Универзитет „Св.Кирил и Методиј“

Филозофски факултет

Институт за безбедност, одбрана и мир

Последипломски студии од областа на безбедноста

Компјутерскиот криминал и неговите импликации врз безбедноста во современиот свет – со посебен осврт на Република Македонија

- Магистерски труд -

Ментор:

Проф.д-р Митко Котовчевски

Изработил:

Емилија Милковска

Скопје, 2012 година.

Содржина:

1. Вовед

Човештвото и светот воопшто, секојдневно се изложени на голем број закани и ризици од кои најчести и најопасни се: организираниот криминал во сите негови облици и видови, тероризмот, регионалните конфликти, распаѓање на државите, како и пролиферацијата на оружјето за масовно уништување (биолошко, хемиско, нуклеарно).

Исто така, сведоци сме дека денешниот свет не може да опстојува и нормално да функционира ако нема изграден информациски и комуникациски систем .Неможе да се замисли секојдневното функционирање на било кој дел од општественото живеење без употреба на компјутер и компјутерска технологија.

Заканите на овие системи се и потенцијални закани за современиот свет, закани за уништување на сите општествени вредности, за ограничување на човековите основни слободи и права, за нанесување огромни штети во секој поглед.

Во овој труд ќе се обидам да ги наведам карактеристиките на компјутерскиот криминал, колку е овој вид на криминал деструктивен за општеството, а исто така ќе бидат наведени и некои од начините за заштита од овој вид на криминал, иако е многу тешко тој да се предвиди, па и да се спречи. Исто така, ќе бидат наброени и неколку карактеристични примери на компјутерски криминал во светски рамки, но и примери со кои се соочила Република Македонија.

Информатичката технологија денес допира до секој аспект на животот, без разлика на локацијата на светот. Распространувањето на информатичката технологија во светот сепак има и негативни страни: ја отвора вратата на антисоцијалното и криминално однесување на начин кој досега бил невозможен.Отвара можности да се влезе во сечиј дом, во секоја компанија, без притоа дирекно да се тропне на врата, без да се најави доаѓањето, дури и да не се забележи присуството.

Компјутерските системи нудат и нови високо софистицирани можности за кршење на законот и креираат потенцијал за извршување на традиционални типови на криминал на нетрадиционални начини. И покрај економските консеквенци од

компјутерскиот криминал, општеството се потпира на компјутерски системи за сите области на секојдневното опстојување и функционирање.

Со оглед на тоа дека на Интернет се поврзани преку 200 земји, компјутерскиот криминал станува глобален проблем кој бара големо учество и соработка меѓу општествениот и приватниот сектор во сите земји, вклучувајќи ги и земјите во развој.

Главна компонента на информационата и структурната безбедност е способноста на нацијата да спречи, открие, истражи или судски да гони криминални активности во врска со компјутерите и компјутерската технологија.

Слабостите во било која од овие области, може да предизвикаат загрозување на безбедноста не само во одредена земја, туку и ширум целиот свет. Било да е во облик на хакинг, економска шпионажа, уништување на веб станици, саботирање податоци или други дела против компјутери, мрежи и податоци, компјутерскиот криминал дејствува врз граѓаните, претпријатијата и државите.

Ерата на компјутерскиот тероризам или популарно наречен ***ciber terrorism,*** *допрва доаѓа.Со забрзаниот развој на технологијата се повеќе ќе се користат методите и техниките на ваквиот вид тероризам за да се нанесуваат штети на поединци, групи, организации па и на држави. Значи, компјутерскиот тероризам беше присутен во минатото, е присутен во сегашноста, но ќе биде многу по присутен и поопасен во иднината.*

Република Македонија е во фаза на компјутеризација на државните служби и постепено поврзување во една единствена мрежа на информации. За тоа постојат многу примери, како што се: компјутеризација на Управата за јавни приходи, Македонски телекомуникации, Фонд за пензиско и здравствено осигурување, банки, министерствата и други, при што сето ова поврзување е интерно, само за сопствени потреби, без пристап за други корисници кои сакаат да дознаат било какви информации за овие служби.

Откако оваа компјутеризација ќе биде завршена во целост, ќе следува поврзување на сите органи во еден единствен систем, за да се скрати времето и да се поедностави пристапот до одредени информации и вадењето на потребни документи. Исто така, од многу голема важност е и поврзувањето на судовите, со што нивната соработка ќе биде на повисоко ниво. Во фаза на изработка е архива во која ќе бидат сместени сите предмети,

кои ќе бидат достапни за јавноста и кои ќе може да се користат во расветлување на голем број случаи.

Во тек е компјутеризацијата во здравството, а завршени е компјутеризацијата во Министерството за внатрешни работи, во финансиите, економијата итн. Многу важно за целокупниот компјутерски развој на една земја е употребата на компјутерите во домаќинствата и тоа да бидат опфатени сите возрасни групи.

Како илустрација и заради појасно разбирање на поимот компјутерски криминал ќе ги разгледаме и анализираме анкетите на Државниот завод за статистика на Република Македонија, спроведени во 2007 година, 2008, 2009, 2010 и 2011 година, на територија на целата држава.

Соработката меѓу приватниот и јавниот сектор е од голема важност за сузбивање на последиците од компјутерскиот криминал, исто така од голема важност е да се продлабочи соработката на меѓународен план, да се разгледаат различните искуства и да се помогне во различните кривични дела предизвикани со помош на компјутер и компјутерска технологија.

2. Терминолошко определување на безбедноста и компјутерскиот криминал и извори на загрозување на безбедноста

Безбедноста како поим, односно нејзиното толкување е многу сложено и комплексно, поради што доаѓа до појава на различни мислења и толкувања на овој поим. За попрецизно терминолошки да го определиме поимот безбедност мора да наведеме дека тој како поим има повеќе значења, односно под овој поим се подразбира определена состојба, организација, функција, систем или комбинација од сите претходно наведени наведени поими.

Глобалната безбедност, подразбира мошне широко подрачје за истражување, кое е тешко прецизно да се дефинира.

Таа претставува безбедност детерминирана од глобалните интереси и глобалните закани, која ја опфаќа индивидуалната, националната и регионалната безбедност помеѓу кои постои идеалполитичка и/или реалполитичка врска помеѓу секторите (политичко – правен, воен, економски, социјален или еколошки), чија суштина е меѓусебно корегирање, контролирање и моделирање со цел постигнување на мирот и безбедноста на планетата и луѓето.

Компјутерскиот криминал се однесува на компјутерски системи во сите области во животот, од воздушна, железничка, автобуска контрола, до координација на медицински сервиси и национална безбедност. Само мала грешка во работењето на овие системи може да предизвика огромни штети за општеството во целина, па дури и по цена на човечки животи.

Интернетот е многу ранлив поради огромниот број на корисници, отвореноста и слободниот пристап, нерегуларноста, е идеално место за развој на криминалот од секаков вид, затоа што контролата е на ниско ниво или воопшто неможе да се спроведе.

Безбедноста на граѓаните, државите и на општествата во современиот свет, се почесто ќе биде загрозувана од криминални дејства чие остварување е поврзано со компјутер и компјутерска технологија.

Во денешно време, ниту една област од секојдневното функционирање и опстојување не може да се замисли без компјутерска активност и поврзаност во мрежа или во цел систем и меѓусебно соработување и размену̀вање информации и податоци. Тенденциите за во

иднина се уште поголема и покомплексна компјутеризација на општеството во целина, меѓу сите институции и организации. Токму поради ваквата меѓузависност и поврзаност меѓу сите институции и организации, истите ги прави уште поранливи и поосетливи на компјутерски криминални дејства.

2.1. Терминолошко определување на безбедноста и на компјутерскиот криминал

Новиот милениум започна со непредвиден економски развој, чиј темел е Интернетот, како и порастот и ефикасноста на продуктивноста како резултат на напредокот на дигиталната технологија кои ја сочинуваат " информатичката револуција".

Оваа револуција, заедно со брзо променливата природа на информатичката технологија, засекогаш го промени начинот на кој организациите ја извршуваат својата работа. [1]

Секој човек се потпира на клучните делови на инфраструктурата, како што се мрежите на електрична струја, железнички патишта, авионски линии, нафта, гас, банкарски и финансиски системи и мрежи на комуникации. Сите овие делови на инфраструктурата зависат од информатичката технологија и глобалните, меѓусебно поврзани мрежи. Затоа компјутерската безбедност е одговорност на секој, почнувајќи од поединците до компјутерските мрежи на големите компании и државни установи.

Во овој труд подетално ќе го разгледаме компјутерскиот криминал како современа и моќне опасна појава, но за негово детално разгледување мораме првин да посветиме внимание на безбедноста, да ја дефинираме како поим и потоа да го објасниме влијанието на компјутерскиот криминал врз неа и тоа на глобално ниво, но и влијанието врз безбедноста во Република Македонија.

Безбедноста[2] како феномен, односно нејзиното толкување е многу сложено и комплексно поради што доаѓа до појава на различни мислења и толкувања на поимот

[1] „ Medjunarodni vodic za borbu protiv kompjuterskog kriminala", Amerikanska advokatska komora, 2003, str.216.

[2] „Национална безбедност" (прв дел), М. Котовчевски, Македонска Цивилизација, 2000, Скопје, стр.17.

безбедност. За попрецизно терминолошки да го определиме поимот безбедност мора да наведеме дека тој како поим има повеќе значења, односно под овој поим се подразбира определена состојба, организација, функција, систем или комбинација од сите наведени поими.

Дефинирањето[3] на овој поим зависи од теоретските стојалишта на авторите, првенствено од агол на набљудување на одредена проблематика. Важно е да потенцираме дека разликите произлегуваат од тоа дали поимот безбедност е во корелација со заштитната функција на државата, дали поимот безбедност е поврзан за определени работни активности, од политичките стојалишта и слично.

Системот на безбедност како функција во една држава може да биде различно организиран, односно во оваа област разликуваме три основни функции:

1. Систем за безбедност заснован врз чисто воени принципи за заштита и типично милитантни облици на воена организација.

2. Систем за безбедност како вид на класична државна заштита.

3. Систем за безбедност како облик на координација на државниот, односно општествениот механизам на заштита.

Универзалните видови на системот за безбедност во современото општество се познати како: државна, јавна и воена безбедност.

Безбедноста како состојба претставува заштитеност на некое материјално или културно добро, вредност или придобивки на општеството.

Во политичко – безбедносна смисла, безбедноста ја опфаќа целокупната заштитеност на државата од сите видови на непријателски, субверзивни дејства, од носителите на внатрешните и надворешните извори на загрозување и на другите штетни влијанија и загрозувања.

Со оглед на ризиците и опасностите – носителите на внатрешни и надворешни извори на загрозување – безбедноста може да биде внатрешна и надворешна.

Надворешната[4] безбедност во суштина се однесува на заштитата на независноста, суверенитетот на земјата и територијалната целокупност.

[3] „Поим за глобална безбедност“, Питер Хју, Табернакул, 2009, Скопје, стр.2.
[4] „Поим за глобална безбедност“, Питер Хју, Табернакул, 2009, Скопје стр.4.

Внатрешната безбедност се однесува на непречено функционирање на конкретниот уставен поредок, односно на функционирањето на општествено – економскиот систем на државата, како и заштитеноста на другите вредности и добра и објекти за заштита.

Во реализацијата на безбедноста како состојба, организацијата и функцијата во обезбедувањето на внатрешната и надворешната заштитеност на државата и општеството, паралелно учествуваат државната и јавната организација на воените сили, воената безбедност, односно севкупната национална безбедност на земјата.

Безбедноста, во политичко – правна смисла ги опфаќа мерките и активностите на зачувување и заштита од сите видови на загрозување на независноста и територијалната целокупност на една земја и заштита на внатрешниот државен и правен поредок.

Функцијата на безбедноста во современите држави е посложена и претставува мошне сложена функција која во голема мерка се разликува од дејностите на органите на безбедност.

Поимот безбедност, опфаќа цела низа различни аспекти на човековото постоење и делување во општеството, но и во природата. Воспоставувањето на состојбата на безбедност ги опфаќа сите оние појавни облици на општествениот живот кои се вбројуваат меѓу општествените вредности.

Безбедноста може да се третира како состојба во која е осигуран урамнотежениот физички, духовен, душевен и материјален опстанок на поединецот и на општествената заедница во односот кон другите поединци, општествени заедници и природата. Безбедноста во суштина претставува иманентен структурен дел на општеството кој во себе вклучува определена состојба, односно определени особини на состојбата, а исто така и дејност, односно систем. Безбедноста се однесува и на општеството, односно на државата во целина, т.е. национална безбедност, а исто така и на меѓународната заедница.

Дефиницијата на Организацијата на Обединетите Нации [5]од 1985 година, во која е дефинирана безбедноста, гласи: „безбедноста е состојба во која државите сметаат дека нема опасност од воен напад, политички принуди или економски присили, така што можат слободно да се развиваат“.

[5] „Национална безбедност“ (прв дел), М.Котовчевски, Македонска цивилизација, 2000, Скопје,стр.38.

Терминолошкото определување на поимот безбедност е неопходно, бидејќи тоа е потребно за успешно функционирање на современите држави. Во современите општества, безбедноста е неопходен предуслов за остварување на сите витални општествени функции.

Глобалната безбедност подразбира мошне широко подрачје кое е тешко прецизно да се дефинира. Таа претставува безбедност детерминирана од глобалните интереси и глобалните закани, која ја опфаќа индивидуалната, националната и регионалната безбедност помеѓу кои постои идеалполитичка и/или реалполитичка врска помеѓу секторите (политичко – правен, воен, економски, социјален или еколошки), чија суштина е меѓусебно корегирање, контролирање и моделирање со цел постигнување на мирот и безбедноста на планетата и луѓето.

Системот за глобална безбедност претставува процес и потреба на актерите на глобалната безбедност (човек, држава, мега – држава, владини и невладини организации, глобални сојузи), преку функционалистичкиот пристап и глобалното управување да си понуди адекватен одговор на предизвиците на глобалните закани и глобалните интереси.

Се соочуваме со револуционерен период во областа на безбедноста која се почесто се загрозува со помош на средствата за комуникација и со средствата за информирање. Интернетот е средство кое се користи за глобално комуницирање, средство кое не знае за граници.

Може да се претпостави дека компјутерски базираната комуникација претставува најмоќно средство кое води кон светска глобализација, а тоа значи напуштање на мрежната експанзија од централно контролирани транснационални корпорации и движење кон ново политичко и ново социјално живеење.

Во иднина, војните нема да ги водат големи армии, туку организирани групи, кои денес ги нарекуваеме терористи, герилци, бандити, ограбувачи, но кои несомнено ќе присвојат поформални титули за да се опишат себеси.[6] Нивните организации најчесто се втемелени врз харизматични, наместо врз институционални линии и помалку се мотивирани од „професионализам“, а повеќе од фанатична, идеолошка лојалност. Нема да се користи ниту класичното оружје кое се користеше во досегашните војни, односно главното оружје ќе бидат компјутерите и компјутерската технологија.

[6] „Трансформација на војната“, Мартин Ван Кревелд, Табернакул, 2009, Скопје, стр.209.

Информатичката технологија денес допира до секој аспект на животот, без разлика на локацијата на светот. Распространувањето на информатичката технологија во светот сепак има и негативни страни: ја отвора вратата на антисоцијалното и криминално однесување на начин кој досега бил невозможен.

Компјутерските системи нудат и нови високо софистицирани можности за кршење на законот и креираат потенцијал за извршување на традиционални типови на криминал на нетрадиционални начини. И покрај економските консеквенци од компјутерскиот криминал, општеството се потпира на компјутерски системи за сите области на секојдневното опстојување и функционирање.

Новата технологија ќе игра огромна улога во иднината на војната. Наместо да се користат огромни машини, како што се тенкови, топови, авиони ќе се користат се помали направи, а за разлика од претходните многу побрзи и поефикасни.[7]

Веќе наголемо се користат идентификационите картички, за влез и излез од објекти, за користење на банкомати, исто така може да бидат користени за следење на нивните корисници. Исто така, во тек е и натпреварот меѓу уредите за попречување и прислушување. Сите овие, но и уште огромен број современи технички средства полека стануваат дел од секојдневието на секој човек, без разлика на кој дел од планетата се наоѓа.

Информатичката војна, е широко призната како војна која ќе има улога во следниот конфликт или војна, а дури и тогаш на национално – државните војски ќе им биде екстремно тешко целосно да ги сфатат уривачките импликации кои Интернет војната ќе ги има врз нивните хиерархиски организациски структури и западното водење на војните.

