МЕЃУНАРОДЕН СЛАВЈАНСКИ УНИВЕРЗИТЕТ

„ГАВРИЛО РОМАНОВИЧ ДЕРЖАВИН“

СВЕТИ НИКОЛЕ – БИТОЛА

РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА



ФАКУЛТЕТ ЗА ПРАВНИ НАУКИ

СТУДИСКА ПРОГРАМА: КАЗНЕНО ПРАВО

МАГИСТЕРСКИ ТРУД

КОМПЈУТЕРСКИ КРИМИНАЛ – МЕЃУНАРОДНИ ДОГОВОРИ И НАЦИОНАЛНО ЗАКОНОДАВСТВО

СТУДЕНТ: МАРТИН ВЕЛИНОВ

БРОЈ НА ИНДЕКС: М187019

МЕНТОР: ПРОФ. Д-Р МАРИЈА ГРОЗДАНОВСКА

Свети Николе, 2020

ИЗЈАВА

Јас, Мартин Велинов, студент на втор циклус на студии организирани на Факултетот за правни науки во МСУ „Г. Р. Державин" Свети Николе - Битола, на студиската програма по казнено право со постојано место на живеење на ул. Ванчо Прке, број 54/6 во Штип, со ЕМБГ 2808995490018 и број на индекс М187019, изјавувам под морална и кривична одговорност дека поднесениот магистерски труд под наслов „Компјутерски криминал – меѓународни договори и национално законодавство'' претставува мој самостоен труд и истиот претставува резултат на самостојна научна работа спроведена во текот на истражувањето.

Согласен сум да ги сносам сите последици и одговорности кои произлегуваат од неовластеното користење на туѓ текст или плагијатство согласно важечките законски и подзаконски акти кои ги регулираат авторските и сродни права.

Давател на изјава:

Мартин Велинов

Апстракт

Динамичното темпо на развој на информатичката технологија отвори нови врати за појавата на еден нов софистициран вид на криминал познат како компјутерски криминал и компјутерски тероризам. Денес овие видови на криминал се едни од најчестите со кои се соочуваме во нашето секојдневие, бидејќи речиси секој еден од нас има достап до компјутер, мобилен телефон, интернет. Појавата на овој вид на криминал и неговото тешко откривање ги стави пред нови предизвици форензичарите, но и меѓународните и националните законодавства и зајакнувањето на борбата против овој вид на криминал.

Во овој магистерски труд е обработен компјутерскиот криминал преку неговоите облици т.е видови со нивно дефинирање преку нивните карактеристики. Исто така се дадени едни од најпознатите примери за компјутерски криминал кои му се имаат случено на светот, но и криминал од овој тип кој е регистиран и во Република Северна Македонија, каде е вклучена и статистика од Министерството за внатрешни работи на Република Северна Македонија.

Во овој труд се разгледани и обработени меѓународното и националното законодавство во кои е правно уредено и дефинирано што претставува компјутерски криминал и кои се санкциите за прекршување на одредени права и норми кои ги има уредено преку закони и договори нашиот законодавач.

Клучни зборови: Компјутерски криминал, меѓународно и национално законодавство, санкции.

Abstract

The dynamic pace of information technology development has opened new doors for the emergence of a new sophisticated type of crime known as cybercrime and cyber terrorism. Today, these types of crime are one of the most common we face in our daily lives, as almost every one of us has access to a computer, cell phone, internet. The emergence of this type of crime and its difficult discovery have brought forensicists, as well as international and national legislatures, a new challenge and the strengthening of the fight against this type of crime.

This master's thesis deals with cybecrime through its forms, or types, by defining them through their characteristics. This master's thesis sets out to distinguish cyber crime from cyber terrorism. It also gives some of the most famous examples of cybercrime that have happened to the world, but also a crime of this type that is also registered in the Republic of North Macedonia, where it is involved. and statistics from the Ministry of Interior of the Republic of North Macedonia.

This master's thesis examines and elaborates international and national legislation that regulates and defines what constitutes cybercrime and what are the sanctions for violating certain rights and norms that our legislator has enacted through laws and treaties.

Keywords: Cybercrime, cyber terrorism, international and national legislation, sanctions.

СОДРЖИНА

Листа на кратенки 8
Вовед 9
1. Предмет на истражување 11
2. Општествена и научна оправданост на истражувањето 13
3. Хипотези 14
4. Методологија на истражувањето 15
ГЛАВА ПРВА – ПОИМ ЗА КОМПЈУТЕРСКИ КРИМИНАЛ 16
1. Историја на интернетот 16
2. Дефинирање на поимот криминал 18
3. Поим и видови на комјутерски криминал 19
3.1. Видови на компјутерски криминал 21
4. Поим и видови на сајбер криминалитет 25
ГЛАВА ВТОРА – КОМПЈУТЕРСКИОТ КРИМИНАЛ НА МЕЃУНАРОДНО НИВО 34
1. Уредување на компјутерскиот криминал на меѓународно ниво 34
1.1. Конвенција за компјутерски криминал 34
1.2. Дополнителен Протокол на Конвенцијата за компјутерски криминал за инкриминација на дела од расистички и ксенофобистички вид по пат на информатички системи 39
1.3. Интерпол 41
1.4. ЕВРОПОЛ 43
2. Анализа на познати Случаи на компјутерски криминал на меѓународно ниво 45
2.1. Случај број 1 - Руски хакери – 10 милиони долари 45
2.2. Случај број 2 - Тинејџер кој ги хакира Министерството за одбрана на САД и НАСА 46
2.3. Случај број 3 -Роберт Тапан Морис и Црвот Морис (1988) 47
3. Статистички податоци на дела поврзани со компјутерски криминал во 2017 и 2018 година во Република Хрватска 48
ГЛАВА ТРЕТА – КОМПЈУТЕРСКИОТ КРИМИНАЛ НА НАЦИОНАЛНО НИВО 50
1. Правна регулатива на компјутерскиот криминал во Република Северна Македонија 50
1.1. Кривични дела во Кривичниот Законик на Република Северна Македонија 52
1.1.1. Член 144 – Загрозување на сигурноста 52
1.1.2. Член 147 - Повреда на тајноста на писмата или други пратки 52
1.1.3. Член 149 – Злоупотреба на лични податоци 53
1.1.4. Член 149-а – Спречување на пристап кон јавен информатички систем 54
1.1.5. Член 157 – Повреда на авторско право и сродни права 54
1.1.6. Член 157-а - Повреда на правото на дистрибутерот на технички посебно заштитен сателитски сигнал 55

1.1.7. Член 157-б – Пиратерија на аудиовизуелно дело 56
1.1.8. Член 157-в – Пиратерија на фонограм 56
1.1.9. Член 193 – Прикажување на порнографски материјал на дете 57
1.1.10. Член 193-а - Производство и диструбуција на детска порнографија 57
1.1.11. Член 193-б - Намамување на обљуба или друго полово дејствие на малолетник кој не наполнил 14 години 58
1.1.12. Член 251 Оштетување или неовластено навлегување во компјутерски систем 58
1.1.13. Член 251-а - Правење и внесување на компјутерски вируси 59
1.1.14. Член 251-б - Компјутерска измама 60
1.1.15. Член 271 – Правење, набавување или отуѓување средства за фалсификување 61
1.1.16. Член 274-б - Изработка и употреба на лажна платежна Картичка 61
1.1.17. Член 286 - Повреда на правото од пријавен или заштитен пронајдок и топографија на интегрални кола 62
1.1.18. Член 379-а - Компјутерски фалсификат 62
1.1.19. Член 394-г – Ширење на расистички и ксенофобичен материјал по пат на компјутерски систем 63
2. Истражување и статистички податоци на дела поврзани со компјутерски криминал во период од 2001 – 2019 во Република Северна Македонија 64
2.1. Статистички податоци – Државен завод за статистика на РСМ 78
3. Анализа на случаи на национално ниво 91
3.1. Случај бр. 1 – Компјутерска измама 91
3.2. Случај бр. 2 – ДАРКОД – Изработка и употреба на лажна платежна картичка 92
3.3. Случај број 3 – Загрозување на сигурноста и Ширење на расистички и ксенофобичен материјал по пат на компјутерски систем 95
3.4. Случај број 4 – Прикажување порнографски материјал на дете 96
3.5. Случај број 5 – Јавна соба 98
3.6. Случај број 6 – Хакерски напад на официјалната страна на Државна Изборна Комисија 99
4. Начини на дознавање, мерки за откривање на извршителите, докажување и извршители на компјутерскиот криминал 100
4.1. Извршители на компјутерскиот криминал 101
4.1.1. Аматери 102
4.1.2. Професионални криминалци 102
4.1.3. Хакери 103
ГЛАВА ЧЕТИРИ – ПРЕВЕНЦИЈА ОД КОМПЈУТЕРСКИ КРИМИНАЛ 106
1. Основни совети за заштита од компјутерски криминал 106
1.1. Инсталирајте и користете анти-вирусни програми 106
1.2. Наградување на софтвер 106

1.3. Обратете внимание при читање на е-маилови и отварање фајлови 107
1.4. Користете огнен зид (firewall) 107
1.5. Користете добри лозинки 108
1.6. Внимателност при инсталирање или преземање програми 108
1.7. Поставување и користење на лозинка за влез во датотеки. 108
Заклучок 109
Користена литература 112
Учебници и монографии 112
Нормативни акти 113
Веб страни 114

ЛИСТА НА КРАТЕНКИ

РСМ – Република Северна Македонија

МВР – Министерство за внатрешни работи

СВР – Сектор за внатрешни работи

ООН – Организација на обединетите нации

ФБИ – Федерално истражно биро

ОЈО – Основно Јавно Обвинителство

САД – Соединети Американси Држави

ЕУ – Европска унија

КЗ – Кривичен законик

ВОВЕД

Со почетокот на постоењето на човечкото општество, се појавуваат и првите облици на криминал. Со минувањето на годините, со доаѓањето на сцена на модерните информатички технологии, се проширува и просторот на кој се може да се изврши одредено дејствие спротивно на законот.

Во изминатите години, криминалот се повеќе се оддалечува од кражба на физички добра поради се поголемото усовршување на информатичката технологија, а тоа значи дека дејствијата поврзани со криминал се одвиваат на поинаков начин, односно електронски, а наједноставно кажано дејствијата се вршени "од дома".

Развојот на новите технологии и модерното време во кое живееме, доведе до тоа средствата за грабежи да се усовршуваат и менуваат. Подемот кој го зазема информатичката технологија доведе до појава на еден нов вид на криминал, кој ќе биде објаснет во овој магистерски труд.

Компјутерскиот криминал претставува нов вид на криминал што практично не остава никаква трага, односно немаат никаков физички облик како традиционалните физички докази под формата на пишани документи, траги кои се физички видливи, кои би можеле да доведат до сторителот, предмети итн. Голем дел од интернет економијата се повеќе е насочена кон онлајн продажбата на добра како и рекламирањето, а тоа значи дека се отвараат нови пазари, односно нови полиња за дејствување на компјутерските криминалци.

Во изминатите десетина години информатичката технологија (ИТ) тивко, но мошне ефективно трансформираше различни сектори на човековото живеење; производство, научните истражувања, транспортот, болниците, владата, образованието, дипломатијата, финансиските усллуги итн. Ако на крајот на шеесетите години на минатиот век најголемиот технолошки успех беше слетувањето на човекот на Месечината, денеска перформансите на персоналниот компјутер го надминуваат бројот на операциите кои беа извршени за управување на лунарниот модул од контролниот центар на вселенската мисија. Историската анализа покажува дека секој нов развој на компјутерската технологија е проследен со соодветна адаптација на криминалот, а истото важи и за законските измени.

За да се одговори на предизвиците што ги предизвикуваат новите видови на криминални активности, многу земји во Европската унија го разгледуваат своето кривично право со цел да спречат недостаток на законски уредувања на компјутерски криминал. Правните норми мора да ги опфаќаат и да ги следат тредновите на новите форми на криминал кои се појавуваат во општеството. Така, тие се ажурираат и одат во чекор со правната реалност во секоја земја пооделно. Меѓународната соработка е неопходна за ефективна отпорност на компјутерски криминал, еден од најголемите предизвици на сајбер криминалот е дека злосторството може да се изврши од и врз која било земја во светот, криминалецот може да ги брка своите жртви насекаде, да се скрие нечиј идентитет преку комуникација преку многу компјутери лоцирани во бројни странски земји и да се чуваат доказите на различни места. Оваа околност, како и транснационалната природа на мрежите, бараат заеднички меѓународен напор и унифициран пристап кон спречување на компјутерски криминал.

Затоа, во согласност со принципите на суверенитет, заштитата на човековите права, демократските слободи и правото на приватност, општествата мора да собираат и разменуваат информации на меѓународно ниво. Ова мора да се направи што е можно поскоро со цел да се открие компјутерска злоупотреба, зачувување на електронските податоци и утврдување на локацијата и идентитетот на криминалецот.

Како што ни една земја во светот не е изолирана од овој вид на криминал, така и Република Северна Македонија има негативни последици во ерата на компјутерскиот криминал.

Во овој магистерски труд, ќе го согледаме движењето на бројките на интернет корисниците во последните неколку децении, со што ќе се долови колку всушност е во напредна фаза информатичката технологија и зошто се повеќе го има овој вид на криминал. Ќе бидат дадени општите дефиниции поврзани со компјутерскиот криминал, поткрепени со неговите видови, некој од познатите случаи на меѓународно и национално ниво, како и истражувачкиот дел со бројки поврзани со тоа колку кривични дела поврзани со овој вид на криминал биле сторени на територија на Република Северна Македонија, како и бројки од други земји од Европа.

1. ПРЕДМЕТ НА ИСТРАЖУВАЊЕ

Предмет на истражување на овој магистерски труд е компјутерскиот криминал со сите негови облици, неговиот исторски развој, правните уредувања на национално и меѓународно ниво и потенцирањето на потребата на постојано следење со цел и создавање на нови правни уредувања кои би биле во тек со развојот на овој тип на криминал кој е апсолутно непредвидлив со развојот на информатичките технологии.

Особено внимание во овој труд се посветува на нелегалениот пристап до компјутерски системи и злоупотребата на податоци, дистрибуција на детска порнографија на интернет, кривични дела против авторските права и сродните права, кражба на лични податоци, кривични дела против платежните инструменти итн.

Сајбер криминалот по својата природа ги надминува националните граници и борбата против нив може да биде ефективна само на меѓународно ниво и соработка. Ова ја одредува потребата да се проучи овој аспект и важната улога на заедничките напори на меѓународното право. Со својот предмет на истражување овој магистерски труд претстаувува длабинска студија на кривичното право и регулирање на компјутерскиот криминал во Република Северна Македонија. Анализирани се и главните извори на меѓународното право што управуваат различни видови на компјутерски криминал. Презентирани се главните дефиниции и поими користени во кодификацијата на наведените кривични дела што тие ги сочинуваат основа за толкување и практична примена на правните норми. Проучено е и нивото на меѓународна и национална заштита против компјутерски криминал, преку сеопфатно проучување на главните органи кои постојат на терен, но и различните информациони технологии кои се состојат во различни форми на антивирусни програми и слично.

Трудот се состои од воведен дел, главен дел и заклучок, кои се структурирани во четири поглавја.

Првото поглавје претставува вовед во проблемот, краток историски преглед на потеклото на компјутерскот криминал, дефинирање на компјутерскиот криминал и објаснување на неговите облици.

Во **второто поглавје** се дава осврт на компјутерскиот криминал на меѓународно ниво, меѓународна правна рамка, конвенции, протоколи, меѓународни тела кои се бават со оваа проблематика и анализа на познати случеви.

Следните две поглавја презентираат длабинска анализа на компјутерски криминал во националното кривично право и превенцијата од него.

На крајот на овој труд преку **заклучокот** се сумираат празнините во кривичното право за компјутерски криминал и се дадени препораки за нив.

2. ОПШТЕСТВЕНА И НАУЧНА ОПРАВДАНОСТ НА ИСТРАЖУВАЊЕТО

Научната оправданост на темата на овој магистерски труд произлегува од самото истражување кое ќе биде спроведено за уредувањето на национално и меѓународно ниво на комјутерскиот криминал и податоците кои ќе излезат од истото и нивна анализа. Со самата идентификација на недостатоците на постојното законодавство од овој труд ќе произлезат и препораки за негово подобрување, а со тоа и надежта дека овој труд ќе го разбуди интересот кај јавноста да се спроведат и други истражувања поврзани со оваа тема која е повеќе од актуелна. Од статистичката слика на национално ниво поврзана со дела каде се користи компјутерска технологија и нивната тендецнција за зголемување ќе се нагласи и исклучителната важност на овој вид на кривична дела.

Прогресивниот развој на информатичката технологија и компјутерските системи предизвикаа појава на досега непознати кривични дела. Оваа искучително нова категорија на кривични дела, бара создавање соодветни правила на однесување, прилагодени на нивните технички карактеристики. Во поглавјето за превенција се дава јасна слика за општествената оправданост на овој труд бидејќи овде се доаѓа до израз истражувањето направено во делот за начини на кои можеме да се заштитиме од овој вид на криминал. Од друга страна тезата која ја обработува овој труд е условена од потребата да се спроведе во длабочина проучување на процесот на интеграција на технолошките концепти во правната материја, односно сите овие нови облици на криминал да бидат вметнати во националоното законодавство со цел заштита на граѓаните.

3. ХИПОТЕЗИ

Хипотеза бр. 1

Компјутерскиот криминал е нов облик на софистициран криминал од чие што присуство не е поштедена нашата држава.

Хипотеза бр. 2

Меѓународните активности и соработка се една од основните алатки во борбата против компјутерскиот криминал.

Хипотеза бр. 3

Компјутерскиот криминал бележи тендеција на пораст во Република Северна Македонија.

4. МЕТОДОЛОГИЈА НА ИСТРАЖУВАЊЕТО

Со цел да се постигнат целите на истражувањето, беше искористен комплексен метод на истражување, кој вклучува: нормативен метод, системски метод, анализа, компарација, статистика. Како резултат на обемно истражување, поглавјата се претставени на систематски начин меѓународни акти што содржат законско регулирање на одделните видови компјутерски криминали. Претставени се правните конструкции на овие кривични дела во кривичното законодавство во Република Северна Македонија. Користен е метод на студија на случај за одредени познати дела од оваа проблематика како на национално така и на меѓународно ниво.

ГЛАВА ПРВА – ПОИМ ЗА КОМПЈУТЕРСКИ КРИМИНАЛ

1. ИСТОРИЈА НА ИНТЕРНЕТОТ

Почетоците на интернетот како мрежа датираат уште од далечната 1969 година, но како официјален датум за создавање на интернетот се смета 1 јануари 1983 година, чијашто употреба била од страна само на универзитетите, војската, како и некој други државни организии во САД. Употребата на интернетот на глобално нивно започнува некаде во 90-тите години и со се поголема негова употреба и поголемо распространување, денес интернетот е мрежа без која поголемиот дел од светот не би функционирал. Показател за тоа е и моменталната ситуација во која светот се наоѓа со т.н. биолошка војна, со вирусот кој направи прекин во нормалните активности на народот, најголемиот дел од гигантските компании во светот како Google, Facebook и други компании, вработените своите работни задачи и обврски ги извршуваат од нивните домови, а без интернетот тоа не би било возможно.

Во последните 30 години, статистичките податоци за бројот на интернет корисниците ни покажуваат огромен пораст, односно од 1990 година до 2020 низ бројки тоа изгледа вака[1]

- 1990 година – 2.6 милиони корисници
- 1994 година – 44.4 милиони корисници
- 2000 година – 412.8 милиони корисници
- 2005 година – 1.026 милиони корисници
- 2010 година – 1.992 милиони корисници
- 2016 година – 3.408 милиони корисници
- 2020 година – 4.650 милиони корисници[2]

Овие бројки ни покажуваат колку всушност информатичката технологија е во напредна фаза, како минуваат годините истата се повеќе и повеќе е застапена и самиот период од 2010 до 2020 година ни покажува дека бројот на корисници е покачен за

[1] Види повеќе на - https://www.internetworldstats.com/stats.html - превземено на ден 27.08.2020

[2]Види повеќе на - https:// www.visualcapitalist.com/30-year-timeline-world-wide-web/ превземено на ден 27.08.2020

нешто повеќе од 2.6 милијарди корисници за помал временски период, во споредба со периодот од 1990 до 2010 година каде таа бројка е исто така нешто повеќе од 1.5 милијарди корисници. Овие статистички податоци го покажуваат динамичниот раст и брзото темпо на пораст на бројот на корисниците. Со оглед на тоа дека светот брои нешто повеќе од 7 милијарди народ, овие податоци се потврда дека за само триесетина години, колку што постои интернетот како мрежа, повеќе од 60% од населението во светот го има интернетот во своите домови.

