопродажба на интернет портали, пресретнување на e-mail комуникација помеѓу приватни фирми со цел нивна измама, насочување и плаќање на друга банкарска сметка.

Годишен извештај 2019: Во делот на компјутерски измами, се регистрирани 12 кривични дела, а се карактеризираат по значително покомплексниот начин на извршување, како и со причинување на голема материјална штета во однос на другите кривични дела од оваа област, која во 2019 изнесувала 36,3 милиони денари или 85,2% од вкупната материјална штета. Кај интернет измамите најчести се лажните огласи за купопродажба на интернет портали, како и пресретнување на e-mail комуникација помеѓу приватни фирми со цел нивна измама, насочување и плаќање на друга банкарска сметка.

2020	
Видови и застапеност на компјутерски криминал	Компјутерски измами (3)
Висина на материјалната штета	околу 1,5 милиони денари
Начини и средства за извршување	Електронска уплата за изнајмување на стан, подигнати парични средства од кредитни картички на правно лице, пресретнување на email комуникација помеѓу приватни фирми со цел нивна измама, насочување и плаќање на друга банкарска сметка.

Годишен извештај 2020: Во делот на компјутерски измами, во 2020 е забележано намалување од 75% на кривичните дела. Регистрирани се само три кривични дела, кои се извршени со измама при електронска уплата за изнајмување на стан, подигнати парични средства од кредитни картички на правно лице и со пресретнување на email комуникација помеѓу приватни фирми со цел нивна измама, насочување и плаќање на друга банкарска сметка. Вкупната матријална штета е околу 1,5 милион денари.

2021	
Видови и застапеност на компјутерски криминал	Компјутерски измами (6)
Висина на материјалната штета	над 15,5 милиони денари
Начини и средства за извршување	Неовластен упад во електронската комуникација помеѓу правен субјект од нашата земја и странско правно лице од Лондон, со менување и прикривање односно пренасочување на компјутерските податоци се доставиле лажни фактури со што ги довеле во заблуда правните субјекти. Неовластено навлегување, менување и внесување на лажни податоци во финансовата картица на даночен обврзник. Измама на лица при уплата на сретства за изнајмување на стан, уплата на сретства за стекнување ваучер со криптовалути, уплата на парични по основ на наводна добивка на награда.

Годишен извештај 2021: Во текот на 2021, за разлика од 2020, забележано е двојно зголемување на КД компјутерска измама. Регистрирани се шест кривични дела од кои две се расветлени, а кривично се пријавени пет сторители. Модусот на извршување на овој вид на кривични дела е специфичен што ги прави тешки за откривање а во текот на годината имаме и десеткратно зголемување на материјалната штета во однос на лани и истата изнесува над 15,5 милиони денари. Карактеристичен е случајот во кој од страна на четири унгарски државјани со привремен престој во Велика Британија во период од август до декември 2020 година во повеќе наврати извршен е неовластен упад во електронската комуникација помеѓу правен субјект од нашата земја и странско правно лице од Лондон, при што со менување и прикривање односно пренасочување на компјутерските податоци доставиле лажни фактури со што ги довеле во заблуда правните субјекти, поради што

биле извршени четири уплати на различни сметки во банки во Велика Британија. На тој начин пријавените остварале противправна имотна корист од вкупно 15 милиони денари на правниот субјект од Република Северна Македонија. Исто така, од страна на вработен во единица на локална самоуправа извршено е неовластено навлегување, менување и внесување на лажни податоци во финансовата картица на даночен обврзник, додека останатите кривични дела се извршени преку измама на лица при уплата на сретства за изнајмување на стан, уплата на сретства за стекнување ваучер со криптовалути, како и уплата на парични сретства кон лица од Р. Турција по основ на наводна добивка на награда.

2022	
Видови и застапеност на компјутерски криминал	Компјутерски измами (6)
Висина на материјалната штета	1,1 милион денари
Начини и средства за извршување	Електронски пораки, неевидентирање при наплата на сметки од странки и внесување на податоци од друг корисник, бришење на компјутерски податоци од страна на вработен во правно лице

Годишен извештај 2022: Во делот на компјутерските измами забележан е стабилизирачки тренд на регистрираните кривични дела кои се на исто ниво како и 2021 година. Во 2022 повеќекратно е намалена материјалната штета која изнесува 1,1 милион денари. Регистрирани се шест кривични дела, од кои три се расветлени, кривично се пријавени три лица, а карактеристичен е случајот во кој бугарски државјанин, преку испраќање на електронски пораки од странски повикувачки број довел во заблуда лице преку ветување за стекнување на наследство при што во неколку наврати успеал да издејствува парични средства од оштетениот во износ од 570 илјади денари. Исто така, регистриран е случај во кој шалтерски работник од АД Македонска Пошта при наплата на сметки од странки истите не ги евидентирал во системот, односно внесувал податоци од друг корисник со кое вршел препечатување на претходно уплатени сметки, а паричните

средства ги задржувал за себе, а едно од кривичните дела е извршено и од страна на вработен во правно лице кој извршил бришење на компјутерски податоци со што го оштетил правниот субјект за околу 494 илјади денари.

Од погоре наведеното, во последните пет години материјалната штета за кривичното дело компјутерска измама е над 60 милиони денари (околу еден милион евра). (https://mvr.gov.mk/statistiki/kriminal)

Од направената анализа на годишните извештаи, можеме да заклучиме дека во Република Северна Македонија во последните пет години се забележува стабилизирачки тренд. Меѓутоа, и покрај овој факт, компјутерските измами се релативно честа појава што предизвикува значителни штети (над 60 милиони денари т.е. над еден милион евра во последните пет години). Најчесто овие измами се однесувале на неовластено навлегување во компјутерски систем, менување и внесување на лажни податоци, испраќање на лажни СМС-пораки, измама при електронска уплата, лажни огласи за купопродажба на интернет портали, пресретнување на e-mail, насочување и плаќање на друга банкарска сметка. И покрај стабилизирачкиот тренд и расветлувањето на поголем дел од случаите, превенцијата на компјутерските измами треба да остане еден од врвните приоритети.

НАДЛЕЖНОСТИ ЗА КРИМИНАЛИСТИЧКО ИСТРАЖУВАЊЕ НА КОМПЈУТЕРСКИТЕ ИЗМАМИ

1. Координација и соработка

Како што беше наведено и во претходните поглавја, услов за почеток на кривичната постапка е успешно водена предистражна постапка во која се вклучени надлежните државни органи што поседуваат полициски овластувања, кои заедно со Јавниот обвинител треба да ги најдат сите докази за успешно водење на кривичната постапка и натамошниот прогон од судската власт и изрекување на соодветна санкција на сторителот. Новата улога на Јавното обвинителство со претстојната промена на законската регулатива, особено на Законот за Кривична постапка и според неговите одредби треба да овозможи тоа да стане независен орган, кој ќе биде способен на компетентен и објективен начин да ја води предистражната постапка. Многу е значајно тоа што во Законот за Јавно обвинителство е направен напредок во врска со ова. Министерството за внатрешни работи е најстар државен орган во борбата против криминалот, но последниве години се направени крупни промени во организациона и функционална смисла со цел успешно спротивставување на новите облици на криминални однесувања, со елементи на организираност и криминални однесувања, со кои се нанесуваат огромни штети на државата и на граѓаните. Министерството за внатрешни работи, во согласност со Законот за кривична постапка, кога постојат основи на сомнение дека е извршено кривично дело за кое се гони по службена должност, е должно да ги преземе потребните мерки и дејствија за да се пронајде сторителот на кривичното дело, сторителот или соучесникот да не се сокрие или да не побегне, да се обезбедат трагите на кривичното дело и предметите што можат да послужат како доказ, како и да се соберат сите известувања што би можеле да бидат од корист за успешно водење на постапката. Работата на Министерството за внатрешни работи е уредена со Законот за внатрешни работи (Николоска 2013).

Секторот на МВР за компјутерски криминал и дигитална форензика е надлежно за справување со компјутерскиот криминал во Република Македонија, вклучително и со компјутерските измами, и структурно е под Бирото за јавна безбедност. Организациската

единица за компјутерски криминал е воспоставена во 2005 година, и нејзиното формирање беше поттикнато од фактот што Република Северна Македонија ја потпиша Европската конвенција за компјутерски криминал во 2001 година, како и од нејзиното ратификување во 2004. Сепак, клучна причина е идентификувањето на кривични дела од областа на компјутерскиот криминал во Република Северна Македонија. Оваа единица дава поддршка за успешна идентификација и истражување на компјутерскиот криминал. Подоцна, во 2013 година, Министерството за внатрешни работи одлучи да формира Сектор за компјутерски криминал и дигитална форензика, со цел здружување на капацитетите и добивање на соодветна оперативна надлежност во согласност со новиот Закон за кривична постапка.