Силите кои би биле дел од ваков вид војување, ќе ги наречеме „сајбер“ или буквално како, „борци надвор од просторот“.[8]

Компјутерскиот криминал, се однесува на компјутерски системи во сите области во животот, од воздушна, железничка, автобуска контрола, до координација на медицински сервиси и национална безбедност. Само мала грешка во работењето на овие системи може да предизвика огромни штети за општеството во целина, па дури и по цена на човечки животи.

Интернетот е многу ранлив поради огромниот број на корисници, отвореноста и слободниот пристап, нерегуларноста, е идеално место за развој на криминалот од секаков вид, затоа што контролата е на ниско ниво или воопшто неможе да се спроведе.

---

[7] „Трансформација на војната“, Мартин Ван Кревелд, Табернакул, 2009, Скопје, стр.214.
[8] „ Не-државни закани и идни војни“, Роберт Џ. Бункер, Нампрес, 2009, Скопје, стр.97.

Криминалот врзан за компјутерска мрежа (Crime related to computer networks),[9] од Десеттиот Конгрес на Обединетите Нации, посветен на превенцијата од криминал и третманот на сторителите од април 2000 година, работната група експерти, која го сочинувала овој Конгрес, под ***компјутерски криминалитет*** подразбира, криминал кој се однесува на било кој облик на криминал кој може да се извршува со компјутерски системи и мрежи, во компјутерски системи и мрежи или против компјутерски системи и мрежи.

Тоа е всушност криминал во електронското опкружување.

Ако под ***компјутерски систем*** се подразбира „секој уред или група уреди кои се меѓусебно поврзани со кои се врши автоматска обработка на податоци", како што е дефинирано во Конвенцијата за компјутерскиот криминал (Convention on Cybercrime) на Советот на Европа.[10]

Терминот компјутерски криминал е мета на дефинирање на многу институции во светот. Така, на пример, според ФБИ [11](Federal Bureau of Investigation) во компјутерски криминал спаѓаат:

1. Нелегални влегувања во мрежите на телефонски компании;
2. Нелегални влегувања во поголеми мрежи на видни компании;
3. Загрозување на интегритетот на компјутерските мрежи;
4. Загрозување на приватноста;
5. Индустриска шпионажа;
6. Пиратски компјутерски софтвер;
7. и било какво криминално дејство, каде компјутерот е главен фактор за криминален престап.

Освен овие дејствија, во компјутерски криминал спаѓаат и многу криминални дејствија како што се: кражби, измами и сл., но се разбира во овој случај, разликата е тоа што е вклучен и компјутерот како алатка за криминално дејство.

Под компјутерски криминал спаѓаат и вируси, тројански коњи или црви кои се користат за уништување на цели компјутерски системи или за компјутерска шпионажа.

Нелегалното влегување во компјутерски систем или пробивање на компјутерски мрежи, е работа што ја извршуваат т.н. хакери. Нелегалното копирање на софтвер исто така е економски удар со големи последици.

---

[9] " Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders", 2000,www.oun.org.
[10] „Конвенција за компјутерски криминал", април 2000, www.europa.eu.int.
[11] „Најсилно оружје досега", О.Бакрески, Современа македонска одбрана, бр.9, стр.165.

Компјутерската мрежа, односно, информациско комуникациската технологија се појавува во неколку улоги и тоа:

- ***цел на напад*** – се напаѓаат сервиси, функции и содржини кои се наоѓаат во мрежата. Се крадат услуги, податоци или идентитет, се оштетуваат или уништуваат делови или цела мрежа и компјутерски системи. Во секој случај, цел на сторителот, е мрежата во која се уфрлуваат вируси или црви, се упаѓа на сајтови, хакерите вршат разни услуги и сл.

- ***алат*** – компјутерската мрежа како алатка за извршување криминални дела (детска порнографија, злоупотреба на туѓи оригинални трудови, „on – line" продажба на недозволена роба (дрога, човечки органи, бело робје, оружје и сл.).[12]

- ***доказ*** – компјутерска мрежа и информатичко – комуникациската технологија (ICT).

Компјутерскиот, односно сајбер криминалот е таков облик на криминално однесување кај кое сајбер просторот е опкружување, во кое компјутерските мрежи се појавуваат како средство, цел, доказ или опкружување за извршување на кривични дела, на многу поедноставен и побрз начин, без да бидат вклучувани повеќе луѓе и средства.

Под ***сајбер простор*** се подразбира „заедница сочинета од мрежи на компјутери во која елементите од традиционалното општество се наоѓаат во облик на битови и бајти". Овој вид криминал се вбројува во најизразен облик на транснационален криминал против кој ни борбата не може да биде конвенционална. Компјутерскиот криминал е многу специфичен криминал затоа што се одвива во специфичен простор, виртуелен простор, без дирекни контакти, без дирекни напади.

Стратегијата на информатичкото војување (сајбер војување) на повеќето основни нивоа, главно се базира врз одбрана и напад на информациите и информатичките системи.

Денес е прифатен фактот дека информатичката војна е еден од виталните делови на сегашните воени операции и на операциите што ќе се изведуваат во иднина и дека таквите напади можат да претставуваат потенцијална стратешка ранливост за критичната инфраструктура на нациите.

[12] "Cyber-crime and cyber-terrorism. Security Electronic Business Processes" ,Highlights Of The Information Security Solutions Conference, јануари 2004, стр.75.

Постојат огромен број несогласувања во врска со информатичките војни, кои се насочени кон самиот термин и неговото влијание на целокупниот поим за војувањето. Некои групи сметаат дека компјутерите, софтверот и Интернетот се основните подрачја за информатичките операции, дека тие делуваат во ограничен свет. Други пак, сметаат дека можат да се воведат и измама, пропаганда, психолошки операции, електронско војување во објаснувањето на овој поим.

2.2. Современи извори на загрозување на безбедноста во современиот свет – со посебен осврт на Република Македонија

Евидентно е дека меѓународниот поредок порано бил многу поразличен во сите области на општественото дејствување, отколку денес, па од таму и заканите и опасностите биле поразлични од тие во денешно време.

Нерамномерноста во развојот на одделни високоразвиени држави, се манифестирала во вид на се попродлабочен јаз меѓу државите кои го креираат денешниот свет и може да се каже, дека тоа се суштински противречности што го потресуваат современиот свет. Борбата за превласт на одредени територии, борбата за поседување на извори од витално значење доведуваат до големи компликации во меѓународните односи.

Живееме во свет во кој се присутни непредвидливи ризици и опасности по мирот и стабилноста на државите. Се повеќе сме убедени, дека класична воена закана не е можна, но за разлика од неа се повеќе се веројатни асиметричните закони кои се повеќе добиваат во интензитет.[13]

Во поновата историја се среќаваме со се поголем број на закани и опасности за бзбедноста кои се поврзани со социјалните, економските и меѓуетничките прашања, кои би можеле да го исфрлат од колосек нормалното функционирање на државите во светот, а со тоа и на Република Македонија, која како млада и недоволно развиена држава, е многу осетлива на овие полиња.

[13] „Основи на системот на национална безбедност“, Т.Гоцевски, Филозофски факултет, Скопје, 2006, стр.63.

Поради ова мора да истакнеме дека денешните глобални предизвици, можат да се најдат во 4 области:

1. во мирот и сигурната стабилност на државата;
2. во човековите права и хуманитарни прашања;
3. во природните извори и животната средина;
4. економски и социјален развој.

Основните извори на војните во иднина нема да произлегуваат од карактерот на односите меѓу државите, туку од она што ќе се случува во самите држави. Во последно време се повеќе се препознаваат недржавни елементи кои сакаат да ја наметнат својата моќ.

Организираниот криминал во современи услови со сите свои карактеристики и белези, со својата огромна виталност и флексибилност, со огромната финансиска и друга моќ што ја поседува, секако е еден од најсилните центри на моќ во сенка на легалните, националните и меѓународните институции. Во денешни услови се позачестен облик на организираниот криминал е компјутерскиот криминал.

Компјутерскиот криминал е криминал кој се врши со помош на компјутерите и компјутерската технологија. Во современиот свет е незамисливо да се живее без компјутер, тој има огромно влијание врз целокупното функционирање на општеството, па поради тоа се појавуваат се поголем број облици на негова злоупотреба, од најситни грешки во софтверот, до ограбување на банки и терористички напади во кои има и огромен број на жртви.

Покрај организираниот криминал денес се поголем замав зема и тероризмот. Тој има големи цели и настојува да ги оствари по секоја цена. Тероризмот е претставен како организиран облик на борба на определени сили за конкретизирање политички цели.

Најголем проблем на денешницата е што државите немаат изградено ефикасен систем за одбрана и превенција од ваквиот вид напади.

Ако ги анализираме горе наведените елементи, ќе дојдеме до заклучок дека заедничко кај сите нив е тоа што „никој не ги контролира“ и никој не влијае на нивните одлуки, што им го дава приматот на потенцијални закани за современиот свет. Ако кон овие елементи ги додадеме и информациите и комуникациите, тогаш може да кажеме дека полека се оформува сликата за актуелните и потенцијлните закани по безбедноста на државите.

Новите ризици за меѓународниот поредок можат да се манифестираат и во областа на информациите и комуникациите. Новиот светски поредок во информирањето и во комуникациите може повеќе да се дефинира како процес, отколку каков било даден збир на услови и практики.

Посебно ќе биде изразен сајбер криминалот, пиратството и злоупотребата на информатичката технологија, особено во делот на личните податоци на граѓаните, деловната, службената и државната тајна.

Исто така, како еден од современите извори на загрозување на безбедноста во светот, а со тоа и во Република Македонија ќе го споменеме и нуклеарното оружје.

Во овој контекст треба да посочиме, дека заканите доаѓаат до израз, особено во денешниот интегриран и меѓузависен свет, каде секоја закана претставува општ светски проблем кој силно влијае врз развојот, врз мирот и безбедноста во светот, но и врз опстанокот на државите и народите.

Меѓузависноста и интензивната соработка меѓу државите на регионален и глобален план во сите области ќе овозможи просперитет и побогат општествен развој и ќе претставува основна одредница и ориентација на новиот развој.

Остварувањето на овие процеси во меѓународни односи суштествено влијае врз меѓународниот мир и безбедност, а во тие рамки и врз безбедноста на сите држави, па со тоа и на Република Македонија.

Кога станува збор на Република Македонија, и таа не може да биде имуна на ваквиот тип на современи ризици, закани и опасности по безбедноста на државата и за нормалното функционирање на целокупното општество.

За справување со тероризмот и со сите облици на организираниот криминал, Република Македонија ќе треба да ги пренасочи своите капацитети и можности и да вложи поголеми напори кон отстранување на овие глобални закани, што во секој случај ќе биде тешко за остварување.

За да може, Република Македонија, да им се спротивстави на тероризмот и организираниот криминал, таа мора да развие дополнителни капацитети, да изврши реформи во областите што се занимаваат со оваа проблематика и да вложи огромни средства за компјутеризација и современа информатичка технологија за откривање и спречување на дејства од ваков вид.

Република Македонија, мора да вложи огромни средства и труд за да ги следи актуелните и потенцијалните закани кои се појавуваат во современиот свет, за де не биде во ситуација, поради немоќта на државата, да функционира како делотворен систем за распределба и контрола и да доживее неуспех на својот систем.

Брзиот развој на технологијата ја наметнува потребата за прилагодување на целокупниот систем кон новите потреби и новите предизвици, со кои може да се соочи во иднина.

Според поголем број автори, во современи, а воедно и глобални извори за загрозување на безбедноста се вбројуваат: меѓународниот организиран криминал, меѓународниот тероризам, пролиферацијата на оружје за масовно уништување, тирани, еко-закани, верски секти, сиромаштија, глад, хидроцид, ито така и генетскиот инженеринг како современа закана.[14]

Меѓународниот организиран криминал се дефинира, како плански ангажман, посветен на криминални акти, мотивиран од потрагата по профит и борба за власт, кои претставуваат суштински интерес од индивидуална и колективна гледна точка, каде што повеќе од два дела организирано соработуваат во еден сектор на работа, во еден временски период, со ограничено или неограничено трошење.[15]

Големиот напредок на информатичката технологија и нејзината се поширока употреба во општеството отвара нови можности на криминалните групи и создава серија на специфични предизвици пред авторитетите, одговорни за применување на законот. Организираните криминални групи имаат надмоќна улога во фалсификувањето на компјутерски програми. Измамите со кредитни картички се чест облик на компјутерски криминал.

Информатичките пирати стануваат моќни и можат да навлезат во информатичките системи на општествата, организации кои се занимаваат со кредитни картички, со што можат да направат огромни штети. Опасностите од сајбер криминалот се мултиплицираат затоа што алатките за пиратство на Интернет, се се подостапни, со што се отвараат повеќе можности за негово искористување во негативни активности.

---

[14] „Извори на загрозување на мирот и националната безбедност“, М,Котовчевски, Балкански центар за мир, Напредок, Тетово, 1999, стр.47.

[15] „Национална безбедност“ (трет дел), М.Котовчевски, Македонска Цивилизација, Скопје, 2000.стр.34.

Проширувањето на технологијата за шифрирање е во полна експанзија, што им овозможува послободно комуницирање меѓу криминалците и криминалните групи без некој да се посомнева во нивните намери. Во овој контекст ќе го споменеме истражувањето на ФБИ [16] (федерално истражно биро), со кое се укажало на Европската Комисија на ААН, дека тие констатирале спектакуларен пораст на бројот на бесправни влегувања во информатичките системи на индивидуалци, но и на огромни корпорации и многу „напади“ на корисниците, со што им нанесувале огромни штети на материјален и на финансиски план. Тие, исто така опишале една пирамидална шема на Интернет, преку која направиле детален приказ на незаконско користење на Интернетот и неговите можности. Преку 2500 членови во САД биле активирани за да ги поделат приходите (околу 25% годишно) од една нова, т.н. „банка“ односно недозволена трансакција.

Република Македонија, како и сите земји во светот, не е имуна на ваквиот вид напади, се почесто се забележуваат грабежи на банкомати и банки, незаконско користење на телефонски линии и други провајдери, плаќање при купување различни производи во продавници, бензински пумпи, хотели, пробивање на веб страни на компании, владини институции, медиуми и огромен број други примери на кривични дела, извршени со помош на компјутер и компјутерска технологија.

2.3. Потенцијални закани за безбедноста на Република Македонија

Во поновата историја се среќаваме со се поголем број на закани и опасности за безбедноста кои се поврзани со социјални, економски и меѓуетнички прашања, кои би можеле да го исфрлат од колосек, нормалното функционирање на државите во светот, а со тоа и на Република Македонија, која исто така е многу осетлива на овие полиња. Заканите во современиот свет се поделени во повеќе групи, во зависност од нивните карактеристики и облици со кои се појавуваат во општеството.

Закани кои во големи размери ги загрозуваат нормалните услови за живот во целокупното општество се: организираниот криминал, кој завзема се поголеми размери и во

[16] http://www.fbi.com

современи услови многу тешко се разоткрива, тероризмот, исто така е опасна закана за безбедноста на државите во современи услови, а со тоа и безбедноста на Република Македонија.

Мошне опасна закана во современи услови е, и пролиферацијата со оружје за масовно уништување посебно производството на нуклеарно оружје и вршење постојани притисоци и закани дека може да дојде до употреба на таквото оружје. Република Македонија беше сведок на користење на осиромашен ураниум, во нападите на НАТО врз тогашна Југославија.

Како современи закани кои ја засегаат и Република Македонија ќе ги спомнеме и еко-заканите, генетскиот инженеринг, компјутерскиот (сајбер) криминал, како се позастапен облик на организиран криминал.

Како и секоја држава и Република Македонија, поради сплет на историски, географски, економски, етнички, демографски и други настани е предмет на загрозување од различни извори кои со различен интензитет се манифестираат во различно време.[17]

Во рамките на овој труд, посебно важно е дали ќе се користи оружје за одредена закана, каков вид на оружје, во колкава мерка, какви ќе бидат последиците од евентуална употреба на истото.

Зависно од големиот број фактори кои го условуваат нивното манифестирање, изворите на загрозување подлежат на повеќе класификации. Во зависност од потеклото, изворите на загрозување може да се поделат на: општествени, природни и техничко-технолошки извори на загрозување.