2. ДЕФИНИРАЊЕ НА ПОИМОТ КРИМИНАЛ

Правилата за однесување во општествената заедница од страна на нејзините членови се основен услов за нејзиното опстојување. Тие правила на однесување зависат само од карактерот и развиеноста на тоа општеството.

Системот на едно општество е во состав од морални, обичајни и правни норми. Сепак секое од правилата, како и секоја од нормите може да наиде на непочитување од страна на членовите на општествената заедница.

Следствено на непочитувањето на правните норми и правила се појавуваат и првите облици на криминалот кој што ни претставува еден социјален и економски феномен за кој може да се каже дека постои од кога постои и човечкото општество. Речиси и да не постои ден, а да не се случи било каков вид на криминал, од најситен до најтежок вид.

Според правната дефиниција за криминалот, криминални дејствија се само поведенијата што се изрично забранети со нормите на казненото право. Поимот на криминалното однесување со изедначува со поведението на човекот, со кое поединецот доаѓа во конфликт со социјалните норми.

Човековото однесување, независно од неговиот асоцијален карактер, неговата штетност за други или општество во целина, станува казнено-правно релевантно дури кога е забрането со казнениот закон и кога за таквото однесување е пропишана казна или друга санкција. Се работи за формална или позитивно-правна дефиниција на криминалот.[3]

Според законот на САД, криминалот се дефинира како: „Чинот на кршење на кривичните закони на одредена држава или Соединетите Американски Држави. Позитивен или негативен чин на кршење на законот “.Според Европската унија, криминалот се дефинира како: „Акт на кршење на државното право или загрозување на јавната благосостојба. Анти-криминалните активности кои работат надвор од границите на државите се координирани на ниво на Европската заедница “.

[3] Камбовски В. - , Казнено право – Општ дел , Скопје, 2005

3. ПОИМ И ВИДОВИ НА КОМЈУТЕРСКИ КРИМИНАЛ

Во криминологијата, криминалистиката, разните законодавства и науки кои ја прочуваат феноменологијата на компјутерскиот криминал даваат различни дефиниции, кои главно водат до тезата дека криминалот кои се врши со помош на средствата за онлајн комуникација и информатичката технологија, каде основно средство за вршење на овие дејства е компјутерот.

Европската комисија во 2001 година преку соопштение ја има дадено дефиниција за комјутерскиот криминал која гласи вака: Комјутерскиот криминалот се состои од кривични дела што се вршат преку Интернет со користење на електронски комуникациски мрежи и информациони системи.[4]

Имено, тоа е криминал кој е насочен против безбедноста на информациските (компјутерски) системи во целина или во нејзин поединечен дел на различни начини и со различни средства со намера да за себе или за друг да се прибави некаква корист или на друг да му се нанесе некаква штета.[5]

Потребата од дефинирање на компјутерскиот криминал и сајбер криминалот и наговестувањето на замавот кој ќе биде земен од овој нов вид на неконвенционален криминал се докажува и со одржувањето на Десетиот конгрес на Собранието на Обединиетите Нации во далечната 2000 година, кој бил посветен на Превенцијата од криминалитетот и третманот на извршителите. Како резултат на сите активности кои биле превземани на овој конгрес е донесувањето на еден многу значаен документ за борбата со компјутерскиот криминал со наслов, “Криминалитет поврзан за компјутерските мрежи”, (Crime related to computer networks). Групата од експерти кои работеле на оваа тематика имаат дадено заедничка дефиниција на компјутерскиот криминал, односно : “Криминалитет кој се однесува на било кој облик на криминално однесување кое може да се изврши со помош на компјутерски системи и мрежи, во самите компјутерски системи и мрежите или против компјутерските системи и мрежи”

[4] Види повеќе на - https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en-преземено на ден 30.08.2020

[5] Јовашевиќ Д., Лексикон кривичног права, ЈП Службени лист СРЈ, Београд, 2002

Проф. д-р Владимир Водинелиќ го има дефинирано компјутерскиот криминал во реална (тесна) и во погрешна (поширока) смисла, така што во потесна смисла опфаќа компјутерска измама саботажа и шпионажа, додека пошироко се однесува на незаконско присвојување на компјутер и него компоненти од кражба, измама и слично.[6]

Проучувањето на различните дефиниции на меѓународно ниво, не води и до дефинирањето на оваа појава која ја има дадено Проф.Зоран Сулејманов кој под компјутерски криминал го подразбира секое дејствие во кое компјутерот претставува основно средство и цел за извршување на кривично дело.[7]

Она што е својствено за компјутерскиот криминал, односно по што тој е познат и која е неговата улога, имаме:

- ***Цел на напади*** – целта на нападите се сервиси, фунцкии и содржини кои се наоѓаат на мрежа. Се извршува кражба на услуги, податоци или идентитет, се оштетуваат или се уништуваат поединечни делови на мрежата или цела мрежа и компјутерски системи или се спречува правилно извршување на работата на функциите. Во секој случај целта на сторителот е мрежата во која се вметнуваат вируси или црви, се хакуваат сајтови, упаѓаат хакери, се извршува „одбивање на услугите“.
- ***Алатка*** – како алатка која ја користат криминалница во извршувањето на ваквите дела е мрежата.
- ***Околина*** во која нападите се иршуваат.
- ***Докази*** – во делот на докази во компјутерскиот криминал се мрежата и ICT и тие појавуваат во доказната постапка на компјутерскиот криминал.[8]

[6] Šarkić N., Prlja D., Damnjanović K., Marić V.,Ţivković V.,Vodinelić V., Mrvić-Petrović N.: Pravo informacionih tehnologija, Beograd, 2011, str.3.

[7] Сулејманов З. ,Криминологија, Скопје, 2003, стр. 631

[8] Мирчевска Н., научен труд Сајбер тероризам – современ облик на тероризмот колку Република Македонија е ранлива од сајбер тероризам

3.1. ВИДОВИ НА КОМПЈУТЕРСКИ КРИМИНАЛ

Појавни облици[9] на компјутерскиот криминал се:

- ***противправно користење на услуги и неовластено собирање на информации,***
- ***компјутерски кражби;***
- ***компјутерска измами;***
- ***компјутерска саботажа и компјутерски тероризам;***
- ***криминал поврзан за компјутерските мрежи.***

- **Противправно користење на услуги и неовластено собирање на информации**

Противправното користење на услуги се состои во неовластена употреба на компјутери или овластена употреба на истите од неавторизиран корисник. Пример за неовластена употреба на компјутерите е кога компјутерот се користи во било кои други цели, освен во цели кои претставуваат намена на компјутерот во информациониот систем. Еден од најчестите облици на неовластеното користење на компјутерите со кои се среќаваат работодавачите ширум светот е злоупотребата на интернетот од страна на вработените. Неовластеното собирање на информации претставува своевидна кражба на податоци содржани во компјутерските системи, најчесто со цел за остварување на противправна имотна корист.

- **Компјутерски кражби**

Компјутерските кражби заземаат високо место во областа на овој вид на криминал, како најчеста компјутерска кражба која се случува е кражбата на идентитетот. Овој вид на кражба има особено значење во општевство бидејќи

[9] Ачковски Ј., Сигурност на компјутерски системи, компјутерски криминал и компјутерски тероризам., Скопје, 2012.

покрај се останато, ја намалува довербата на интернет трансакциите, а и ја загрозува индивидуалната приватност.

Со тоа што криминалците ќе ги поседуваат информациите на одредени луѓе, односно нивниот идентитет, би можеле да отворат електронски сметки во банки, да купуваат работи, како и да добијат кредити од банки, купување на автомобил, стан и слично при што ќе предизвикаат финансиско оштетување на жртвата. Лошото за жртвата во ваквите кражби е што во поголемиот број на случаеви, таа не знае дека е мета на кражба се додека не стигне „сметка за наплата“.

- **Компјутерски измами**

Компјутерските измами се извршуваат со намера за стекнување за себе или за друг со противправна материјална корист [10] . Компјутерските измами претставуваат најраширен облик на компјутерски криминал, од причина што 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.

- **Компјутерска шпионажа**

Кога се споменува компјутерската шпионажа, станува збор за кривично дело во кое сторителот не само што прибавува, туку и неовластено користи компјутерски податоци, неовластено го репродуцира софтверот и сл. По правило, се работи за податоци кои претставуваат деловна, односно стопанска тајна. Компјутерските шпионажи бараат обученост и голема посветеност од страна на шпионите. Шпиони, во овој случај, не се само обични луѓе кои одат наоколу и прислушкуваат, туку тие мора да знаат да ги следат и најсовремените телекомуникациски и информатички технологии, мора да знаат да да работат со секаков софтвер и навлегувањето во туѓи компјутери и компјутерски системи за нив треба да биде секојдневие.

[10]Ачковски Ј., Сигурност на компјутерски системи, компјутерски криминал и компјутерски тероризам., Скопје, 2012.

Компјутерските шпионажи најчесто ги користат разузнавачките служби на влади и држави, но и огромен број на нелегални организации.

- **Компјутерска саботажа**

Претставува уфрлање вируси преку кои се врши расипување или уништување на програма или системот за автоматска обработка на податоци. Со оглед на мрежната поврзаност на компјутерите, заразата предизвикана од некој од бројните компјутерски вируси, по правило се шири во невидени размери. Како сторители на компјутерска саботажа се јавуваат амбициозни поединци во самата фирма, припадници на конкурентските претпријатија и првенствено во странство - политички мотивирани лица. Компјутерски саботажи најчесто се вршат заради остварување на друг вид на криминално дело, многу ретко се врши саботажа сама по себе без последователно друго дело. Најчесто се саботира еден компјутер, за да се нападне друг и притоа да се извршат кражби, измами, фалсификати. Исто така, може да се саботираат сигурносни и алармни системи, за да следуваат други активности поврзани со криминални дејствија и сл.

- **Компјутерски тероризам**

Во современи услови е се почеста појава, затоа што терористите се почесто го оставаат оружјето и во своја корист ја стават оваа технологија.

Компјутерската технологија станува мошне ефикасно средство во рацете на терористот, овозможувајќи му начини на дејствување со огромна ефикасност. Една од најпознатите терористички групи Ал-Каеда, нејзините терористи се добро обучени за користење на компјутерската технологија, поставуваат различни web локации на кои ги доловуваат нивните идни чекори и напади. При нивното апсење всушност се докажува и нивната умешност во компјутерската технологија затоа што често се наоѓаат компјутери со шифрирани фајлови. Компјутерскиот тероризам е во голема мерка поврзан со компјутерскиот криминал, дури и се преклопуваат со своите активности еден со друг. Најчести цели за нивен напад се банките, владини податоци, сите видови на сообраќај, како и големите гиганти (компании, нафтени рафинерии, социјални мрежи)

- **Електронско провалување во компјутерски системи и кражби на време од компјутерски системи**

Електронското провалување во компјутерски системи подразбира многу суптилно, по електронски пат изведено, нарушување на тајноста, поединечен компјутерски систем, односно неовластен електронски упад во централниот компјутерски систем и неговата база на податоци. Провалувањето во компјутерски системи се врши за остварување на одредена цел, најчесто нарачано од страна која може да има корист од ваквиот вид на вровалување. Ваквите дела обично ги извршуваат хакери, кои се добро упатени во тоа што го работат, најчесто користејќи Интернет, пронаоѓајки слабост во механизмите за заштита на компјутерските системи, по што навлегуваат и сменуваат или превземаат податоци, кои потоа може да се искористат во најразлични активности.

4. ПОИМ И ВИДОВИ НА САЈБЕР КРИМИНАЛИТЕТ

Честопати компјутерскиот криминал на меѓународно ниво може да го сретнеме под името Сајбер криминал, но овој поим и појава се сврзува со апсолутно други дејствија различни од оние кои го отсликуваат компјутерскиот криминал. Со дефинирањето на компјутерскиот криминал како нова појава, се појави и потреба за дефинирање на сајбер криминалот, но имајќи ја во предвид феноменологијата на овој вид на криминал како и дејствијата кои се превзимаат при извршување на ваков тип на криминал, не води до фактот од недостигот на една унифицирана дефиницција на истиот.

Со појавата на овој вид на криминал се почесто се зборува и за една нова гранка на криминологијата или таканаречената „Сајбер криминологија„[11]

Според Бановиќ сајбер криминалот може да го дефинираме како извршување на кривични дела кои за свој субјект или објект го имаат интернетот како глобална компјутерска мрежа и кои се вршат од страна на лица кои добри ги познаваат информатичките технологии, а со цел предизвикување на штетни последици или прибавување на противправна имотна корист.[12]

Сајбер криминалот всушност ги опишува криминалните активности кои се извршени со користење на електронски медиуми за комуникација. Во најширока смила сајбер криминалот е секоја криминална активност која се извршува преку употреба на компјутери и компјутерски системи и мрежи.[13]

Според проф. Д-р Видој Спасиќ сајбер криминал претставува криминал извршен во дигиталното опкружување и е специфична форма на незаконско однесување во кое компјутерските мрежи се појавуваат како средства, завршувања или докази за сторено кривично дело.[14]

---

[11] Jaishankar K. Cyber Criminology: Evolving a novel discipline with a new journal. International Journal of Cyber Criminology, Vol 1 , Issue 1 January 2007

[12] Бановић Б., Обезбеђење доказа у криминалистичкој обради кривичних дела привредног криминала, Полицијска академија, Земун, 2002, стр. 136

[13] Drakulic M., Drakulic R., "Cyber kriminal", Fakultet organizacionih nauka, Begorad, 2009, str. 56

[14] Spasić V, Aktuelna pitanja u oblasti sajber kriminala (članak), Bilten sudske prakse Vrhovnog suda Republike Srbije broj. 1/2006, Beograd, str.107.

Сајбер криминалот опфаќа широк спектар на недозволени, односно незаконски активности, како на пример неовластен пристап до компјутерска мрежа, ширење вируси, малолетничка порнографија, злоупотреба на платежни картички итн. Овој вид на криминал е криминал кој се одвива во сајбер просторот, затоа за да го разбереме подобро потребно е и дефинирање на околината во кој тој дејствува.

Поимот сајбер криминалитет ги опфаќа не само делата поврзани со мрежата на интернет, туку и со други компјутерски мрежи и уреди од информатичката и комуникациската технологија, па дури и телефонски линии и мобилни мрежи[15]

Кога се споменува самата класификација на сајбер криминалитетот би можеле да кажеме дека дел од нив при самото нивно кажување веќе ги познаваме, од нашето секојдневие, па така облиците на сајбер криминалот би можеле глобално да се класифицираат на неколку групи и тоа:

1. Кражби и измами;
2. Компјутерска шпионажа;
3. Хакирање и неовластено навлегување во компјутерскиот систем;
4. Дистрибуција на вируси и други облици на злонамерен софтвер (MALWARE);
5. Cyberstalking;
6. Производство и дистрибуција на нелегална порнографија;
7. Сајбер тероризам;
8. Повреда на правата од интелектуална сопственост.;

- **Кражби и измами**

Кражбите и измамите се можеби и најчестите облици кои се поврзани со злоупотребата на информатичката и комуникациската технологија, па дел од нив се – измамата со кредитни картички и хартии од вредност, кражба на идентитетот и попречување и присвојување на компјутерски услуги.

[15]Наумовси Г., Докмановиќ М., Право и информатичка технологија, Скопје, март 2009, страна 146

- **Измама со кредитни картички и хартии од вредност**

Самиот поим измама со кредитни картички ни кажува дека сторителот користи податоци од туѓа кредитна картичка, со цел неовластено да изврпи одредена набавка на стоки или услуги или да изврши други промени на сметката.[16]

Исто така постои можност за измама и во случаите на трговија со хартии од вредност, доколку таа се одвива преку интернет. Со самото тоа што се зголемува бројот на корисници на интернетот, се повеќе се усовршува и трговијата, односно се зголемува процентот на online трговијата. Постојат три вида на категории кои се поврзани со измама со хартии од вредност: Манупилирање со пазарот, нудење на измама и Против правно посредување и застапување.

Манупилирањето на пазарот всушност ги опфаќа обидите за распространување на лажни информации, се со цел вештачко зголемување на цената на пазарот со зголемување на побарувачката за помалку вредните хартии од вредност.[17]

- **Кражба на идентитетот**

Најопштата дефиниција за кражбата на идентитетот е, противправното стекнување и користење лични податоци со цел стекнување на стоки и услуги во име на друг. Во облици на кражба на идентитет би ги вброиле измамите во електронското договарање за продажба на недвижнини и слично, како и електронското плаќање на сметки.

[16] Наумовски Г.,Докмановиќ М., Право и информатичка технологија, Скопје, март 2009, страна 149

[17] Наумовски Г.,Докмановиќ М., Право и информатичка технологија, Скопје, март 2009, страна 150

- **Попречување, присвојување и вмешување во компјутерски и телекомуникациски услуги**

Попречувањето и присвојувањето на компјутерски услуги ги опфаќа сите облици на вмешување или прекинување на компјутерски или телекомуникациски услуги со што се предизвикуваат штетни последици на широкиот круг на корисници на овие услуги.[18]

Како најчести облици од овој вид компјутерски криминал се јавуваат кражба на сигнал емитуван од провајдери на кабловска телевизија, напад со цел одбивање на услуги, испраќање на несакани и вознемирувачки електронски пораки и инсталирање на програми со рекламни содржини.

- **Кражбата на сигнал емитуван од провајдери на кабловска телевизија**

Најчесто опфаќа модификување на постојните уреди за да се овозможи физички пристап до сигналот, како и употреба на нови уреди со цел да се конвертира кодираниот сигнал, во сигнал кој може да биде видлив на телевизискиот приемник.

- **Нападот со цел одбивање на услуги или Denial of service attack – DOS**

Опфаќа напад врз компјутери со цел да се оневозможат услугите на овластените корисници. Најчести напади кој се поврзани со овој вид криминал, се разделувањето на составни делови на компјутери или мрежата, како и напади врз софтверот за да се оневозможи неговото функционирање, како и преоптоварувањето на системот и неговите ресурси и капацитети со цел тој да падне и да се оневозможи да работи.[19]

[18] Наумовски Г.,Докмановиќ М., Право и информатичка технологија, Скопје, март 2009, страна 150

[19] Наумовски Г.,Докмановиќ М., Право и информатичка технологија, Скопје, март 2009, страна 151

- **Испраќање на несакани и вознемирувачки електронски пораки**

Под овој термин се подразбира испраќање на голем број на електронски пораки од комерцијална или маркетиншка природа кои честопати имаат и вознемирувачки или навредливи содржини. Пораките кои се праќаат на овој начин се именуваат како spam пораки.[20]

- **Инсталирање на програми со рекламни содржини или ADWARE**

Ни претставува облик на компјутерска програма која овозможува ненадејно појавување на одредена содржина од рекламна природа или на десктопот или во комуникацискиот софтвер.

- **Компјутерска шпионажа**

Компјутерската шпионажа всушност опфаќа дејствија на употреба на посебен компјутерски софтвер кој се внесува во компјутерот, за се постигне контрола врз системот преку – собирање и добивање на информации, инсталирање на други типови софтвер пренасочување на интернет пребарувачот на други страници и слично.[21]

- **Хакирање (Неовластено навлегување во компјутерскиот систем)**

Компјутерското хакирање претставува пристап до компјутерскиот систем без изречна или посредна дозвола на сопственикот на компјутерскиот систем.[22]

[20] Наумовски Г.,Докмановиќ М., Право и информатичка технологија, Скопје, март 2009, страна 151

[21] Наумовски Г.,Докмановиќ М., Право и информатичка технологија, Скопје, март 2009, страна 152

[22] Наумовски Г.,Докмановиќ М., Право и информатичка технологија, Скопје, март 2009, страна 152

Хакирањето, односно неовластеното навлегување во компјутерскиот систем, како еден вид облик на сајбер криминалитет означува противправно стекнување на пристап до еден или повеќе компјутерски системи преку злоупотреба на безбедносните недостатоци, односно ги пробива и надминува безбедносните пречки како што е пасвордот, се со цел за искористување на податоци или нивна кражба, како и вметнување на нова програмска функција.

- **Дистрибуција на вируси и други облици на злонамерен софтвер (MALWARE)**

Дистрибуцијата на компјутерски вируси е еден од најчестите облици на сајбер криминалитет. Компјутерските вируси опфаќаат четири категории на злонамерен софтвер

- Логички бомби
- Тројански коњи (тројанци)
- Вируси
- Црви

Во однос на фазите на внесување на вирусот во компјутерскиот систем и негово постоење се разликуваат:

- Инфекција - претставува ширење на вирусот во нападниот компјутерски систем
- Инкубација – претставува опстанок на вирусот во компјутерскиот систем
- Реализација – претставува разболување на компјутерскиот систем.