Одделението за истрага на компјутерски криминал има национална одговорност за истрага на компјутерски криминал и е лоцирано во Скопје со развиени регионални единици за истрага на компјутерски криминал во 8 сектори во државата. Од друга страна, Одделението за дигитална форензика е одговорно за испитување компјутери, мемориски уреди и мобилни уреди кои се запленети како дел од истрагата и за кои постои веројатност дека содржат докази кои се однесуваат на кривичното дело под истрага. (Стоилковски 2019).

Дел од активностите што ги преземаат надлежните институции се наведени во Годишниот извештај на МВР (2022), во кој е нагласено дека МВР е едно од министерствата на Владата на Република Северна Македонија кое е вклучено во опфатот на договорот потпишан со Microsoft, за зајакнување на безбедноста на системите во МВР кои ги користат Microsoft технологиите Active Directory и MDE за Windows OS, заедно со DART тимот на Microsoft е спроведена активноста Cybersecurity Operations Service (COS) за потребите на МВР. Покрај тоа, како дел од проектот „Зајакнување на безбедносната состојба при примање на интернет email во МВР – Exchange Online Protection“- извршено е зајакнување на постојните механизми за заштита од несакани пораки т.н. spam, malware, virus, phishing и други закани преку email.

Во поглед на надлежните органи за овој вид на кривични дела, односно МВР тесно соработува со Јавното обвинителство на Република Северна Македонија во насока на превенција и сузбивање на компјутерските измами. Нивните дејства се координирани т.е. МВР спроведува истражителни активности по наредба на ЈО, а потоа се преминува кон

формирање на предмет. Исто така, ЈО организира активности за обучување и зголемување на свесноста за ваквиот вид криминал. На пример, Академијата за судии и јавни обвинители организира онлајн советување на тема: „Компјутерски криминал, обезбедување и изведување на електронски докази“, кое се одржа на 22 март 2022 година.

Значајна активност беше и кампањата за подигнување на свеста за измами при интернет купопродажба, #ПродавајБезбедно, предводена од Европол и австриската Служба за криминалистчко разузнавање, во 2020 година. Нејзината цел беше да ги информира купувачите и е-трговците како безбедно да купуваат и продаваат преку интернет, со цел заштита во пресрет на најголемата малопродажна сезона во годината „сајбер викенд“. Република Северна Македонија беше една од шеснаесетте земји учеснички во кампања под покровителство на Акцијата за е-трговија за 2020 година, насловена како #SellSafe (#ПродавајБезбедно) и #BuySafePaySafe (#КупувајБезбедноПлаќајБезбедно), чија цел е подигање на свесноста за измами при купопродажба на интернет.

Во оваа кампања беа вклучени Министерството за внатрешни работи, преку Секторот за компјутерски криминал и дигитална форензика, во соработка со Европол и „Стопанска Банка“ АД Скопје, во која органите за спроведување на законот од Австрија, Колумбија, Хрватска, Чешка, Германија, Грција, Унгарија, Ирска, Италија, Малта, Северна Македонија, Полска, Португалија, Романија, Шпанија и САД се здружија со Европскиот центар за компјутерски криминал на Европол и Советот за заштита на трговците од ризик за да споделат практични насоки за тоа како да се надмудрат криминалците и со тоа да се намали злоупотребата на е-трговијата (https://www.stb.com.mk/novosti/kampanja-za-podignuvanje-na-svesnosta-za-izmami-pri-internet-kupoprodazba/).

ПРЕВЕНЦИЈА ОД КОМПЈУТЕРСКИ ИЗМАМИ

Според стратегијата за заштита од компјутерски измами, како ако за поединците така и за компаниите е исклучително важно да бидат запознаени со начините за тоа како да ги превенираат компјутерските измами. Така тие можат да ја спречат измамата уште пред таа да се случи. Но и доколку препознаат дека станале жртви на ваква измама, значајно е да знаат како да постапат за да ја минимизираат штетата. За ефикасна превенција, неопходни се и технички и организациски мерки. Тие вклучуваат редовни ажурирања на софтверот и оперативниот систем, користење на антивирусни програми и Firewall, обука на вработените и подигање на свеста за безбедноста во интернет пространството, воспоставување безбедносни политики и контроли на пристап, усогласеност со заштитата на податоците и преземање неопходни мерки на претпазливост за заштита на личните податоци, како и следење на компјутерските системи и редовни безбедносни контроли. Ако компјутерската измама веќе се случила, препорачливо е веднаш да се поднесе кривична пријава и сите засегнати системи да бидат внимателно прегледани од експерти (https://www.juraforum.de/lexikon/computerbetrug)

Николоска (2013) истакнува дека, поради фактот што компјутерските измами најчесто се иницираат со помош на електросна комуникација и преку електронска пошта, жртвите треба особено да внимаваат на следните нешта:

- Да не се даваат лични информации на некој или на некоја компанија за која претходно личноста не слушнала. Тука се вбројуваат име и презиме, адреса. телефонски број, број на кредитна картичка, броеви на социјално осигурување или информации за членови на семејството.
- Да не се отвораат пораки од странци
- Да се инсталираат анти-вирусни програми и програми за блокирање на спам
- Да не се прифаќаат прикачувања од непознати личности
- Да се едуцираат децата во врска со и безбедна комуникација на Интернет
- Да не се чуваат лозинки на компјутерот, да не се користат заеднички лозинки, лесни лозинки, и да не се дава лозинката на некој друг.

Се препорачува граѓаните за да се заштитат себеси и своите пари со тоа што секогаш ќе побараат финансиски совети пред да дадат пари или да инвестираат средства и да ги одбијат ненајавените повици за можности за инвестирање. Исто така, потребно е да добијат непристрасни финансиски совети пред да инвестираат пари во понудите што ветуваат сигурна инвестиција, гарантирани приноси и голем профит. Според МВР, ако некогаш граѓаните инвестирале во измама, измамниците, најверојатно, ќе ги наведат повторно или ќе ги продадат нивните информации на други измамници, па последна препорака е веднаш жртвите да стапат во контакт со полицијата доколку се посомневаат во нешто. Секторот за компјутерски криминал и дигитална форензика апелира граѓаните и правните субјекти да не отвораат сомнителни линкови и прикачени документи во прилог на пораки што не доаѓаат од верификувани и за нив познати испраќачи, да не наседнуваат на измами од ваков тип и правните субјекти да преземат соодветни мерки за заштита на нивните компјутерски системи од потенцијален малициозен софтвер во согласност со нивните интерни процедури за компјутерски криминал.

Во однос на заштитата од вакви измами, од Европол велат дека граѓаните треба да бидат многу внимателни кога станува збор за брзи заработки. Оттаму велат дека е потребно да се истражи добро местото каде што се бара да се направи инвестиција, и граѓаните да бидат претпазливи кога плаќаат со криптовалути, бидејќи кога трансферот еднаш е направен, потоа не може да се повлече. Ако личноста добие понуда за инвестиција од страна на пријател, треба да се потврди дека навистина станува збор за споменатиот пријател. Од Европол апелираат, граѓаните да бидат посебно внимателни со апликациите за пронаоѓање сродни души на социјалните мрежи, бидејќи тука се најголеми понудите за инвестиции во наводни криптовалути. На крајот, според советите од Европол, ако некој донесе одлука да инвестира, треба добро да истражи каде ќе инвестира, и да го анализира и проектот што толку лесно ветува голема сума пари.

Безбедноста на информацискиот систем вклучува збир од неопходни мерки и постапки кои треба да се преземат со цел овозможување на оптимално функционирање на информацискиот систем како и интегритет на неговата содржина во сите вообичаени облици на неговото дејствување. Со тоа се дава еден вид гаранција дека ќе се обезбеди непречено извршување на сите операции, одвивање на деловните процеси и исполнување

на барањата што се поставени. Одредувањето на степенот на сигурност се прави со помош на квантитативни големини до кои се доаѓа со математички и статистички методи за проценка на ризикот, отпорноста на ризикот и отпорноста на ризични ситуации. Со цел да се спроведе соодветна заштита на информацискиот систем, треба да се преземат следните чекори:

- Да се процени важноста на содржината со податоци која се прави врз основа на анализата на односот на државата кон одделните видови на податоци, според евиденцијата која се води во деловниот систем и врз основа на интересите на раководни структури во деловниот систем.