Со оглед на тоа што, компјутерскиот криминал е релативно нова појава, мораме да посветиме внимание и на иднината на заканите, односно дали тие ќе ги следат досегашните патишта или ќе се менуваат и доколку се менуваат во која насока ќе одат тие промени. Потребно е да се изврши проценка на силите и средствата на носителите на одредена закана, времето на траење на заканта, дали таа ќе се проширува или ќе се намалува и штетите кои ќе ги претрпи општеството и граѓаните од таков вид на закани.

Заканите во современиот свет најчесто се групираат во две групи и тоа:

- закани од воена природа (закани во кои има директна употреба на огнено оружје),
- закани од невоена природа (нови облици на закани, без директно присуство на конвенционално оружје).

---

[17] „Основи на на систем на национална одбрана“,Т.Гоцевски; Филозофски факултет, Скопје,2006.стр.126.

2.3.1 Закани од воена природа

Закани од воена природа за безбедноста на државите во современиот свет се оние закани во кои има директна употреба на различни видови оружје, без разлика дали станува збор на вооружување на поединци, групи или на цели држави. Покрај конвенционалното оружје, во овој контекст се вбројува и користењето на разни видови на современи оружја, во кои се вбројуваат разните видови на оружје за масовно уништување, биолошко, хемиско и нуклеарно оружје и најразлични облици на економски, политички, еколошки и идеолошки репресалии.

Како најзастапен облик на воена закана е вооружената агресија, која според Резолуцијата на Генералното Собрание на ООН,[18] дефинирана како: „употреба на сили на една држава против суверенитетот, територијалниот интегритет и политичката независност на друга држава, или која на кој било друг начин е неспоива со Повелбата на ОН".

Во зависност од тоа дали заканите ги поминуваат границите на една држава или остануваат ви рамките на таа држава, заканите се поделени во внатрешни и надворешни облици на загрозување на безбедноста.[19]

- Надворешни вооружени облици на загрозување на безбедноста во современиот свет се: вооружена агресија, воена интервенција, погранични воени судири.
- Внатрешни вооружени облици на загрозување на безбедноста се разни облици на граѓански конфликти, вооружена побуна и тероризам.
- Карактеристично е тоа што постојат и огромен број на комбинирани облици на загрозување на безбедноста, без разлика дали се внатрешни или надворешни облици на загрозување на безбедноста. Како надворешни комбинирани облици на загрозување ќе ги наведеме: доктрина на судир со низок идентитет, специјално војување, воени интервенции, селективна примена на различни облици на сила, државен удар. Во групата на внатрешни облици на загрозување, покрај државниот удар, се наоѓаат и голем број од претходно споменатите облици.

---

[18] Резолуција на Генерално Собрание на ООН, 1974 година.

[19] „Национална безбедност на Република Македонија (трет дел)", М.Котовчевски, Македонска Цивилизација, Скопје, 2000, стр. 25.

Република Македонија, поради својата географска положба, не е имуна на разни видови на закани. Таа се наоѓа на простор кој е постојано под одредени закани и надворешни влијанија, заради остварување на најразлични цели. Од сите страни е опколена од соседни земји кои имаат најразлични претензии кон неа и нејзината територија. Интересите на соседните земји се насочени кон територијални сегменти на Република Македонија, како и кон нејзините многубројни природни богатства, кон културата и културните разновидности, идеологијата, религијата, археолошки и историски пронајдоци.

Во Република Македонија, вооружена агресија би се вршела поради завземање на целата или дел од територијата, доколку би дошло до употреба на овој вид воена закана.

Агресија врз Република Македонија, со оглед на целта, може да биде: со радикални цели и со ограничени цели.

Во зависност од видот на војната, агресијата врз Република Македонија, би била: агресија во локална, во регионална и во светска војна.

Потоа, како облик на воена закана ќе ја споменеме и воената интервенција, која претставува облик на недозволено мешање на една или група држави во внатрешните работи на друга држава со употреба на вооружени сили.

Воена интервенција, како облик на воена закана во Република Македонија, би се применила поради територијални аспирации, борба за човекови права, заштита на одделни малцинства и сл. Република Македонија не е имуна и на разновидни облици на терористички дејства, од поголем или помал размер.

Како вооружени закани ќе ги споменеме и пограничните вооружени судири, кои претставуваат посебен вид на вооружени судири помеѓу две или повеќе соседни држави, поради различни нерешени погранични прашања, помеѓу поединци, населби, па дури и цели држави.

Главни карактеристики на овој вид закани се следниве: како причини се појавуваат нерачистени погранични проблеми, територијални претензии на некоја од соседните држави кон територијата на другата држава и обемот и структурата на вооружените сили се ограничени и тоа на доста помал број, а борбените дејства ќе се одвиваат само на одреден дел од територијата.

Во современи услови посебно опасна закана за секоја држава е тероризмот, кој се појавува во различни облици, на различни начини без разлика за која страна од светот станува збор. Тероризмот се вбројува и во вооружени закани, но во поново време се повеќе е комбинирана закана, па дури постојат и голем број на невооружени облици на терористички дејства.

Универзалната и се полесна достапност до сите видови оружја, експлозиви и технолошки софистицирани тајмери и средства за активирање, во голема мера ги зголемуваат можностите и способностите на терористите.[20] Секој може да има пристап до одреден вид на оружје, само доколку пројави желба за тоа. Во современиот свет оружјата се застапени во огромен број и количина, без разлика дали е тоа на легален или нелегален начин.

Глобалната комуникациска револуција претставува уште една цивилизациска придобивка која терористите вешто ја вклопуваат во своите шеми за осигурување на нивните поамбициозни цели.

Зголемувањето на техничките и квалитативните можности, овозможува скоро едновремено и координирано изведување на терористичките напади во повеќе држави, праќање на закани со смрт, но и можност за споредба на листите со терористички цели преку компјутерите и компјутерските мрежи.

Развојот на современата технологија во денешно време, во голема мерка ги комплицира заканите, а со тоа ги комплицира и начините за одбрана и превентивна заштита од ваквите закани, но уште повеќе ги зголемува можностите на терористите за успешно остварување на планираните цели.

Денес, на терористите на располагање им стои огромен арсенал на разновидно оружје, од конвенционалните оружја па се до хемиско, нуклеарно и билолошко оружје. Нивните арсенали може успешно да предизвикаат огромни еколошки катастрофи, пожари, труења, загадувања на системи за вода. За нивната идна промоција тие предвидуваат напади на трговски центри, разурнување брани, насипи, кои би предизвикале големи разурнувања, но и голем број на човечки загуби.

---

[20] „ Национална безбедност на Република Македонија (втор дел)“, М.Котовчевски, Македонска цивилизација, Скопје, 2000, стр. 113.

Со тоа што употребата на сила може да се предизвикаат несакани промени, воените закани традиционално имаат највисок приоритет во однос на национално безбедносните грижи. Карактеристика на воените загрозувања, е тоа што тие се надополнети, или проследени со високо чуство на страв. [21] Тие најчесто се користат за да предизвикаат страв кај населението, а тоа ќе го искористат за остварување на целите заради кои всушност и ги започнале вооружените закани.

Воените загрозувања, претставуваат специјална категорија на закани за националната безбедност, поради самиот факт што вклучуваат употреба на сила. Тие се најопасни закани, предизвикуваат и најголем број на жртви, човечки животи и материјални и финансиски штети.

2.3.2. Закани од невоена природа

Со забрзаниот развој на технологијата и индустријализацијата, заканите од невоена природа се се позачестена појава во современиот свет и завземаат уште поголем замав во сите области на секојдневното живеење, заради остварување на одредени желби и интереси на поединци, групи или држави во целина.

За разлика од заканите од воена природа кои во минатото биле многу честа појава, односно, ни една војна, ниту било какво прашање не се решавало без употреба на оружје, во современиот свет се почесто оружјето се остава на страна и како начин на решавање на проблемите се употребуваат други средства и техники.

Заканите од невоена природа претставуваат закани во кои не се користат класичните оружја, туку различни видови на психолошко – пропагандни дејства, разузнавачки дејства, економски и финансиски криминал и различни видови на криминал предизвикан со користење на компјутер и компјутерска технологија, различни облици на политички репресалии заради остварување на политички цели и интереси на одредена политичка структура или на држава во целина.

[21] „Творење на мирот – Мирот, безбедноста и конфликтите по студената војна“, Л. Георгиева, Виладорф,Скопје, 2004, стр.96.

Заканите од невоена природа, гледани како закани насочени против една држава се поделени на внатрешни невоени закани и надворешни невоени закани за загрозување на безбедноста.

● Како ***надворешни облици*** на загрозување на безбедноста, од невоена природа, ќе ги наведеме: неконвенционалните дејства (разузнавачко – субверзивни, воени, политички, економски и други активности), тоа се дејства кои прикриено или отворено се водат на подрачјето, кое се наоѓа под вистинска контрола или влијание на силите или државите чии интереси се спротивни на интересите на силата која ја води специјалната војна. [22]

Потоа, како невоени закани за безбедноста ќе ги споменеме и субверзивна – пресвртничка дејност, политичката индоктринација, користење и вештачко создавање на општи кризи и психолошко – пропагандни дејства,.

Во оваа група на закани за безбедноста спаѓаат и други закани за безбедноста, како што се и, економските притисоци, технолошките агресии, ембарго - поставувано од други држави, разни видови блокади, потоа забрани за користење на сообраќајната инфраструктура и слични активности.

● ***Внатрешни облици*** на загрозување на безбедноста, од невоена природа, се: разузнавачко – извидувачка дејност, шпионажи, саботажи, диверзии, разурнувачки демонстрации, изразување на граѓанска непослушност, психолошко – пропагандна дејност, криминалитет, социо – патолошки појави и техничко – технолошки акциденти.[23]

Од интерес на овој труд е компјутерскиот криминал, кој се појавува како придружен елемент за остварување на сите закани од невоена природа. Тој е главното оружје за изведување на голем број на недозволени дејства и со негова помош се остваруваат различни цели и интереси.

Закани за безбедноста во современиот свет од невоена природа се оние кои го спречуваат нормалното остварување на секојдневните функции во општеството, а притоа нема применување на вооружени сили или било каков вид на огнено оружје.

---

[22] „Основи на системот на националната одбрана“, Т.Гоцевски, Филозофски Факултет, Скопје, 2006, стр. 41.
[23] „Национална безбедност на Република Македонија (втор дел)“, М.Котовчевски, Македонска цивилизација, Скопје, 2000, стр 130.

Заканите од ваков вид се се позачестени во денешни услови, тие се многу поопасни од користењето на каков и да било вид на оружје и се потешко се наоѓаат начини за нивно навремено откривање и спречување.

Закани од невоена природа се и психолошко-пропагандните дејства, кои претставуваат збир мерки со кои се влијае врз свеста, определувањата и однесувањата на граѓаните на една држава или одреден регион заради остварување на одредена цел.

Во теоријата и праксата психолошко-прпагандните дејства се манифестираат преку различни притисоци и тоа: политички, економски и воени притисоци.

Политичката индоктринација исто така е облик на невоена закана, технолошки агресии, ембарго и блокади, разни забрани за користење на сообраќајна и друг вид инфраструктура. Заканите од невоена природа, во современиот свет се нарекуваат и асиметрични закани, кои се повеќе добиваат во интензитет, а класична воена закана е помалку веројатно или воопшто нема да се случи.

Организираниот криминал и тероризмот претставуваат глобална опасност во современиот свет. Тие имаат големи цели, кои настојуваат да ги остварат по секоја цена, без да размислуваат на штетите и на последиците од нивните активности.

Новите ризици за меѓународниот поредок можат да се манифестираат и во областа на информациите и на комуникациите. Посебно тука ќе биде изразен, сајбер криминалот, приатството и злоупотребата на информатичката технологија, особено во делот на личните податоци на граѓаните, деловната, службената и државната тајна.

Маѓузависноста и интензивната соработка меѓу државите на регионален и глобален план во сите области, обезбедува просперитет и развој, но и поголема осетливост на информатичко – комуникациски план.

Од претходно наведените невоени закани и ризици за безбедноста во современиот свет ќе забележиме дека како, најраспространет и најопасен облик на невоена закана се повеќе се истакнува компјутерскиот криминал, односно криминал во кој компјутерот се користи како средство за вршење на криминални активности.

Терористите, денес многу лесно оперираат во кибернетскиот простор. Можат да уништуваат определени податоци, но и вешто да манипулираат со значајни информации од

посебен интерес за нивното успешно и несметано дејствување. [24] Денес, воопшто не е невозможно вештите „компјутерски крадци“ со терористички намери да навлезат во компјутерските сиситеми на најдобро чуваните банки, со цел да извршат кражби на информации, потоа да извршат нивна промена, а според актуелните потреби и да ги уништат или да ги блокираат за определен временски интервал.

Компјутерскиот криминал е една од актуелните и потенцијални безбедносни закани и предизвици во современиот свет. Со помош на компјутерскиот криминал, се вршат различни облици на невоени закани, и тоа: компјутерски измами и компјутерски фалсификати, компјутерски шпионажи и саботажи, компјутерски грабежи и недозволени трансфери.[25]

Компјутерскиот криминал е криминал, во кој главно оружје и кој се врши само со помош на компјутерите и компјутерската технологија.

Во современиот свет е незамисливо да се живее без компјутер, тој има огромно влијание врз целокупното функционирање на општеството, па поради тоа се појавуваат се поголем број облици на негова злоупотреба, од најситни грешки во софтверот, до ограбување на банки и терористички напади во кои има и огромен број на жртви, без разлика дали станува збор за човечки животи или за материјални и финансиски средства.

Ваквиот вид закани против Република Македонија, имаат за цел нејзино слабеење и дискредитирање како држава и намалување на ефикасноста во функционирањето на нејзините витални органи.

Кампањата против Република Македонија, за промена на нејзиното име, медиумската кампања, во 2001 година, ембаргото од страна на Грција, се примери на закани од невоена природа врз безбедноста во Република Македонија.

Сите овие закани имаат единствена цел за компромитирање на Република Македонија во регионални, но и во меѓународни рамки. Затоа е потребно, да се посвети поголемо внимание на кривичните дела предизвикани со компјутер и компјутерска технологија, за да не дојде до огромни штети за одредени компании, па и на државата во целина.

---

[24] „Национална безбедност на Република Македонија (втор дел)“, М.Котовчевски, Македонска цивилизација, Скопје, 2000, стр.115.

[25] “Novi oblici drustveno opasnih ponasanja I problem njihove krivicno pravne zastite”,JRKKP,Beograd,1990, str.56.

Потребно е да се прошират веќе постоечките закони, да се разгледаат досегашните искуства и да се разгледаат искуствата на други држави и тоа без разлика дали се на исто развојно ниво со Република Македонија или се чекор понапред или поназад, затоа што секое искуство во оваа област може да биде полезно.

Заканите од невоена природа ќе бидат се посериозни, па дури и најопасни закани во иднина. Во иднина војните нема да се водат со конвенционално оружје, туку со компјутер и компјутерска технологија, без директни контакти меѓу завојуваните страни. Огромни материјални штети, финансиски малверзации, па дури и огромен број на човечки жртви ќе се направат само со едноставно само со еден клик со глувчето или со стискање само на едно копче на компјутерот.

3. Компјутерски криминал

Во зависност од забрзаниот развој на информатичкото општество и влезот на Интернетот во сите области на приватниот и општествениот живот на луѓето, компјутерскиот криминал станува доминантен облик на злоупотреба, кршење на законите и други норми на однесување.

Современата информациона и компјутерска технологија донесе нови и драстични промени во сите сфери на општествениот живот. Тие промени покрај позитивните и корисни новини, донесуваат и низа проблеми поврзани со појави и ширење на компјутерски криминал од различни облици, форми и видови на остварување.[26]

Сите овие промени може да се сведат на следново: нови форми на вредности, нови методи и техники на дејствување, независни од време и простор за дејствување, помал ризик од откривање на дејствата.

Основни елементи на кривичното дело, компјутерски криминал се: [27]

- случај, односно што е проблемот во тој случај;
- околности или како се случило;
- менталната состојба на сторителот на криминалното дело.

Најважно е првин да се дефинира компјутерскиот криминал, различните видови и облици на компјутерски криминал, типолошко определување на овој поим, факторите за појава на компјутерски криминал.

Компјутерскиот криминал зема се поголем замав во современиот свет, неговите дејства немаат граници. Компјутерските криминалци многу тешко се откриваат, па со тоа и штетите може да бидат катастрофални, без разлика дали жртвите се поединци, компании, па дури и цели држави.

---

[26] „Kompjuterski criminal",P.Dimitrijevic, Beograd,2007. стр. 38.