- **Cyberstalking**

Под поимот cyberstalking како облик на сајбер криминалитет се подразбира употреба на компјутер или други облици на информатичка технологија за следење на

активноста и движењето на луѓето без нивно знаење, со цел заплашување, сексуално задоволство и доминација, или други недозволени мотиви.[23]

Cyberstalking криминалитетот опфаќа два елемента:

- ***Собирање информации за жртвата*** – најчесто станува збор за собирање на податоци од интернет или некој други извори.
- ***Следење, вознемирување, заплашување на жртвата*** – овој елемент најчесто е без физички контакт, а пак опфаќа појавување на сторителот пред домот на жртвата, телефонски повици, оставање на писмени пораки, како и оштетување на имотот на жртвата и слично.

Постојат три категории на cyberstalking и тоа:

1. ***Убедување*** – праќање на e-mail на жртвата од страна на сторителот, чија што содржина најчесто е закани, заплашување, обиди за започнување или обновување на љубовна врска и слично.
1. ***Контрола*** – под оваа категорија на cyberstalking спаѓа контролата на компјутерот и другите уреди на жртвата од страна на сторителот. Како најчест пример за овој тип на cyberstalking е отварање на CD drive на компјутерот на жртвата со цел тој да и докаже дека може да го контролира нејзиниот компјутер.
1. ***Широк опфат*** – пример за ваков вид на cyberstalking е ставање на порнографски слики или пак лични податоци за жртвата на одредени веб страници.

Се со цел заштита од вакви напади, светол примерок кој треба да го практикуваат повеќето држави, е примерот со Велика Британија, со донесувањето на Законот за заштита од вознемирување (Protection from Harrasment Act) од 1997 година, во кој се содржани правила за овој тип на сајбер криминалитет.

[23] Наумовски Г.,Докмановиќ М., Право и информатичка технологија, Скопје, март 2009, страна 154

- **Производство и дистрибуција на нелегална порнографија**

Анонимноста е основна причина за лесно производство и дистрибуција на детска и други видови нелегална порнографија и ваквата дистрибуција најчесто се одвива преку било кој софтвер за пренос на податоци, односно софтвер за комуникација и интернет разговори.

- **Сајбер тероризам**

Терминот сајбер тероризам ги опфаќа сите дејствија кој комбинираат форми на на тероризам и сајбер простор.

Сајбер тероризмот, односно неговите дејствија имаат две важни карактеристики:

1. Тоа се противправни напади и закани за напади на компјутери, мрежи и информации со цел заплашување на влади и народи во насока да се оствари одредена политичка или социјална цел; и
2. Напади кој резултираат со насилство врз лица или имот или барем ги загрозуваат лицата или имотот во одреден степен, со цел да се предизвика страв.[24]

- **Повреда на правата од интелектуална сопственост**

Повреда на правата од интелектуална сопственост како облик на сајбер криминалот постои секогаш, кога како средство се користи информатичката или компјутерска технологија. Криминализацијата на овие повреди, може да биде покриена или со кривичните законици или пак со законите кои го регулираат правото на интелектуална сопственост.[25]

[24] Наумовски Г.,Докмановиќ М., Право и информатичка технологија, Скопје, март 2009, страна 157

[25] Наумовски Г.,Докмановиќ М., Право и информатичка технологија, Скопје, март 2009, страна 159

- **Дигитална пиратерија**

Дигиталната пиратерија како облик на повреда на авторските и сродните права се дефинира како нелегална репродукција на дела кои припаѓаат на друг, со цел без надомест да бидат употребени или пренесени како сопствени интелектуални творби.[26]

[26] Наумовски Г.,Докмановиќ М., Право и информатичка технологија, Скопје, март 2009, страна 160

ГЛАВА ВТОРА – КОМПЈУТЕРСКИОТ КРИМИНАЛ НА МЕЃУНАРОДНО НИВО

1. УРЕДУВАЊЕ НА КОМПЈУТЕРСКИОТ КРИМИНАЛ НА МЕЃУНАРОДНО НИВО

1.1. КОНВЕНЦИЈА ЗА КОМПЈУТЕРСКИ КРИМИНАЛ

Прикажаните бројки на интернет корисниците, односно големиот пораст на бројот со минувањето на годините и земањето на се поголем замав на информатичката технологија на глобално ниво, го вклучи алармот за пронаоѓање на начин на регулирање на новиот вид криминал, односно негово спречување.

Свесни за промените коишто доаѓаат во светот поврзано со компјутерските мрежи, а и загриженоста поради ризикот што компјутерските мрежи и електронските информации можат да бидат лесно искористени за извршување на кривични дела и со оглед на тоа што кривичните дела коишто се поврзани со компјутерски криминал се во постојан пораст. Верувајќи дека само со меѓународна соработка може да се сузбие секаков вид на криминал, па така и компјутерскиот криминал.

Од страна од Советот на Европа е усвоена **Конвенцијата за компјутерски криминал на 23 ноември 2001 година**, а нашата држава истата ја има ратификувано на **16 јуни 2004 година**.

Во преамбулата на самата Конвенција изречно е нагласена потребата за откривање на сторителите на компјутерскиот криминал кои имаат меѓународен карактер како еден од главните приоритети за борба против ваквиот криминал, е всушност подобрување на соработката на надлежните национални власти.

Конвенцијата се состои од преамбула и 4 глави, и тоа:

1. **Значење на изразите;**
2. **Мерки што треба да се превземат на национално ниво;**
3. **Меѓународна соработка;**
4. **Завршни одредби;**

Во **првата глава** на Конвенцијата ни се претставени збир од дефиниции и основни поими кои се користени во самата Конвенција.

Во **втората глава** на Конвенцијата се регулирани мерките што треба да се превземат на национално ниво, односно материјално кривично правните одредби и процесните одредби кои се однесуваат на земјите потписници со што тие се обврзани да ги воведат во нивното законодавство и надлежност.

Материјалното кривично право во Конвенцијата е поделено на следниот начин:

1. Дела против тајноста, интегритетот и достапноста на компјутерските податоци и системи;

   Недозволен пристап;

   Недозволено пресретнување:

   Упад (вмешување во податоци);

   Упад (вмешување во систем);

   Злоупотреба на уред;

2. Дела чие извршување е поврзано со компјутер;

   Фалсификување поврзано со компјутер;

   Измама поврзана со компјутер;

3. Дела поврзани со содржински податоци;

   Дела поврзани со детска порнографија;

4. Дела поврзани со повреда на авторските и други сродни права;
5. Одговорност за соучешништво и санкции;

   Обид, помагање и поттикнување;

   Одговорност на правните лица;

   Санцкии и мерки;

Процесните одредби во Конвенцијата за компјутерски криманал се опфатени со членовите од 14 до 22 во Конвенцијата, кадешто е наведено дека секоја страна ќе се залага во воведувањето, имплементацијата и примената на овластувањата и постапките предвидени во овој оддел да подлежат на условите и гаранциите коишто се предвидени со домашното право со кое се обезбедува заштита на човековите права и слободи, односно обврските што произлегуваат на земјите потписнички на Конвенцијата за заштита на човековите права и основни слободи на Советот на Европа од 1950 година и Меѓународниот пакт за граѓански и политички права на ООН од 1966 година како и други меѓународни инструменти за заштита на човековите права.[27]

Исто така во овој дел е наведено дека земјите потписнички ќе усвојат законодавни и други мерки кои се неопходни на нејзините надлежни органи да можат да наредат или на сличен начин да обезбедат експедитивно зачувување на точно определени компјутерски податоци, притоа со издавањето на таквата наредба до одредено лице да ги зачува определените компјутерски податоци, страната ќе воведе мерки кои се неопходни за да наметне обврска на тоа лице да го сочува и одржува интегритетот на компјутерските податоци онолку време колку што е потребно, но не повеќе од 20 дена.[28]

Во делот на процесното право исто така е наведено дека страната ќе усвои законодавни и други мерки кои се неопходни за нејзините надлежни органи да бидат овластени да вршат претрес или да превземат други дејствија со кои ќе обезбедат пристап до компјутерски систем како и до складираните податоци во него кога постојат основи да се верува дека бараните податоци се чуваат во компјутерските систем или дел од него.[29]

Во чл. 22 од Конвенцијата за компјутерски криминал е наведено дека секоја страна ќе усвои такви законодавни и други мерки кои се неопходни за да воспостави надлежност или јурисдикција над делата во случаите кога делото е сторено:

1. На нејзината територија;

[27] Член 15 од Конвенција за компјутерски криминал на Советот на Европа(Сл. Весник на Република Македонија број 56, Скопје, 2005

[28] Член 16 од Конвенција за компјутерски криминал на Советот на Европа(Сл. Весник на Република Македонија број 56, Скопје, 2005

[29] Член 19 од Конвенција за компјутерски криминал на Советот на Европа(Сл. Весник на Република Македонија број 56, Скопје, 2005

2. На брод кој плови под знамето на таа страна;
3. Во воздухоплов кој е регистриран според законот на таа страна;
4. Од нејзин државјанин, доколку делото е казниво според кривичниот закон онаму кадешто е сторено или доколку делото е сторено надвор од територија која потпаѓа под јурисдикција на било која страна.

Третата глава на Конвенцијата е посветена на меѓународната соработка помеѓу земјите потписнички дека ќе соработуваат меѓусебно во согласност со одредбите наведени во оваа Конвенција преку примена на релевантните меѓународни инструменти за меѓународна соработка во кривичните предмети со цел спроведување истрага на дела поврзани со комјутерски криминал, како и екстрадиција на сторителите, под услов лишувањето од слобода да биде со казна затвор од најмалку една година или поголема.[30]

Државите потписнички можат да побараат од друга држава потписничка да изврши претрес, да заплени или на друг начин да обезбеди податоци складирани со помош на компјутерскиот систем, во случај кога:

1. Постојат основи да се верува дека релевантните податоци се особено подложни на загуба или модификација, или
2. Инструментите, аранжманите или законите предвидуваат експедитивна соработка[31]

Конвенцијата за компјутерски криминал предвидува дежурни служби кои ќе работат денонокно, односно седум дена во неделата по 24 часа, со цел спроведување истражни и други процесни дејствија во однос на кривични дела поврзани со овој вид на криминал, или заради прибирање докази во електронска форма за одредени кривични дела.

Во рамки на оваа помош директно можат да се спроведат следниве мерки:

1. Давање на техички совети;

[30] Член 24 од Конвенција за компјутерски криминал на Советот на Европа(Сл. Весник на Република Македонија број 56, Скопје, 2005

[31] Член 30 од Конвенција за компјутерски криминал на Советот на Европа(Сл. Весник на Република Македонија број 56, Скопје, 2005

2. Зачувување на податоци;
3. Прибирање докази, давање правни податоци и лоцирање на сомнителни лица.

1.2. ДОПОЛНИТЕЛЕН ПРОТОКОЛ НА КОНВЕНЦИЈАТА ЗА КОМПЈУТЕРСКИ КРИМИНАЛ ЗА ИНКРИМИНАЦИЈА НА ДЕЛА ОД РАСИСТИЧКИ И КСЕНОФОБИСТИЧКИ ВИД ПО ПАТ НА ИНФОРМАТИЧКИ СИСТЕМИ

Додатниот Протокол на Конвенцијата за компјутерски криминал е донесен 23 јануари 2003 година на Совет на Европа во Стразбур и истиот се однесува за инкриминација на дела од расистички и ксенофобистички вид по пат на информатички системи. Република Северна Македонија го има ратификувано на 5 јули 2005 година.

Целта на овој Протокол е да се комплетира, за страните на Протоколот одредбите на Конвенцијата за компјутерски криминал во поглед на инкриминацијата на делата од расистички и ксенофобички вид по пат на информатички системи.

Овој Протокол и дава обврска на државите потписнички во своите законодавства да ги воведе следните кривични дела:

1. Распростанување на расистички и ксенофобички материјал по пат на информатички системи;
2. Закана со расистичка и ксенофобистичка цел;
3. Навреда со расистичка и ксенофобистичка цел;
4. Негирање, грубо минимизирање, одобрување или оправдување на геноцид или криминал против човештвото, и
5. Помагање или соучешништво.[32]

Дејствијата кој што се поврзани со расизам и ксенофобија најчесто претставуваат навреда на личноста, но не и закана. Овој протокол, на потписничките држави и ја остава можноста слободно да одлучи дали ваквите постапки ќе подлежат на кривична одговорност или не.

Навредите поврзани со расизмот и ксенофобијата во преден план ги става поединци или група на лице и дали спрема нив ќе биде извршено некое кривично

[32] Член 3-7 од Дополнителен Протокол на Конвецијата за компјутерски криминал за инкриминација на дела од расистички и ксенобистички вид по пат на информатички системи (Службен весник број 56/05 - Скопје, 05.07.2005 година)

дело кое што е одредено и во националното законодавство, а тие поединци или група на луѓе треба да се разликуваат по бојата на кожа, потеклото, националноста, верската или етничката припадност за да би можело тоа дело да има специфичен облик кој што ќе биде предвиден со протоколот.

1.3. ИНТЕРПОЛ

Меѓународната организација за криминалистичка полиција – ИНТЕРПОЛ или The International Criminal Police Organisation е најголемата меѓународна полициска организација во светот, во која членуваат 192 земји од светот. По бројот на земји членки, поголема светска организација од ИНТЕРПОЛ е само Организацијата на Обединетите Нации. Меѓународната организација за криминалистичка полиција е формирана на 7 септември, 1923 година во Виена, Австрија, а од 1989 година нејзиното седиште се наоѓа во францускиот град Лион. Основната цел на ИНТЕРПОЛ е:

1. Да осигура и унапредува најшироко, заедничко помагање на сите органи на криминалната полиција во границите на важечките закони во различните земји и во духот на Универзалната декларација за човекови права.
2. Да воспостави и развие сите институции кои можат ефикасно да придонесат во превенцијата и сузбивањето на обичните кривични дела.[33]

ИНТЕРПОЛ, односно меѓународната организација за криминалистичка полиција си има свои правила за соработка кој треба да ги почитуваат земјите членки, а тоа се:

1. Строго е забрането за Организацијата да преземе било каква интервенција или активност да политички, воен, верски или расен карактер[34]
2. Соработката се однесува исклучиво за таканаречени вообичаени криминални дејствија.
3. Во секое барање, изрично мора да биде наведена причината за собирање на потребните информации, како и да точно да се наведе одредено казнено дејствие.

Во 2014 година, Владата на Сингапур подарила еден современ центар кој бил направен за борба против сајбер криминалот. Тој современ центар е една од организионите единици на ИНТЕРПОЛ наречена IGCI (INTERPOL Globar Complex for Innovation) во кое што постои одделение кое е посебно за борба против сајбер

[33] Член 2 од статутот на Интерпол - Article 2 of The Constitution of the ICPO-INTERPOL adopted by the General Assembly at its 25th session (Vienna - 1956). I/CONS/GA/1956(2008)

[34] Член 3 од статутот на Интерпол - Article 3 of The Constitution of the ICPO-INTERPOL adopted by the General Assembly at its 25th session (Vienna - 1956). I/CONS/GA/1956(2008)

криминалот, или INTERPOL Digital Crime Centre IDCC и одделение за развој, односно Cyber Innovation and Outreach CIO.

Како основни активности на овој центар за борба против сајбер криминалот се собирање, анализирање и обработување на податоци, а воедно и предупредување на полициските служби на национално ниво за евентуални закани поврзани со ваков вид на криминал, се со цел зајакнување и проширување на меѓународната полициска соработка, односно помош при истрагите на националните полициски служби да ги спречуваат ваквите кривични дела.

Според проценките на Интерпол, овој центар за борба против сајбер криминалот на годишно ниво би можел да спречи повеќе од 1000 кривични дела поврзани со ваквиот вид на криминал со што ќе се спречи големото стекнување на противправна имотна корист.

1.4. ЕВРОПОЛ

Европол, или Европска полициска управа е агенција на Европската Унија, која е основана со Договорот за основање на Европската Унија од Мастрихт 1992 година. Европската полициска управа започна со работа со ограничени надлежности на 3-ти јануари 1994 година и таа е задолжена да собира разузнавачки информации од областа на криминалот.

Целта на формирањето на Европол е да се подобри соработката на националните полициски служби како и ефикасноста на надлежните органи во борбата против најсериозните форми на криминал, кој влијае на повеќе земји. Главните задачи на Европол се оперативни, за да би можеле да ја олеснат размената на информациите помеѓу земјите членки, со што би имале олеснување и помош при водење на истрагите.

Европската полициска управа нема надлежност да апси криминалци, но сепак благодарение на базата на податоци која што ја поседува, им овозможува на полициските служби во брзо време да ги решаваат своите истраги, а тие податоци ги поседуваат преку специјализиран информативен систем, во кој земјите членки имаат увид, обработуваат податоци како и разменуваат податоци.

Центарот за борба против сајбер криминалот е одделение на Европол и е основан во 2013 година. Центарот е составен со цел да помогне во заштитата од компјутерските напади во Европа. Главните задачи на овој центар се:

1. Борба против организираните криминални групи
2. Борба против детската порнографија и сексуална експлоатација на Интернет
3. Заштита на податоците од кражби
4. Заштита на виталните информативни системи на Европската Унија.

Центарот за борба против сајбер криминалот големо внимание посветува на злоупотребата на платежните картички бидејќи на ниво на Европската Унија годишно штетата достигнува до милијарда евра и повеќе. Една од најекспонираите акции во јавноста на Европол се однесува токму на оваа област, е операцијата Blue Amber[35]. Во истата билансот се сведел на учество на повеќе од 50 полициски служби, а резултатот е

[35] Види повеќе на - https://www.computerweekly.com/news/4500248925/Police-arrest-130-in-global-anti-cyber-fraud-operation

апсењето на повеќе од 130 лица кои успеале преку злоупотреба на платежните картички да купуваат и препродаваат авионски карти преку интернет, со што оштетиле 38 авио компании и присвоиле милијарда евра. Овој проблем константно се провлекува на тлото на Европа, со оглед на фактот дека само во една година постојат над 20.000 пријави за злоупотреба на картички.

2. АНАЛИЗА НА ПОЗНАТИ СЛУЧАИ НА КОМПЈУТЕРСКИ КРИМИНАЛ НА МЕЃУНАРОДНО НИВО

2.1. СЛУЧАЈ БРОЈ 1 - РУСКИ ХАКЕРИ – 10 МИЛИОНИ ДОЛАРИ

Далечната 1994 година, во САД во одредена експозитура на некоја банка, од страна на неколку корисници на услугите на таа банка, било пријавено недостаток на повеќе од 400.000 американски долари. Американската банка случајот го пријавила во ФБИ, биро кое подоцна спроведело оперативна истрага и при истрагата утврдиле и идентификувале околу 40 нелегални трансакции за краток временски период, за кој се проценува дека биле украдени околу 10 милиони американски долари.

Сметките на кој хакерите ги префрлувале парите, повеќето од нив биле во земји надвор од САД, а само една во Сан Франциско. ФБИ работејќи на овој случај, ги апси хакерите во експозитурата во Сан Франциско, во обид да подигнат финансиски средства.

При вршењето на службените разговори и сослушувањето на хакерите, тие им ја кажале ситуацијата и планот за "збогатување", односно дека биле вработени во компјутерска фирма во Санкт Петербург, чиј газда бил русин со име Владимир Левин.

По спроведување на истрага во Руската престолнина, Федералното Биро за истраги, успеало да го намами газдата на компјутерската фирма да замине во Лондон, каде што во 1995 година бил уапсен, а во наредниот период да биде и екстрадиран во Соединетите Американски Држави.

Владимир Левин, "мозокот" на целата организација, бил прогласен за виновен во јануари 1998 година.[36]

[36]Види повеќе на https://www.fbi.gov/news/stories/a-byte-out-of-history-10-million-hack преземено на ден 20.08.2020

2.2. СЛУЧАЈ БРОЈ 2 - ТИНЕЈЏЕР КОЈ ГИ ХАКИРА МИНИСТЕРСТВОТО ЗА ОДБРАНА НА САД И НАСА

Далечната 1999 година, тогаш малолетникот Џонатан Џејмс на само 15 годишна возраст, влезе во елитата на великаните кога се споменува хакерството. Тинејџерот Џејмс во тоа време успеа да навлезе во компјутерите на американскиот министер за одбрана, со што си овозможи и пресретнување на илјадници електронски пошти кој беа од различни владини организации, како и кориснички имиња и лозинки на разни воени компјутери

Со украдените информации кој ги поседувал, Џејмс можел да прибави парче софтвер на НАСА кој чинел 41.000 американски долари, додека пак целиот софтвер се претпоставува дека вредноста му била 1.7 милиони долари.