- Да се проценат изворите и обликот на закани на содржината на податоци која се изработува на темелите на претходно споменатите проценки (Божиновски 2018: 4)

1. Креирање на безбедна лозинка

Една од најважните заштитни мерки при користењето на Интернетот се безбедните лозинки. Најопшто земено, за да генерирате безбедна лозинка треба да ги почитувате следните правила:

- Не треба да се користи иста лозинка за различни сметки, а лозинките треба да се менуваат редовно. За ова може да помогне генераторот за лозинки.
- Избегнете го повторувањето на исти обрасци на тастатура (на пр. qwerty или 1234321)
- Исто така, не треба да користите зборови кои лесно се наоѓаат во речник. Овде можете, доколку е потребно, да ги замените буквите со слични специјални знаци (на пр. Password >Pa§$w0rd). Имињата и датумите на раѓање кои многу лесно може да се поврзат со вас или со оние околу вас треба да бидат апсолутно табу.
- Сигурната лозинка треба да содржи и големи и мали букви. Покрај буквите, секогаш треба да се користат броеви и специјални знаци како /[(%&§$_:?!+#)]\. Не е секогаш можно да се избере од целиот збир на специјални знаци. Но, секогаш треба да има неколку вклучени.

- Ако сакате да креирате безбедна лозинка, важна е и нејзината должина. Ако сакате да ги шифрирате датотеките или да пристапите со добра лозинка, таа треба да има најмалку осум знаци. За важно шифрирање како што е лозинката за WLAN, треба да изберете лозинки од најмалку 20 знаци составени од бројки, букви и специјални знаци.
- Покрај тоа, можете и да користите реченици како основа ако сакате да креирате безбедна лозинка. Само помислете на реченица што можете да ја запомните. Сега можете да ги споите првите букви од секој збор и, доколку е потребно, да ги замените поединечните делови со специјални знаци. Таква криптична лозинка не може лесно да се дознае (https://www.datenschutz.org/ebook-sicheres-passwort.pdf)

2. Превенција при онлајн-банкарство и трговија

Купувањето преку Интернет станува сè попопуларно кај потрошувачите. Предностите се очигледни: денонoќно пазарување без стрес и без чекање во ред. Ако нешто не ви се допаѓа или не ви одговара, едноставно го враќате назад. Затоа, не е изненадувачки што 9 од 10 корисници на Интернет веќе купувале онлајн барем еднаш. Освен тоа, изминатата пандемија дополнително го зголеми процентот на индивидуи што купувале или веќе редовно купуваат преку Интернет. Генерално, потрошувачите се добро заштитени со постоечките закони кога купуваат онлајн. Сепак, треба да се биде особено внимателен, затоа што и на овој начин може да се случат компјутерски измами.

Особено треба да се внимава на тоа дали е јасен и познат идентитетот на трговецот и како може да се стапи во контакт со него во случај на сомнеж. Исто така, треба да се обрне внимание на изгледот на страната т.е. дали таа изгледа пристојно и уредно, кои податоци се бараат за купување и на тоа дали веќе има мислења од клиентите за трговецот.

Со онлајн банкарство или други услуги, корисниците треба да користат различни уреди за бројот за автентикација на трансакцијата и податоци за најавување - на овој начин криминалците немаат пристап до сите информации во исто време. Финансиските трансакции, исто така, никогаш не треба да се вршат преку јавен WLAN.

Во секој случај, главен приоритет е внимателно да ја погледнете веб-страницата на која ги внесувате вашите податоци. Банкарските страници што бараат чувствителни информации од корисник секогаш користат безбеден протокол за пренос на хипертекст („https“ = безбеден протокол за пренос на хипертекст) (https://www.justiz.bayern.de/media/images/behoerden-und-gerichte/sicher_surfen.pdf)

3. Превенција на phishing

Напаѓачите намерно користат стратегии како поттикнување љубопитност, стрес или страв. Целта е да ве измамат да кликнете на злонамерни документи или да откриете чувствителни информации, како што се лозинки.

Како заштита од phishing сајтови, корисниците можат да го проверат сертификатот на страницата за време на чувствителни онлајн процеси - препознатливи како зелена брава лево од лентата за адреси. Наставката за адреса „https“ означува шифрирана комуникација. Софтверот, исто така, треба да се одржуваа ажуриран за да се спречи онлајн измама.

За да се заштитите, не верувајте во која било е-пошта што бара итно да дејствувате. Никогаш не ги давајте вашите лозинки. Генерално, ниту една реномирана компанија или банка нема да побара од вас да внесувате лични податоци како лозинки и сл. преку е-пошта. Ова исто така важи и за е-пошта од семејството, пријателите или работното место.

Во случај на сомнителна е-пошта, прашајте каква врска имате со испраќачот и дали повикот за акција навистина може да биде веродостоен. Никогаш не кликајте на линкови или прилози од сомнителна е-пошта. Бидете особено внимателни со прилозите во формати како што се .exe или .scr (https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/)

Проверете ја лентата за адреси на веб-прелистувачот. Често, само еден поглед е доволен за да сфатите дека ова воопшто не е вистинската веб-страница. Ако не сте сигурни, рачно внесете ја адресата што ја знаете. Поставете ги вашите важни почетни страници, како што се банкарски пристап итн. како омилени во вашиот прелистувач, користете ги само нив, и пристапувајте само кон официјалните страници. (https://bundeskriminalamt.at/202/Betrug_verhindern/files/Phishing_Juli_2015.pdf

4. Сегашни и идни предизвици

Од направеното теориско проучување, станува јасно дека справувањето и превенцијата од компјутерски измами може да претставува вистински предизвик за надлежните институции, компаниите, но и за човекот како индивидуа. Навлегувањето во приватноста и материјалните штети се причината зошто компјутерската измама е предизвик на сегашното време, но веројатно ќе претставува предизвик и во иднина.

Интернет-криминалците се принудени брзо и ефикасно да се приспособат на новите технички реалности и да ги „надмудрат“ новововедените или изменетите безбедносни мерки. За разлика од полицијата, тие можат целосно да ги искористат сите можности на Интернет: додека сторителите чуваат релевантни податоци на сервери во други земји или се претставуваат со различен идентитет, потребни се недели или месеци пред органите на прогонот да добијат информации од мрежните оператори или на пример операторите на платформата. Во случај на сервери или оператори лоцирани во странство, мора да се почитуваат и договорите за правна помош.

Но, договорите за правна помош не се единствената пречка. Законите како што е Законот за кривична постапка (КПП) особено мора да се почитуваат при истрагите. Сторителите лесно можат да ги користат услугите за анонимизација, па затоа полицијата мора секогаш да дејствува отворено. При спроведување на тајни мерки, полицијата е обврзана со строги законски барања.

Но, дури и ако сторителите се појават на Интернет без анонимизација, полицијата има ограничени можности кога станува збор за нивно идентификување. IP-адресите во моментов се недоволно складирани од мрежните оператори поради недостаток или контроверзни сметки. Сепак, често е можно само да се идентификува сторителот со одредување на IP адресата. Меѓутоа, бидејќи законодавниот дом често не е во состојба да го следи динамичниот развој на Интернетот, честопати недостасува правна основа за прелиминарните истраги. А таму каде што веќе постојат законски барања, постои одреден степен на правна несигурност, бидејќи судовите ги достигнаа своите граници при

оценувањето на кривичните дела и начините на извршување на кривични дела поради сложеноста и динамиката на феноменот, а се уште нема повисоки судски одлуки. за ориентација. (https://www.ihk-nuernberg.de/de/IHK-Magazin-WiM/WiM-Archiv/WIM-Daten/2012-12/Special/recht-steuern/herausforderung-computerkriminalitaet)

Борбата против компјутерската измама е голем предизвик за агенциите за спроведување на законот, бизнисите и поединците поради постојано зголемениот број на сајбер напади и напредокот на технологијата. Тековните трендови и предизвици во областа на компјутерската измама се наведени во продолжение:

- Меѓународна соработка

Транснационалната природа на сајбер криминалот ја прави меѓународната соработка помеѓу агенциите за спроведување на законот од суштинско значење. Сепак, често има правни и практични пречки кои ја отежнуваат соработката, како што се разликите во законодавството, прописите за заштита на податоците и достапноста на ресурсите.

- Анонимност

Криминалците често користат технологии за анонимизирање како што се VPN (Виртуелни приватни мрежи), прокси-сервери и мрежата Tor за да ги прикријат своите идентитети и локација. Ова го попречува спроведувањето на законот и го отежнува да се бара одговорност од сторителите.

- Зачувување на докази

Собирањето и зачувувањето на доказите во случаите на компјутерска измама е често сложено и бара специјализирано знаење од областа на ИТ форензиката. Важно е правилно да се обезбеди и да се анализираат дигиталните траги со цел да се идентификуваат сторителите и да се добијат докази кои ќе застанат на суд.