[27] Milosavljevic.M, Grubor,G. " Istraga kompjuterskog kriminala, metodolosko – tehnoloske osnove", Univerzitet Singidunum, Beograd, 2009, стр.19

Компјутерот, не е само средство со кое се решаваат проблеми и задачи, се комуницира, се учи, туку се почесто се јавува и како оружје, но и жртва на напади. Современото функционирање на општеството, во најголема мера е во зависност од правилното функционирање на компјутерите и компјутерската технологија.

Злоупотребата на компјутерите и компјутерската технологија, претставува една од најголемите закани за користење на информациско – комуникациските технологии низ целиот свет.

Без разлика дали тоа ќе е во облик на хакинг, економска шпионажа, напади на веб страници од различни причини, саботирање на податоци, виируси, измами, неовластен пристап и откривање на податоци, и други активности кои влијаат врз граѓаните, компаниите па и врз цели држави.

Компјутерот и компјутерската технологија во рамките на компјутерскиот криминал , се појавуваат како цел, но и како средство на напад.

Кога се појавува како цел на напад, компјутерот е жртва во спроведување на одредени криминални активности, за да се украдат некои податоци, за да се спречи нормалното функционирање на самиот компјутер, а со тоа и на компјутерската мрежа во целина, без разлика дали тој се наоѓа во некој дом, во компанија, банка, во општинска или државна институција.

Кога компјутерот пак, се појавува како средство за напад, тогаш станува збор за овозможување на реализирање на одредена криминална активност во која компјутерот се користи како главно оружје. Преку тој компјутер, се вршат различни видови напади, се откриваат разни важни шифри, се откриваат и се објавуваат доверливи податоци, се вршат недозволени трансакции, или едноставно се уништуваат софтверските делови на важни компјутери, за да се забави или оневозможи работата на нападнатата компанија, институција или дури и на поединец.

Во ова поглавје, ќе ги разгледаме поимот и обидите за дефинирање на компјутерскиот криминал, различните видови на појавување на компјутерскиот криминал, факторите кои придонесуваат за појава на компјутерски криминал, сето тоа е за полесно да го разбирање на компјутерскиот криминал, за да може најбрзо и најлесно да се воочи неговото појавување и можностите за негово превенирање и спречување.

3.1. Поим и дефинирање на компјутерски криминал

Дефинирањето на компјутерскиот криминал е прилично тешко, поради тоа што, станува збор за релативно нов облик на криминално однесување, кој уште не се издвоил во целост од другите облици на криминал и компјутерскиот криминал, претставува голема феноменолошка разновидност, која тешко може да се опфати со една дефиниција. Компјутерскиот криминал е многу комплициран, опфаќа во себе голем број на активности, средства, луѓе и технологии, кои се повеќе ја комплицираат можноста за давање на сеопфатна, веродостојна и јасна дефиниција.

Под поимот компјутерски криминал,[28]се подразбира, некое дејство, во кое компјутерот воедно е средство, но и цел за извршување на одреден вид на кривично дело.

Во рамките на наведената дефиниција на компјутерскиот криминал, денес во светот може да се сретнат повеќе инкриминации, со кои се врши заштита од компјутерскиот криминал:

1. Приод во компјутерски систем;
2. Компјутерска измама и компјутерски фалсификат со кои се опфаќаат манипулации со податоци, (употреба на неисправни и нецелосни податоци, неовластено употребување на податоци, неовластено влијание врз текот на обработка на програми);
3. Компјутерски шпионажи и саботажи;
4. Кражби на време од компјутерски системи и сл.

Постојат огромен број автори кои дале свој придонес во дефинирањето на поимот компјутерски криминал. Во теоријата на кривичното право можат да се сретнат различни појмовни одредувања на кривичниот криминалитет: [29]

[28] „Криминологија“,З.Сулејманов, Графос,Скопје, 2007, стр.31.
[29] „ Криминологија“, З.Сулејманов,Графос,Скопје,2007, стр.36.

- ***Дон Паркер (Don Parker)*** го одредува компјутерскиот криминал како: злоупотреба на компјутерите во смисла на секое случување кое е во врска со употребата на компјутерската технологија, во кое жртвата трпи или би можела да трпи загуба, а извршителот делува со намера да дојде до корист за себе од секаков вид.

- ***Бого Брвар (Bogo Brvar),*** ја дава следнава дефиниција за компјутерскиот криминал: тоа се кривични дела кај кои компјутерот се појавува како средство, предмет или објект на напад, за чие вршење или обид е неопходно поголемо познавање од областа на информатиката.

- ***Ѓорѓе Игнатовиќ (Gorge Ignatovic),*** под компјутерски криминал подразбира посебен вид инкриминирано однесување кај кое компјутерскиот систем се појавува или како средство за извршување или како објект на кривично дело, доколку делото на друг начин или спрема друг објект, воопшто не би можело да се изврши или би имало други карактеристики.

- ***Според Роберт Мур (Robert Moore),*** американски истражувач во оваа област, компјутерскиот, односно сајбер криминал се однесува на било кои криминални активности, кои вклучуваат компјутери и компјутерски мрежи. Компјутерот може да се користи во изведувањето на кривичното дело, но компјутерот може да биде и цел на напад.[30]

Во овој контекст ќе го споменеме и поимот сајбер војна, кој исто така е од големо значење за појаснување на компјутерскиот криминал. Овие два поими се тесно поврзани, односно во многу случаи се преклопуваат еден со друг. Истражувачот Мур наведува дека сајбер војната се однесува на политички мотивирано хакирање, со цел да се спроведе саботажа и шпионажа. Сајбер војната е форма на информациска војна која понекогаш се гледа како аналогија на конвенционалното војување, иако оваа аналогија е контроверзна и од страна на точноста и од страна на својата политичка мотивација.

- ***Ричард А. Кларк (Richard, A.Clark),*** експерт за безбедност на Владата на САД, во својата книга „Сајбер војна“ (CyberWar), ***сајбер војната*** ја дефинира како: „одредени акции превземени од страна на нација или држава, за да зе навлезе во компјутерите или мрежите на друга нација, со цел да се предизвика штета или нарушување.“ [31]

---

[30] Moore,R. “Cybercrime: Investigating High- Tehnology Computer Crime”, Anderson Publishing, Cleveland, Mississippii, 2005, str. 46.

[31] Clark,A.Richard, “ CyberWar – The Next Threat to National Security and What to do About it”, Harper&Collins Publishers, 2010, str. 78.

- Хрватскиот автор, ***Јован Курбалија***[32] ***(Jovan Kurbalija),*** во својата книга „ Uvod I upravljanje Internetom", се обидел најсоодветно и прецизно да го дефинира поимот сајбер криминал, наведувајќи дека - „Реално – правниот пристап истакнува дека сајбер криминалот е исто што и реалниот криминал, но обично се врши со користење на компјутер кој најверојатно е поврзан со Интернет. Криминалот е ист, само се разликуваат средствата за извршување".

Како попрецизен обид за дефинирање на сајбер криминалот, направен од истиот автор (Јован Курбалија), ќе го наведеме следново:

„ Дефинирањето на сајбер криминалот е едно од главните прашања на сајбер правото, затоа што ќе пружи практичен правен резултат, вршејќи влијание на следење на сајбер криминалот. Ако станува збор за прекршоци направени против компјутерски системи, сајбер криминалот би вклучувал: неовластен пристап; оштетување на компјутерски податоци и програми; саботажи заради спречување на функционирање на некој компјутерски систем или мрежа; неовластено пресретнување податоци, кон или од некој систем или мрежа; како и компјутерска шпионажа.

Исто така, ***Јован Курбалија,*** направил обид за дефиниција поврзувајќи ги поимот криминал со поимот Интернет – „ Под сајбер криминал се подразбираат сите недела сторени преку Интернет и компјутерски систем, што подразбира поширок дијапазон недела, вклучувајќи ги и оние наведени во Конвенцијата за сајбер криминал: компјутерски подвали, повреди на авторски права, детска порнографија и мрежна безбедност".

- Тајванскиот професор ***Dr. Wu Kuo – Chen***[33], од Одделот за Информациска Технологија на National Central Taiwan University, наведува дека сајбер криминалот има најразлична природа, од традиционална, до бескрајна и анонимна. Со помош на природните мрежни технологии, сајбер криминалот се шири над области, региони и држави. За истражувачите е многу тешко да направат вистинска слика за целиот криминален процес, поради дисперзирани елементи на различни места. Вистинскиот профил на сајбер криминалот, може да се претстави само преку анализа на технологиите и нивниот брз развој".

[32] Kurbalija,Jovan. "Uvod I upravljanje Internetom"- 2 izdanje, Albatros Plus, Beograd, 2011, str.101.
[33] http://itlaw.wikia.com/wiki/Cyberterrorism - дефиниции за сајбер криминал.

- Делата на ***Дороти Денинг (Dorothy Denning[34]),*** се од голема важност во областа на сајбер тероризмот. Таа сајбер тероризмот го дефинира како: „ политички дефинирани хакерски операции, наменети да предизвикаат големи штети, како што се дури и загуби на човечки животи или големи економски штети".

- ***Роберт Џ. Бункер,***[35]во своето дело пак истакнува дека влијанието на информатичката војна треба да се вкотви во некоја форма на дефиниција. Прашањето е дали треба да се базира само врз компјутерите и нивните електро – оптички мрежи или дали треба да се вклучат техниките, како на пример електронското војување. Точниот одговор е дека не треба да се направи ни едното ни другото. Таквите дефиниции се премногу традиционални. Наша грижа е да видиме како ќе се води постмодерна војна.

- Терминот „интернет војување" го вовеле ***Џон Аркила*** и ***Дејвид Ронфелдт***, во 1993 година, опишувајќи го како: „ на високо ниво информатички поврзан конфликт меѓу нациите и општествата. Тоа значи обид да се прекине, оштети или да се модифицира она што популацијата го знае или мисли дека го знае, за себе или за светот околу себе.

Кога станува збор за дефинирање на компјутерскиот криминал, или како што почесто се нарекува и сајбер криминал, постојат огромен број на дефиниции во рамките на институциите кои се занимаваат со оваа проблематика.

Па така, ***Канцеларијата за контролирање на валути[36] (Office of the Comptroller of the Currency),*** при обидите за дефинирање на компјутерскиот криминал ја истакнува следнава дефиниција: „ користење на компјутерски ресурси против личности или приоритети, за да се заплашат влади, цивилно население или одредени сегменти, за унапредување на политички и социјални цели".

Федералната агенција за управување со итни случаи (Federal Emergency Management Agency – FEMA), свој придонес дава преку следнава дефиниција: „Незаконски

[34] Denning,D. "Activism,Hactivism and Cyberterrorism:The Internet as a Tool for Influencing Foreign Policy, Networks and Netwars, Rand, 2001, str.241.
[35] „Не-државни закани и идни војни", Р.Џ.Бункер, Нампрес, Скопје, 2009, стр.103.
[36] http://itlaw.wikia.com/wiki/Cyberterrorism

напади и закани против компјутери, мрежи и бази на информации, со цел да се заплашат или присилат влади или граѓани, за остварување на одредени политички или социјални цели".

Конгресната истражувачка служба (Congressional Research Service), компјутерскиот криминал го дефинира како: „ политички мотивирано користење на компјутерот како оружје или цел, од страна на субнационални групи или тајни агенти, со намера преку насилство да влијаат на народните маси или да влијаат врз владите да ги сменат своите политики".

Од претходно наведените дефиниции можеме да ги извлечеме основните карактеристики на поимот компјутерски криминал, и тоа:

- колективно опасно, противправно однесување за кое законот пропишува кривични санкции;
- специфичен начин и средство за вршење кривични дела со помош или со подсредство на компјутери и компјутерска технологија;
- посебен објект на заштита – безбедноста на компјутерските податоци или информатичките системи во целина или во поединечни сегменти;
- намера на извршителот за себе или за друг, на овој начин да дојде до корист, или на друг да нанесе штета.

Државите членки на Советот на Европа [37]и други потписнички, сметајќи дека целта на Советот на Европа, е да оствари поголемо единство помеѓу членките во борбата против криминалот, а со тоа и против компјутерскиот криминал. Меѓу другото, тоа ќе го остварат со донесување одговарачки закони и прописи и јакнење на меѓународна соработка.

Свесни заради големите промени во дигитализацијата и глобализацијата на компјутерските мрежи, загрижени поради заштитата на компјутерските мрежи и електронските податоци кои би можеле да се користат во вршење на компјутерски кривични дела, потребите за заштита на личните податоци и легитимните интереси ја донеле Конвенцијата за компјутерски (сајбер) криминал.

[37] Конвенција за компјутерски криминал, Будимпешта, 23.11.2001.

Други конвенции кои се занимаваат со слична ваква проблематика се:

- Конвенција на Советот на Европа за заштита на човековите права и темелни слободи, донесена во 1950 година;
- Маѓународниот пакт на ОН за граѓански и политички права, од 1966 година;
- Конвенција на Советот на Европа за заштита на личности во поглед на автоматска обработка на податоци, од 1981 година;
- Конвенција на ОН за правата на децата, од 1989 година;
- Конвенција на Меѓународната организација на трудот за најлошите облици на детски труд, од 1999 година;
- Протокол за закани од компјутерски криминал, 2002 година;
- Дополнителен протокол на Конвенцијата за сајбер криминал, 2003 година[38].

Конвенцијата за компјутерски криминал, има за цел да ги дополни и да ги направи поделотворни сите претходно споменати конвенции, како и да овозможи собирање податоци за кривични дела во електронска форма, развој на меѓународната соработка во борба против компјутерскиот криминал, а посебно мерките што ги превземаат Обединетите Нации, Европската Унија и членките на Групата 8 (Г8).

Поради проблемите од компјутерскито криминал е формиран Европскиот Комитет за криминални проблеми (CDPC – European Committee on Crime Problems).

Според оваа Конвенција за компјутерски криминал, под ***компјутерски криминал*** се подразбираат: кривични дела кои се вршат против тајноста на различен вид податоци, достапноста и распростанувањето на различни податоци кои може да доведат до огромни штети.

Како незнаконски кривични дела, во оваа Конвенција се наведени:
-незаконски пристап до податоци;
-незаконско престретнување на податоци;
-попречување на податоци;
-попречување на работата на компјутерските системи;
-злоупотреба на различен вид уреди и сл.

[38] http://conventions.coe.int/Treaty/en/Treaties/html/189.htm

Исто така, важно е тука да ја споменеме и дефиницијата, дадена на ***Десеттиот Конгрес на Обединетите Нации,*** во документот кој е наречен - Криминал врзан за компјутерска мрежа, (Crime related to computer networks).

Во овој документ компјутерскиот криминал е дефиниран како:[39]

„ Криминал кој се однесува на било кој облик на криминал, кој може да се извршува со компјутерските системи и мрежи, во компјутерските системи и мрежи или против компјутерските системи и мрежи".

Терминот компјутерски криминал , покрај досега споменатите дефиниции има обиди за дефинирање и од страна на ***Федералното Истражно Биро*** (ФБИ).[40]

Така, според ФБИ, во компјутерски криминал спаѓаат:

- нелегални влегувања во мрежите на телефонските компании;
- нелегални влегувања во поголеми мрежи на видни компании;
- загрозување на интегритетот на компјутерските мрежи;
- загрозување на приватноста;
- индустриска шпионажа;
- пиратски компјутерски софтвер;
- било какво криминално дејство, каде компјутерот е главен фактор за криминален престап.

Интернет војната може да се фокусира кон јавното или кон мислењето на елитата. Тоа може да и вклучува јавни дипломатски мерки, пропаганда, психолошки кампањи, политичка и културна субверзија, измама од страна или мешање на локалните медиуми, инфилтрација во компјутерските мрежи и бази на податоци и напори да се промовираат дисидентни или опозициски движења преку компјутерските мрежи".

---

[39] Tenth United Nations Congress on the Prevention of Crime and treatment of Offenders, www.oun.org

[40] „Најсилно оружје до сега", О.Бакрески,Современа македонска одбрана, бр.9, стр.165.

Оваа дефиниција,[41] во 1996 година, била малку проширена и прецизирана:

„ Почетен стадиум на конфликт (и криминал) на општествено ниво, кој вклучува мерки кои не се типични за војната, во која протагонистите користат и зависат од мрежни форми на организација, доктрина, стратегија и комуникации. Овие протагонисти се состојат од расфрлани, честопати мали групи кои се договараат да се координираат и да дејствуваат преку Интернет, честопати без прецизно лидерство и штаб. Донесувањето на решенија може намерно да е децентрализирано или расфрлано“.