Сагата на тинејџерот Џејмс траела кратко, поради негово апсење, но висината на казна била мала, поради неговата младост. Во 2008 година Џонатан Џејмс извршува самоубиство, поради обвинение за заговор со други хакери да украдат информации за кредитни картички. Во неговото писмо пред самоубиството, Џејмс го негирал обвинението. [37]

[37] Види повеќе на https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/ преземено на ден 20.08.2020

2.3. СЛУЧАЈ БРОЈ 3 -РОБЕРТ ТАПАН МОРИС И ЦРВОТ МОРИС (1988)

Студентот на Cornel University во САД, Роберт Тапан Морис, во 1988 година, сакајќи да ја утврди пространоста на сајбер просторот, стори штета од десетици милиони американски долари. Работата излезе од контрола кога црвот наиде на грешка и влезе со вирус кој што бргу се регпилицира и почна да инфицира и други компјутери.

Се претпоставува дека е наштетено на над 6000 компјутери заразени од Црвот Морис, а вредноста на штетата за поправка на компјутерите се движела меѓу 10 и 100 милиони долари.

Иако овој настан би можел да биде закачен како несреќа, несомнено одигра улога во инспирирањето на незгодниот дистрибуиран тип на напади што ги гледаме денес.[38]

[38] Види повеќе на https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/ преземено на ден 15.08.2020

3. СТАТИСТИЧКИ ПОДАТОЦИ НА ДЕЛА ПОВРЗАНИ СО КОМПЈУТЕРСКИ КРИМИНАЛ ВО 2017 И 2018 ГОДИНА ВО РЕПУБЛИКА ХРВАТСКА

Во Република Хрватска кривичните дела поврзани со компјутерски криминал се систематизирани во Кривичниот закон во посебна глава и се предвидени неколку кривични дела како што се неовластен пристап, компјутерска измама, злоупотреба на уред, попречување во работата на компјутерските системи, искористување на деца во порнографија, неовластено следење на компјутерски податоци, компјутерски фалсификат, оштетување на компјутерски систем, оштетување на компјутерски податоци.

Од страна на Министерството за внатрешни работи на Република Хрватска се води евиденција за пријавени и разрешени кривични дела поврзани со компјутерски криминал, а во следната табела се прикажани бројки токму од пријавени случаи и разрешени случаи за 2017 и 2018 година[39]

Кривично дело	Пријавени 2017	Пријавени 2018	Разрешени 2017	Разрешени 2018
Искористување на деца во порнографија	140	55	139	55
Неовластен пристап	7	16	5	13
Попречување во работата на компјутерски системи	11	1	10	1

[39]Види повеќе на https://mup.gov.hr/UserDocsImages/statistika/2018/Statisticki%20pregled%20temeljnih%20sigurnosnih%20pokazatelja%20i%20rezultata%20rada%20u%202018.%20godini.pdf?fbclid=IwAR1MV9CTRgNvURIXAqfw0yyFnJW_v4Yq72qOOAr3OUc9inLbzd8ATDWJt9s преземено на ден 01.09.2020

Оштетување на компјутерскиот систем	7	0	7	0
Неовластено следење на компјутерски податоци	1	0	0	0
Компјутерски фалсификат	37	32	35	39
Компјутерска измама	1114	1310	915	1162
Злоупотреба на уредот	9	17	7	17
Оштетување на компјутерски податоци	80	130	80	130
Вкупно	1406	1561	1198	1417

***Табела број 1* – Статистички податоци достапни на официјалната страна на Министерството за внатрешни работи на Република Хрватска**

Според статистичките податоци прикажани во табелата, околу 3000 кривични дела поврзани со компјутерскиот криминал биле пријавени на територијата на Република Хрвтска, но најмногу се издвојува компјутерската измама како најзастапено кривично дело, со над 2000 пријавени случаи за 2 години. Она што би било позитивно да се издвои од овие податоци е бројот на решени случаи. Доколку се направи споредба во однос на пријавени и разрешени случаи, процентот на решените случаи е над 80, со што се прави заклучок дека Хрватското МВР се справува мошне добро со компјутерскиот криминал.

ГЛАВА ТРЕТА – КОМПЈУТЕРСКИОТ КРИМИНАЛ НА НАЦИОНАЛНО НИВО

1. ПРАВНА РЕГУЛАТИВА НА КОМПЈУТЕРСКИОТ КРИМИНАЛ ВО РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

Потребата за воедначување и систематизирање на глобално ниво на материјалните и процесните норми од областа на компјутерсиот криминал и електронските докази, свој одраз најде во Конвенцијата за компјутерски криминал на Советот на Европа. Иако претходно постоеја обиди за дефинирање на материјалните норми кои ја регулираат меѓународно правната соработка, сепак Конвенцијата по својата сеопфатност, флексибилност и можност за лесно инкорпорирање во националните законодавства, иако првично наменета за државите во Европа, стана препознатлив механизам за лесна комуникација меѓу државите од целиот свет.

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. Советот на Европа ја усвои Конвенцијата за компјутерски криминал во Будимпешта во 2001 година. Вкупно 58 држави се потписнички на Конвенцијата, од кои 28 со ратификација.

Конвенцијата содржи материјални, процесни 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. 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. Домашната правна рамка која ја регулира областа на компјутерскиот криминал ги вклучува:

- ***Кривичниот Законик ;***
- ***Законот за кривичната постапка;***
- ***Законот за електронските комуникации;***
- ***Законот за следење на комуникациите;***
- ***Законот за електронска трговија;***
- ***Законот за електронско управување;***
- ***Законот за парнична постапка ;***
- ***Законот за податоците во електронски облик и електронски потпис ;***
- ***Декларација за побезбеден интернет;***

Во светски рамки постојат повеќе принципи на инкорпорирање на овие норми во домашните законодавства, на пример во Романија и Тахити нормирањето на оваа проблематика е направено со посебен закон во кој се содржани и материјално правни и процесно правни одредби, целосно издвоени од конвенционалните казнени закони.

Домашното законодавство го задржува континенталниот пристап и нормите кои ја регулираат оваа материја се внесени во постојните закони, притоа водејќи сметка за заштитата на основните човекови права во врска со правото на слободно изразување и слобода на мислата и правото на приватност. И покрај тоа што компјутерскиот криминал претставува материја која постојано се менува и има новитети кои не може едноставно да се дефинираат (нови технологии во мобилната телефонија, примена на посебни истражни мерки итн), а особено кога станува збор за транснационална комуникација, сепак Конвенцијата во целост е инкорпорирана во нашето законодавство. На овој начин се овозможува полесна меѓународна соработка, како и можност за лесно прилагодување на соодветните одредби на новите облици на овој вид на криминал. Материјалните одредби за кривичните дела од областа на компјутерскиот криминал се содржани во КЗ и се однесуваат на:

1.1. КРИВИЧНИ ДЕЛА ВО КРИВИЧНИОТ ЗАКОНИК НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

1.1.1. ЧЛЕН 144 – ЗАГРОЗУВАЊЕ НА СИГУРНОСТА

Овој член од Кривичниот законик е директно поврзан со уставно загарантираните права и слободи на граѓаните, односно нивната сигурност, чувството на слободата тогаш кога неговиот живот не е доведен до опасност. Оваа опасност се однесува кога станува збор за закана дека ќе биде извршено кривично дело, закана која се пренесува преку пат на информатички системи. За сторителите на ова дело е пропишана казна затвор од пет години или потешка казна против некое лице поради нивната припадност на одреден пол, раса, боја на кожа, род, припадност на маргинализирана група, етничка припадност, јазик, државјанство, социјално потекло, религија или верско уверување, други видови уверувања, образование, политичка припадност, личен или општествен статус, ментална или телесна попреченост, возраст, семејна или брачна состојба, имотен статус, здравствена состојба, или на која било друга основа предвидена со закон или со ратификуван меѓународен договор, Кривичниот законик предвидува затворска казна од една до пет години за овие сторители.[40]

1.1.2. ЧЛЕН 147 - ПОВРЕДА НА ТАЈНОСТА НА ПИСМАТА ИЛИ ДРУГИ ПРАТКИ

Слободата на службеното, деловно и приватно комуницирање на човекот на некој начин ја претставува и слободата на изразување неговите мисли, чувства или ставови. Прекршувањето на ваквата слобода всушност ја прекршува и заштитата на личноста како и неговата приватност. Од начелото на неповредливост на тајната на писмата би можело да се отстапи само на еден начин, доколку постои судска одлука за истото, односно ако тоа е неопходно за непречено водење на казнена постапка. Во Кривичниот законик на РСМ се предвидени казни од парична казна до казна затвор до пет години, во зависност од тоа што е сторено. Во тој случај, доколку лицето без

[40] Член 144 од Кривичен законик („Службен весник на Република Северна Македонија” број 199/14)

согласност од лицето спрема кое е упатена пратката или пак без судска одлука, ќе отвори туѓо писмо, телеграма, обезбедена електронска пошта или некое друго затворено писмо, со што ќе стори повреда на нивната тајност, со прикривање, уништување или ќе ја предаде на друг таа пратка, ќе се казни со парична казна или затвор до шест месеци. А, пак доколку станува збор, делото да биде сторено од страна на службено лице во вршење на службата, во Кривичниот законик е предвидена казна затвор од три месеци до три години.

Во ставот 2 од овој член е наведено дека лицето кое со намера за себе или за друг ќе прибави некаква корист или ќе нанесе штета на друго лице или ќе ја соопшти тајната што ја дознал од писмото, телеграмата или електронската пошта, ќе биде казнет со парична казна или казна затвор до една година. Доколку се случи, ова дело да го стори службено лице во вршење на службата, КЗ предвидува казна затвор од три месеци до пет години.

Делото ќе се смета за довршено, со самото отварање на пратката, а гонењето за ова дело се презема по приватна тужба[41]

1.1.3. ЧЛЕН 149 – ЗЛОУПОТРЕБА НА ЛИЧНИ ПОДАТОЦИ

Уставот на РСМ во член 18 ги гарантира сигурноста и тајноста на личните податоци. Самата заштита на личните податоци всушност е и основа и за други слободи и права на човекот, што во денешното "модерно" време помалку стануваат ограничени. Кривичниот законик на РСМ го регулира овој член каде што е наведено дека за лицето што спротивно на законите и без согласност на граѓанитот ќе прибира, обработува или користи негови лични податоци, е предвидено парична казна или затворска казна до една година. Современата информатичка ера и "модерното" време кое што го споменавме направи ваквите дела да бидат лесно остварливи. Па така во став 2 од овој член е наведено дека лицето што ќе злоупотреби лични податоци со намера да нанесе штета или да оствари некаква корист, со навлегување во компјутерски информатички систем, Кривичниот законик предвидува парична казна или затворска казна до една година. Доколку сторителот на делото е службено лице и

[41] Член 147 од Кривичен законик („Службен весник на Република Северна Македонија" број 199/14)

го сторил делото во вршење на службата, за истиот е предвидена затворска казна во времетраење од три месеци до три години. Делото ќе се смета за довршено со самото навлегување во компјутерскиот систем односно не е потребно сторителот да започне да ги користи податоците кој ги пронашол. И самиот обид за сторување на ова дело е казниво. Исто така во КЗ постои казна и за правните лица, односно доколку правно лице е сторител на вакво дело ќе се казни со парична казна.[42]

1.1.4. ЧЛЕН 149-А – СПРЕЧУВАЊЕ НА ПРИСТАП КОН ЈАВЕН ИНФОРМАТИЧКИ СИСТЕМ

Дејството како што е неовластеното спречување или ограничување на поединецот да не може да дојде до информации или пристапот до информациите да биде ограничен е спротивно на загарантираното право на слободен пристап кон информациите и нивно пренесување според Уставот на РСМ. Во КЗ на РСМ е предвидена парична казна или казна затвор до една година за лицето што неовластено спречува или ограничува друго лице во пристапот кон јавен информатички систем. А, пак доколку делото е сторено од службено лице во вршење на службата или на одговорното лице во јавен информатички систем, предвидена е парична казна или затворска казна од три месеци до три години. Поради тоа што со ова дела е поврзано индивидуалното чувство на повреда, гонењето се презема по приватна тужба.[43]

1.1.5. ЧЛЕН 157 – ПОВРЕДА НА АВТОРСКО ПРАВО И СРОДНИ ПРАВА

Правата кој произлегуваат од научното, уметничко или некој друг вид на интелектуално творештво се уставно загарантирани права кој што се посебно уредени и во Законот за авторски и сродни права. Во КЗ на РСМ овој член е регулиран со казни од парична казна до казна затвор од пет години, во зависност кој го има извршено делото и колкава штета е сторена. Тој што во свое име или во име на друг неовластено ќе објави, прикаже, репродуцира, дистрибуира, изведе,емитува или на друг начин неовластено ќе посегне по туѓо авторско право иди сродно право,односно авторско дело, изведба или предмет на сродно право, КЗ предвидува изрекување на парична

[42] Член 149 од Кривичен законик („Службен весник на Република Северна Македонија” број 199/14)

[43] Член 149-а од Кривичен законик („Службен весник на Република Северна Македонија” број 199/14)

казна или затвор до една година. Доколку лицето прибавило поголема имотна корист, Кривичниот законик предвидува затворска казна од три месеци до три години. А, доколку прибавил значителна имотна корист, во став 3 од овој член, Кривичниот законик предвидува затворска казна во времетраење од шест месеци до пет години. Ако делото е сторено од страна на правно лице, за истото е предвидена парична казна. Поради опасноста која произлегува од ова дело, уште започнувањето односно обидот за извршување на делото е казнив, а исто така предвидено е и задолжително одземање на авторските дела и предметите на сродните права. Гонењето за повреда на морално право се презема по предлог.[44]

1.1.6. ЧЛЕН 157-А - ПОВРЕДА НА ПРАВОТО НА ДИСТРИБУТЕРОТ НА ТЕХНИЧКИ ПОСЕБНО ЗАШТИТЕН САТЕЛИТСКИ СИГНАЛ

Членот 157-а е регулиран во КЗ со следниве ставови, односно тој што без одобрение од овластениот дистрибутер на технички посебно заштитен сателитски сигнал произведува, увезува, дистрибуира, изнајмува или на друг начин става на располагање на јавноста, односно дава услуги на поставување на материјален или нематеријален уред или систем заради пробивање на таков сигнал, му е предвидена затворска казна во времетраење од шест месеци до три години. При извршувањето на ова кривично дело, постои и потежок облик, а тоа е висината на противправната имотна корист, односно во став 2 е наведено дека доколку лицето прибави значителна имотна корист или пак е предизвикана значителна штета, го следува казна затвор од една година до пет години. Став 3 од КЗ вели дека тој што прима технички посебно заштитен сателитски сигнал чија заштита е пробиена без одобрување на неговиот овластен дистрибутер или врши натамошна дистрибуција на таквиот сигнал, предвидена му е затворска казна од шест месеци до три години. Доколку постои случај каде што е прибавена значителна имотна корист во однос на делото од став 3 казната затвор е од една до пет години. Став 5 од овој член е наменет за правните лица, на кои им следува парична казна доколку сторат вакво кривично дело.

[44] Член 157 од Кривичен законик („Службен весник на Република Северна Македонија” број 199/14)

Доколку се користени предмети или биле наменети за користење при сторување на вакво кривично дело, истите се одземаат.[45]

1.1.7. ЧЛЕН 157-Б – ПИРАТЕРИЈА НА АУДИОВИЗУЕЛНО ДЕЛО

Доколку правото на филмскиот продуцент или овластениот дистрибутер на аудиовизуелно дело биде доведено до прашање, односно одредено лице без одобрение на филмскиот продуцент го дистрибуира, репродуцира или на некој друг начин го прикажува достапно на јавноста, а со тоа противправно го користи аудиовизуелното дело, КЗ предвидува затворска казна од шест месеци до три години. Потешкиот облик на ова дело е доколку со самото сторување на делото, сторителот прибави значителна имотна корист или предизвика значителна штета, а за ова е предвидена затворска казна од една до пет години. За правните лица е предвидена парична казна. Предметите кои биле наменети или користени за сторување на делото или кои настанале со сторувањето на делото се одземаат.[46]

1.1.8. ЧЛЕН 157-В – ПИРАТЕРИЈА НА ФОНОГРАМ

КЗ на РСМ го регулира овој член на тој начин што е изрично наведено дека тој што без одобрение од производителот на фонограм или здружението за колективно остварување на правата на производителите на фонограми произведува, репродуцира, дистрибуира, изнајмува, пушта во промет или на друг начин става на располагање на јавноста, или презема други дејствија заради дистрибуција, изнајмување, пуштање во промет, ставање на располагање на јавноста или на друг начин противправно го користи фонограмот или неговите неовластено умножени примероци, подлежи на затворска казна предвидена во Кривичниот законик и тоа од шест месеци до три години. Исто како, сличноста меѓу ова кривично дело и неколкуте горе наведени се казните, во однос на големината на прибавената противправна имотна корист. И за ова кривично дело, ако е направена значителна имотна корист или предизвикана значителна штета, казната затвор за сторителот е од една до пет години, додека пак ако за сторител се појави правно лице, предвидена е парична казна. Предметите кои биле

[45] Член 157-а од Кривичен законик („Службен весник на Република Северна Македонија” број 199/14)

[46] Член 157-б од Кривичен законик („Службен весник на Република Северна Македонија” број 199/14)

наменети или користени за сторување на делото или кои настанале со сторувањето на делото се одземаат.[47]

1.1.9. ЧЛЕН 193 – ПРИКАЖУВАЊЕ НА ПОРНОГРАФСКИ МАТЕРИЈАЛ НА ДЕТЕ

Најопасниот вид на криминалитет со развојот на информатичката технологија и достапноста на интерент речиси на секого претставува можност за подведување и искористувањето на малолетните лица. Од гледна точка на анонимноста на корисникот уште повеќе се олеснети овие дејствија за производство и дистибуција на порнографски содржини и нивното прикажување на малолетни лица. Ова кривично дело во нашето законодавство е правно уредено со член 193 од Кривичниот законик на РСМ, а дејствието на извршување на ова делото се карактеризира со продавање, прикажување, правење достапни слики, аудиовизуелни и други предмети со порнографска содржина или прикажување порнографска претстава на дете и за основниот облик на делото. За овие сторители се предвидува затворска казна во времетраење од шест месеци до три години. А, пак во став 2 од овој член, е предвиден и потешкиот облик на делото, односно доколку делото е сторено преку пат на средствата за јавно информирање, за сторителот е предвидена затворска казна од три до пет години.[48]

1.1.10. ЧЛЕН 193-А - ПРОИЗВОДСТВО И ДИСТРУБУЦИЈА НА ДЕТСКА ПОРНОГРАФИЈА

Правилниот развој на децата, почитувањето на нивното достоинство може да се ограничи со производството и дистрибуцијата на детската порнографија. Тоа претставува опасен облик за поттикнување на сексуално насилство спрема деца. Во Кривичниот законик на Република Северна Македонија е инкриминирано ова дело со

[47] Член 157-в од Кривичен законик („Службен весник на Република Северна Македонија” број 199/14)

[48] Член 193 од Кривичен законик („Службен весник на Република Северна Македонија” број 199/14)

високи казни, односно во ставот 1 од овој член е наведено дека тој што произведува детска порнографија со цел за нејзина дистрибуција или ја пренесува или ја нуди или на друг начин ја прави достапна детската порнографија, му е предвидена затворска казна од најмалку пет години. Потешкиот облик на овој вид кривично дело е доколку производството на детска порнографија и нејзино дистрибуирање биде сторено преку компјутерски систем или пак некое друго средство за масовна комуникација, каде и КЗ предвидува поголема казна, односно најмалку осум години затвор. Доколку ова кривично дело биде сторено од право лице, предвидена е парична казна.[49]

1.1.11. ЧЛЕН 193-Б - НАМАМУВАЊЕ НА ОБЉУБА ИЛИ ДРУГО ПОЛОВО ДЕЈСТВИЕ НА МАЛОЛЕТНИК КОЈ НЕ НАПОЛНИЛ 14 ГОДИНИ

Правата кои ги имаат децата на правилен психо-физички развој и воспитување, лесно можат да бидат прекршени доколку се стори некое дело спрема нив кој ќе им го промени правиот тек на животот. Едно од тие дела е и намамувањето на обљуба на малолетник. Дејствијата на поттикнува за да се изврши вакво кривично дело се различни, но најчесто се случува привлекување на малолетникот со лажно претставување, убедување и ветување, преку компјутерско-комуникациски средства. Кривичниот законик на РСМ го регулира овој член со затворска казна од една до пет години на лицето што преку компјутерско-комуникациски средства ќе намами дете кое не наполнило 14 години на обљуба или некое друго полово дејствие. Ова дело ќе се смета за довршено доколку е остварена непосредна средба со малолетникот. Во спротива ќе се работи за обид.[50]

1.1.12. ЧЛЕН 251 ОШТЕТУВАЊЕ ИЛИ НЕОВЛАСТЕНО НАВЛЕГУВАЊЕ ВО КОМПЈУТЕРСКИ СИСТЕМ

Карактеристично за делата кој се уредени со овој член е дека постојано се усовршуваат и модифицираат, овие дела се извршуваат со помош на комјутери и комјутерски мрежи и најчесто објект на заштита претставува комјутерски систем односно одредени комјутерски податоци, а се заштитува правото на сопственост на

[49] Член 193-а од Кривичен законик („Службен весник на Република Северна Македонија" број 199/14)

[50] Член 193-б од Кривичен законик („Службен весник на Република Северна Македонија" број 199/14)

имот. Согласно овој член секој кој што уништи, оштети, и онеспособи комјутерски систем, Кривичниот законик за тоа лице предвидува парична казна или затвор до три години.