- Правна експертиза

Ефикасната борба против компјутерската измама бара правно знаење во областа на ИТ законот и кривичното гонење. Како што технологиите и методите што ги користат сајбер-криминалците продолжуваат да се развиваат, важно е истражителите, обвинителите

и судиите да бидат соодветно обучени и ажурирани за ефикасна борба против овој вид криминал. (https://kanzlei-herfurtner.de/computerbetrug/)

5. Обуки за компјутерска безбедност

Еден од најзначајните и најефективните начини за превенција од компјутерски измами е да се вложува во континуирани обуки за новите трендови и закани како и подигнување на свеста кои може да доведат потенцијална жртва да биде лесен плен за оној кој однапред ја таргетирал како таква. За таа цел постојат и многу различни онлајн курсеви од институциите во државата како на пример бесплатните обуки од Националниот центар за одговор на компјутерски инциденти (ЦИРТ – МКД) при Агенцијата за електронски комуникации (АЕК) каде на својата веб страна нуди основни обуки за компјутерска безбедност за вработени во јавната администрација и приватниот сектор со цел заштита од ризиците на интернет просторот. Дополнително на веб страната има повеќе соопштенија за актуелните трендови каде преку употребата на социјалните апликации за комуникација постојат рекламни веб страни кои пренасочуваат до повеќе видови на компјутерски измами најчесто до цедење на крипто паричниците на оние кои се намамени од тие реклами.

ЕМПИРИСКО – АНКЕТНО ИСТРАЖУВАЊЕ

Емпирискиот дел е неизоставен дел од научното истражување, со цел постигнување на поголема релевантност на истражувањето. Во овој магистерски труд, емпириското истражување се состои од два дела, и тоа 1. Интервју (СВР Скопје) и 2. Интервју (Анализа на граѓани).

1. Интервју (СВР Скопје)

Во интервјуто учествуваа вкупно 6 лица, вработени во Министерството за внатрешни работи на Република Северна Македонија (СВР Скопје, Единица за економски и компјутерски криминал). Интервјуто беше составено од десет прашања, кои имаа за цел да дадат одговор во врска со зачестеноста, карактеристиките и разрешувањето на компјутерските измами во Република Северна Македонија. Во прилог се дадени прашањата од анкетата, и одговорите на испитаниците, соодветно:

1. Според Вашето искуство, колку се чести компјутерските измами во Република Северна Македонија?

Двајца од испитаниците одговориле дека компјутерските измами стануваат сè почести во последно време, со развојот на технологијата. Еден испитаник одговорил дека тие се многу честа појава. Двајца од испитаниците одговорија дека тие се ретка појава во Република Северна Македонија, додека пак еден испитаник одговорил дека тие се многу ретка појава во Република Северна Македонија.

2. Кои се најголемите тешкотии при расветлувањето на компјутерските измами?

Тројца од испитаниците се осврнаа на проблемот дека не постои доволна комуникација со странските служби, како и на тоа дека постои тешкотија во добивањето на одговори т.е. информации од нивна страна. Еден испитаник наведе дека е проблематично долгото чекање на одговор од социјалните мрежи. Друг испитаник, пак, нагласи дека најголемата тешкотија е констатирањето и лоцирањето на фактичкиот

сторител. Еден испитаник истакна дека најголема тешкотија претставува добивањето на доказен материјал.

3. Според Вас, дали се доволни напорите што ги прават надлежните органи во Република Северна Македонија за справување со ова кривично дело? Во кои аспекти би можело да има подобрување?

Во врска со напорите што ги прават надлежните органи во Република Северна Македонија, еден испитаник наведе дека тие не се доволни и дека се потребни повеќе обуки и кадар. Исто така, уште еден испитаник ја нагласи потребата од зачестени обуки. Друг испитаник даде сличен одговор, со тоа што овде беше наведена и потребата од поголема соработка и подобра комуникација со странските служби. Потоа, еден испитаник ја истакна потребата од поголеми и пософистицирани надградби во технолошките системи. Еден испитаник, пак, наведе дека надлежните органи во Република Северна Македонија преземаат сè што е во нивна моќ. Уште еден испитаник даде сличен одговор, но ги нагласи тешкотиите при собирањето доказен материјал и потребата од подобрување на соработката.

4. Дали е доволна соработката на македонските надлежни органи со странските институции во насока кон справување со компјутерските измами?

Сите испитаници одговорија дека соработката помеѓу македонските надлежни органи и странските институции не е доволна т.е. дека е потребна поблиска и поефективна соработка.

5. Според Вас, на кој начин оваа соработка може да помогне во справувањето со компјутерските измами?

Еден испитаник наведе дека нема конкретен начин на кој оваа соработка би помогнала. Друг испитаник, пак, нагласи дека поради недостатокот на соработка, справувањето на македонските институции со компјутерските измами е многу отежнато. Потоа, еден испитаник наведе дека соработката би била од помош преку организирање на обуки и семинари на интернационално ниво.

6. Кој аспект на кривичното дело компјутерска измама има најзначителни импликации во општественото функционирање?

Како најзначителни импликации, еден испитаник ги истакна злоупотребата на личните податоци и материјалната штета. Уште еден од испитаниците посебно го нагласи нанесувањето на материјална штета, додека пак тројца испитаници се осврнаа на нанесувањето на голема материјална штета т.е. финансиска штета (на правни лица). Друг испитаник, пак, го истакна менувањето и бришењето на податоци во компјутерскиот систем.

7. Кој аспект на кривичното дело компјутерска измама го прави најкомплицирано за превенција и расветлување?

Во врска со најтешките аспекти при превенција и расветлување, тројца испитаници го наведоа недостатокот на соработка со странските служби, странските правни лица и странската полиција. Еден испитаник нагласи дека најголемиот број компликации произлегуваат од недоволната информираност на правните лица и недоволната соработка меѓу службите. Еден испитаник одговори дека најпроблематичен аспект е лесниот и незаштитен пристап до лични податоци.

8. Дали сте биле (потенцијална) жртва на компјутерска измама?

Ниту еден од испитаниците не бил (потенцијална) жртва на компјутерска измама.

9. Од каде (локациски) доаѓаат најчесто обидите за компјутерски измами на македонски граѓани?

Во врска со локацијата од која најчесто доаѓаат обидите за компјутерски измами на македонски граѓани, еден испитаник одговори дека нема правило, а друг исто така нагласи дека тие доаѓаат преку Интернет од секаде во светот. Еден испитаник одговори дека обидите доаѓаат преку Интернет апликации. Двајца испитаници ја наведоа Африка т.е. Нигерија, а еден испитаник ја наведе и Азија.

10. Според Вас, какви мерки треба да се преземат за едукација на граѓаните во врска со препознавањето и спречувањето на ова кривично дело?

Како најзначајни мерки за едукација на граѓаните, двајца испитаници наведоа дека тоа би биле повеќе релевантни телевизиски емисии на оваа тематика, како и часови т.е. едукација во училиштата, предавања и семинари. Друг испитаник нагласи дека комуникацијата не треба да биде само електронска туку и лична. Потоа, еден испитаник ја нагласи важноста на превентивните мерки преку разговори со лица во самите правни лица и укажување на можностите на кои тие би можеле да бидат измамени. Еден од испитаниците одговори дека е многу важна редовната месечна комуникација со граѓаните, како и одржувањето на обуки. Потоа, еден испитаник нагласи дека е исклучително важно да се внимава на начинот на комуникацијата.

2. Интервју (Анализа на граѓани)

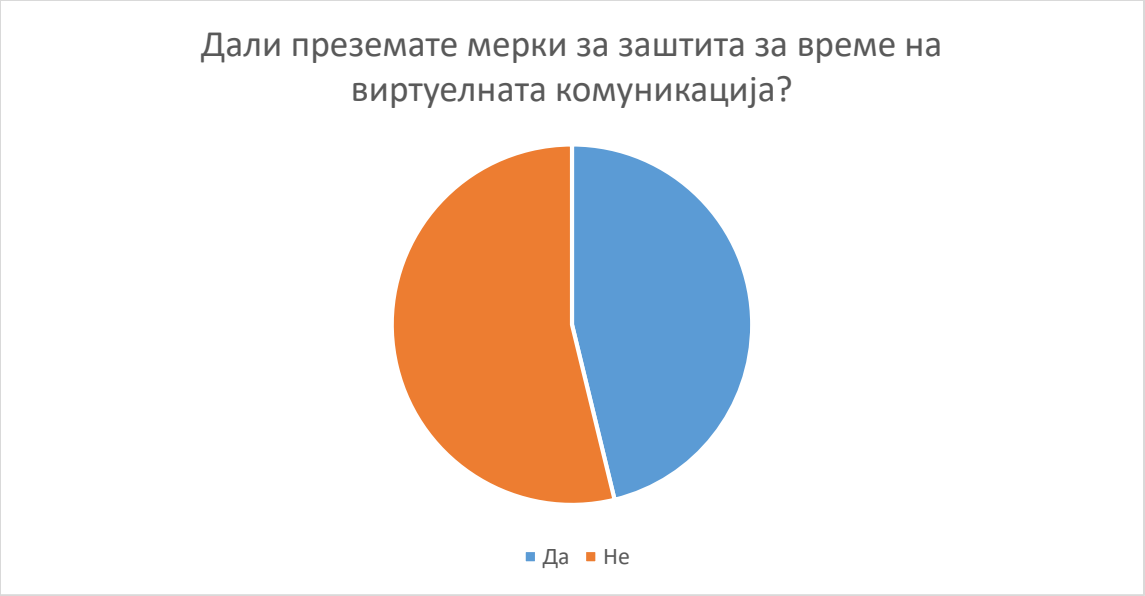
Во онлајн-интервјуто учествуваа вкупно педесет граѓани од машки и женски пол, од различни етникуми. Во прилог се претставени прашањата од анкетата, како и анализата на одговорите на испитаниците:

1. Колку сте запознаени со терминот компјутерска измама?