Во декември 1997 година, Групата 8, одржала состанок посветен на меѓународното движење во употребата на информациско – комуникациска технологија во организираниот криминал.[42]На тој состанок биле прифатени десет Принципи за борба против криминалот на високата технологија и Акционен план за борба против криминалот на високата технологија. Тогаш е основана и Мрежа за контакт на Групата 8, која работи 24/7, за помош во случаи на компјутерски криминал.

Во Република Македонија недоволно внимание му се посветува на ваквиот вид на криминал, иако тој завзема се поголеми размери и штетите се огромни без разлика дали станува збор за материјални придобивки или човечки животи. Најсериозни обиди за дефинирање на компјутерски криминал има во - Кривичниот Законик на Република Македонија, во член 251, каде што се спомнува кривично дело - Навлегување во компјутерски систем. [43]

Членот 251, од Кривичниот Законик на Република Македонија, гласи:

„ 1- Тој што неовластено ќе внесе, измени, ќе објави, скрие, избрише или уништи компјутерски податоци или програми или на друг начин ќе навлезе во компјутерски систем со намера за себе или за друг да прибави имотна корист или да оштети друг, ќе се казни со парична казна или со казна затвор до три години.

---

[41] „Не-државни закани и идни војни“, Р.Џ.Бункер, Нампрес, Скопје, 2009, стр.104.

[42] „Medjunarodni vodic za borbu protiv kompjuterskog kriminala“, Amerikanska advokatska komora, 2003, стр.35.

[43] Кривичен Законик на Република Македонија, член 251, Скопје, 2003.

2 – Ако со делото од став 1 е прибавена поголема имотна корист или предизвикана поголема имотна штета, сторителот на вакво кривично дело, ќе се казни со затвор од една до три години.

3 – Гонењето се превзема со предлог ".

Република Македонија својата легислатива на овој план, ја темели на Конвенцијата за сајбер криминал, донесена од страна на Советот на Европа, во 2001 година, а која Република Македонија ја ратификувала во 2004 година.

Значи, дефиниран поопширно, ***компјутерскиот криминал*** може да опфати широк репертоар на криминални престапи, активности, теми и содржини. Придавајќи му важност на компјутерот во секојдневниот живот, вклучувајќи ги животите на оние кои не виделе компјутер, скоро секогаш постои некоја неизбежна и нераскинлива врска, помеѓу компјутерот и криминалот.

Со споредување и детално анализирање на сите претходно споменати дефиниции, можеме да извлечеме една сеопфатна, а притоа и јасна и разбирлива дефиниција, која компјутерскиот криминал ќе го разбере како: *криминал* кој наместо со оружје се извршува со помош на компјутер или врз компјутер, со цел да се стекне одредена материјална корист, да се менуваат важни одлуки, да се влијае на јавното мислење, дури и да се предизвикаат човечки жртви, од што произлегува дека нападите се вршат поради политички, економски и социјални цели, а може да ги изведуваат поединци или добро организирани групи зад кои стои криминална организација, легални институции па дури и влади и држави и секој кој би имал било каков интерес од ваквиот вид на напади.

Во современиот свет неможе да се замисли организирање на било каков криминал без да се употреби компјутер и компјутерска технологија.

Ова е озобеновен и сеопфатен случај, кога компјутерот се користи во големи размери во секојдневниот живот и тоа за евиденција, администрација, полициски досиеја и секаков друг вид на досиеја, осигурувања, банкарски сметки и сл.

3.2. Видови на компјутерски криминал

Во однос на видовите на компјутерски криминал, постојат повеќе поделби и документи во кои тие се наведуваат. Врз основа на технологиите што се користат, врз основа на карактеристиките софтверот и хардверот што се користи , врз основа на особините на криминалците (хакерите), и голем број други карактеристики се издвојуваат и различни видови на компјутерски криминал.

Компјутерскиот криминал многу тешко се спречува, а уште потешко навремено се открива од причина што многу доцна се забележуваат направените штети, за тоа време сторителот на ваков вид на кривично дело има време да ги избрише или да ги прикрие трагите или дури да ги наведе истражувачите во сосема друг правец.

Различни автори и истражувачи на различен начин го согледуваат овој проблем. Некои наведуваат дека компјутерскиот криминал дури и не е криминал само е сегмент без кој немозже да се изведе организиран криминал. Додека други пак, детално го разработуваат овој вид на кримина, со сите негови форми и облици, наведувајќи дека постојат повеќе видови на компјутерски криминал.

Според Кајзер,[44]во зависност од засегнатото правно добро можат да се разликуваат три вида компјутерски злоупотреби:

1. Компјутерски повреди на личноста, особено на приватната сфера на граѓанинот;
2. Компјутерски деликти против индивидуалните или социјални правни добра;
3. Компјутерски имотен криминалитет во потесна смисла.

Различни документи, на различни начини ги класифицираат облиците на сајбер криминал. Така во материјалите за криминалот поврзан со компјутерски мрежи од Десеттиот Конгрес на ОН [45] се констатира дека постојат две категории на овој криминал:

- ***Сајбер криминал во потесна смисла-*** во кој се вбројува секое незаконско однесување насочено на електронски операции, сигурноста на компјутерските системи и податоци кои во нив се обработуваат.

---

[44] „Криминологија-вовед во основите“, К.Гинтер, Александрија, Скопје, 1996. стр.41.
[45] Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, www.oun.org.

- Сајбер криминал во поширока смисла – како секое незаконско однесување врзано за или во однос на компјутерските системи и мрежи, вклучувајќи и таков криминал, како што се поседувањем нудење и дистрибуција на информации преку компјутерски системи и мрежи.

Во истиот овој документ, од Десеттиот Конгрес на Обединетите Нации, се наведуваат и конкретни облици на овој криминал, во согласност со Препораката на Советот на Европа. Тоа се: [46]

1. Неавторизиран пристап во компјутерски системи или мрежи со прекршување на сигурносните мерки (хакирање);
2. Оштетување на компјутерски податоци и програми;
3. Компјутерска саботажа;
4. Неовластено пресретнување на комуникации од и во компјутерски системи и мрежи;
5. Компјутерска шпионажа.

Секој од наведените облици може да се вкрсти во комбинација со секој друг, односно не постои, т.н. „чист“ облик на компјутерски (сајбер) криминал. Тој секогаш се појавува како придружен елемент на било кој друг вид на криминал, а неговата улога е во зависност од видот на криминалната активност.

Од делата на компјутерскиот криминал во поширока смисла, најчесто се појавуваат:[47]

1. компјутерски фалсификати;
2. компјутерски кражби
3. техничка манипулација со уреди или електронски компоненти на уредите;
4. злоупотреба на системите за плаќање како што е манипулација и кражба на електронски картички или користење на лажни шифри во незаконски финансиски активности.

[46] Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, www.oun.org.
[47] Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, www.oun.org.

Европската Конвенција за Сајбер (компјутерски) криминал[48], предвидува 4 групи на кривични дела, и тоа:

1. Дела против доверливоста, интегритетот и достапноста на компјутерските податоци и системи – овие дела се состојат во незаконит пристап, пресретнување, влез во податоци и системи, користење на уреди (производство, продажба, увоз и дистрибуција), програми и пасворди;

2. Дела поврзани со компјутерите – во кои како најтипични и најчести примери се наведуваат фалсификувањето (без разлика дали станува збор за фалсификување на хартии од вредност, банкноти, лични документи, разни имотни документи и сл.) и различни видови на електронски кражби;

3. Дела поврзани со софржината – детската порнографија е најчеста содржина која се појавува во оваа група, а опфаќа: поседување, дистрибуција, трансмисија, чување или овозможување поголема достапност на овие материјали, нивно производство заради дистрибуција и обработка во компјутерски системи или на носители на податоци, побрзо пренесување и рекламирање преку недозволени канали, заради стекнување на поголема финансиска корист.

4. Дела поврзани со повреда на авторските или сродни права – опфаќа репродукција и дистрибуција на неавторизирани примероци на дело во компјутерските системи, како што е примерот со пиратеријата која е доста проширена во денешно време, а опфаќа продажба на филмови и музика кои се преснимувани од оригинални, симнувани од Интернет страници или директно снимани со камери во живо.

Во зависност од типот на сторените дела, криминалитетот може да биде:

1. Политички:

- сајбер шпионажа;
- хакирање;
- сајбер саботажа;
- сајбер тероризам;
- сајбер војување.

[48] European Committee on Crime Problems,Convention on Cyber Crime, april 2000, www.europa.eu.int.

2. Економски:

- сајбер измами;
- хакирање;
- кражба на интернет услуги;
- пиратерија на софтвери, микрочипови и бази на податоци;
- сајбер индустриска шпионажа;
- измами со Интернет аукции (неиспорака на производи, лажна презентација на производи и сл.).

3. Производство и дистрибуција на недозволени и штетни содржини, во кои спаѓаат:

- детска порнографија;
- педофилија;
- верски секти;
- ширење на расистички, националистички и слични идеи и ставови;
- злоупотреба на жени и деца.

4. Манипулирање со забранети производи и супстанции, како што се:

- дрога;
- човечки органи;
- оружје.

5. Повреда на сајбер приватноста, во која спаѓаат:

- надгледување на електронска пошта;
- спам (spam);
- прислушкување и снимање разговори;
- следење на е- конференции и сл.[49]

Поради големиот број на различни класификации се покажува разновидноста на ваквиот вид кривични дела и комплексноста на нивните појавни облици, но и разликите на критериумите кои се користат.

[49] European Committee on Crime Problems,Convention on Cyber Crime, april 2000, www.europa.eu.int.

Она што е неоспорно е, дека компјутерскиот криминал повеќе е поврзан со активност на поединци, а криминалот поврзан со компјутерски мрежи е дело на групи и тоа организирани, професионални, па се почесто и многу добро специјализирани и организирани. Овие групи, од една страна се традиционални на организираниот криминал, кои се усовршиле и осовременииле со примена на информатичко–комуникациска , а од друга страна, се појавуваат и посебно организирани сајбер групи, односно сајбер мафија, кои се наоѓаат во сопствен свет, користат тајни јазици, шифри и програми и многу тешко може да се откријат.

3.3. Типолошко определување на компјутерски криминал

Сите облици на компјутерски операции и активности се осетливи на криминална активност, без разлика дали станува збор за цел на криминални дејства, или тие едноставно се инструмент за изведување криминал (претставуваат главно оружје во изведување на било каков вид на криминал).

Операциите за внесување на податоци во компјутер или компјутерски систем, обработка на податоци, операциите за излез и комуникациите од различен тип, се користат за забранети цели,[50]од страна на сторителите на кривични дела од областа на компјутерите и компјутерската технологија.

Компјутерите и компјутерската технологија можат да се злоупотребат на различни начини, а самиот криминалитет кој се реализира со помош на компјутер може да има облик на било кој од традиционалните видови на криминалитет.

Традиционални видови кои добиваат и посовремен облик со помош на компјутерска технологија се: кражба, проневера, провала, додека податоците кои неовластено се придобиваат со злоупотреба на информационите системи, можат на разни начини да се искористат за стекнување на противправна корист.

[50] „Компјутерски криминалитет“, Н.Тупанчевски, Годишник на правниот факултет, Скопје 1991, стр.204.

Како најчесто користени типови на сајбер криминал се:

1. Противправно користење на услуги и неовластено придобивање на информации, односно манипулација со податоците;
2. Компјутерска кражба;
3. Компјутерска измама и компјутерски фалсификат;
4. Измама со компјутери „со неверојатни средства“;
5. Компјутерска саботажа, шпионажа и компјутерски тероризам;
6. Електронско провалување во компјутерски систем и кражби на време од компјутерски систем и сл. [51]

1. Противправното користење на услуги и неовластено придобивање на информации, односно манипулацијата со податоците, се состои во неовластена употреба на компјутерот или негова овластена употреба, но за остварување на потребите на неовластен корисник. Пример, за неовластена употреба на компјутерот, е кога тој се користи за други цели освен оние кои се дел од неговата намена во информатичкиот систем.

Како пример за објаснување на неовластена употреба на компјутерите и компјутерската технологија ќе го наведеме примерот кога, вработените во една фирма собираат податоци за идниот работодавец или кога расположливото време го користат за некои свои дополнителни активности. Како најчест и наједноставен пример е злоупотребата на Интернетот од страна на вработените.

Неовластеното придобивање на информации претставува своевидна кражба на податоци од компјутерски системи, најчесто заради остварување на противправна сопствена корист. Техничките и технолошките можности за неовластено придобивање на информации со појавата на Интернетот драстично се зголемија, па така, мета може да биде и нечиј личен компјутер или било кој поврзан или изолиран компјутерски систем. [52]

Манипулацијата со податоци се врши на различни начини и со различни цели. Манипулациите се состојат од едноставни, не толку успешни операции, до комбинации на

[51] „Криминологија-вовед во основите“, К.Гинтер, Александрија, Скопје, 1996,
[52] „Криминалистика“, Ж.Алексиќ, З.Миловановиќ, Белград, 1994, стр.54.

активности кои бараат висок степен на познавање на системот и темелно познавање на техничката контрола и воедно бараат и извршител со исклучителна интелигенција. Врз основа на овој план, во германското право се врши заштита на сопственикот на податоците, во прв ред на софтверот. Всушност, делото не е насочено ниту кон заштитата на авторот на софтверот, ни кон заштитата на оној на кого податоците се однесуваат, туку кон заштитата на сопственикот на податоците.

Под поимот податоци, се опфатени сите податоци, без оглед на кое ниво и во која фаза на обработка се наоѓаат.[53]

Во САД, на пример, дознавањето на податоците од компјутерски систем од страна на неовластени лица е инкриминирано како кривично дело. Делото е извршено со самото остварување на неовластен програмски приод кон определени програмски или бази на податоци.

Со оваа одредба, всушност, се казнуваат како успешните, така и неуспешните лица што неовластено влегуваат во туѓ компјутерски систем. Неовластениот програмски приод, исто така, се казнува и во Шведска и во Австралија и во поголем број земји во светот.

2. Компјутерска кражба. Во современиот свет, обичната кражба станува незначителна во споредба со компјутерската кражба.

Под компјутерска кражба се подразбира криминално дело преку кое се придобива одредена материјална или било каква корист, а која се остварува со помош на компјутер, односно компјутерот е главното средство за извршување на кражбата.

Компјутерска кражба може да се остварува на илјадници километри оддалеченост од жртвата, без извршителот на кражбата да биде директно присутен на местото на настанот.

Најчест пример на компјутерска кражба е кражбата на идентитет, која е посебно општествено опасна активност. Ваквите видови на кражба растат со зголемувањето на електронската трговија, со тоа што крадците можат да отворат сметки во банка, различни видови дозволи, можат да купуваат производи со туѓи пари.

Многу често се вршат недозволени трансакции, на поголеми или помали суми на пари или на хартии од вредност, користејќи ги методите на компјутерски криминал. Жртвите во

[53] "Novi oblici drustveno opasnih ponasanja I problem njihove krivicnopravne zastite", M.Vesovic, JRKKP, Beograd,1990, str.56

вакви случаи, најчесто и не знаат дека некој го користи нивниот идентитет, додека не ги видат крајните сметки.

Многу важен е фактот дека потрошувачите се во голема опасност при користење на нивните картички, поради усовршената криптографска технологија.

Тешко е откривањето на сторителите на компјутерски кражби, поради начинот на изведување, поради местоположбата на сторителите, поради шифрираните напади и комплицираниот пристап до податоците.

Опасни се и компјутерски кражби со кои се крадат документи, без разлика дали се лични документи на поединци или документи на компании и институции, па и на влади и држави. Опасноста е во тоа што тие документи и податоци подоцна се користат за најралични криминални цели и активности. Поради овие опасности, луѓето се уште со несигурност гледаат на on-line набавките.[54]

Кражбата е кривично дело, без разлика со кое средство таа се остварува, дали е со метални направи, огнено оружје или компјутер.

3. Компјутерските измами и компјутерскиот фалсификат се вршат заради сопствена придобивка или придобивка која ќе биде од некој друг индивидуалец или организација. Компјутерот најчесто се користи за вршење измами во кривично-правна смисла.

Компјутерските измами се најраширен облик на компјутерски криминалитет. Во поглед на останатите елементи ова дело кореспондира со класичното дело измама. Овде, всушност, се работи за најопасни компјутерски манипулации во кои спаѓаат оние кои се вршат со компјутерски програми, со оглед на тоа што имаат подолг рок на делување.