Доколку овие дејствија се насочени кон посебни програми кои се од посебни мерки на заштита или се користат во јавните институции, државни органи, го прикажува и потешкиот на ова дело, па според член 251 став 4 од Кривичниот законик, за сторителите е предвидена поригорозна казна затвор од една до пет години.

Доколку пак со делото од став 3 е прибавена поголема имотна корист или е предизвикана поголема штета за сторителот е предвидена затворска казна од една до десет години.

Посебните направи, средства. компјутерски програми или податоци наменети за извршување на делото ќе се одземат.[51]

1.1.13. ЧЛЕН 251-А - ПРАВЕЊЕ И ВНЕСУВАЊЕ НА КОМПЈУТЕРСКИ ВИРУСИ

Правењето и внесувањето на компјутерски вируси можеби на одредени лица е секојдневие поради умешноста кој ја поседуваат и ја употребуваат во компјутерските системи. Кривичниот законик предвидува казни од парична до затворска казна од пет години, во зависност што е сторено. Тој што ќе направи или ќе преземе компјутерски вирус со намера да направи внесување во друг компјутер, го следува парична казна или затворска казна до една година. Потешкиот облик на ова дело е доколку се направи штета со самото внесување на компјутерскиот вирус во компјутерскиот систем. Поради тоа во КЗ постои казна од шест месеци до три години за лицето кое ќе нанеси штета во тој систем. А, доколку е предизвикана поголема штета или пак делото е сторено од страна на група на луѓе, КЗ предвидува затворска казна од една до петок години. Поради специфичноста на ова дело и самиот обид за нанесување на штета е казнив. Ако делото од овој член го стори правно лице, ќе се казни со парична казна.[52]

[51] Член 251 од Кривичен законик („Службен весник на Република Северна Македонија” број 199/14)

[52] Член 251-а од Кривичен законик („Службен весник на Република Северна Македонија” број 199/14)

1.1.14. ЧЛЕН 251-Б - КОМПЈУТЕРСКА ИЗМАМА

Кога се спомнува измамата како кривично дело, е асоцијација на секојдневието на одредени луѓе. Потребата од брзо и лесно доаѓање до одредени финансиски средства, истите ја барат во измамата. Компјутерската измама како кривично дело кое што е инкриминирано во КЗ е специјален облик на делото измама кое се разликува само според начинот на извршување, односно противправната имотна и манипулациите кои ќе бидат сторени, се постигнуваат по електронски пат, со менување на одредени податоци. КЗ на РСМ предвидува казна од парична до затворска казна од десет години, во зависност од обликот на делото. Лицето кое има намера да прибави противправна имотна корист на начин со внесување на на невистинити податоци, бришење, менување или нивно прикривање, според КЗ му се препишува парична казна или затворска казна во времетраење до три години. Казните кој што се предвидени во КЗ се всушност врзани со висината на стекнатата противправна имотна корист. Доколку сторителот прибавил поголема имотна корист, нему му е предвидена затворска казна од три месеци до пет години. Доколку прибавил значителна имотна корист, предвидена е казна затвор од една до десет години. А, доколку ќе го стори со намера само да нанесе штета на друго лице, КЗ предвидува парична казна или затворска казна до една година. Исто така во КЗ е предвидено доколку штетата е поголема, казната е од три месеци до три години. Во став 6 од овој член е предвидена и парична казна или затворска до една година за лицето што изработува, продава, набавува средства кој се наменети за извршување на делото. Поради самата опасност од извршување на делото и самиот обид е казнив. Став 7 е предвиден за правните лица и за нив следува парична казна доколку се сторители на вакво кривично дело. 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.[53]

[53] Член 251-б од Кривичен законик („Службен весник на Република Северна Македонија” број 199/14)

1.1.15. ЧЛЕН 271 – ПРАВЕЊЕ, НАБАВУВАЊЕ ИЛИ ОТУЃУВАЊЕ СРЕДСТВА ЗА ФАЛСИФИКУВАЊЕ

Дејствието на извршување кај ова кривично дело се појавува во неколку облици и тоа како основно дело се појауваат правењето, набавувањето или отуѓување на средства за фалсификување. КЗ предвидува парична казна или затворска казна до една година за лицето кое прави, продава или дава на употреба средства за правење на лажни знаци.

Како потежок облик на овој вид кривично дело претставува неовластеното изработување, набавување или продавање на средствата кои служат против фалсификување или пак неовластено ќе ги монтира на банкарските уреди тие средства со цел да прибави банкарски податоци, сторителите ги следува затворска казна од три до десет години. Средствата кој се употребуваат за извршување на ова дело ќе се одземат.[54]

1.1.16. ЧЛЕН 274-Б - ИЗРАБОТКА И УПОТРЕБА НА ЛАЖНА ПЛАТЕЖНА КАРТИЧКА

Последнава деценија можеме да ја наречеме и новата ера на информатиката и информатичките системи. Усовршувањето на ваквите системи доведе и до зголемен број и до постојани нови видови на криминал, како што е компјутерскиот. Можеби и едно од најчестите кривични дела е изработката и употребата на лажна платежна картичка. Кривичниот законик на РСМ ги регулира казните врз основата на тоа каква противправна имотна корист ќе биде прибавена, дали поголема или значителна имотна корист, па во однос на тоа казните се движат од парична казна до казна затвор од пет години. Доколку е прибавена поголема противправна имотна корист, за сторителот е предвидена парична казна или затворска казна до три години, а додека пак ако лицето прибави значителна противправна имотна корист предвидена му е затворска казна од

[54] Член 271 од Кривичен законик („Службен весник на Република Северна Македонија” број 199/14)

една до пет години. Но исто така и сторителот на делото може да се ослободи од казна во случај да обезбеди покритие пред да дознае дека е откриен.[55]

1.1.17. ЧЛЕН 286 - ПОВРЕДА НА ПРАВОТО ОД ПРИЈАВЕН ИЛИ ЗАШТИТЕН ПРОНАЈДОК И ТОПОГРАФИЈА НА ИНТЕГРАЛНИ КОЛА

Во член 286 од Кривичниот законик на РСМ е наведено дека тој што неовластено ќе употреби, објави, отстапи или пренесе туѓ пријавен или заштитен пронајдок или софтвер, му се предвидува парична казна или казна затвор до три години, а доколку станува збор за правно лице, постои само парична казна. Предметите кои ќе бидат искористени при вршењето на кривичното дело се одземаат, а гонењето се презема по предлог.[56]

1.1.18. ЧЛЕН 379-А - КОМПЈУТЕРСКИ ФАЛСИФИКАТ

Кривичното дело компјутерски фалсификат е предвидено во КЗ на РСМ за лицето што со намера да ги употреби како вистински неовластено ќе изработи, внесе, измени, избрише или направи неупотребливи компјутерски податоци или програми што се одредени или подобни да служат како доказ за факти што имаат вредност за правните односи или тој што таквите податоци или програми ќе ги употреби како вистински, и тоа парична казна или казна затвор со времетраење до три години.

Потешкиот облик на ова кривично дело е во корелација со објектот на дејствие, односно ако дејствие на извршување се компјутерски податоци или програми што се користат во работењето на државните органи, претпријатија, правни и физички лица кои вршат работи од јавен интерес, јавни установи и со нивна употреба е предизвикана значителна штета, на сторителот на кривичното дело му се предвидува затворска казна од една до пет години.

Во ставот три од овој член предвидено е тој што неовластено изработува, набавува, продава, држи или прави достапни на друг посебни направи, средства,

[55] Член 274-б од Кривичен законик („Службен весник на Република Северна Македонија” број 199/14)
[56] Член 286 од Кривичен законик („Службен весник на Република Северна Македонија” број 199/14)

компјутерски програми или компјутерски податоци наменети или погодни за извршување на делото од став 1, дека ќе се соочи со парична казна или со затвор до три години.

Поради опасната од самото извршување на ова дело и неговата комплицираност и самиот обид е казнив. Посебните направи, средства, компјутерски програми или податоци за извршување на делото, ќе се одземат.[57]

1.1.19. ЧЛЕН 394-Г – ШИРЕЊЕ НА РАСИСТИЧКИ И КСЕНОФОБИЧЕН МАТЕРИЈАЛ ПО ПАТ НА КОМПЈУТЕРСКИ СИСТЕМ

Во широка смисла, под говор на омраза користејќи ги комуникациските технологии се подразбира која било употреба на електронски комуникации за ширење расистички, ксенофобични, дискриминаторски, екстремистички содржини.

Денес ширењето на расистички и ксенофобичен материјал може да сретнеме на веб-страници односно портали , социјалните мрежи, блогови, апликации и т.н.

Во Кривичниот законик на Република Северна Македонија, за сите они кои со помош на комјутерски системи ќе го сторат ова дело и се предвидени затворски казни од една до пет години. Доколку делото биле извршено по пат на јавно информирање, му е предвидена иста казна како во став 1 од овој член.

Доколку некој ги стори делата од став 1 и став 2 , но со злоупотреба на неговата службена положба, но со содржината која ја пропагирал ќе предизвика масовни нереди, насилста , а со тоа да предизвика и огромна имотна штета според став 3 од овој член му се предвидува затворска казна во времетраење од една до десет години.[58]

[57] Член 379-а од Кривичен законик („Службен весник на Република Северна Македонија” број 199/14)

[58] Член 394-г од Кривичен законик („Службен весник на Република Северна Македонија” број 199/14)

2. ИСТРАЖУВАЊЕ И СТАТИСТИЧКИ ПОДАТОЦИ НА ДЕЛА ПОВРЗАНИ СО КОМПЈУТЕРСКИ КРИМИНАЛ ВО ПЕРИОД ОД 2001 – 2019 ВО РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

Како што во секоја земја во светот е присутен компјутерскиот криминал, така и Република Северна Македонија не е исклучена. Како што се усовршуваше информатичката технологија и бројот на интернет корисниците беше и е во постојан пораст, така и стапката на овој вид на криминал се зголемува од година во година.

Од страна на Министерството за внатрешни работи на Република Северна Македонија се води евиденција, како и статистички податоци за периодот од 2001 година до 2010 година во областа на економскиот криминал, каде што е наведено дека најзастапено кривично дело е злоупотребата на службена должност, додека пак бројот на делата поврзани со компјутерскиот криминал во таа деценија, се повеќе зема замав од 2008 година па наваму. По испратено барање на официјалната е-маил адреса на МВР за подетални информации поврзани со компјутерски криминал, односно за период од 2011 до 2020 година, од нивна страна беше одговорено потврдно и испратени податоци кои што ќе бидат приложени во табелите. Кривичното дело, оштетување и неовластено навлегување во компјутерски систем, низ бројки за пријавени кривични дела и регистрирани кривични дела во периодот 2001 – 2019 година според статистиката на Министерството за внатрешни работи изгледа вака:

Оштетување и неовластено навлегување во компјутерски систем Член 251	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Регистрирани кривични дела	0	2	1	7	2	2	7	20	63	36
Пријавени	0	2	3	7	1	4	11	30	73	43

кривични дела										

Табела број 2 – статистички податоци преземени од официјалната страна на МВР на РСМ

Според горе наведените статистички податоци кои се јавно достапни на Министерството за внатрешни работи на РСМ, ни даваат до знаење дека со минувањето на годините, односно со усовршувањето на информатичката технологија се зголемува и стапката на овој вид на криминал, во случајот, во 2010 година МВР не бележи вакво кривично дело, додека 2009 и 2010 година бројките се трицифрени.

Во следнава табела се прикажани бројки на евидентирани кривични дела како и евидентирани сторители за кривичното дело "загрозување на сигурноста", кое е регулиран во член 144 од Кривичниот законик на РСМ.

Загрозување на сигурноста, **член 144 став 4**	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
кривични дела	1	4	3	2	2	3	3	5	20	29
Сторители	1	4	5	1	2	2	1	2	21	24

Табела број 3 **– Статистички податоци испратени од МВР на РСМ по претходно поднесено барање**

Индивидуалноста во извршувањето на ова дело можеме да ја заклучиме со споредбата меѓу регистрираните кривични дела и сторителите, од прилика 1 сторител за 1 кривично дело. Од самиот почеток на деценијата, до 2017 година, се извршени помалку кривични дела отколку во 2018 и 2019 година, сумирајќи ги споменатите резултати. Повторно се доаѓа до истиот заклучок, подемот кој го зазема информатичката технологија, доведува до зголемување на обемот на работа на институциите кој се борат против компјутерскиот криминал.

Злоупотребата на личните податоци е регулирана со член 149 од Кривичниот законик на РСМ и за ова дело подолу во табелата ќе ја прикажеме неговата застапеност на територија на Република Северна Македонија.

Злоупотреба на лични податоци, член 149 став 2	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Кривични дела	1	1	1	3	0	0	1	1	2	19
Сторители	1	0	0	3	0	0	1	1	0	10

***Табела број 4* – Статистички податоци испратени од МВР на РСМ по претходно поднесено барање**

Преку бројките во табела број 4 може да заклучиме дека постои "незаинтересираност" за извршување на кривичното дело, злоупотреба на лични податоци, односно стапката на извршени дела е релативно помала, во однос на други кривични дела кој оставаат полни раце работа на институциите задолжени за откривање на криминалот.

Во следнава табела е се прикажани податоци за кривичното дело Повреда на авторско право и сродни права, преку кривичните дела кој се евидентирани од страна на МВР, како и бројот на сторители.

Повреда на авторско право и сродни права, член 157 став 2	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019

кривични дела			2	0	0	0	0	0		1
Сторители			2	0	0		0			0

***Табела број 5* – Статистички податоци испратени од МВР на РСМ по претходно поднесено барање**

Според статистичките податоци од оваа табела, можеме да кажеме дека, слабиот процент на евидентирани кривични дела и сторители на истото, е позитивна работа кога станува збор за овој вид кривично дело, поради неговото не извршување.

Во следната табела се прикажани податоци низ бројки, за евидентирани кривични дела и број на сторители за кривичното дело Повреда на правото на дистрибутерот на тхннички посебно заштитен сателитски сигнал, дело кое е инкриминирано во Кривичниот законик со членот 157-а.

Повреда на правото на дистрибутерот на технички посебно заштитен сателитски сигнал член 157 – а	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
кривични дела	11	2	17	6	3	1	0	0	1	0
сторители	11	2	19	8	3	1	0	0	1	0

***Табела број 6* – Статистички податоци испратени од МВР на РСМ по претходно поднесено барање**

Во поголемиот број од прикажаните податоци видовме дека со минувањето на годините бројките на извршени кривични дела е во постојан пораст, додека пак за ова кривично дело, бројките се намалуваат што е исто така позитивна работа кога ќе се

согледа дека во последните 5 години се извршени само 2 кривични дела. Доколку трендот на опаѓање продолжи, тоа ќе биде еден вид успех за нашето законодавство

Во следната табела се прикажани податоци за евидентирани кривични дела и број на сторители за кривичното дело Пиратерија на аудиовизуелно дело кое е регулирано со член 157-б од Кривичниот законик на РСМ

Пиратерија на аудиовизуелно дело член 157 – б	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
кривични дела	11	9	1	0	0	0	0	0		0
Сторители	12	10	1	0	0	0	0	0		1

***Табела број 7* – Статистички податоци испратени од МВР на РСМ по претходно поднесено барање**

И во оваа табела можеме да ја согледаме позитивноста во извршувањето, односно неизвршувањето на ова кривично дело, а бројките се показател дека за само една деценија се евидентирани 20-тина дела и ист број на сторители, што е позитивно во однос на други кривични дела.

Во следната табела ќе бидат прикажани податоци за евидентирани кривични дела како и број на сторители за кривичното дело Пиратерија на фонограм, дело регулирано со Кривичниот законик со член 157-в.

Пиратерија на фонограм – член 157 – в	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
кривични дела	2	0	0	0	0	0	0	0		0
Сторители	3	0	0	0	0	0	0	0		0

***Табела број 8* – Статистички податоци испратени од МВР на РСМ по претходно поднесено барање**

Според податоците во оваа табела, ова дело е изоставено од страна на сторителите на кривични дела, бидејќи за 10-тина години евидентирани се само 2 кривични дела, со тројца сторители.

Во следната табела ќе бидат прикажани статистички податоци низ бројки за кривичното дело прикажување на порнографски материјал на дете, кое е регулирано со член 193 во Кривичниот законик.

Прикажување на порнографски материјал на дете, член 193	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
кривични дела	4	8	2	2	6	3	8	0	2	4
Сторители	4	9	2	2	8	3	5	0	1	2

***Табела број 9* – Статистички податоци испратени од МВР на РСМ по претходно поднесено барање**

Според овие бројки, можеме да заклучиме само на една позитивна работа, тоа што во 2017 не се евидентирани ниту кривични дела ниту сторители за истото, додека пак цела деценија МВР е со полни раце работа кога станува збор за кривично дело.

Во следната табела ќе бидат прикажани статистички податоци низ бројки за евидентирани кривични дела и број на сторители од страна на МВР на РСМ за кривичното дело производство и дистрибуција на детска порнографија, дело кое е регулирано со член 193-а од Кривичниот законик на РСМ.

Производство и дистрибуција на детска порнографија, член 193-а	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019

кривични дела	2	0	1	2	5	7	7	4	2	6
Сторители	2	0	1	1	6	7	5	6	1	5

***Табела број 10* – Статистички податоци испратени од МВР на РСМ по претходно поднесено барање**

И покрај тешкиот облик на ова кривично дело и големите казни предвидени во КЗ, сепак, евидентирани се 30-тина кривични дела со ист број на сторители на ова кривично дело. Позитивноста можеме да ја извлечиме со тоа што тие 30-тина сторители се за период од 10 години.

Во следната табела ќе бидат прикажани статистички податоци низ бројки за евидентирани сторители и број на кривични дела поврзани со делото намамување на обљуба или друго полово дејствие на дете кое не наполнило 14 години, регулирано со член 193-б во Кривичниот законик на РСМ.

Намамување на обљуба или руго полово дејствие на дете кое не наполнило 14 години, член 193-б	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
кривични дела	0	2	0	0	0	0	0	2		0
сторители	0	2	0	0	0	0	0	2		0

***Табела број 11* – Статистички податоци испратени од МВР на РСМ по претходно поднесено барање**

Во однос на тежината на ова дело и предвидените големи казни во КЗ, всушност се показател и за бројот на извршители на ова кривично дело.

Во следната табела ќе бидат прикажани статистички податоци низ бројки за евидентирани кривични дела и број на сторители од страна на МВР на РСМ за кривичното дело оштетување и неовластено навлегување во компјутерски систем, кое е регулирано со член 251 од Кривичниот законик.

Оштетување и неовластено навлегување во компјутерски систем член 251	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
кривични дела	36	47	31	74	76	40	70	43	53	65
Сторители	43	29	14	15	22	33	40	34	28	37

Табела број 12 **– Статистички податоци испратени од МВР на рсм по претходно поднесено барање**

Во една од горе наведените табели се прикажани бројот на евидентирани кривични дела во периодот од 2001 до 2010 година. Од тие податоци извадивме заклучок дека со минувањето на годините се зголемува и бројот на евидентирани кривични дела. Веќе во наредната деценија имаме пораст од можеби четири пати повеќе во однос на истото кривично дело. Негативниот тренд на порастот на кривичните дела и бројот на сторители, се показател за подобро регулирање на овие кривични дела во Кривичните законици.

Во следната табела се прикажани статистички податоци низ бројки за евидентирани кривични дела и број на сторители за кривичното дело правење и внесување на компјутерски вируси, регулирано со член 251-а од Кривичниот законик на РСМ.

Правење и внесување на компјутерски вируси, член 251-а	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
кривични дела	0	0	0	0	0	0	0	0		0
Сторители	0	0	0	0	0	0	0	0		0

***Табела број 13* – Статистички податоци испратени од МВР на РСМ по претходно поднесено барање**

Во период од 10 години, Министерството за внатрешни работи не е евидентирало број на сторители и број на кривични дела, поврзани со членот 251-а од Кривичниот законик.