Еден испитаник одговори дека е детално т.е. многу добро запознаен со терминот компјутерска измама. Четириесет и четири испитаници одговорија дека се доволно добро запознаени со овој термин. Двајца истакнаа дека се делумно запознаени. Тројца испитаници наведоа дека се минимално т.е. недоволно запознаени.

2. Дали преземате мерки за заштита за време на виртуелната комуникација?

Шеснаесет испитаници одговориле дека преземаат мерки за заштита, додека пак триесет и четири испитаници одговорија негативно на ова прашање.



3. Ако да, какви мерки преземате?

Мерките наведени од испитаниците вклучуваат: Користење на силни лозинки со големи и мали букви, бројки и симболи, и нивно редовно менување, избегнување на отворање на спам пораки и сомнителни пораки и внимателно проверување на идентитетот на испраќачот, користење на сигурносни апликации, двојна автентификација, максимална заштита на личните и другите податоци, посветување на особено внимание на тоа каква содржина се споделува и проверка на туѓите искуства во врска со веб страната, користење само на апликации што се дозволени од корпорацијата, користење на антивирусна заштита, малвер заштита, користење на ад блокер, енкрипција, VPN и избегнување да се започне со сомнителни обиди за комуникација.

4. Дали сте биле жртва на компјутерска измама?

Шестмина испитаници одговорија потврдно на ова прашање. Четириесет и четири не биле жртва на компјутерска измама.

5. Ако да, како се справивте?

Испитаниците што наведоа дека била жртва на компјутерска измама, наведоа дека се справиле на следните начини: со пријава во дирекцијата за заштита на лични податоци, со пријавување на платформата, пријава до банка, Т-Мобиле и МВР, пријава до Интерпол. Еден од испитаниците одговори дека лично го нашол измамникот, му дал до знаење дека има евиденција за измамата, а потоа го добил бараното обештетување.

6. Дали сметате дека надлежните институции во Република Северна Македонија преземаат соодветни мерки за превенција и заштита од компјутерска измама?

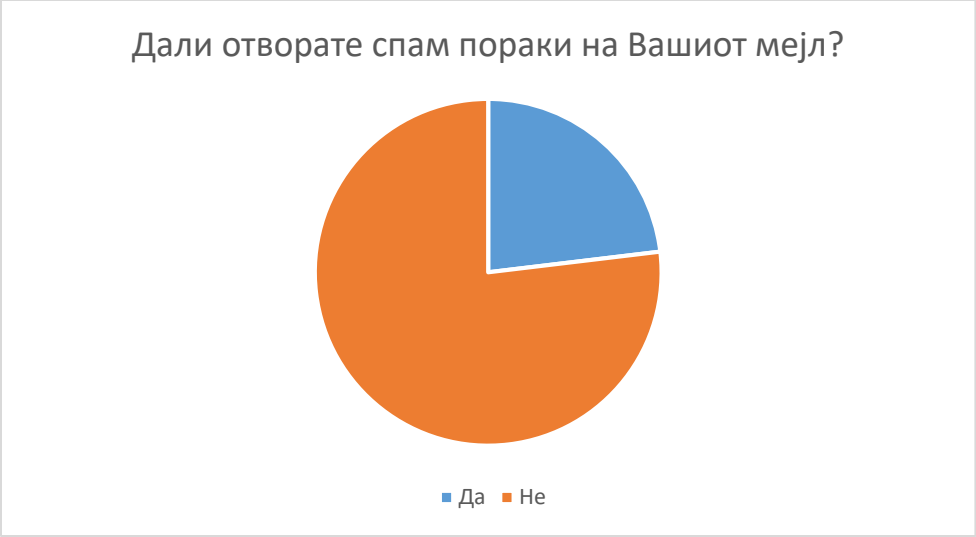
Дванаесет испитаници одговорија дека надлежните институции во Република Северна Македонија преземаат соодветни мерки, а триесет и осумина дадоа негативен одговор на ова прашање.

7. Според Вас, што е најважното што секој поединец може и треба да го направи за да се заштити од компјутерска измама?

Испитаниците ги дадоа следните одговори: користење на двојни проверки и фактори на автентификација, несподелување на личните податоци во какви било обрасци, едукација и зголемена информираност, следење на упатствата од надлежните, неотворање на сајтови со непознато потекло, пријавување на измамата на самите платформи а доколку е потребно и во надлежните институции, во зависност од тоа каков тип на измама е, поголемо внимание при употреба на лични податоци, информираност во врска со компјутерските измами (начини, видови итн), читање на рецензии и искуства на сајтовите, особено внимание кога се купува онлајн, да се внимава со кого се комуницира и да се нема безрезервна доверба, користење на антивирус програми, VPN, како и едукација уште од најрани години (за што треба да имаат улога и училиштата преку соодветни програми, но и родителите).

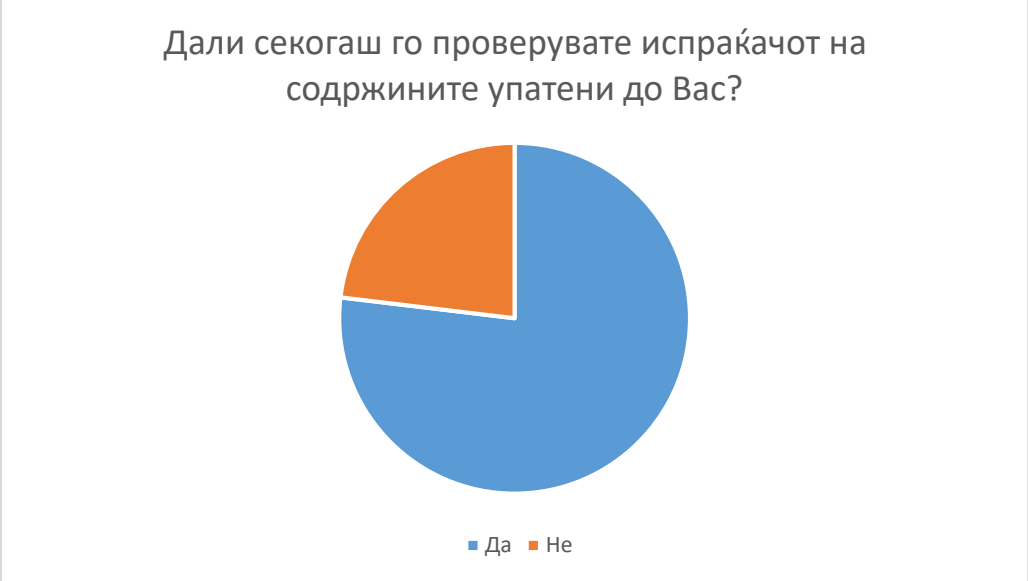
8. Дали отворате спам пораки на Вашиот мејл?

Пет испитаници одговорија потврдно на ова прашање. Четириесет и пет одговорија дека не отвораат спам пораки.