Секаков вид на измами и фалсификати многу полесно се остваруваат со компјутер и со компјутерска технологија. Со помош на компјутер и компјутерска технологија, секаков вид на документ може да се фалсификува, без да има било какава разлика од оригиналот.

Тука повторно ќе го споменеме примерот со кредитните картички и нивната злоупотреба во различни активности. Она што ги карактеризира компјутерските измами, е тоа што тие можат да допрат на огромна далечина, благодарение на распространетоста на Интернетот како медиум, брзината на остварување и ниските трошоци за остварување на ваквите измами.

---

[54] http://www.ii.edu.mk (21.07.2009), Институт за информатика,Природно-Математички факултет,УКИМ,Скопје.

4. Измами со компјутери „со неверојатни средства“. Овој вид на измама е еден од најголемите извори на нелегална заработка на Интернет. Листата со нови производи „со неверојатни средства“ секојдневно се зголемува, а соодветно на тоа, се подобруваат и „убедувачките способности“.

Како примери кои се подразбираат под поимот „неверојатни средства“, се разните видови продукти, енергетски средства, пилули за слабеење, за кондиција, за концентрација и безброј други продукти, кои сосема бесплатно се рекламираат на Интернет страниците и нивното ширење меѓу луѓето е многу брзо.

Компјутерските измами „со неверојатни средства“ ја карактеризираат само онлајн продажбата, рекламирањето и распространувањето на одредени производи, кои не се доволно добри и квалитетни и со својства како што е наведено при нивното рекламирање и продажба.

Луѓето пребарувајќи на Интернет се одлучуваат да купат одредени производи од кои имаат потреба. За тие производи постојат соодветни карактеристики и својства кои се објавени и истакнати на производот, но кога ќе го платат производот и ќе го добијат, забележуваат дека производот воопшто не е таков каков што го сакале да го купат и со такви својства какви што пишувало дека треба да има.

Кога станува збор за ваквиот вид на измами, мора да споменеме дека најподложни на нив се стари лица, сиромашни, недоволно информирани и недоволно образовани лица, кои се доволно наивни за да поверуваат во својствата што ќе ги прочитаат, без притоа попрецизно да ја проверат веродостојноста на тие податоци..[55]

5. Компјутерска шпионажа, саботажа и компјутерски тероризам.

- ***Компјутерската шпионажа*** е 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 центри се почесто стануваат цели на шпионажа на тајни служби и конкуренти. Шпионите овде на мал простор, се наоѓаат концентрирани сите информации кои можат да бидат од нивни интерес.

[55] http://www.aek.mk (22.07.2009)

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.

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, се саботираат сигурносни и апармни системи за потоа да следува друга активност и сл. Компјутерска саботажа може да направи било кој, без разлика дали е добро обучен за работа со компјутер или е само аматер, дури може да му биде подметнато на некој да изврши саботажа, без тој самиот да биде свесен дека го направил тоа.

- ***Компјутерскиот 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. Како пример, ќе го споменеме нападот на ИРА, во 1997 година, со кој ја шокираше англиската јавност, со тоа што покрај бомби, атентати и други терористички напади, започна да користи и електронски напади врз службените и владините компјутерски системи.

Исто така, и терористите на Ал-Каеда се добро обучени за користење на компјутерската технологија, поставуваат различни web локации на кои ги пропагираат своите фундаменталистички идеи, а кај апсените терористи 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.

Тој е се позачестена појава во современиот свет, но многу често меѓу експертите од оваа област се појавува прашањето, што ќе се случува во иднина, кога сме сведоци на се побрз развој на компјутерите и компјутерската технологија. Дали идните напади, па дури и војни ќе се водат со компјутер и компјутерот ќе биде единствено оружје и за напад и за одбрана.

Терористичките организации, најчесто ваквите експерти ги пронаоѓаат меѓу: технолошки платеници, навработени технолошки експерти од земјите од третиот свет, западни технолошки експерти, високостручни кадри од бивши тајни служби. Генерален заклучок кога се работи за компјутерски тероризам би бил дека, во времето што доаѓа се повеќе ќе се користат технолошките достигнувања во постигнување на терористички цели и идеали. Најчести цели на напад, ќе бидат банките, банките на податоци, владини комуникациски системи, електроцентрали, сите видови на сообраќај, големи компании, нафтени рафинерии и сл. [56]

6. 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.

[56] „Investigating Computer- related crime", P.Stefenson, CRCPRESS, 2000, str.30

Цел на овие сторители, најчесто се мрежите кои се очекува дека се заштитени од електронски провали, и тоа: воени компјутерски комуникации, служби за известување, државни институции, банки и други финансиски институции и сл.

Во кривично-правна смисла, доколку ваквите дела не произведат одредени, конкретни, штетни последици, обично се врши повредување на службена или воена тајна и тоа преку увид во заштитена компјутерска банка на информации. [57]

Најчесто провалувањата во компјутерските системи се врши поради кражби на време. ***Кражбите на време,*** во системот се посебни групи од компјутерскиот криминалитет. Кражбите на време на системот, се престап кој се смета за специфично компјутерски и кој на извршителот може да му донесе значителна корист на сметка на сопственикот на компјутерскиот систем. Овде, всушност, станува збор за неовластена употреба на службени компјутери и компјутерски системи за приватни цели. [58]

Кражбите на време, најчесто се забележуваат во телекомуникациските и информатички услуги, при пробивање на веб страни на медиуми и сл. Кражбите на време најчесто опфаќаат користење на туѓи телекомуникациски и Интернет врски, нивно трошење за сопствени потреби и правење на огромни сметки на штета на жртвата на ваквиот вид кражби.

Од посебна важност се законите и прописите за компјутерски криминал,[59] кои имаат за цел: да го штитат интегритетот на владите и државите, да спречат државата да стане прибежиште на негативни структури, спречуваат државата да стане прибежиште на податоци за компјутерски криминал, заштита на државни тајни информации, ги штитат корисниците, ја зголемуваат државната безбедност и безбедноста на сите граѓани во државата и нивните компјутери и сите податоци што тие ги имаат во компјутерот и во компјутерскиот сиситем во целина, можност за судско гонење и соодветно казнување и сл.

---

[57] „Investigating Computer- related crime", P.Stefenson, CRCPRESS, 2000, str.32.

[58] "Kompjuterski kriminalitet I potreba koncipiranja krivicnog dela kompjuterske zloupotrebe",JRKKP, Beograd,1991, str.72.

[59] „Medjunarodni vodic za borbu protiv kompjuterskog kriminala", Amerikanska advokatska komora, 2003, str.39.

3.4. Фактори за појава на компјутерски криминал

Земјите во развој, па меѓу нив и Република Македонија, главно се борат со тоа како да ја користат електронската трговија и информациско – комуникациската технологија во секојдневните операции.

Поголем број од државите воопшто и немале почнато со прашањето за компјутерски криминал, па со тоа и со закони за компјутерски криминал. Во овие држави нивото на заштита на телекомуникациите и на информатичката технологија е многу ниско, или воопшто го нема. Затоа земјите во развој често постануваат најслаба алка во ланецот на компјутерска безбедност.

Причини, односно фактори, за појава на компјутерски криминал има во многу голем број и тоа од различни размери. Причините што доведуваат до злоупотреба на компјутери и компјутерска технологија, можат да бидат од различна природа, а негативните ефекти што се постигнуваат можат да бидат катастрофални и да направат штети од глобални размери.

Како пример, ќе наведеме дека, иако дознавањето на податоците од компјутерот, може да биде мотивирано од чисто авантуристички причини, без некоја посериозна цел, но со оглед на тоа што податоците се од доверлив карактер, тие можат понатаму да бидат искористени за остварување на други цели и тоа најчесто економски, финансиски, социјални, па дури и религиозни и идеолошки цели.

Мотивите можат да бидат и заради остварување одредена противправна имотна корист, материјални и финансиски средства, но покрај тоа и злоупотребата може да биде насочена кон уривање на целокупното општествено уредување на една земја, рушење на некоја политичка организација итн.

Американскиот автор Шерман (Sherman, Stacy)[60], анализирајќи го компјутерскиот криминал, го разделува во три групи и тоа:

- криминал во кој компјутерот е предмет, жртва;
- компјутерот како носител на податоци;
- и криминал во кој компјутерот се појавува како оружје.

[60] http://stacysherman.pbworks.com/w/page/27786098/Cyber%20Crime%20Project

Како мотиви за спроведување на компјутерски криминал, Шерман ги наведува следниве:

- злоба на незадоволните корисници;
- комерцијални (војни на компании на пазарите);
- прикривање казниви дела;
- политички или идеолошки мотиви (промена на идентитет);
- за да се отргне вниманието на јавноста.

Како главни причини за појава на кривични дела предизвикани со компјутер и компјутерска технологија се, остварување на идеолошки, политички, економски, верски и идеолошки цели. Компјутерскиот криминал може да направи огромни штети во индустријата и тоа во светски рамки, со што извршителот, со овој вид на криминална активност ќе добие одредена материјална и финансиска корист. [61]

Сајбер криминалот ја загушува експанзијата на електронската комерцијална работа, а со тоа претставува потенцијална опасност за општествената сигурност, посебно имајќи ја во предвид ранливоста на критичните инфраструктури во самото општество (како што се, банкарскиот систем, воздушна контрола на летање во светот, а кај нас компјутеризацијата на правосудството, банкарскиот систем, јавниот сообраќај од секаков вид, и др.), сектори во кои секојдневната работа се темели на компјутерите и компјутерската технологија.

Исто така, како причина за појавата на компјутерскиот криминал може да биде и од чисто аматерски причини, односно младите во современи услови се почесто настојуваат да ги откријат тајните на компјутерите, компјутерската технологија и Интернетот, без да сметаат на сериозноста на штетите што тие може да ги предизвикаат.

Младите настојуваат да се докажат меѓусебно, кој е посовршен во компјутерските вештини, па така успеваат да продрат во доста добро заштитени и обезбедени компмјутери и компјутерски системи и успеваат да дојдат до информации кои не би смееле да паднат во погрешни раце.

Најтешки и најопасни фактори за појава на компјутерски криминал, се оние фактори кои имаат верска и идеолошка позадина. Заради остварување на идеолошките и верските

[61] „Сајбер-криминалитет-нови можности за криминогено однесување“,С.Патоски, Legal yournal - Lawyer,март 2003,стр.87.

цели не се бираат средства, ниту методи, за да се дојде до остварување на тие цели. За остварување на овие цели не се штедат финансиски средства, но исто така не се штедат ни човечки животи.

Постојат огромен број причини за пристапување кон извршување на кривични дела со помош на компјутер и компјутерска технологија. Врз основа на тоа се појавуваат и различни видови на кривични дела.[62]

Според ФБИ - Федералното Истражно Биро, кривични дела поврзани со компјутер и компјутерска технологија се: различни видови измами и перење пари, економска шпионажа, детска порнографија, туризам заради сексуална злоупотреба на деца, проституција, и поттикнување на малолетници да се занаимаваат со проституција, извршување недозволени трансакции во било кој дел од светот, продажба на артикли регулирани со прописи, превари во врска со хартии од вредност преку Интернет, употреба на пристапни уреди за измами и слични активности.

[62] „Medjunarodni vodic za borbu protiv kompjuterskog kriminala“, Amerikanska advokatska komora, 2003.стр.73.

4. Извршители, методи и средства за вршење на компјутерски криминал

Компјутерскиот криминал е многу сложена активност и за разлика од другите видови криминал бара поголема мисловна активност, поголема интелигенција и поголема концентрација, за разлика од физичката која е потребна за секој друг вид.

За изведување на компјутерски криминал е потребна поголема интелигенција, затоа што е потребно да се знаат голем број програми и шифри, посебно ниво на концентрација и внимание и усовршени компјутерски вештини.

Извршители на компјутерски криминал може да бидат од најрана возраст, уште од основното образование, од различни социјални слоеви, со различна материјална и финансиска позадина.

Бројот и видот на досега познатите компјутерски престапи се уште не дозволуваат да се формулираат конечни ставови за типовите на нивните извршители [63], сепак веќе може да се утврди дека по правило овде се среќаваат високо квалификувани стручњаци во оваа област, кои според природата на својата работа најчесто се наоѓаат во позиција на доверба и од нив не се очекува дека ќе направат нешто што не е дозволено со закон и нешто што може да наштети на фирмата во која се наоѓаат или било која владина или невладина организација.

Веќе, само по себе е тешко да им се влезе во трага на извршителите на овој вид криминалитет, а особено тешко е тогаш кога се работи за поединец, што е правило на подрачјето на манипулациите со податоци и програми. По поединците потешко се трага, тешко е да се откријат нивните активности, тешко е да се влезе во трага на нивните компјутери, затоа што тие знаат како најсоодветно да си ги заштитат своите компјутери и како најсоодветно да си ги прикријат трагите од сопствените активности.

Додека, пак во поново време се почесто се случува, извршителите на вакви кривични дела да се организираат и тоа од било кој дел од светот, без да стапат во лични контакти, но си ги разменуваат искуствата и знаењата, за се поуспешно остварување на своите цели, а оставајќи што е можно помалку траги зад себе.

---

[63] „Компјутерски криминалитет“, Н.Тупанчевски, Годишник на правниот факултет, Скопје 1991, стр.203.

Притоа, мора да се додаде дека најчесто се работи за почетници кои порано не биле казнувани и на работното место случајно нашле погодна прилика за извршување на наведените манипулации. Недостигот на финансиски средства во приватниот живот, во најголемиот број случаи била главната причина за вршење на престапи од ваков вид.

4.1. Извршители на кривични дела поврзани со компјутери и компјутерска технологија

Извршителите на кривични дела поврзани со компјутер се појавуваат на различни места, во различни услови, од различни причини. Извршители на компјутески криминал, најчесто се личности кои имаат прилично високи познавања од областа на компјутерите и компјутерската технологија.

Извршителите на кривични дела поврзани со компјутери и компјутерска технологија, ваквите активности ги извршуваат, главно заради докажување во информатичката средина, а потоа заради финансиска и материјална корист или заради остварување на некои други идеи.

За извршителите на кривични дела од овој вид, постојат и специфични називи, меѓу кои доминираат: хакери, крекери и фрикери. [64]

♦ ***Хакерите*** се лица кои неовластено влегуваат во туѓи компјутери, компјутерски системи и компјутерски мрежи и притоа не остануваат само на тоа што неовластено ќе влезат. Тие вршат измени на податоци, ги крадат податоците за користење во свои цели или едноставно уништуваат некој дел или цел компјутер или систем.

Тоа обично се, млади лица на возраст од 15 до 30 години, кои со часови седат пред своите компјутери, соочени со предизвикот да ги откријат софтверските тајни и да дојдат до таков фонд на знаења кој за нив во прв ред значи определено докажување, односно престиж меѓу другарите и поширокаата околина, а подоцна тие способности може да ги претворат и во

[64] „Криминологија“, З.Сулејманов, Графос, Скопје,2007, стр.143.

добра материјална заработка и своите услуги да ги нудат од самостојни персонални компјутери во домаќинствата до компјутери и компјутерски мрежи во помали или поголеми компании па се до држави и владини институции.

Хакерството[65] прв пат е забележано во 1969 година, кога го напаѓале тогашниот систем. Тогаш хакерите се собирале и секој ги изнесувал своите идеи, а потоа тимски ги разгледувале сите опции. Нивното внимание во тоа време најмногу било насочено кон телефонските централи.

Една од подеталните дефиниции за хакерите е онаа на веб страната Webopedia, во која е наведено следново: „ ***Хакер*** – жаргон за компјутерски ентузијаст. Меѓу професионалните програмери, зборот „хакер", значи аматер или програмер кому му недостига официјална обука. Во зависност како е искористен зборот, може да биде пофалбен или навредлив.

Хакерите се личности кои добро ги познаваат компјутерите, нивниот хардвер и нивниот софтвер. Поприфатено и пошироко значење на овој збор, благодарение на медиумите, е дека тоа се индивидуалци кои успеваат да добијат недозволен пристап до компјутери или компјутерски системи, со цел да украдат или уништат важни податоци. Хакерите објаснуваат дека точниот збор на таквите издивидуи е Cracker". [66]

Хакерите, секогаш се подготвени за навлегување во зоната на забранетите дејства во врска со користењето на туѓите податоци и програми без разлика дали тие имаат некоја витална важност или не. Најчесто се повлечени личности, затворени во себе и недружељубиви за околината, кои бегаат од себеси во светот на компјутерските системи и компјутерските мрежи. Самите си измислуваат псевдоними преку кои се препознаваат во виртуелниот свет, кај нас најчесто делуваат како поединци, но во западните земји и пошироко се почесто се групираат во групи и меѓусебно си помагаат во остварувањето на ваквите активности. Разменуваат знаења и вештини до кои стигнале со сопствен труд.