Во следната табела ќе бидат прикажани статистичките податоци низ бројки евидентирани од страна на МВР, за кривичното дело компјутерска измама кое е регулирано со член 251-б во Кривичниот законик на РСМ.

Компјутерска измама, член 251-б	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
кривични дела	5	1	7	4	4	8	12	13	14	12
Сторители	6	2	5	1	5	3	3	12	10	7

***Табела број 14* – Статистички податоци испратени од МВР на РСМ по претходно поднесено барање**

Покрај тоа што измамата ја наведовме како најлесен и најбрз начин на сторителите на ова кривично дело за доаѓање до финансиски средства и други работи, сепак овие бројки се показател дека во нашето законодавство нема многу евидентирани кривични дела. Во првата половина на деценијата бројот на сторители и кривични дела е едноцифрен, а порастот го имаме во последните неколку години. Интересно е да се напомене 2016 година, каде што само тројца евидентирани сторители, биле извршители на дури 12 кривични дела.

Во следната табела ќе бидат прикажани статистички податоци низ бројки за евидентирани кривични дела како и бројот на сторители за кривичното дело правење, набавување или отуѓување средства за фалсификување, регулирано со член 271 од Кривичниот законик.

Правење, набавување или отуѓување средства за фалсификување, член 271 став 3	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
кривични дела	0	0	1	1	0	0	2	1		0
Сторители	0	0	5	7	0	0	2	1		0

***Табела број 15* – Статистички податоци испратени од МВР на РСМ по претходно поднесено барање**

Комплицираноста во извршувањето на ова кривично дело можеме да ја заклучиме од овие бројки, бидејќи за 2 кривични дела, во 2 години, биле потребни дури 12 сторители. А, можеби и тоа е причина за малиот број на евидентирани кривични дела, што е сепак позитивна страна кога станува збор за нашето законодавство.

Во следната табела ќе бидат прикажани статистички податоци низ бројки за евидентирани кривични дела како и бројот на сторители за кривичното дело ширење на расистички и ксенофобичен материјал по пат на компјутерски систем, дело кое е регулирано со член 394-г од Кривичниот законик на Република Северна Македонија.

Ширење на расистички и ксенофобичен материјал по пат на компјутерски систем, член 394 – г	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
кривични дела	0	0	0	0	0	0	0	0	5	27
сторители	0	0	0	0	0	0	0	0	5	26

***Табела број 16* – Статистички податоци испратени од МВР на РСМ по претходно поднесено барање**

Од прикажаните бројки, се извлекува прашањето, што се случило во 2019 година? Во период од 8 години, нема евидентирано никакво кривично дело ниту сторител, а последните 2 години дури 30-тина кривични дела.

Во следната табела ќе бидат прикажани статистички податоци на евидентирани кривични дела како и бројот на сторители за кривичното дело изработка и употреба на лажна платежна картичка, дело кое е регулирано во Кривичниот законик со член 274-б.

Изработка и употреба на лажна платежна	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019

картичка, член 274 – б										
кривични дела	0	0	10	13	18	9	13	12	4	8
Сторители	0	0	28	13	20	6	25	14	2	7

***Табела број 17*– Статистички податоци испратени од МВР на РСМ по претходно поднесено барање**

Изработката и употребата на лажна платежна картичка, според прикажаните бројки, можеме да заклучиме дека е мошне комплексно дело кога станува збор за негово извршување. Во 2012 биле потребни дури 28 сторители за 10 кривични дела, односно по околу тројца сторители за едно кривично дело, а истото се случувало и во другите години, кога биле евидентирани кривични дела и сторители. Позитивноста е што во последните години трендот на извршување на ова комплексно дело опаѓа.

Во следната табела ќе бидат прикажани статистички податоци низ бројки за евидентирани кривични дела и број на сторители од страна на МВР на РСМ за кривичното дело компјутерски фалсификат, дело кое е регулирано во Кривичниот законик на РСМ со член 379-а.

Компјутерски фалсификат член 379 – а	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
кривични дела	1	0	1	1	1	0	0	0	1	3
сторители	1	0	1	0	0	0	0	0	3	3

***Табела број 18* – Статистички податоци испратени од МВР на РСМ по претходно поднесено барање**

Едноцифрениот број на евидентирани кривични дела и бројот на сторители за 10-тина години е можеби реткост во однос на било кое друго кривично дело. Откривањето на сторителите и решавањето на овие случаи од страна на МВР би било полесно во однос на други кривични дела.

Во следната табела ќе бидат прикажани статистички податоци на вкупен број на регистрирани и пријавени кривични дела низ призмата на Министерството за внатрешни работи на РСМ.

ВКУПНО	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Регистрирани кривични дела	0	2	1	7	2	2	7	20	63	36
Пријавени кривични дела	0	2	3	7	1	4	11	30	73	43

***Табела број 19* – статистички податоци достапни на официјалната страна на МВР на РСМ**

Со овие бројки, повторно се доаѓа до заклучок дека информатичката технологија се усовршува од година во година, а со неа и видовите на компјутерски криминал се повеќе распространети, а приказ за тоа се и бројките на сторени кривични дела во претходната деценија.

Во следната табела ќе бидат прикажани статистички податоци на вкупен број на кривични дела и вкупен број на сторители за последните 10-тина години, евидентирани од страна на Министерството за внатрешни работи.

ВКУПНО	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
кривични дела	74	74	77	108	115	71	116	81	104	174
сторители	84	58	83	62	66	55	82	72	72	122

***Табела број 20* – Статистички податоци испратени од МВР на РСМ по претходно поднесено барање**

Според наведените податоци, скоро и да нема година, а да не постојат трицифрени евидентирани кривични дела и нивни сторители. Според податоците од 2019 година, се доаѓа до претпоставка дека негативниот тренд и порастот во однос на извршување на дела од компјутерски криминал, ќе продолжи и во иднина.

2.1. СТАТИСТИЧКИ ПОДАТОЦИ – ДРЖАВЕН ЗАВОД ЗА СТАТИСТИКА НА РСМ

Покрај горе наведените статистички податоци кои ги прикажавме, односно прикажувајќи ја умешноста во работата на Министерството за внатрешни работи на Република Северна Македонија, како и зголемувањето на бројот на сторители низ годините, на облик на криминал како што е компјутерскиот, ќе бидат прикажани и податоци, односно евиденцијата на пријавени, обвинети и осудени лица низ призмата на Државниот завод за статистика врз основа на видот на кривичното дело, видот на одлука која е донесена, како и разликата во полот.

Во следната табела ќе бидат презентирани статистички податоци за пријавени полнолетни лица според видот на кривичното дело, видот на одлуката и полот за 2015 година. Статистичките податоци се јавно достапни на официјалната страна на Државниот завод за статистика на Република Северна Македонија.

2015 година	Вкупно	Вкупно познати сторители	Жени	Отфрлена пријава	Прекината истрага	Запрена истрага	Поднесен обвинителен предлог	Непознати сторители
Компјутерска измама	2	2		1			1	
Оштетување и неовластено навлегување во компјутерски систем	50	21	3	7			14	29
Повреда на авторски и сродни права	9	9	2	2			7	
Повреда на	3	3		1			2	

правото на дистрибутерот на технички посебно заштитен сателитски сигнал								
Загрозување на сигурноста	378	367	24	141			226	11

Табела број 21 - Пријавени полнолетни лица според кривичното дело, видот на одлука и пол

Со самото прикажување на овие статистички податоци, можеме да воочиме дека директно се неутрализира негативната страна, односно вкупниот број на сторители, на начин што повеќе од 90 проценти од пријавените лица се познати на органите на прогонот. Според податоците единствено во делот на оштетување и неовластено навлегување во компјутерски систем бројот на непознати сторители е голем. А, и исто така, покрај тоа што е голем бројот на пријавени лица, голем е и бројот на лицата спрема кој е поднесен обвинителен предлог.

Во следната табела ќе бидат презентирани статистички податоци за обвинети полнолетни лица според видот на кривичното дело, видот на одлуката и полот за 2015 година. Статистичките податоци се јавно достапни на официјалната страна на Државниот завод за статистика на Република Северна Македонија.

2015 година	Обвинети	Жени	Прогласени за виновни	Запрена постапка	Ослободени од обвинение	Обвинението е одбиено	Мерки за безбедност
Компјутерска измама							

Оштетување и неовластено навлегување во компјутерски систем	20	4	20				
Изработка и употреба на лажна платежна картичка	25	5	15				
Повреда на авторски и сродни права	12	2	9		1	2	
Повреда на правото на дистрибутерот на технички посебно заштитен сателитски сигнал	3	1	3				
Загрозување на сигурноста	288	19	210	41	13	21	3

Табела број 22 - Обвинети полнолетни лица според видот на кривичното дело, видот на одлука и пол

Од прикажаните статистички податоци за обвинети полнолетни лица за 2015 година кој се сторители на кривични дела може да се заклучи дека правосудството во РСМ функционира на релативно добар начин согледувајќи ги бројките на лицата кој се прогласени за виновни. Најголем број на обвинети лица и лица кој се прогласени за виновни има кај кривичното дело загрозување на сигурноста. Интересно е да се напомене дека се повеќе жени учествуваат во извршување на овие кривични дела.

Во следната табела ќе бидат презентирани статистички податоци за осудени полнолетни лица според видот на кривичното дело, видот на одлуката и полот за 2015 година. Статистичките податоци се јавно достапни на официјалната страна на Државниот завод за статистика на Република Северна Македонија.

2015 година	Компјутерска измама	Оштетување и навлегување во компјутерски систем	Изработка и употреба на лажна платежна картичка	Повреда на авторски и сродни права	Повреда на правото на дистрибутерот на технички посебно заштитен сателитски сигнал	Загрозување на сигурноста
Мажи		16	20	7	3	197
Жени		4	5	2	1	13
Вкупно		20	25	9	4	210

Табела број 23 - Осудени лица според кривичното дело и полот

Сумираните резултати за осудени лица за 2015 година, покажуваат дека кривичното дело загрозување на сигурноста било најзастапено, па од таму и големиот број на осудени лица. Најмал е бројот на осудени лица за кривичното дело повреда на правото на дистрибутерот на технички посебно заштитен сателитски сигнал, додека пак за 2015 година нема евидентирано осудени лица за кривичното дело компјутерска измама.

Во следната табела ќе бидат презентирани статистички податоци за пријавени полнолетни лица според видот на кривичното дело, видот на одлуката и полот за 2016 година. Статистичките податоци се јавно достапни на официјалната страна на Државниот завод за статистика на Република Северна Македонија.

2016 година	Вкупно	Вкупно познати сторители	Жени	Отфрлена пријава	Прекината истрага	Запрена истрага	Поднесен обвинителен предлог	Непознати сторители
Компјутерска измама	2	1					1	1
Оштетување и неовластено навлегување во компјутерски систем	74	24	8	2			22	50
Повреда на авторски и сродни права	5	5	1	3			2	
Повреда на правото на дистрибутерот на технички								

посебно заштитен сателитски сигнал								
Загрозување на сигурноста	339	319	22	123			196	20

Табела број 24 - Пријавени полнолетни лица според кривичното дело, видот на одлука и пол

Во 2016 година според податоците кој се прикажани има повторно голем број на пријавени, а повторно на врвот на пријавени сторители е кривичното дело загрозување на сигурноста со вројка од над 300 пријавени.. Споредбено со 2015 година, во делот на непознати сторители повторно своето место го зазема кривичното дело оштетување и неовластено навлегување во компјутерски систем, но 2016та има два пати повеќе непознати сторители во однос на 2015.

Во следната табела ќе бидат презентирани статистички податоци за обвинети полнолетни лица според видот на кривичното дело, видот на одлуката и полот за 2016 година. Статистичките податоци се јавно достапни на официјалната страна на Државниот завод за статистика на Република Северна Македонија.

2016 година	Обвинети	Жени	Прогласени за виновни	Запрена постапка	Ослободени од обвинение	Обвинението е одбиено	Мерки за безбедност
Компјутерска измама							

Оштетување и неовластено навлегување во компјутерски систем	18	3	16			2	
Изработка и употреба на лажна платежна картичка	4		4				
Повреда на авторски и сродни права	2	1	1		1	1	
Повреда на правото на дистрибутерот на технички посебно заштитен сателитски сигнал							
Загрозување на сигурноста	293	18	239	27	15	10	2

Табела број 25 - Обвинети полнолетни лица според видот на кривичното дело, видот на одлука и полот

Според прикажаните податоци во 2016 година најмногу обвинети лица има за делото загрозување на сигурноста од кои голем дел од нив се прогласени за виновни. Вреди да се напомене дека за кривичното дело повреда на правото на дистрибутерот на технички посебно заштитен сателитски сигнал и компјутерска измама нема обвинети лица, со што се намалува стапката на криминал во РСМ.

Во следната табела ќе бидат презентирани статистички податоци за осудени полнолетни лица според видот на кривичното дело, видот на одлуката и полот за 2016 година. Статистичките податоци се јавно достапни на официјалната страна на Државниот завод за статистика на Република Северна Македонија.

2016 година	Компјутерска измама	Оштетување и навлегување во компјутерски систем	Изработка и употреба на лажна платежна картичка	Повреда на авторски и сродни права	Повреда на правото на дистрибутерот на технички посебно заштитен сателитски сигнал	Загрозување на сигурноста
Мажи		13	4			224
Жени		3		1		15
Вкупно		16	4	1		239

Табела број 26 - Осудени лица според видот на кривичното дело и полот

Во делот на осудени лица за 2016 година, според прикажаните статистички податоци, доколку се направи споредба во однос на 2015 година, се бележи драстичен пад на бројот на осудени лица во однос на сите кривични дела, додека пак се порастот на осудени лица е кај кривичното дело загрозување на сигурноста, односно бројот на осудени лица е зголемен за 30 во однос на 2015 година.

Во следната табела ќе бидат презентирани статистички податоци за пријавени полнолетни лица според видот на кривичното дело, видот на одлуката и полот за 2017 година. Статистичките податоци се јавно достапни на официјалната страна на Државниот завод за статистика на Република Северна Македонија.

2017 година	Вкупно	Вкупно познати сторители	Жени	Отфрлена пријава	Прекината истрага	Запрена истрага	Поднесен обвинителен предлог	Непознати сторители
Компјутерска измама								
Оштетување и неовластено навлегување во компјутерски систем	74	20	6	6			14	54
Повреда на авторски и сродни права	5	3		2			1	2
Повреда на правото на дистрибу								

терот на технички посебно заштитен сателитски сигнал								
Загрозување на сигурноста	370	319	15	122		3	194	51

Табела број 27 - Пријавени полнолетни лица според видот на кривичното дело, видот на одлука и полот

Според статистичките податоци од Државниот завод за статистика на РСМ за пријавени сторители на кривични дела за 2017 година, јасно се гледа дека има зголемување на бројот на пријавени сторители за повеќето кривични дела во однос на претходните две години. Покрај таа негативност, исто така се бележи и значителен пораст на бројот на непознати сторители.

Во следната табела ќе бидат презентирани статистички податоци за обвинети полнолетни лица според видот на кривичното дело, видот на одлуката и полот за 2017 година. Статистичките податоци се јавно достапни на официјалната страна на Државниот завод за статистика на Република Северна Македонија.

2017 година	Обвинети	Жени	Прогласени за виновни	Запрена постапка	Ослободени од обвинение	Обвинението е одбиено	Мерки за безбедност
Компјутерска измама	1		1				

Оштетување и неовластено навлегување во компјутерски систем	18	3	17		1		
Изработка и употреба на лажна платежна картичка	10		8			2	
Повреда на авторски и сродни права	1				1		
Повреда на правото на дистрибутерот на технички посебно заштитен сателитски сигнал	1		1				
Загрозување на сигурноста	266	21	194	41	7	17	7

Табела број 28 - Обвинети полнолетни лица според видот на кривичното дело, видот на одлука и полот

Според податоците на Државниот завод за статистика обвинети се вкупно над 300 лица, а за над 200 е поднесено обвинение, за кривични дела поврзани со компјутерски криминал. Споредбено со претходните години се бележи пад на бројот на обвинети, а најмногу во делот на загрозување на сигурноста, како досегашно најзастепено кривично дело.

Во следната табела ќе бидат презентирани статистички податоци за осудени полнолетни лица според видот на кривичното дело, видот на одлуката и полот за 2017 година. Статистичките податоци се јавно достапни на официјалната страна на Државниот завод за статистика на Република Северна Македонија.

2017 година	Компјутерска измама	Оштетување и навлегување во компјутерски систем	Изработка и употреба на лажна платежна картичка	Повреда на авторски и сродни права	Повреда на правото на дистрибутерот на технички посебно заштитен сателитски сигнал	Загрозување на сигурноста
Мажи	1	15	8		1	181
Жени		2				13
Вкупно	1	17	8		1	194

Табела број 29 - Осудени лица според видот на кривичното дело и полот

Овие податоци покажуваат значителна намаленост на бројот на осудени лица во 2017 година во споредба со 2015 и 2016 година. Умешноста во справувањето на Министерството за внатрешни работи на РСМ со сторителите на кривичните дела поврзани со компјутерски криминал, навременото откривање и решавање на овие случаи се предизвик за сторителите за нивно откажување од натамошно извршување на кривични дела.

Статистичките податоци кои ги прикажавме низ бројки за пријавени, обвинети и осудени лица, евидентирани од страна на Државниот завод за статистика на Република Северна Македонија за сторени кривични дела поврзани со компјутерски криминал за 2015, 2016 и 2017 година, може да се каже дека најзастапено кривично е загрозување на сигурноста и тоа со над 1000 сторители за трите години, а пак кривичното дело компјутерска измама е со едноцифрен број за период од 3 години. Најголем број на непознати сторители се бележи кај кривичното дело оштетување и

неовластено навлегување во компјутерски систем, со над 100 непознати сторители за периодот 2015, 2016 и 2017 година.

Според тие бројки се доаѓа до заклучок, дека нашата држава не е одмината од компјутерскиот криминал и дека од година во година бројките се во постојан пораст. Тој негативен тренд е претпоставка дека ќе продолжи и во наредните години, со поголем број на сторители за различни кривични дела.

Од овие статистички податоци, се извлекува и позитивната страна, односно умешноста на органите на прогонот во извршувањето на нивните задачи како и справувањето со компјутерскиот криминал, во однос на бројот на лица кој се откриени како сторители и против кој е поднесен соодветен поднесок.

3. АНАЛИЗА НА СЛУЧАИ НА НАЦИОНАЛНО НИВО

Модерното време и модерниот софистициран модел на информатичка технологија направи така да видовите на компјутерски криминал бидат едно секојдневие, односно да нема ден, а да не се стори вакво дело. На официјалните веб страници на Министерството за внатрешни работи на Република Северна Македонија, како и на други веб страни, најдовме и издвоивме неколку случаи, со кој се е соочила нашата држава.

3.1. СЛУЧАЈ БР. 1 – КОМПЈУТЕРСКА ИЗМАМА

Компјутерската измама веќе ја објаснивме дека преставува брзо и лесно доваѓање до финансиски средства на одредени луѓе. Првиот случај на национално ниво кој ќе биде прикажан, е поврзан со компјутерска измама и истиот е спречен. Кривична пријава е поднесена М.Ш и А.Ш поради компјутерска измама и истите имале цел да стекнат противправна имотна корист на начин што формирале Фондација Допир, а исто така креирале и веб страна https://bidihumansega.mk која работела активно на собирање финансиски средства за помош на деца со ретки болести и посебни потреби. Од страна на секторот за компјутерски криминал и дигитална форензика при МВР на РСМ е спроведена истрага за таа фондација и веб страна и констатирано е дека поголемиот дел од корисниците не постојат, односно креираните профили се измислени или лажни. Од страна на Секторот е утврдено дека биле собрани 3.531.199 денари и истите биле користени од страна на претседателот на фондацијата за свој лични потреби. По претходно обезбедна судска наредба за претрес, е извршен претрес во стан во Скопје и биле пронајдени голем број на докази кој укажуваат на тоа дека лицата се сторители на кривично дело. Паричните средства од фондацијата се замрзнати, додека против сторителите ќе биде поднесено обвинение.[59]

[59] Види повеќе на - https://www.pravdiko.mk/krivichna-prijava-za-kompjuterska-izmama/ преземено на ден 22.08.2020

3.2. СЛУЧАЈ БР. 2 – ДАРКОД – ИЗРАБОТКА И УПОТРЕБА НА ЛАЖНА ПЛАТЕЖНА КАРТИЧКА

Во меѓународна координирана акција против хакерскиот форум и неговите корисници, полициски службеници од цел свет ги откриja сајберкриминалците кои го користеа Даркод форумот за размена и подобрување на нивното хакерско искуство, малвер вируси и ботнет мрежи како и да најдат партнери за нивните следни спам активности или напади со вируси.