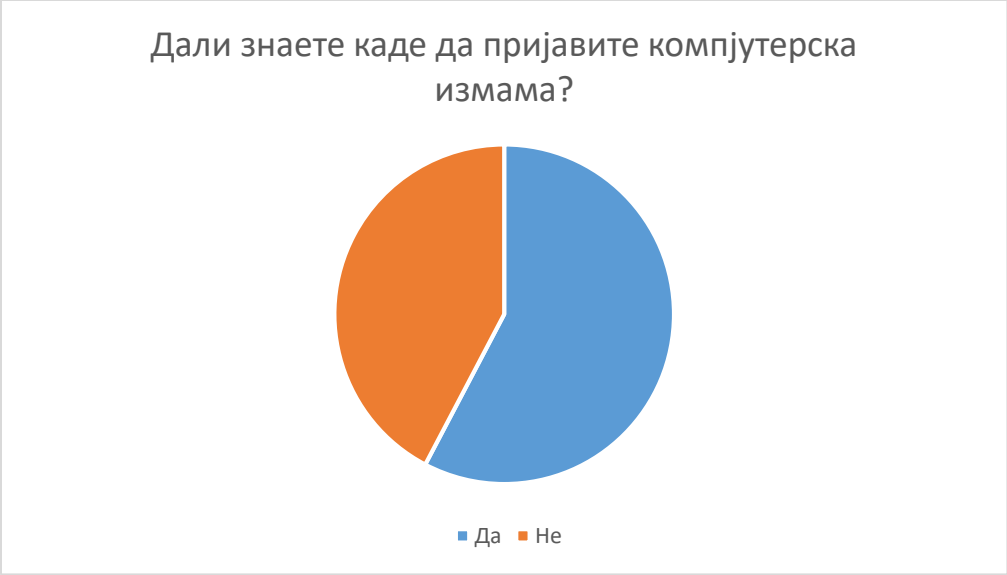
9. Дали секогаш го проверувате испраќачот на содржините упатени до Вас?

Четириесет и два од испитаниците одговорија дека секогаш го проверуваат испраќачот, додека пак осум не прават ваква проверка.



10. Дали знаете каде да пријавите компјутерска измама?

Четириесет и два од испитаниците се запознаени со тоа каде треба да пријават компјутерска измама. Осум испитаници одговорија негативно на ова прашање.



3. Дискусија за резултатите од емпириско-анкетното истражување

Во спроведеното интервју учествуваа шестмина вработени во Министерството за внатрешни работи на Република Северна Македонија (СВР Скопје, Единица за економски и компјутерски криминал). Нивните одговори на понудените десет прашања ни понудија корисен осврт и интересни резултати во врска со компјутерските измами во Република Северна Македонија. Можеме да заклучиме дека некои од резултатите беа неочекувани. На пример, таков е случајот со првото прашање, во врска со зачестеноста на компјутерските измами во Република Северна Македонија, на кое двајца од испитаниците одговорија дека тие се ретка појава во Република Северна Македонија. Еден испитаник дури одговори дека тие се многу ретки во Република Северна Македонија. Од друга страна, некои од резултатите беа очекувани, на пример, дека е потребна зголемена соработка на македонските и странските институции, во насока на поефикасно сузбивање на компјутерските измами. И покрај тоа што неколку испитаници одговорија дека институциите во Република Северна Македонија преземаат напори за сузбивање на компјутерските измами, сепак помеѓу испитаниците владее ставот дека е неопходно вложување на поголеми напори, меѓу другото, преку зачестени обуки, зголемување на

кадарот, поголема соработка и подобра комуникација со странските служби, како и поголеми и пософистицирани надградби во технолошките системи.

Во врска со локацијата од која потекнуваат обидите за компјутерски измами на македонски граѓани, интересен е фактот што неколкупати беше спомената Африка т.е. Нигерија. Тоа се совпаѓа со фактот дека Нигериската измама важи за еден од најзачестените начини на компјутерска измама, од која не се поштедени ниту македонските граѓани.

Интервјуто направено на педесет граѓани-испитаници од машки и женски пол и различни етникуми, покажа дека повеќето од испитаниците се запознаени со терминот компјутерска измама. Охрабрувачки е тоа што најголемиот број од испитаниците преземаат мерки за време на виртуелната комуникација, го проведуваат испраќачот на содржините и не отвораат спам и други сомнителни пораки. Голем дел од испитаниците ја истакнаа важноста на соодветната едукација и информираност како основа за превенција и заштита од компјутерски измами. Анализата покажа и дека мнозинството од испитаниците, за среќа, немаат лично искуство со компјутерска измама: Имено, 16% од испитаниците одговорија потврдно на ова прашање, додека пак 84% не биле жртва на компјутерска измама.

Меѓутоа, само нешто повеќе од половина од испитаниците знаат каде да пријават, ако се најдат во позиција на жртва од компјутерска измама. Исто така, загрижува фактот што граѓаните немаат доверба во надлежните институции. Имено, помал број од испитаниците одговорија дека надлежните институции во Република Северна Македонија преземаат соодветни мерки, а поголем број дадоа негативен одговор на ова прашање.

ЗАКЛУЧОК

Предметот и целта на истражувањето на овој труд беше проучување на криминалистичките карактеристики на компјутерските измами во Република Северна Македонија. Од направеното истражување, можеме да заклучиме дека компјутерските измами преставуваат растечка закана за безбедноста и приватноста, како на индивидуалците така и на претпријатијата, но и на државата во целост. Во Република Северна Македонија, компјутерската измама е инкриминирана со кривично дело „Компјутерска измама“, во Членот 251 - б од Кривичниот законик на Република Северна Македонија. Овој вид измама е најчестиот вид компјутерски криминал, и е дефинирана како измама што се извршува со цел стекнување на противправна корист за себе или за некој друг, со тоа што во заблуда не се доведува и одржува некое лице туку заблудата се однесува на внесување на неточни податоци во компјутер, или пак, алтернативно, се избегнува внесувањето на точните податоци (Ачкоски, 2012).

Во овој труд беа одредени криминалистичките и криминолошките карактеристики на компјутерската измама во Република Северна Македонија. Најопшто земено, секоја компјутерска измама се карактеризира со следните одлики: начин на извршување (modus operandi), време и период на извршување (tempus operandi), средства на извршување (instrumentum operandi), простор и место на извршување (radius i locus operandi) и организираност на сторителите.

Надлежните институции во Република Северна Македонија, Министерството за внатрешни работи и Јавното обвинителство, засилено работат на преземање мерки за превенирање и санкционирање на компјутерските измами. Исто така, тие се во тесна соработка со ЕВРОПОЛ, што е обележано и преку Меморандумот за разбирање за воспоставување на безбедна комуникациска врска помеѓу Северна Македонија и ЕВРОПОЛ и Билатералниот договор за поврзување на компјутерски мрежи.

Клучен дел од откривањето и расветлувањето на компјутерските измами е методиката на истражување на овој вид криминалитет. Генерално, форензичката истрага се состои од два дела и тоа корпорациска дигитална истрага и званична т.е. јавна дигитална форензична истрага. Од најголема важност е навремената и брза реакција, уште

при првите сомневања дека нешто нелегално се случува во одреден компјутерски систем. Исто така, неопходно е ефикасно и усогласено работење на сите надлежни. Само на овој начин може да ја намалиме или да ја елиминираме веројатноста од штети и последици, кои можат да бидат далекусежни.

Со помош на изведените теоретски и емпириски истражувања како и со помош на наведените примери, се потврдија општата хипотеза, но и петте помошни хипотези кои беа поставени на почетокот на истражувањето. Со помош на општата хипотеза претпоставивме дека компјутерските измами се имотни кривични дела кои се издвојуваат од класичната измама и од останатите компјутерски кривични дела по специфичните начини на извршување, односно способноста на измамниците во делот на манипулација со компјутерските податоци и стекнување на високи криминални приноси кои се поврзани со временскиот период на криминалното делување и умешноста во електронската комуникација со „жртвите“ и наведување за нивен придонес во криминалната реализација на сторителите. Тоа се потврди, бидејќи навистина, компјутерските измами се издвојуваат од класичната измама бидејќи за нивно извршување е потребен т.е. неопходен компјутерот, и не секогаш постои физички контакт помеѓу измамникот и жртвата. Ова може да го заклучиме и преку дефиницијата, во која се наведува дека компјутерската измама е најрашириот облик на компјутерски криминал, подвид на компјутерскиот криминал, кои се извршуваат со цел да се стекне противправна корист за себе или за некој друг, со тоа што во заблуда не се доведува и одржува некое лице туку заблудата се однесува на внесување на неточни податоци во компјутер, или пак испуштање на внесување на точните податоци (Ачкоски, 2012).

Помошна хипотеза 1: Компјутерските измами се вршат заради остварување на финансиска добивка како противправна имотна корист. Оваа помошна хипотеза се потврди преку извештаите на МВР, како и преку наведените примери за компјутерски измами. Речиси сите сторители ги извршувале измамите со цел да постигнат финансиска добивка како противправна имотна корист.

Помошна хипотеза 2: Органите на Република Северна Македонија прават напори за справување со компјутерските измами, преку преземање на соодветни оперативни активности, превентивни дејства и слично. Оваа хипотеза се потврди со помош на извештаите од МВР на Северна Македонија, во кои се детално изнесени мерките и

оперативните активности што ги презема МВР со цел спречување и справување со компјутерските измами во Северна Македонија.