Денес, кога корпоративните системи изобилуваат со чуствителни и доверливи информации, банкарски податоци, хакерите се опишуваат како вистински специјалци, кои сакаат профит, а нивните вештини се достапни на црниот пазар, за оној кој најмногу може да

[65] http://hr.wikipedia.org/wiki/Hakeri
[66] http://www.webopedia.com

понуди, а дури постојат информации дека зад најпрофитабилните и најисклучителните хакери стои дури и руската мафија.[67]

Меѓусебната комуникација, исто така е специфична, односно користат жаргонски термини, кои не се специфични за секојдневната комуникација. Нивната филозофија е да се најдат слабите страни на компјутерите и компјутерската технологија, да се откриваат лозинки за да се навлегува во секакви програми, Интернет страни или дури и големи корпорации.

Основата на хакерството е пробување и откривање, како што велат и самите хакери, денес постојат многу добри „алатки" наменети за скенирање на компјутерите и компјутерските мрежи и за автоматско откривање на нивните заштитни шифри. Тие, таканаречени алатки, хакерите ги откриваат, ги разработуваат и меѓусебно ги разменуваат, за потоа да ги усовршат или само да ги искористат во сопствени активности.

♦ За разлика од хакерите, кои се најраспространети и најбројни, постои и друга група на компјутерски криминалци, наречени ***крекери***.

Крекерите, се компјутерски криминалци, кои се техновандали, тие провалуваат во компјутери и компјутерски системи, со главна цел да предизвикаат штети на тој компјутер или на целиот систем, да украдат важни и доверливи информации или да извршат компјутерски измами од секаков вид. Тие се информатички занесеници, чие навлегување во компјутерите и компјутерските системи е исклучиво за да нанесат штети.

Крекерите се делат во три групи и тоа:

- **бели** (личностите кои своето знаење го користат за тестирање и подобрување на програмите, соработувајќи со производителите на софтверски делови);
- **црни** (криминалци, кои намерно ги уништуваат системите);
- **сиви** (комбинација од белите и црните крекери).

Називот крекери[68], го превзеле од христијанско верско движење, но идеите и активностите се сосема различни. Компјутерските крекери не се занимаваат ниту со верски, ниту со религиозни проблеми, тие само го користат името.

---

[67] http://www.catb.org/-esr/faqs/hacker-howto.html (17.07.2009)

Крекерите навлегуваат во компјутери и компјутерски системи, зафаќаат одредени фајлови и постепено ги уништуваат или им ги менуваат својствата, така што ја пренасочуваат нивната работа во своја корист.

На нападите на крекерите се изложени буквално сите, предизвикувајќи различни проблеми на компјутерите. Тие не бираат дали нивна жртва ќе биде компјутер на поединец или на некоја важна компанија. Најголемо задоволство на крекерите е, кога ќе успеат да навлезат или да дејствуваат во компјутерски систем или мрежа на некоја добро чувана и обезбедувана компанија или институција.

Тие себе си се сметаат за посупериорни од другата популација, а со криминалните активности сметаат дека напарвиле некакво добро дело, остварилe некаква предност, која обичните луѓе никогаш нема да ја постигнат.

- ***Фрикерите***, се компјутерски криминалци кои се претходници на квекерите. Тие се познати по тоа што нивната активност е ограничена само на одредени сегменти од општественото живеење, односно на телекомуникацискиот и информатичкиот сообраќај.

Нивната првобитна активност била да пробиваат во компјутери и компјутерски системи со цел да украдат телефонски импулси, а во поново време се почесто се краде и интернет сообраќај.

Тие уште во седумдесеттите години на дваесеттиот век успеале да пронајдат начин како да ги користат бесплатно телефонските импулси од тогашните телефонски централи, да остваруваат комуникации во било кој дел од светот и да направат големи финансиски штети за тие компании. Исто така, успевале да ги прикријат тие пробивања за подолг рок, со што ги отежнувале активностите на компаниите во нивното откривање и спречување на понатамошни дејства.

Нивните активности најчесто се насочени кон компаниите што даваат телекомуникациски и Интернет услуги, во поретки случаи кон поединци и организации.

Овој вид на компјутерски криминалци поседуваат исклучителни знаења во врска со телекомуникациските системи и постојано се усовршуваат на тој план. Знаат на кој начин функционираат овие централи, добро ја познаваат целосната хардверска и софтверска

[68] http://hr.wikipedia.org/wiki/Kvekeri

структура на телекомуникациските централи и со нивните вештини успеваат да ги пробијат безбедносните лозинки и да ја насочат работата за сопствена корист.

Фрикерите преку своите активности успеваат да направат огромни финансиски штети на телекомуникациските компании, а притоа многу е тешко навремено и ефикасно да се откријат нивните активности.

4.2. Начини за вршење на компјутерски криминал

Компјутерскиот криминал се извршува на многу специфични начини, со методи и средства кои тешко се детектираат при различните упади во компјутерите и компјутерските системи, а уште потешко се спречуваат нивните активности.

Во извршувањето на компјутерскиот криминал е специфично тоа што, не се користи никакво оружје, не се потребни никакви договори, стратегии, тактики, потребно е само една личност и еден персонален компјутер.

Според специфичните називи на извршителите на компјутерски криминал, се истакнуваат и соодветни називи на начините на извршување на компјутерскиот криминал, како што се: хакирање, кракирање, фрикирање, фишинг.

- Под терминот ***хакирање***, [69]се подразбира активност на програмерите во истражување на границите на компјутерите и компјутерската технологија. Тука е опфатено се: од игри, бизнис апликации, надземни и сателитски комуникациски системи и секаков вид на мрежна работа, до регулирање на работата на огромни финансиски корпорации.

Генетските корени на се она што денес се нарекува хакерство, може да се лоцираат во шеесетите години на 20 век, период во кој мини компјутерите беа во сопственост на корпорациските монолити со длабок џеб, заедно со телефонските компании. Со малку поголема мотивација од тоа да заштитат финансиски средства, при телефонски повици, млади деца ги пробиваат телефонските системи. Ова хоби стана популарно и добива свое

[69] "Cyber terrorism-Political And Economic Implications",E.M.Colaric,Idea group publishing,2006,стр.37.

име - phone phreaking (телефонско фрикирање). Набргу потоа, овие млади луѓе, почнуваат да копаат малку подлабоко во мрежите што ги подржуваат трелефонските системи.

Тие беа заведени под називот „crackers“ (кракери), затоа што тие научиле како најдобро да го разберат системот разбивајќи го целосно и разгорувајќи ги неговите пропусти. Употребувањето на зборот хакерство, за да се опише напад врз компјутерска мрежа со цел да се направи пакосна штета, всушност е застранување од неговото оригинално значење.

Хакерството во основа објаснува, како техничките способни тинејџери можат да го доизменат или пробијат програмскиот код, за да ги зајаканат неговите можности. Негативната конотација на овој поим датира од осумдесетите години на 20 век, кога медиумите го искористија овој термин за да опишат некои компјутерски ентузијасти.

Терминот се задржал и денес и се користи како општ поим за нелегалните активности на сајбер – криминалците.[70]

Ерик Рејмонд (Eric Raymond), авторот на „***The New Hacker's Dictionary***“, едноставно инсистира на тоа дека сите оние, кои што разбиваат и влегуваат во нечии компјутерски системи се кракери и хакери. Според него, „добар хак“, е да се најде паметно решение на програмерски проблем, а „хакирање“ е чинот на самото наоѓање. Тој ги навел и главните карактеристики на хакерот.

Листата[71] од пет карактеристики, изгледа вака:

- Личност која ужива во учењето на деталите од еден и повеќе програмерски јазици или компјутерски системи;
- Личност која го прифаќа програмирањето брзо и лесно;
- Личност која може лесно да ги сфати хакерските способности и вештини на некој друг;
- Личност која всушност ужива да програмира, наместо да зборува и да кажува теории за програмирањето;
- Личност која е експерт за некој специфичен компјутерски јазик или систем, на пример UNIX.

[70] http://www.sciencedaily.com/newa/computers-math/hacking (17.07.2009)
[71] "The New Hacker's Dictionary", E.S.Eaymond,The MIT Press Cambridge,Mass London,England, 1993.

Хакерите испитуваат софтвер и системи од грешки, пропусти, слабости и тоа најчесто без дозвола од сопствениците. Тие развиваат решенија за слободна дистрибуција, позната како слободен софтвер и софтвер за распределба.

Една од главните цели на хакерската заедница, е целиот софтвер да биде бесплатен и да може слободно да се користи за секоја потреба, да нема ограничувања за пристап кон веб страни, ниту пак да има ограничувања на пристапот до одредени информации.

Ако ја погледнеме историјата на хакерството, јасно можеме да видиме дека, штом се развие некоја нова технологија таа претставува неодолива привлечност за хакерската заедница. Подемот на организираните хакерски банди и на он-лајн мафијата, која ги подржува нивните активности е загрижувачки тренд.

Во период кога хакерските вештини се достапни на црниот пазар, секој со технички способности лесно може да се вмеша во организиран криминал. Медиското портретирање на хакерската заедница, како примамлива субкултура, е атрактивно за генерацијата израсната во светот во кој доминира технологијата.

Во современиот свет постојат огромен број хакерски банди, дури и деца од најамала возраст ги учат хакерските вештини. Најголема и најопасна хакерска банда е Anonyomous, која покрај бројните достигнувања, како најголем хакерски напад до сега го смета блокирањето на сајтот на ФБИ, со што и официјално објавуваат онлајн војна.[72] Повеќе од 5.000 активисти на групата, дејствувале координирано при блокирањето на веб-страниците на американското Министерство за правда, на Филмската асоцијација на Америка и на Асоцијацијата на музичката индустрија на Америка. Покрај веќе срушените страници, анонимните хакери, најавиле и напади на други цели, како страницата на Белата куќа, но се чини дека се помал е бројот на страници, што тие се уште не успеале да ги срушат. Како повод за оваа акција групата ги наведе лошите закони за антипиратерија, со кои американската администрација ќе може да побара затворање на некоја Интернет страница.

Околу овие закани се уште не е донесен конечен став, но тие може да предизвикаат огромни промени во cyber просторот, може да дојде до затворање на огромен број на страници.

[72] http://www.vest.com.mk/?section=arhiva (02.10.2010)

♦ Називот ***кракирање,***[73]е добиен од англискиот збор crack, што значи пукнатина, распрснување, распукување. Во суштина, се работи за луѓе кои влегуваат во нешто и притоа го распукнуваат истото.

Во основа, кракер е некој кој намерно влегува во нечиј компјутерски систем без дозвола. Ова се случува доста често, во секаков вид мрежи. Целта е одбегнување на лозинки и разни лиценци, што ги побаруваат некои компјутерски програми или пак оперативниот систем. Или пак, понекогаш намерно го уништуваат сигурносниот систем на компјутерите, за да остварат некои свои идеи. [74]

Кракерите најчесто, формираат мали и елитни групи, кои се нарекуваат со грандиозни имиња, како на пример: Легија за осуда (Legion Of Doom), и најчесто во групата има три до четири лица. Тие своето име го превзеле од позната верска и религиозна група, но активностите и идеите им се сосема различни и не се подударааат во ниту еден сегмент, Кракерите остварувајќи одредена цел можат да нарушат други систем, само од љубопитство, без да имаат некаква намера.[75]

Кракирањето претставува искористување на одредени грешки во системот и нивно користење за сопствени цели. Откривањето на ваквите грешки, се главната активност на кракерите и користењето на овие грешки во менување или уништување на системот, крадење на податоци, користење на апликации од системот за свои цели и спроведување на голем број други активности.

Најчести грешки,[76] кои доведуваат до опасни последици за компјутерот или компјутерските системи, а што најчесто ги прават почетници, односно оние кои не се доволно упатени во компјутерите и компјутерската технологија се:

- Конектирање на тест системи на интернет со default accounts/ passwords;
- Не правење на update на системот кога ќе се откријат сигурносни дупки;
- Користење некриптирани протоколи за работа на компјутери, рутери и огнени ѕидови;
- Давање на лозинка по телефон или електронска пошта;

---

[73] http://dmor.org/computers/hacking (17.07.2009)
[74] [74] "Cyber terrorism-Political And Economic Implications",E.M.Colaric,Idea group publishing,2006,стр.45.
[75] "Investigating Computer-related Crime",P.Stephenson,CRC PRESS,2002, стр.93.
[76] http://www.brighthub.com/engineering/civil/articles/47197.asph (08.07.2009)

- Ненавремено обновување на антивирусниот софтвер;
- Неедуцирање на корисниците, на што да внимаваат и што да направат при евентуален, можен сигурносен проблем.

Кракерите лесно и брзо се откриваат, затоа што тие не сметаат дека направиле нешто лошо и најчесто нивните искуства јавно ги изнесуваат на форуми.

Тие своите активности ги сметаат за свои спствени успеси и затоа бараат погодни начини да ги истакнат тие успеси.

Тие сакаат компјутерската, а посебно хакерската јавност да ги знае нивните достигнувања и да ги бара нивните услуги. Многу поретко кракерите работат за материјални придобивки, а почесто за слава и престиж во информатичкиот свет. Следењето на форумите од ваков вид допринесуваат до најдобро следење и откривање на кракерите и нивните дејства.

♦ ***Фрикирањето,*** како начин на остварување на компјутерски криминал, подразбира навлегување во компјутери и компјутерски системи заради одредена материјална корист. Односно, навлегување во компјутерски системи на телефонски и интернет провајдери, заради кражба и неограничено користење на нивните услуги.

Фрикирањето било почесто застапено во подалечната историја на информатичкото општество, во денешно време тоа е се по проширено и разнесено во сите области на човековото живеење, не само во светот на комуникациите.

Најчест пример во минатото биле кражбите на телефонски импулси, а во поново време и се среќава и забрзување и зголемување на Интернет сообраќајот. Најголеми успеси на фрикерите биле кога ќе успеат да ги искористат услугите на телекомуникациските компании бесплатно, а со тоа нанесуваче огромни финансиски загуби на тие компании. Денес, тоа се почесто им се случува на гоелмиот број на Интернет провајдери, каде тие се јавуваат како жртви, но честа е појавата жртви да бидат и индивидуалните корисници, како и комапниите кои ги користат услугите на тој провајдер.

Компјутерскиот криминал посебно се однесува на пресретнувањето на информациите и податоците во сајбер просторот.

Потенцијални ризици, од пресретнувањето на информациите се: [77]

- Откривање на информации за сопственикот и осетливи информации;
- Опасности за репутацијата на организациите и вредноста на имотот;
- Прераспределба на ресурси;
- Прекинување на работните операции;
- Одговорност, заради пресретнување на информации.

За да постои ефикасна и безбедна размена на информации, најчесто државите донесуваат и соодветни закони, кои се најважните мерки за заштита на податоците во сајбер просторот. Закони од оваа област се, законите против монопол, потоа законите за слободата на информирањето, закони кои ја заштитуваат приватноста на податоците, закони за пуштање на информациите во промет, закони за заштита на информациите за кои некој поседува авторски права.

♦ ***Мрежно рибарење*** (или ***фишинг***, од англ. *phishing*)[78], е поим што се користи кога се работи за присвојување на идентитетот на легитимната организација или мрежно место, употребувајќи фалсификувана е-пошта, односно е-пошта и/или мрежна страница.

Фишингот се извршува, главно, со цел да се убедат корисниците да ги споделат своите кориснички имиња (usernames), лозинки (passwords) и личните податоци (име, броеви на кредитни картички, матични броеви или броеви за социјално осигурување), со цел тие да бидат злоупотребени.

Овој вид на компјутерска криминална активност, исто така, се вика и кражба на идентитет. „*Phishing*“ е релативно нов термин, употребен во некои извештаи уште во 1996 година, а во медиумите е спомнат во 1997 година.

---

[77] „Medjunarodni vodic za borbu protiv kompjuterskog kriminala“, Amerikanska advokatska komora, 2003, стр.231.