Операцијата беше водена од страна на ФБИ и подржана од Европскиот центар за компјутерски криминал на Европол со учество на полициските служби од 20 држави во и надвор од ЕУ. Активностите и приведувањата беа координирани од команден штаб поставен во ФБИ, Питсбург САД и во Европол ЕЦЗ во Хаг, Холандија. Во командниот штаб имаше претставници од Република Српска (БИХ), Кипар, Македонија, Данска, Финска, Германија, Латвиа, Романија, Србија, Шведска, Обединето Кралство и ФБИ кои го координираа техничкото симнување на форумот покрај останатите други полициски активности, кои резултираа со 28 приведувања и 37 претреси на дом, и огромен број на одземени компјутери и компјутерска опрема.

На сајберкриминалниот форум кога сајтот беше симнат се појави завеса и беше поставен банер укажувајќи на тоа дека ФБИ, ЕСЗ и меѓународните партнери имаат контрола врз сајтот. Ова го означува крајот на Даркод, најпопуларниот форум на англиски јазик од рангирани петте најдобри криминални форуми ширум светот. Пред повеќе години 250 до 300 активни корисници на Даркод формираа затворена заедница. Членството се стекнувало исклучително со покана и потоа после извршена проверка од страна на доверлива личност на форумот. Имено, досега имало неколку скандали и гласини дека форумот бил компромитиран за време на неговото постоење. Популарниот сајберкриминален центар опфаќал размена и тргување со предмети и услуги вклучувајќи малициозни софтвери (Malware), сајбер напади кои ги искористуваат маните на софтверот (Zero day Exploits) и пристап до компромитирани сервери. Симнување на форумот исто така го обележува крајот на криминалната заедница на корисниците и сериозно нарушување на нивните малициозни активности , рангирани од хакирање и крадење банкарски податоци од платежни картички, до изнајмување ботнет мрежи и сајбер нападите.

Учесници во меѓународната операција заедно со Република македонија се и Австралија, Бразил, Канада, Хрватска, Колумбија, Кипар, Данска, Финска, Германија, Индиа, Израел, Латвија, Нигерија, Република Српска (БИХ) Романиа, Србија, Шведска, Обединето кралство и САД.

Поконкретно, Сектор за компјутерски криминал и дигитална форензика при МВР, во рамки на глобалната операција изврши претрес на дом и други простории кај две лица во Скопје и Пробиштип. При претресите пронајдени се и одземени повеќе компјутери, мобилни телефони и друга компјутерска опрема која ќе биде доставена на вештачење со цел обезбедување дополнителни докази во постапката.

При операцијата Секторот за компјутерски криминал и дигитална форензика го приведе М.Л.(25) од Штип и поднесе кривична пријава против истиот до ОЈО Штип за постоење на основано сомнение дека сторил кривично дело „Изработка и употреба на лажна платежна картичка“ по чл.274-б ст.3 вв ст.1 и 2 и казниво според Кривичниот Законик на Република Македонија.

Осомниченият во период од 2011 година со употреба на малициозни софтвери прибавувал банкарски податоци од странски државјани преку интернет, а потоа истите ги употребувал за купување разни луксузни предмети, но повеќето банкарски податоци од странски државјани ги продавал на други лица односно ги продавал на повеќе интернет страни, кои се креирани за продавање на нелегално стекнати банкарски податоци од платежни картички. Овие интернет страни (форуми) се креирани и одржувани од негова страна. Од продажбата на банкарските податоци од платежни картички на интернет истиот се стекнувал со голем износ на парични средства, кои најчесто ги подига преку Сервисот за брз трансфер на пари „Вестерн Унион“ каде му уплаќаат пари лица странски државјани од повеќе држави и тоа од Мексико, Лисабон, Русија, Кина, САД и други. До сега е утврдено дека на овој начин пријавениот се стекнал со имотна корист од 82,601,00 Американски Долари и 71.358,00 денари,

Македонските државјани опфатени со меѓународната акција се познати од предходно на македонската полиција и нивните активности биле предмет на истрага на Секторот за компјутерски криминал и дигитална форензика. Со вклучување во меѓународната истрага Секторот за компјутерски криминал и дигитална форензика соработуваше со ФБИ и Европскиот центар за компјутерски криминал на Европол со цел размена на информации за нелегалните активности на македонските државјани на интернет

страните и форумите кои беа предмет на истрага. Сите добиени информации и докази се доставени до надлежните Јавни обвинителства.[60]

[60] Превземано во целост од https://mvr.gov.mk/vest/233 на ден 22.08.2020

3.3. СЛУЧАЈ БРОЈ 3 – ЗАГРОЗУВАЊЕ НА СИГУРНОСТА И ШИРЕЊЕ НА РАСИСТИЧКИ И КСЕНОФОБИЧЕН МАТЕРИЈАЛ ПО ПАТ НА КОМПЈУТЕРСКИ СИСТЕМ

Навредите и заканите преку социјалните мрежи се дел од секојдневието и во иднина нема да престанат. Несовесен граѓанин од Битола, споделил објавата на социјалната мрежа Фејсбук со која што предизвикал загрозување на сигурноста на пратеници во Собранието на РСМ и ширење на расистички и ксенофобичен материјал по пат на компјутерски систем и против него имало основано сомнение за сторени кривични дела по член 144 и член 394-г.

По повикувањето во полициска станица на службен разговор, лицето објаснило дека објавите на социјалната мрежа ги сторил преку својот мобилен телефон.

За него ќе биде поднесен соодветен поднесок.[61]

[61] Види повеќе на https://mvr.gov.mk/vest/7693 преземено на ден 22.08.2020

3.4. СЛУЧАЈ БРОЈ 4 – ПРИКАЖУВАЊЕ ПОРНОГРАФСКИ МАТЕРИЈАЛ НА ДЕТЕ

СВР Скопје-Единица за економски и компјутерски криминал, поднесе кривична пријава до надлежното ОЈО Скопје против И.Ц.(18) од Скопје, поради основи на сомнение дека во временскиот период јули-август 2016 година користејќи ја социјалната мрежа „Фејсбук“, на 12-годишно девојче од Скопје во повеќе наврати и' прикажал фотографии со порнографска содржина.

За кривичното дело „прикажување порнографски материјал на дете“, предвидено и казниво по член 193, од страна на Судија на претходна постапка на сега пријавениот му е одземена патната исправа, забрането му е да го напушта домот во кој живее и задолжително еднаш во неделата да се пријавува во надлежен Суд.

Имено, И.Ц. на социјалната мрежа „Фејсбук“ креирал профил со лажни податоци и лажно име и на 28/07/2016 година испратил понуда за пријателство на 12-годишно девојче од Скопје, кое ја прифатило понудата и започнало електронска комуникација со пријавениот. Во комуникацијата И.Ц. и' кажал дека има 16 години и дека учи во гимназија и дека профиот од кој и' го испратил барањето за пријателство, ќе го исклучи, а ќе и' прати барање за пријателство од нов профил, кој исто така бил со лажни податоци. Откако, девојчето го прифатила пријатеството испратено од новиот профил на пријавениот, истиот и' пуштил фотографија со порнографска содржина и побарал од девојчето да му пушти слика на која ќе биде сликана гола. По ова девојчето ја прекинало комуникацијата со И.Ц., при што истиот во уште два наврати и пуштил фотографии со порнографска содржина, за што девојчето му кажало на својот татко, кој случајот го пријавил во Единицата за економски и компјутерски криминал. По пријавувањето на кривично правниот настан Единицата за економски и компјутерски криминал, превзеде опсежни оперативно тактички мерки за утврдување на идентитет на лицето со Фејсбук-профили, при што е утврден пријавениот и истиот е лишен од слобода, а од домот му е одземен еден преносliв компјутер, еден десктоп компјутер и друга ИТ опрема кои се предадени на вештачење. Во извршениот разговор со И.Ц., тој изјавил дека одземената опрема од неговиот дом е користена само од него и ја

потврдил елктронската комуникација со 12-годишното девојче, во која прикажувал материјали со порнографска содржина.[62]

[62] Превземано во целост од https://mvr.gov.mk/vest/2459 на ден 22.08.2020

3.5. СЛУЧАЈ БРОЈ 5 – ЈАВНА СОБА

Република Северна Македонија па и пошироко беше загрижена од ситуацијата која се рашири како молња низ јавноста. Затворената група на социјалната мрежа Телеграм имаше име "Јавна соба" каде што нејзинита содржина се состоеше од објавување, споделување и коментирани на интимни фотографии и видеа од малолетни девојки од целата земја. Бројот на членови на оваа група за краток временски период надмина нешто повеќе од 7000. Покрај тоа што групата беше затворена, нејзини членови можеа да станат било кој, под било кое име.

Од страна на Секторот за компјутерски криминал и дигитална форензика при МВР на РСМ во координација со Секторот за внатрешни работи Скопје, извршија идентификација и пронаоѓање на сопственикот на групата како и на еден од администраторите. Во текот на оваа истрага се утврдуваа и останатите лица кој имале администратоски улоги во оваа група.

Министерството за внатрешни работи апелираше до членовите на групата, да ја напуштат на своја иницијатива, но сепак апелот не беше ефективен. Исто така од страна на МВР на РСМ, паралелно со оваа истрага, почнаа соработка и со социјалната мрежа Телеграм, за преземање на активности за затварање на групата како и придобивање на други докази кои ќе бидат во интерес на истрагата.[63]

[63] Види повеќе на https://mvr.gov.mk/vest/11018 превземено на ден 22.08.2020

3.6. СЛУЧАЈ БРОЈ 6 – ХАКЕРСКИ НАПАД НА ОФИЦИЈАЛНАТА СТРАНА НА ДРЖАВНА ИЗБОРНА КОМИСИЈА

Избори 2020 година. Зачудувачки, но системот кој Државната изборна комисија го вклопи токму пред одржувањето на предвремените парламентарни избори, имаше за цел навремено и точно да ги прикажува изборните резултати. Неколку дена веб страната за прикажување на изборните резултати беше блокирана.

Од страна на Министерството за внатрешни работи објаснуваат дека „Станува збор за DDoS-напад, кој бил насочен кон страницата https://www.sec.mk/, а кој влијаел на оневозможување на објавувањето на прелиминарните резултати од изборите“

Од таму додаваат дека Секторот за компјутерски криминал и дигитална форензика во соработка со Јавното обвинителство за овој случај ги користи сите механизми за меѓународна соработка со интернет-сервис провајдери кои се надвор од домашна јурисдикција, со цел добивање податоци за корисниците на нивните сервиси.

„Истрагата за овој случај продолжува во насока на утврдување на ИП-адресите од каде што е пристигнат нападот, собирање дополнителни информации за утврдување на нарачателот на овој напад, како и утврдување дали имало други причини кои влијаеле или се поврзани со неможноста на објавувањето на прелиминарните резултати“, се наведува во соопштението.[64]

[64] Види повеќе на https://makfax.com.mk/makedonija/%d1%81%d0%b5%d0%ba%d1%82%d0%be%d1%80%d0%be%d1%82-%d0%b7%d0%b0-%d0%ba%d0%be%d0%bc%d0%bf%d1%98%d1%83%d1%82%d0%b5%d1%80%d1%81%d0%ba%d0%b8-%d0%ba%d1%80%d0%b8%d0%bc%d0%b8%d0%bd%d0%b0%d0%bb-%d0%b8-%d0%bd/ превземено на ден 05.09.2020

4. НАЧИНИ НА ДОЗНАВАЊЕ, МЕРКИ ЗА ОТКРИВАЊЕ НА ИЗВРШИТЕЛИТЕ, ДОКАЖУВАЊЕ И ИЗВРШИТЕЛИ НА КОМПЈУТЕРСКИОТ КРИМИНАЛ

Наједноставниот начин за дознавање на ваков вид на криминал е самата пријава од оштетеното лице, а се дознава и од страна на администраторите кои ги одржуваат информатичките системи на институциите кој подлежале на компјутерски криминал. Во овој случај, како оштетени во овие постапки се јавуваат сите физички и правни лица, а секако тоа можат да бидат и државни институции и влади.

По дознавањето од страна на администраторите кои ги одржуваат информатичките системи дека постои неовластено навлегување во систем кој тие го одржуваат, тие го пријавуваат со соодветен државен орган кој е надлежен за понатамошно преземање на мерки, со цел решавање на целиот случај, односно пронаоѓање и санкционирање на сторителот. [65]

Овластените стручни лица кој ја водат истрагата т.е истражувачите користат оргинална апликација програма, а понекогас и специјален софтвер за анализа и алатки за истражување. Исто така е можно да се следат активностите на компјутерската мрежа и преку интернет, со што полесно се доага до сторителот. Истражувачите најдоа начини за собирање траги од оддалечен компјутер до кој тие немаат непосреден физички пристап, спроведувајќи пристап преку телефонска линија или мрежна конекција.[66]

Докажувањето е можеби и најкомплексната работа кај неовластеното влегување во систем, но сепак лицата кои навлегуваат во таквите системи, на било како начин остават некаква трага, при бришањето на доказите од нивна страна, тие всушност остават трага. Доказот кој тие го остават во компјутерот се нарекува компјутерска форензика и тоа е доказ од компјутер кој треба да биде издржан, убедлив и доволен за да може судот да го прифати.

[65] Македонско сонце 501/ 06.02.2004

[66] Ачковски Ј., Сигурност на компјутерски системи, компјутерски криминал и компјутерски тероризам, Скопје, 2012

4.1. ИЗВРШИТЕЛИ НА КОМПЈУТЕРСКИОТ КРИМИНАЛ

Клучниот чекор за профилирање на компјутерските криминалци е идентификување на специфични заеднички карактеристики што треба да се истражат: Личните карактеристики и карактеристики кои содржат вродени аспекти, како што се отвореност, совесност, екстроверзија, согласност и невротизам. Исто така, личните карактеристики и карактеристики кои се обликувани од животните искуства и настани што доведуваат до макијавелијанизам, нарцизам, психопатија, сензација која бара зрелост, агресивност, проблеми со социјална вештина, површност, недостаток на самодоверба и личен интегритет. Мотивирачките фактори за компјутерски криминалци достигнуваат од хакетивизам, парична добивка, шпионажа / саботажа и политичко / религиозно верување, до здодевност, емоции, сексуални импулси, нетолеранција, потрага по возбуда, подобрување на самопочитта и намера да контролираат / манипулираат други. Покрај тоа, Роџерс Мичел (2006) идентификуваше типови на компјутерски криминалци кои се одликуваат со нивото на вештина и мотивации, како што се почетниците, сајбер-панкерите, интерналите (закана од инсајдер), кодерите, информациите воини , сајбер-терористи, хакери и професионални компјутерски криминалци.[67]

Во пракса, форензичките психолози користат индуктивно или дедуктивно профилирање за да направат едуцирана претпоставка за карактеристиките на криминалците. Индуктивните криминални профили се развиваат со проучување на статистички податоци кои вклучуваат познати модели на однесување и демографски карактеристики што ги споделуваат криминалците. Дедуктивното профилирање користи низа податоци, на пр. вклучувајќи судски докази, докази на местото на злосторството, виктимологија и карактеристики на сторителот. Пример за дедуктивен компјутерски криминален профил содржи информации во врска со жртвата, мотивот, сторителот и сите судски докази.

Друг начин за профилирање на компјутерските криминалци е рамката за разбирање на заканата од инсајдер. Потребно е да се создаде настан (на пр. Одвраќање)

[67] Rogers, M. K. (2006) 'A two-dimensional circumplex approach to the development of a hacker taxonomy', Digital Investigation, 3 (2), pp. 97-102.

за да се разгледаат најразлични карактеристики на актерите и како тие го обликуваат ликот и целта на нападот.[68]

Најзастапената едноставна поделба на комјутерските криминалци е на аматери, професионални криминалци и хакери.

4.1.1. АМАТЕРИ

Аматерите им припаѓаат на групата криминалци кои извршуваат криминал од овој тип без притоа ова да биде нивно примарно професионлано занимање или професија,повремено се ангажираат за вршење на овој криминал и претежно остануваат неоткриени. Како сторители меѓу аматерите правиме разлика помеѓу фрустрирани лица, слаби и ранливи лица и луѓе со порок.[69]

4.1.2. ПРОФЕСИОНАЛНИ КРИМИНАЛЦИ

Професионални криминалци се лица чија единствена занимација и извор се справува со криминал заработка, имаат долгогодишно искуство и претставуваат голема социјална опасност. Во рамките на оваа група правиме разлика меѓу одделни криминалци, организирани групи и криминални организации.

- ***Индивидуални криминалци*** - дејствуваат самостојно и самостојно во остварувањето на нивните цели.Може да соработуваат со други криминалци, но најчесто повремено. Тие работат во локално и тие немаат долгорочен план на дејствување, што има потенцијал да изврши кривични дела работи релативно ограничено.
- ***Организирани групи*** - претставува група на поединци со цел нивно остварување криминални амбиции работат заедно. Групите се движат од лабави здруженија до цврсти здруженија со јасно дефинирани цели.

[68] Nykodym, N., Taylor, R. and Vilela, J. (2005) 'Criminal profiling and insider cyber crime', Computer Law & Security Report, 21 (5), pp. 408-414.

[69] Dimovski D. – Kompjuterski kriminaliter, ĉlanak–Niš, 2010, str.206.

Ограничените групи се локални по природа, но имаат карактеристичен карактер стратегија и тактика. Потенцијалот за кривични дела варира, но во согласност со бројот на и организација, далеку поголема од индивидуалните криминалци, но не толку колку да има последици некој поголем национален ефект.

- ***Криминални организации*** - Тие претставуваат највисок облик на организација и се солидни хиерархија, строга дисциплина, послушност, лојалност со долгорочна стратегија и тактиката на тајност како најзначајниот фактор за опстанок. Организираниот криминал постојано се развива и се развива, и многу лесно се прилагодува на употреба информатичка технологија, користена како алатка за планирање и контрола на криминална активност. Електронскиот трансфер на пари ви овозможува полесно да ги пратите нелегално собраните пари,додека електронската пошта им олеснува на комуникацијата на криминалците. Сето ова ја отежна работата владини агенции, да ја следат и истражуваат работата на криминалните организации, затоа што современата технологијата го олеснува менувањето, модифицирањето и уништувањето на компромитирачките податоци, што на допир на копче, тие можат да бидат избришани и докази уништени.

4.1.3. ХАКЕРИ

Со развојот на информатичката технологија, се појави нов вид специјализиран криминалец хакер. Терминот хакер има повеќе значење и првично значеше почетник играч на голф кој го копа теренот. Хакер е еден вид развивач што прави повеќе или помалку корисни програми, но обично слабо документирани и несакани инцидентни ефекти. Нивниот мотив е често само лично задоволство, но понекогаш и злонамерен направи штета или украде.Хакерите се луѓе опседнати со технологија, и секој аспект од нивниот живот е посветен на тоа.Тој поминува 16 часа секој ден на компјутер, во кој

претежно доминираат мажите, тие се претежно универзитетски дипломирани студенти, иако понекогаш меѓу нив има и некои кои ги стекнаа своите вештини од хоби.[70]

Тие користат комбинација на техничка генијалност и човечка смисла упорност во желбата да ја задоволи желба за знаење. Оваа група извршители го наоѓа своето задоволство во предизвикот да се пробие на заштитата на системите и напаѓаат нечиј друг систем. Тие сакаат да најдат пропусти во програмите, а особено во системите заштита. Постојат чести примери на администратори на системот кои хакираат совети за е-пошта како да се отстранат сфатените недостатоци. Оваа група на сторители на компјутерски криминал сè уште не е позната за светот на психологијата, социологијата и криминологијата, за бројни автори разбирање на нивниот развој и мотивацијата стана едно од главните полиња на нивниот интерес. Криминолозите профилираат хакери погледнете на различни начини и анализирајте од различни аспекти некои од основните карактеристики хакерите се: дека тие се скоро 100% машки; слични на компјутерските програмери, склон кон истражувачко и логично размислување и секогаш во конкурентно расположение тие се љубопитни по природа, не сакаат цензура затоа што тоа доведува до монотонија, тие сакаат да се гледаат себеси како власти зад компјутерот и над секој поврзан со него, што им дава чувство на моќ и контрола, така истото го прават повеќе се заинтересирани да стекнат чувство за моќ отколку за последиците од нивните постапки, тие имаат малку почит според оние кои не знаат ништо за нивните омилени предметни компјутери.[71]

Со текот на годините, хакерите развија и посебен начин на комуникација како дел од нивната култура шифрирана форма на пишување со заменување на букви и броеви, одредени симболи што личат на нив. Примарната цел покрај комуникацијата е да се исклучи несакани лица и меѓусебно препознавање на хакерите. Покрај основната желба за знаење,други стартапи како пари, па со веќе распространетото електронско банкарство, првите напади врз банките и другите финансиски институции наскоро следуваа акциите се: интелектуален предизвик, љубопитност, авантура, забава, чувство на семоќност; потребата за по триумф, елитизам, одмазда, престиж. надомест за чувства со помала социјална или лична вредност. Хакерите според нивните мотиви

[70] Cetinić M.,Kompjuterska krivična dela i pojavni oblici,Časopis Pravni ţivot,broj 10, 1998,, str.266.