Помошна хипотеза 3: Покрај напорите и преземените активности за сузбивање на компјутерските измами од страна на органите на Република Северна Македонија, потребно е и зголемување на граѓанската свест за овој вид криминал. Граѓаните на Република Северна Македонија треба да бидат информирани за тоа како самостојно да умеат да се заштитат од компјутерските измами, и да ги превенираат уште пред да се случат. Превенцијата е клучна алатка и често може да значи спречување на измамата уште пред таа да се случи. Во денешно време, луѓето се' почесто користат Интернет, но истовремено, се зголемува и нивната информираност и информатичка писменост. Тоа значи дека секој поединец може да развие систем за самозаштита.

Помошна хипотеза 4: Компјутерските измами предизвикуваат сериозни импликации и штети во приватниот и професионалниот живот на жртвите. Преку извршување на кривичното дело компјутерска измама, можат да се остварат материјални и нематеријални штети и последици штета, кои бележат значителен пораст низ годините, паралелно со зачестувањето на компјутерските измами. Оваа хипотеза се потврдува со фактот дека најголем дел од измамниците целат да остварат материјална корист, која од друга страна, значи материјална штета за жртвите. Освен тоа, зголемениот број на компјутерски измами во последните неколку години означува дека се зголемува и материјалната штета за жртвите. Ова се потврдува со статистичките податоци од извештаите на МВР, во кои е наведено дека компјутерските измами се зачестена појава, која ја пријавуваат правни и физички лица кои се македонски државјани и се однесуваат на сомненија за измами извршени преку Интернет, а во последните пет години материјалната штета за кривичното дело компјутерска измама е над 60 милиони денари т.е. околу еден милион евра.

Помошна хипотеза 5: Со зголемување на соработката на органите на Република Северна Македонија со надлежните органи од странските држави, може да се спречи и да се намали штетата од компјутерските измами. Оваа хипотеза се потврдува преку наведените активности на органите на Република Северна Македонија со органите од странските држави. На пример, во Годишниот извештај на МВР (2022) е наведено дека МВР е едно од министерствата на Владата на Република Северна Македонија кое е

вклучено во опфатот на договорот потпишан со Microsoft, за зајакнување на безбедноста на системите во МВР кои ги користат Microsoft технологиите Active Directory и MDE за Windows OS, заедно со DART тимот на Microsoft е спроведена активноста Cybersecurity Operations Service (COS) за потребите на МВР. Покрај тоа, како дел од проектот „Зајакнување на безбедносната состојба при примање на интернет email во МВР – Exchange Online Protection"- извршено е зајакнување на постојните механизми за заштита од несакани пораки т.н. spam, malware, virus, phishing и други закани преку email. Исто така, важна активност беше и кампањата за подигнување на свеста за измами при интернет купопродажба, #ПродавајБезбедно, предводена од Европол и австриската Служба за криминалистчко разузнавање (2020). Целта на оваа кампања беше информирање на купувачите и е-трговците во врска со безбедноста при купувањето и продавањето преку интернет, и тоа во пресрет на најголемата малопродажна сезона во годината „сајбер викенд". Република Северна Македонија беше една од шеснаесетте земји учеснички во кампања под покровителство на Акцијата за е-трговија за 2020 година, насловена како #SellSafe (#ПродавајБезбедно) и #BuySafePaySafe (#КупувајБезбедноПлаќајБезбедно).

Во оваа кампања беа вклучени Министерството за внатрешни работи, преку Секторот за компјутерски криминал и дигитална форензика, во соработка со Европол и „Стопанска Банка" АД Скопје, во која органите за спроведување на законот од Австрија, Колумбија, Хрватска, Чешка, Германија, Грција, Унгарија, Ирска, Италија, Малта, Северна Македонија, Полска, Португалија, Романија, Шпанија и САД се здружија со Европскиот центар за компјутерски криминал на Европол и Советот за заштита на трговците од ризик.

Направивме и компаративна анализа на карактеристиките на компјутерските измами во Република Северна Македонија и земјите од регионот (Србија и Албанија) и неколку од земјите-членки на Европската Унија. Компаративната анализа послужи за добивање увид во сличностите и разликите при извршувањето на компјутерските измами во наведените земји. Оваа анализа има големо значење од аспект на наоѓање на слични карактеристики, кои понатаму би можеле да помогнат во откривање на сторителите преку наоѓање на заеднички шеми и начини на дејствување. Од спроведената компаративна анализа заклучивме дека при компарацијата на примерите од Република Северна

Македонија со примерите од земјите од регионот, набљудуваме неколку слични карактеристики. На пример, кај начините на извршување, забележуваме дека во примерите од земјите од регионот, станува збор за измамнички финансиски трансакции на Интернет (Србија) и телефонска измама (Албанија). И во примерите од Република Северна Македонија можеме да воочиме голем број на измамнички финансиски трансакции на Интернет. Од средствата, најчесто се користат компјутери и мобилни уреди, а сторителите најчесто се организираат во групи или делуваат преку иста фирма. Јасно можат да се воочат сличности во средствата за извршување на измамите: компјутери за нелегални трансакции, измамнички веб-страни и мобилни уреди за извршување на телефонски измами. Како во Република Северна Македонија така и во земјите од регионот, сторителите поретко делуваат сами, а многу почесто во организирани групи, на пример, соработувајќи како дел од иста фирма, формирајќи фондации и слично.

При компарацијата на карактеристиките на компјутерските измами од Република Северна Македонија со примерите од земјите од Европската Унија, набљудуваме голем број на сличности. Средствата на извршување се прилично идентични т.е. станува збор за компјутери и мобилни телефони. Постојат голем број сличности и од аспект на организираноста на сторителите, во контекст на тоа дека сторителите на компјутерски измами многу поретко дејствуваат сами, а многу почесто се организирани во групи, на пример, преку фирми или формирање на измамнички фондации. Оттука, донесуваме заклучок дека, без разлика дали станува збор за Република Северна Македонија, регионот или земјите од Европската Унија, можеме да заклучиме дека кај сторителите на компјутерски измами се забележуваат одредени шеми на дејствување, што понатаму може да помогне за влегување во нивните траги.

Можеме да заклучиме и дека, и покрај напорите на надлежните институции, компјутерските измами остануваат реална закана за целото општество. Потребни се засилени мерки за превенција и санкционирање на сторителите. Воедно, корисниците на компјутерите и Интернетот треба да бидат проактивни во врска со безбедноста во виртуелниот простор. Секој кој врши финансиски трансакции преку Интернет или користи смарт телефони и онлајн-софтвер со чувствителни податоци, може и мора да се труди да се заштити од компјутерска и интернет измама.

ЛИТЕРАТУРА

КНИГИ И ТРУДОВИ

- Andriansyah, A et. al (2023) SWOT Analysis in Determining POLRI Organizational Resource Strategies to Anticipate the Development of Cyber Crime in the Framework of Maintaining National Security. Tec Empresarial. Cocta Rica, v. 18, n. p. 464-477.

- Андреески, Ц. (2005). Основи на информатика. Центар за научно истражувачка работа при Факултетот за туризам и организациони науки, Скопје.

- Ачкоски, Ј. (2012) Сигурност на компјутерски системи, компјутерски криминал и компјутерски тероризам, Скопје.

- Bequai, A (1978), Computer crime, Lexington

- Bratić, A (2023). Priručnik o sajber pretnjama: identifikacija i borba protiv rizika za korisnike u javnom I privatnom sektoru i građane. DCAF Geneva Centre for Security Sector Governance.

- Божиновски, М (2018) Компјутерски криминалитет и импликациите врз деловното работење во современите корпорации. Министерство за внатрешни работи

- Безбедност. Меѓународно научно списание. Бр.2, 2019. Република Северна Македонија, Министерство за внатрешни работи.

- Витларов, Т. (2013) Казнено право – посебен дел со практични примери авторизирани предавања. Скопје.

- Denning, E. Dorothy (2001) Activism, Hactivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, Networks and Netwars, Rand.

- Dimovski, D (2010). Kompjuterski kriminalitet. Zbornik radova Pravnog fakulteta u Nišu 2010, br. 55, str. 193-210

- Clark, A. Richard (2010). CyberWar - The Next Threat to National Security and What to do About it. Harper&Collins Publishers

- Goni, O et. al (2022). The Basic Concept of Cyber Crime. Journal of Technology, Innovation and Energy. The Wise Publisher

- Зврлевски, М и сор. (2014). Прирачник за компјутерски OSCE криминал. Скопје: OSCE.

- Камбовски В. (2003) „Казнено право, посебен дел“, Просветно дело АД Скопје.

- Konstantinović - Vilić S. i Nikolić – Ristanović V (2003). , Kriminologija, Niš

- Кошевалиска, О (2013). Скрипта Казнено право. Правен факултет, Универзитет „Гоце Делчев“ Штип

- Matijašević, J, Spalević, Ž. Ignjatijević, S (2012). Vrste internet prevara - pojam, značaj I uticaj na ekonomske i moralne aspekte društvene zajednice, INFOTEH-JAHORINA Vol. 11, March 2012.