[71] Chiesa R., Ducci S., Ciappi S. - Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking, Boca Raton FL, United States, 2008, str.43-44

можат да се поделат на креативни, деструктивни икриминалци. Повеќето хакери сметаат дека е нивна должност да се шират информации и ги споделува своите знаења, како и влегување во системи на други луѓе за истражувачки цели оправдано ако податоците не се украдени и не се ставени на располагање на други хакери.[72]

Овие се програмери кои имаат богатство на знаење, но тие не се доволни заради структуратанивните личности не издржуваат никакви ограничувања и пречки, кои ги уживаат со задоволство. Овој вид хакерите сметаат дека нивните незаконски дејствија се оправдани и етички прифатливи.[73]

Сепак, нивните акции предизвикуваат финансиска штета и оштетување на системот, но софтверските компании ги сметаат за корисни затоа што ги потенцираат слабостите на системот за заштита на податоците.

[72] Види повеќе на http://www.catb.org/jargon/html/ dana 09.08.2015.godine преземено на ден 27.07.2020

[73] Види повеќе на https://www.cs.berkeley.edu/~bh/hackers.html dana 09.08.2015. godine преземено на ден 27.07.2020

ГЛАВА ЧЕТИРИ – ПРЕВЕНЦИЈА ОД КОМПЈУТЕРСКИ КРИМИНАЛ

1. ОСНОВНИ СОВЕТИ ЗА ЗАШТИТА ОД КОМПЈУТЕРСКИ КРИМИНАЛ

Развиеното општество во кое живееме е причина за појавата на криминал како што е компјутерскиот криминал. Откако ќе биде извршен било каков вид на криминал, на сцена стапуваат полициски служби чија работа е спречување на криминалот или доколку е веќе сторено кривичното дело, откривање на сторителот.

Со направениот "бум" на информатичката технологија, се прошири и просторот на дејствување на компјутерските криминалци. Потешкотиите при откривањето на сторителите на компјутерски криминал, често пати е од самото невнимание на жртвата при вклучување на било какви програми и отварање на секаков пристигнат мејл. Сигурноста на компјутерските системи зависи од многу фактори, а пак за да се овозможи соодветна и ефективна заштита на системот е потребно знаење и искуство.

Како основни работи кој би требало да ги знае секој корисник за да се заштити од вакви напади се:

1.1. ИНСТАЛИРАЈТЕ И КОРИСТЕТЕ АНТИ-ВИРУСНИ ПРОГРАМИ

За борба против вирусите најчесто се користат Антивирусните програми, кои спречуваат компјутерот да се инфицира и кои ги уништуваат вирусите.

Доколку Антивирусот е уклучен, постојано, со секое стартување на било каков фајл од компјутерот истиот се скенира бидејќи програмата е активна.

Со цел да се откриваат сите вируси во компјутерот, освен што е потребно да имаат инсталирано антивирусна програма, потребно е и да се прави апдејтување или update на самата програма, со цел повлекување на новите дефиниции од производителот на антивирусната програма.

1.2. НАГРАДУВАЊЕ НА СОФТВЕР

Можеби и од најголемо значење за сигурноста на компјутерскиот систем е неговото наградување со последните верзии на софтверот, со што би имале поголема заштита од новите и непознати закани.

1.3. ОБРАТЕТЕ ВНИМАНИЕ ПРИ ЧИТАЊЕ НА Е-МАИЛОВИ И ОТВАРАЊЕ ФАЈЛОВИ

Секојдневно барем по еднаш поголемиот дел од светската популација користи е-маил адреса, а всушност тоа е и еден од полесните начини на сајбер криминалците да дојдат до посакуваната цел, односно да дојдат до лични информации на самите корисници или пак да пренесат вирус. За да би се заштитиле од ваков напад, препорачливо е при добивањето маил, дали би требале да го отвориме доколку содржината на насловот ни е непозната, а исто така и фајловите добиени преку е-маил би било најдобро да се направи скенирање на истите пред да бидат отворени.

1.4. КОРИСТЕТЕ ОГНЕН ЗИД (FIREWALL)

Најдобра заштита од тројанците е Firewall (мак.огнен ѕид). Вистинската улога на Firewall-от е да го надгледува „сообраќајот“ што излегува од компјутерот. За бебзеден компјутер со пристап на интернет и кој ќе поседува програм кој ќе го мониторира целиот сообраќај што понминал преку модемот или линк и програма која ќе ги надгледува сите портови и која нема да дозволи сомнителните програми или хакерите да воспостават конекција е потребно користењето на Firewall. Заштита од рушење на оперативниот систем и заштита од Back Door најдобро се постигнува со Firewall.[74]

Ако некој се обиде недозволено да пристапи на одреден компјутер (со цел блокирање или рушење на оперативниот систем) или некој програм на кој не му е дадена привилегија да пристапи на интернет и се обиде да воспостави конекција на некој порт, Firewall – от во истиот момент ќе го блокира сомнителниот порт и ќе го постави прашање до корисникот дали ја дозволува конекцијата, што значи дека Firewall-от не дозволува влез и излез од компјутерот без дозвола на корисникот. Како заклучок може да се нагласи дека дека моментално е многу тешко да се заобиколи Firewall-от така да не постои програма која ќе успее да пристапи на интернет со заобиколување на Firewall-от. Тој е непробивен дури и за вештите хакери, па од таа причина истиот се користи на сите системи за кои е потребно многу високо ниво безбедност.

[74] Види повеќе на https://www.it.mk/osnovni-soveti-za-zashtita-od-sajber-kr/ - преземено на ден 05.09.2020

1.5. КОРИСТЕТЕ ДОБРИ ЛОЗИНКИ

Најпрвиот и наједноставниот начин за спречување на компјутерскиот криминал е користењето на добра лозинка, која ќе биде доволна силна со што би ја знаеле само лицето кое ќе ја користи. Како најдобри лозинки се сметаат мешавина од букви, бројки и симболи и за секоја програма е најдобро да се користат повеќе лозинки, не само една.

1.6. ВНИМАТЕЛНОСТ ПРИ ИНСТАЛИРАЊЕ ИЛИ ПРЕЗЕМАЊЕ ПРОГРАМИ

Преземањето на програми, музика, филмови и друго е секојдневие на лицата кои користат интернет. Но, во дел од случаевите, посакуваниот фајл не е според очекуваното, туку е вирус кој само го користи неговото име, со што со самото стартување на програмата, во компјутерскиот систем се внесува и вирусот.

1.7. ПОСТАВУВАЊЕ И КОРИСТЕЊЕ НА ЛОЗИНКА ЗА ВЛЕЗ ВО ДАТОТЕКИ.

Датотеките кој ги користиме во компјутерските системи, е најдобро да бидат осигурани со лозинка, која ќе биде силна, со што се зголемува безбедноста и на самиот систем, затоа што сајбер криминалците ќе подлежат на потешкотии при влез во таквите датотеки, доколку постојат лозинки.

ЗАКЛУЧОК

Навременото и координирано спроведување на стратегиите и мерките за заштита од комјутерски криминал можат да ги спречат измамите кои се се почести во интернет пространството, истовремено да ги намалат штетите од неговото влијание врз општеството во целина. Борбата против компјутерскиот криминал е еден од новите и најинтересните предизвици со кои се соочува човештвото, секој од нас како корисник на информатичките технологии е потенцијална жртва на овие измами. Безбедноста е клучна алка на секое едно општество и заедница.

Дигиталната ера во која живееме заедно со големите предности што ги ужива секој еден од нас во секојдневниот живот во исполнувањето на своите професионални должности на своето работно место, преку различните онлајн обуки кои се нудат, комуникација со секој дел од светот, електронското банкарство, онлајн трговијата и т.н не исправа и пред големи предизвици за приватноста, безбедноста и нашите човекови права. Последиците од овие предизвици може да влијаат не само на поединци туку и на групи на луѓе, нации, земји и целиот свет. Во овој контекст, меѓународната политика за безбедност на сајбер просторот станува суштински дел од процесот на глобализација.

Денес интернетот е една од најважните инфраструктури во светот и нејзиниот обем и темпото на развој отвора неограничени пристапи за модернизација на секојдневниот живот. Во исто време, интернетот е сè повеќе средина во која изврши високо-технолошки криминал и злосторства, вознемирување преку социјални мрежи, интернет сексуална експлоатација на деца, измама во плаќање, групи во различни социјални мрежи и апликации за комуникациа преку кои џихадистите и терористите ги регрутираат своите приврзаници и борци, и истовремено спроведуваат пропаганда. Терористичката пропаганда се шири од една страна на светот до друга , во рамките од локални мрежни заедници па се до глобални мрежи или така наречени платформи како што се Твитер, Фејсбук и Тумблр, каде терористите можат на многу лесен начин да најдат повеќе луѓе за исполнување на нивните цели. Развојот на нови информативни технологии значително се промени и секојдневно сме соочени и исправени пред нови видови на криминал кои се разликуваат од традиционалните кои зад себе кријат голема опасност за јавноста. Овие нови современи видови на криминал сериозно ги загрозуваат човечките права, национална и меѓународна безбедност.

Од целокупното истражување на оваа тема за компјутерскиот криминал доваѓаме до сознание дека за повеќето од овие нелегални активности нема соодветно законодавство и во многу аспекти технолошкиот развојот продолжува да ја надминува еволуцијата на меѓународното право и националните законодавства. Парадоксалниот аспект на информативно-технолошките достигнувања е фактот што од една страна овозможува и дава огромен простор за уживање на човекови права и слободи, но во исто време истите тие ги прави се поранливи од кога и да е. Во ова време во кое живееме на дигитална ера со целото наше опкружување за комуникација, нашата приватност и безбедност и заштита на лични податоци е ставена на тест. Суштински се и ризиците за ограничувања на човековите права од страна на одлуки на одредни влади на држави низ светот , каде под најразлични изговори може да се бара со цел обезбедување сигурност и заштита на граѓаните на тие држави да се воведат цензури, забрани, нелегитимен притисок врз граѓаните каков што и беше примерот за забраната на турската влада за пристап до Твитер во март 2014 година, одлука која предизвика Антивладини демонстрации.

Брзиот развој на Интернет и новите технологии, а со нив и измамите и злосторствата кои произлегуваат од нив отвара простор од апсолутно широк спектар на национални, меѓународни организации, институции и поедици да се вклучат во формирањето на политики и одлуки со цел безбедност на граѓаните од компјутерски криминал. Сите тие активности и напори како и до сега мора и треба да бидат интегрирани во повеќе унифицирани активности. Плеадата на различни конвенции и инструменти на Обединетитие нации и Европската Унија претставувааат стабилна основа, основа врз која треба да се засноваат меѓународните политики и соработка на сите држави. Сите овие соработки треба постојано да се ажурираат со цел поефикасно да се спротивставиме на сајбер предизвиците на различни нивоа. Повеќе од потребни се соработки помеѓу јавниот, приватиот и граѓанскиот сектор односно се почестите иницијативи на граѓанското општество. За справување со компјутерскиот криминал се потребни заеднички напори на сите институции и организации на национално и меѓународно ниво се со цел подобрување на создадените правни средства и механизми. Динамиката со кои се развиваат информатичките технологии побарува и динамичен и одржлив развој на законодавниот пристап во нашата држава.

Овој нов вид на криминал, кој е распространет насекаде низ светот и се бројат илјадници случаи дневно, не ја одмина и нашата држава. Статистичките податоци кој

беа прикажани табеларно во овој магистерски труд, всушност ја потврдуваат и присутноста на компјутерскиот криминал на територија на Република Северна Македонија во последните 2 децении.

Поради тоа, сплотеноста помеѓу државите во светот треба да се преточи во меѓународна соработка во која ќе имаат цел за намалување на негативниот тренд со компјутерскиот криминал. Конвенциите и дополнителните протоколи кој ги имаат ратификувано повеќе земји од светот, како и членството Интерпол и Европол се показател за упорноста на многу светски земји во спречувањето за извршување како и проширување на кривичните дела поврзани со компјутерски криминал.

Евиденцијата извршена од страна на Министерството за внатрешни работи и Државниот завод за статистика на РСМ, го покажуваат усовршувањето на компјутерскиот криминал на територија на нашата држава. Пред 2 децении, речиси и да нема сторено кривично дело поврзано со компјутерски криминал, но веќе претходната година броевите на евидентирани кривични дела во рок од една година се четири цифрени. Од година во година, бројките покажуваат се поголем пораст на застапеноста на компјутерскиот криминал на територија на РСМ.

Областите како што се економија, политика, комуникации, финансиски систем итн. ќе бидат уште позависни од функционирањето преку компјутерски мрежи и интернет.

Сите изводи од истражувањата водат до тоа дека паралелно со таа потребата ќе се зголемуваат на сајбер заканите и нападите. Сајбер предизвиците ќе продолжат да ги надминуваат националните граници и поради што неизбежно безбедноста на сајбер-просторот станува и всушност е глобален проблем што треба да се реши на глобално ниво.

КОРИСТЕНА ЛИТЕРАТУРА

УЧЕБНИЦИ И МОНОГРАФИИ

1. Ачкоски, Ј. Сигурноста на компјутерските системи, компјутерски криминал и компјутерски тероризам, Скопје,2012 година.
2. Ачкоски, Ј, Дојчиновски, М. Сајбер криминал и заштита на дигиталните податоци во компјутерските мрежи.
3. Aleksić, Z., Škulić, M., Kriminalistika, Beograd, 2007
4. Бановић Б., Обезбеђење доказа у криминалистичкој обради кривичних дела привредног криминала, Полицијска академија, Земун, 2002, стр. 136
5. Боцевски, Д., Советување за сајбер криминал – Компјутерски инциденти и истражување на компјутерски криминал во Република Македонија
6. Видојковиќ, М. Компјутерски криминалитет- магистерски труд, Ниш, 2015 година.
7. Габеров,М. Феноменологија на сајбер криминалитетот,2015 година.
8. Габеров, М. Правото на приватност и сајбер просторт,2015 година.
9. Димовски,Д. Компјутерски криминалитет
10. .Drakulić, M., Osnovi kompjuterskog prava, Beograd, 1996. God
11. Drakulić, M., Drakulić, R., CYBER KRIMINAL, , Fakultet organizacionih nauka u Beogradu
12. Јовашевиќ Д. , Лексикон кривичног права, ЈП Службени лист СРЈ, Београд, 2002
13. Jaishankar K. Cyber Criminology: Evolving a novel discipline with a new journal. International Journal of Cyber Criminology, Vol 1 , Issue 1 January 2007
14. Камбовски В., Организиран криминал, Скопје, 2005
15. Калач, Ј. Сајбер тероризмот како закана кон безбедноста на државата,2017 година.
16. Kulic M., Danilovic N., Milosevic Z., Dedic S., Gmajnic R., Kambovski V., Golik J., Hadzigrahic N., Komissarov V., Nogo S., Vuckovic B., Sinanovic F., Tanovic I., Stanovic N. - Pravo I izazovi XXI veka – Zbornik radova sa I medjunarodnog naucnog skupa - Brcko 2013
17. Милошески, В. Компјутерски криминал-предизвици и новини во македонското материјално законодавство,
18. Милошески,В,Зврлевски,М,Андонова,С. Прирачник за компјутерски криминал, 2014 година.

19. Наумовски Г., Докмановиќ М., Право и информатичка технологија, Скопје, март, 2009.
20. Николоска,С. Методика на истражување компјутерски криминалитет,Скопје, 2013 година.
21. Николоска,С. Појавни облици и форми на компјутерски криминал во банкарското работење и кривично правна заштита во Република Македонија.
22. Nikolic-Ristanovic V., Konstantinovic-Vilic S., - Kriminologija, Beograd, 2018
23. Spasić V., Aktuelna pitanja u oblasti sajber kriminala (ĉlanak), Bilten sudske prakse Vrhovnog suda Republike Srbije broj. 1/2006, Beograd, str.107.
24. Тупанчевски, Н. „Компјутерски криминалитет“, Годишник на правниот факултет, Скопје, 1991.
25. Сулејманов З. ,Криминологија, Скопје, 2003, стр. 631
26. Chiesa R. ,Ducci S., Ciappi S. - Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking, Boca Raton FL, United States, 2008, str.43-44
27. Šarkić N., Prlja D., Damnjanović K., Marić V., Ţivković V, Vodinelić V., Mrvić-Petrović N.: Pravo informacionih tehnologija, Beograd, 2011, str.3.

НОРМАТИВНИ АКТИ

28. Кривичен законик на Република Македонија („Службен весник на Република Северна Македонија” број 199/14)
29. Закон за криивчна постапка (Службен весник на Р. Македонија број. 15/97, 44/2002, 74/2004, 18/99, 27/2004, 15/2005,)
30. Европска конвенција за сајбер криминал, Будимпешта, 2001 година.
31. Дополнителен протокол на Конвенцијата за сајбер криминал за инкриминација на дела од расистички, ксенофобички вид по пат на информатички системи-Стразбур, 2003 година.

ВЕБ СТРАНИ

32. https://www.computerweekly.com/news/4500248925/Police-arrest-130-in-global-anti-cyber-fraud-operation
33. https://www.internetworldstats.com/stats.htm
34. https:// www.visualcapitalist.com/30-year-timeline-world-wide-web/
35. https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en
36. http://www.catb.org/jargon/html/ dana 09.08.2015.godine
37. https://www.cs.berkeley.edu/~bh/hackers.html dana 09.08.2015. godine
38. https://www.pravdiko.mk/krivichna-prijava-za-kompjuterska-izmama/
39. https://lider.com.mk/hronika/uapsen-skopjanec-za-kompjuterska-izmama/ 22.11.2018
40. https://mvr.gov.mk/vest/233
41. https://mvr.gov.mk/vest/7693
42. https://mvr.gov.mk/vest/2459
43. https://sitel.com.mk/internet-izmama-ne-e-poznat-brojot-na-makedonci-koi-kupile-avio-bileti-za-1-dolar-od-lazhen-sajt 20.06.2018
44. https://mvr.gov.mk/vest/4203
45. https://mvr.gov.mk/vest/11018
46. https://www.fbi.gov/news/stories/a-byte-out-of-history-10-million-hack
47. https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/
48. https://mvr.gov.mk/analiza/kriminal/19
49. https://mup.gov.hr/UserDocsImages/statistika/2018/Statisticki%20pregled%20temeljnih%20sigurnosnih%20pokazatelja%20i%20rezultata%20rada%20u%202018.%20godini.pdf?fbclid=IwAR1MV9CTRgNvURIXAqfw0yyFnJW_v4Yq72qOOAr3OUc9inLbzd8ATDWJt9s
50. http://www.stat.gov.mk/OblastOpsto.aspx?id=27
51. https://www.netlaw.bg/bg/a/kiber-sigurnost?fbclid=IwAR3fujctiViBvPT9TYNfiEx6mfWAZljJ072OZlyMqPk_cJPZzRjpxLWHgjg
52. http://www.mchamber.mk/upload/Documents/Edukacija/Sovetuvanje%20za%20sajber%20kriminal%20-%20%D0%9A%D0%BE%D0%BC%D0%BF%D1%98%D1%83%D1%82%D0%B5

%D1%80%D1%81%D0%BA%D0%B8%20%D0%B8%D0%BD%D1%86%D0%B8%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%20%D0%B8%20%D0%B8%D1%81%D1%82%D1%80%D0%B0%D0%B6%D1%83%D0%B2%D0%B0%D1%9A%D0%B5%20%D0%BD%D0%B0%20%D0%BA%D0%BE%D0%BC%D0%BF%D1%98%D1%83%D1%82%D0%B5%D1%80%D1%81%D0%BA%D0%B8%20%D0%BA%D1%80%D0%B8%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB.pdf?fbclid=IwAR3zv9QVxzpV6xk9kBTxUJXj1Uuw2DI8Rwr1R6-VoVI2OlvSgCABgmSiamY

53. http://arhiva.mvr.gov.mk/ShowAnnouncements.aspx?ItemID=7343&mid=734&tabId=65&tabindex=0
54. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf?fbclid=IwAR1TEqED_Z_vVT133_5d-Jd_7ToqHCv1txMtOiwnLd6f5B-vHebIh4ALx_Y
55. http://www.stat.gov.mk/Publikacii/2.4.16.08Kor.pdf
56. http://www.stat.gov.mk/Publikacii/2.4.17.09.pdf
57. http://www.stat.gov.mk/Publikacii/2.4.18.07.pdf