- Moore, R. (2005). Cybercrime: Investigating High - Tehnology Computer Crime. Anderson Publishing, Cleveland, Mississippi

- Милковска, Е. (2012). Компјутерскиот криминал и неговмте импликации врз безбедноста во современиот свет - со посебен осврт на Република Македонија. Магистерски труд. Универзитет „Св.Кирил и Методиј“ Филозофски факултет, Институт за безбедност, одбрана и мир

- Mirić, F. (2018). Internet prevara kao oblik kompjuterskog kriminaliteta. Zbornik radova Pravnog fakulteta u Nišu, 2018, vol. 57, 80, 531-542.

- Nikoloska, S. Gjosheva, M. (2019). Criminal law, criminological and criminalist aspects of computer fraud in the Republic of North Macedonia. International Scientific Conference The great powers influence on the security of small states. Faculty of security Skopje, pg. 124 – 136.

- Николоска, С. (2010). Компјутерскиот криминалитет како сериозна закана за безбедноста, Научно стручна конференција на Факултетот за безбедност, Скопје, Охрид, 2010 година.

- Николоска, С. (2010) Компјутерски кривични дела против слободите и правата на човекот и граѓаните во Република Македонија, Хоризонти, Битола

- Николоска, С. Криминалистичките карактеристики на економско – финансискиот, компјутерскиот криминал и криминалот поврзан со перење пари.

- Николоска, С. (2013). Методика на истражување компјутерски криминалитет. Факултет за безбедност Скопје.

- Payne, B.K. (2020). Defining Cybercrime. In: Holt, T., Bossler, A. (eds) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham.

- Petrović S. (2001), Kompjuterski kriminal, drugo izdanje, Ministarstvo unutrašnjih poslova Republike Srbije, Beograd, 2001.

- Radiven, C. Prideaux, S. (2022). State crime, corporate crime and organized crime in the United Kingdom, Saudi Arabia, Yemen and the Congo. Chapter four. Crimes of states and powerful elites. Cambridge

- Radoniewicz, F. (2022). Cybersecurity in the European Union Law. In: Chałubińska-Jentkiewicz, K., Radoniewicz, F., Zieliński, T. (eds) Cybersecurity in Poland. Springer, Cham.

- Reep-van den Bergh, C.M.M., Junger, M. Victims of cybercrime in Europe: a review of victim surveys. Crime Sci 7, 5 (2018).

- Sabillon, R. et. al (2016). Cybercrime and Cybercriminals: A Comprehensive Study. International Journal of Computer Networks and Communications Security 4:165-176.

- Stammer, C. (2012). Einblick in die Cybercrime am Beispiel des Phishing. Diplomarbeit. Hochschule für Wirtschaft und Recht - Berlin.

- Стоилковски, М и др. (2012). Корпорациска истрага на компјутерски криминален инцидент. Четврта конференција за информатички технологии за млади истражувачи.

- Syahril, M. (2023) Cyber Crime in terms of the Human Rights Perspective. International Journal of Multicultural and Multireligious Understanding. Volume 10, Issue 5, Nov 2023

- Сулејманов З. (2003) Криминологија, Скопје, 2003

- Трајчевска, Д. (2013). Компјутерски кривични дела против имотот во Република Македонија. Магистерски труд. Факултет за безбедност - Скопје. Универзитет „Св. Климент Охридски“ - Битола.

- Urošević V. i Uljanov S. (2010), Uticaj karderskih foruma na ekspanyiji i globalizaciji zloupotreba platnih kartica na Internetu, NBP Žurnal za kriminalistiku i pravo, Kriminalističko – policijska akademija, Beograd, 2010.

- V. Urošević (2009). Nigerijska prevara u Republici Srbiji, Bezbednost – časopis Ministarstva unutrašnjih poslova Republike Srbije, Br. 3/2009, Godina LI, Beograd.

- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers and Security, 38, 97–102.

- Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Oxford: Polity.

- Završnik, A. (2008) Cybercrime. Definitional challenges and criminological particularities. Masaryk University Journal of Law and Technology

ЗБОРНИЦИ, ЗАКОНИ, МЕЃУНАРОДНИ КОНВЕНЦИИ

- Babović M. (2004). Računarska prevara i Internet prevara, Zbornik Symorg 2004

- Годишен извештај 2022. Бр.22.4-322/1. Министерство за внатрешни работи. Република Северна Македонија.

- Конвенција за компјутерски криминал (2001). Достапно на: http://www.pravdiko.mk/2786/konventsija-za-kompjuterski-kriminal-ets-185/

- Кривичен законик (2022). Достапно на: http://ecommerce4all.mk/wp-content/uploads/sites/3/2022/07/krivichen_zakonik-samo-aplikativni-chlenovi.pd

- Обука за борба против компјутерски криминал за судии и обвинители: концепт (2009). Македонска верзија. Оддел за информатичко општество и борба против криминалот Генерален директорат за човекови права и правни работи. Стразбур, Франција.

ИНТЕРНЕТ ИЗВОРИ

- Computerbetrug: Definition & Bedeutung in der juristischen Praxis. Достапно на: https://www.juraforum.de/lexikon/computerbetrug

- Годишни извештаи на Министерство за внатрешни работи на Република Северна Македонија. Достапно на: https://mvr.gov.mk/statistiki/kriminal

- Голема акција против бугарска банка за криптовалути. Достапно на: https://fokus.mk/golema-aktsija-protiv-bugarska-banka-za-kriptovaluti/

- Folgen von Cyberkriminalität. Достапно на: http://www.itseccity.de/markt/studien/symantec071216.html

- Herausforderung Computerkriminalität. Достапно на: (https://www.ihk-nuernberg.de/de/IHK-Magazin-WiM/WiM-Archiv/WIM-Daten/2012-12/Special/recht-steuern/herausforderung-computerkriminalitaet)

- Компјутерски податоци. Достапно на: https://www.techtarget.com/searchdatamanagement/definition/data

- Кривичен законик на Република Албанија. Достапно на: https://akshi.gov.al/wp-content/uploads/2020/11/LEGJISLACIONIMBIKRIMINKIBERNETIK.pdf

- Кривична пријава за компјутерска измама, лажно претставување. Достапно на: https://mk.tv21.tv/krivichna-prijava-za-kompjuterska-izmama-lazhno-pretstavuvane/

- Кривична пријава за компјутерска измама. Достапно на: https://www.pravdiko.mk/krivichna-prijava-za-kompjuterska-izmama/

- Кривична пријава за компјутерска измама поднесе ОВР Гевгелија. Достапно на: https://gevgelijanet.com/2023/01/27

- Криминалистички карактеристики. Достапно на: https://www.britannica.com/topic/criminal-law/The-elements-of-crime

- Министерство за внатрешни работи на Република Северна Македонија. Достапно на: http://mvr.gov.mk/page/ministerstvo

- Министерство за внатрешни работи на Република Србија. Достапно на: http://www.mup.gov.rs/wps/portal/sr/

- Нова Македонија. Достапно на: http://novamakedonija.com.mk/category/multimedija/galerija/

- Phishing – Schutz vor Datendiebstahl. Достапно на: https://bundeskriminalamt.at/202/Betrug_verhindern/files/Phishing_Juli_2015.pdf

- The Latest Cybercrime Statistics On The Internet, Tech Watch. Достапно на: http://www.techwatch.co.uk/2008/04/04/the-latest-cybercrime-statistics/

- Schutz vor Phishing. Достапно на: https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/wirtschafts-wissenschaftsschutz/2022-05-31-infoblatt-phishing.pdf?__blob=publicationFile&v=4

- Sicher surfen, sicher handeln. 2. überarbeitete Auflage 2012. Bayerisches Staatsministerium der Justiz und für Verbraucherschutz. Достапно на: https://www.justiz.bayern.de/media/images/behoerden-und-gerichte/sicher_surfen.pdf

- Србија: Апсења поради меѓународна измама на интернет вредна милијарди долари. Достапно на: https://netpress.com.mk/srbi-a-apse-a-poradi-me-unarodna-izmama-na-internet-vredna-mili-ardi-dolari/

- Стопанска банка. Достапно на: https://www.stb.com.mk/novosti/kampanja-za-podignuvanje-na-svesnosta-za-izmami-pri-internet-kupoprodazba/

- Strategien gegen Cybercrime. Достапно на: https://www.bmi.gv.at/magazinfiles/2012/11_12/files/europol_cybercrime.pdf

- Водич низ претходната кривична постапка. Достапно на: https://www.ihr.org.mk/storage/app/media/Publications