[78]http://mk.wikipedia.org/wiki/%D0%9C%D1%80%D0%B5%D0%B6%D0%BD%D0%BE_%D1%80%D0%B8%D0%B1%D0%B0%D1%80%D0%B5%D1%9A%D0%B5

При нападите на мрежно рибарење (фишинг), се користи социјален инженеринг и технички трикови, за да се украдат личните и финансиските податоците на корисникот. При тоа најчесто се користи е-пошта, за да се наведат муштериите да посетат лажни мрежни места кои го имитираат изгледот на легитимни брендови, како банки и компании за е-малопродажба или кредитни картички.

Сличен е резултатот и кога се вршат измами преку системи за директен разговор (chat). Хакерите многу лесно успеваат да го пробијат овој систем, да читаат туѓи разговори, да менуваат разговори и пораки, да ги превземаат, но во најлош случај и да ги користат истите, заради стекнување на одредена материјална корист или остварување на било каква друга корист.

4.3. Средства за вршење на компјутерски криминал

Компјутерскиот криминал, покрај многуте други специфики со кои се разликува од останатите видови криминал, се разликува и преку средствата со кои тој се врши.

За разлика од другите видови криминал, кај компјутерскиот криминал не се користат никакви оружја, не се користи физичка сила, се користат само компјутери и компјутерска технологија и соодветни корисници на компјутерите и компјутерската технологија.

Средства за вршење на компјутерски криминал се различните видови вируси, црви, бубачки и слични средства или комбинации од претходно споменатите.

Како најпознато и најчесто користено средство за вршење на компјутерски криминал, ќе ги спомнеме ***вирусите***.

◄ ***Вирусите*** се главното оружје за војување во информатичките војни. Се што му е потребно на еден хакер, за да ја оствари својата цел е: телефон, компјутер, модем и соодветен софтвер.

Хакерите со нивните активности може да предизвикаат огромни промени и да го нарушат нормалното функционирање во општеството. Така, на пример, тие можат да ги саботираат семафорите, со што ќе предизвикаат блокирање на локалниот и на регионалниот

сообраќај, може да влијаат на електродистрибуцијата, врз системите на рафинериите и на нуклеарните централи. Тие, овие активности ги остваруваат со помош на вметнување и вградување на пенетрациски механизми, како што се вирусите (тројански коњи), логички бомби, црви, заклопна врата и сл.

Компјутерските вируси се мали програми, од по неколку килобајти, а имаат исклучива цел да направат штета на заразениот компјутер. Се размножуваат главно така што самите се „вгнездуваат“ во други фајлови, а штетата ја прават така што ги бришат или мениваат фајловите на дискот. Во случај да се работи за информационен систем, вирусот од заразениот компјутер може да побара друг компјутер, во компјутерската мрежа за да му ги измени или оштети фајловите.

Она што е најважно да се знае, заради безбедноста на податоците во компјутерот и за компјутерската мрежа во целина е дека со вирус, црв или со тројанец, компјутерот може да се инфцира на неколку начини:

- преку каков и да било вид на надворешна меморија (CD, USB, Floppy disk, SD card), преку која намерно или ненамерно може да се внесе во компјутерот;
- преку фајлови кои стигнале по електронска пошта;
- преку фајлови симнати од Интернет;
- со посета на некоја веб страна на која е поставен вирус;
- сигурносни дупки, односно безбедносни пропусти во самиот софтвер и оперативен систем со што се овозможува инфицирање со вирус, црв или тројанец.

Намената на вирусите може да биде различна и тоа најчесто според целите заради кои тие и се употребени од страна на некој извршител и се внесени во некој компјутер или компјутерски систем. Најчесто, вирусите се користат:

1) за да оштетат или избришат компјутерски ресурси, како што се програмите на оперативниот систем, кои може да бидат од голема важност за сопственикот на тој компјутер, базите на податоци или апликативните системи;

2) да се украдат тајни податоци од базата на податоци и истите да се пренесат преку неовластени извори, од каде понатаму следува нивна обработка и пуштање во употреба за остварување на одредени цели.

Постојат неколку типови на вируси и тоа: [79]

- фајл инфектор;
- присутен програм инфектор;
- инфектор на секторот за бутирање;
- комбиниран вирус;
- дропер;
- стелт вирус;
- вирус-следач;
- полиморфен вирус;
- мутациски вирус.

♦ ***Фајл инфектор***

Ваквиот тип на вируси дејствуваат врз извршните фајлови. Тие директно навлегуваат во одредени фајлови и ги менуваат апликацците, користејќи .EXE или .COM екстензии[80]. Тој вирус ќе биде активиран кога ќе биде стартувана таа апликација и ќе го прави сето она што ќе му биде командувано. Тие го вметнуваат нивниот код на почетокот на извршните фајлови.

Секогаш кога некоја програма се извршува, различни кодови прават копија од самите себе во друг извршен фајл. Сето ова резултира со огромен број на ново – инфицирани фајлови. Како дополнение, на фазата на реплицирање на вирусот, исто така, постои и акциона фаза. Ова ја опишува штетата што би требало да ја направи вирусот за која бил создаден. Само еднаш откако вирусот се реплицирал самиот во неколку различни фајлови, тој започнува со неговата активност.

Вирусот може да започне да се реализира врз основа на некој иден настан. Вирусот може својата штета да започне да ја извршува, откако би инфицирал однапред одредени типови и број на фајлови. Истото, може да започне да го прави и на некој однапред одреден

[79] „ Investigating Computer-related Crime",P.Stephenson,CRC PRESS,2002, стр.96.

[80] http://glossary.spamlaws.com/definition/f/file-infector.html

датум, или врз некој друг препрограмиран настан по желба на креаторот, во момент кога креаторот ќе го активира самиот вирус.

Овој вид вируси најчесто се зафаќаат преку инфицирани интернет страници и интернет апликации, преку разновидна надворешна меморија, стикови, дискови и сл. И тоа најчесто во .DLL формат. Така да, со самото рестартирање на компјутерот овој вирус ги започнува активностите во инфицираниот фајл.

♦ ***Присутен програм инфектор***

Присутниот програм инфектор започнува со инфицирање на извршните фајлови. Тој е специфичен вид на компјутерски вирус, кој навлегувјќи во одреден фајл во компјутерот не само што ги запира апликациите во тој компјутер или ги менува истите, туку и се вгнездува и во меморијата на компјутерот или компјутерската мрежа и се задржува и се раширува до понатамошно активирање или пак уништување.

Кога извршните веќе постоечки фајлови се повеќе опфатени, вирусот се сместува во меморијата. Од таа почетна точка, се додека компјутерот не е ресетиран, вирусот ќе го инфицира секој извршен фајл што постои во компјутерот. Тој се шири се повеќе и повеќе, опфќајки ги сите фајлови во меморијата.

Присутниот програм инфектор се шири низ сите фајлови на компјутерот без разлика на форматот во кој тие се зачувани. Овој вид на компјутерски вируси доведуваат до блокирање на нормалната функција на одредени програми и апликации во компјутерот, па се до целосно кочење и рушење на оперативниот систем на тој компјутер или дури и цела компјутерска мрежа.

♦ ***Инфектор на секторот за бутирање***

Инфекторот на секторот за бутирање, како компјутерски вирус е мошне специфичен, затоа што ја инфицира главната партиција за бутирање на хард дискот. Откако секторот за бутирање е веќе инфициран, се започнува со инфицирање на секторите за бутирање на кој и да било флопи диск, што ќе биде сместен во флопи дрејвот.

Инфекторот на секторот за бутирање се шири помеѓу компјутерите преку векторот на флопи дискот. Голем број на вируси, посебно оние што се сместени во меморијата ги

преживуваат бутирањата на компјутерот, а со тоа и остануваат вгнездени во одредени фајлови и се пренесуваат преку надворешна меморија и во други компјутери.

Овој вирус навлегува во фајловите на некои програми на хард дискот, потоа со пренос на овие програми преку бутабилни дискови или други видови на надворешни мемории во друг компјутер си ги задржуваат истите својства, односно вирусот го зафаќа и другиот компјутер.

♦ ***Комбиниран вирус***

Ваквиот тип на компјутерски вирус ги комбинира карактеристиките на инфекторот на секторот за бутирање и фајл инфекторот. Може да ги инфицира и двата сектори, и секторот за бутирање на компјутерот или компјутерскиот систем и сите останати фајлови кои се наоѓаат во меморијта.

Овој вид на вируси се многу распространети, тие тешко се откриваат, а уште потешко се чистат и се поправат штетите настнати од нивното дејство. Додека да се забележи нивното присуство, штетите може да станат непоправливи. Комбинираните вируси се многу честа појава и нивниот број секојдневно се зголемува и се појавуваат се покомплицирани вируси кои се се потешки за откривање и за уништување.

Тој во одредена мерка е покомплициран вид на вирус, затоа што е потешко неговото откривање и уништување, а навлегува, буквално во секаков вид на фајлови и зафаќа секакви програми на хард дискот. Потребни се најсовремени антивирусни програми за откривање на ваквиот вид на вируси. Многу честа е појавата да неможат да се уништат овие вируси без притоа да не се направат штети во програмите и фајловите кои се зафатени од нив.

♦ ***Дропер***

Дропери се мали инфицирани фајлови чија цел е, како и на инфекторот на секторот за бутирање, да го инфицираат секторот за бутирање.

Како и нормалните инфектори на секторот за бутирање, кои што инфекциите ги вршат помеѓу дисковите, дроперот, кога се извршува, го реплицира вирусниот код во сопствениот сектор за бутирање.

Дроперите сами по себе, не се вируси. Понекогаш се само мали извршни фајлови без некоја определена функција освен да ги инфицираат секторот за бутирање. Тие во многу случаи може да бидат и безопасни за фајлот или за компјутерот кој го инфицирале.

Многу често таму и остануваат, зафаќајки само простор, без да извршуваат било каква друга активност и без да нанесуваат штети на тој компјутер или компјутерски систем.

Нивното присуство во многу случаи воопшто и неможе да се забележи, затоа што немаат никакви активности. Но, доколку корисникот ја проверува меморијата на хард дискот и забележи дека е зафатена поголема меморија од таа што ја зафаќаат фајловите на компјутерските програми што тој ги користи, тогаш станува збор за дропер. Понекогаш вирусот е скриен во легален програм, притоа инфицирајќи го секторот за бутирање кога програмот ќе започне да се извршува.

♦ ***Стелт вирус***

Стелт вирус, е таков вид на компјутерски вирус, којшто може да се прикрие од детектирање (без разлика дали детектирањето се врши со антивирусни програми или огнениот ѕид на самиот компјутер).

Прикривањето од антивирусните програми и разните сиситеми за заштита на компјутерите и компјутерските сиситеми не е особина на сите вируси. Тоа го можат само посовремени и специјално изработени вируси.

Можноста да се прикрие од детектирање на антивирусната програма во компјутерот, се врши преку еден од следниве методи:

Еден метод, е тој да се „прикачи“, т.е. спречи и заведе процесот на скенирање околу самиот себе. На тој начин, програмот за скенирање никогаш нема да открие дека кодот постои.

Вториот метод, е да се направи копија на код од дел од некоја програма која постои во компјутерот. На овој начин го наведува програмот за скенирање да го скенира легалниот програм на сметка на себе. Стелт вирусите се многу тешки за детектирање, како и да е, постојат неколку слични кои што можат да бидат детектирани од најголемиот број на програми за скенирање.[81]

[81] Investigating Computer-related Crime",P.Stephenson,CRC PRESS,2002, стр.93.

♦ ***Вирус – следач***

Овие вируси – следачи, сами по себе и не се вируси, тие се мали вметнати фајлови, кои имаат различни функции во фолдерите на компјутерот во кој се вметнати.

Вирусите следачи го користат фактот што, DOS ги извршува фајловите по однапред одреден именски редослед . Оттогоаш .com фајловите, секогаш се извршуваат пред .exe фајловите иако го делат истото име па всушност, следачот е едноставно a.com фајл, со истото име, како a.exe фајлот. Оттука, .com фајлот е многу повеќе, отколку само вирус вметнат во мал извршен фајл.

Кога корисникот ќе го стартува програмот, тогаш ќе се инфицира системот. Следачот прво ќе го инфицира својот прв фајл, и потоа ќе се избрише самиот себе, притоа отстранувајќи ги сите докази за своето постоење или изворот на инфекцијата. Од таа причина тешко е неговото следење, а уште потешко е неговото пронаоѓање.

Бришењето и чистењето на ваквиот вид на вируси е многу тешко, потребни се најсовремени антивирусни програми или целосно форматирање на компјутерот и компјутерскиот систем.

♦ ***Полиморфен вирус***

Полиморфните вируси се способни да ја избегнат детекцијата, преку менување на својот облик. Овој вид вируси во трансформацијата не го менуваат својот код, напротив користат пософистицирана форма на енкрипција за тие да се прикријат или маскираат.

Енкрипција (шифрирање, програмирање), претставува процес на редоследно пишување карактери или код, кој содржи клуч и алгоритам, се додека не се дојде до оној вистинскиот клуч за влез во недозволен дел, односно затворен фајл.

Полиморфниот вирус генерира псевдослучаен код, и со него, го енкриптира вирусниот код. Кога програмот ќе се изврши во целост, полиморфниот вирус го користи клучот да се декриптира себеси, така што подоцна е многу тешко да се утврди неговото присуство.

За да се детектираат полиморфните вируси, треба да се детектира процесот на енкрипција, истиот да се спречи и да се започне наопаку за да се декриптира вирусот. Кога вирусот ќе се декриптира, тој ќе постане доследен модел, кој би можел да се скенира и на крајот да биде откриен.

♦ ***Мутациски вирус***

Мутацискиот вирус,[82] всушност не е класичен тип на вирус туку претставува компјутерски програм кој е способен секој вирус да го направи полиморфен и да влијае врз секој вирус кој на било каков начин ќе биде внесен во компјутерот или компјутерскиот систем.

Многу е тешка детекцијата на ваквиот вид вируси, бидејќи ја менуваат својата форма од еден во друг вид на фајлови. Може да се случи ваквиот вид на вирус, да биде внесен во компјутерот во еден формат, а потоа со активирање да ја смени својата форма во сосема друг формат, непрепознатлив за поголем број на антивирусни програми и заштитни sидови на компјутери и компјутерски системи.

Мутацискиот вирус е се почест вид на вируси, хакерите и информатичките експерти се повеќе им посветуваат внимание токму на нив, затоа што нив најлесно ги внесуваат во компјутерите кои им се цел на напад и лесно можат да ги остварат своите цели. Хакерите своите активности најуспешно ги извршуваат токму со мутациските вируси и тоа најчесто без да бидат забележани од страна на сопственикот на нападнатиот компјутер или компјутерски систем.

Особините и структурата на вирусите ќе ги разбереме ако подетално го разгледаме вирусот, т.н. ***„тројански коњ“,*** кој е најзастапен кај компјутерите и компјутерската технологија.

Тој го добил името според прочуениот коњ од Троја, со кој Грците успеале да ја освојат Троја, по десетгодишни неуспешни обиди. Тие го уфрлиле коњот, полн со грчки војници и така успеале да ја освојат тврдината, ист е случајот и со овој вирус. На ист начин

[82] Investigating Computer-related Crime",P.Stephenson,CRC PRESS,2002, стр.99.

со овој вирус може да се влезе во туѓ компјутер, за да се превземат одредени фајлови, да се дојде до некои шифри и сл.

Тројанскиот коњ е дел од софтверот, кој останува во компјутерот, внесен во некои често користени компјутерски програми, тој во голем број случаи може да остане и неактивиран, но во многу случаи прави катастрофални последици за тој компјутер, па и за цела мрежа компјутери и компјутерски системи.

За обичниот корисник, овој програм функционира како што треба, но тој скришно извршува една од следниве постапки:

- краде тајни податоци од базата на податоци;
- модифицира податоци од базата на податоци;
- брише податоци од голема важност од базата на податоци.

Тројанскиот коњ, всушност, не е вирус, бидејќи ниту се умножува, ниту се шири како што го прават тоа класичните вируси. Најголемата опасност е што постојат повеќе типови на тројански коњи и сите имаат различни дејства, тие може да бидат присутно во компјутерот и да не бидат активни. Голем број од тројанските коњи се недостапни за антивирусните програми. Доколку се активираат тројанските коњи, со активирање на некоја од апликациите во кои е вгнезден, може да дојде до катастрофални последици на самиот компјутер, но и на цела мрежа на компјутери.

Најчесто се користи за превземање на одредени податоци од легитимни компјутери, префрлувајќи ги во нелегални компјутери, така што, за да се открие превземањето на податоците е потребно подолго време. Превземањето се остварува од страна на лица кои имаат потреба од тие податоци и тие податоци може да ги искористат за остварување на некои свои цели и интереси.

Последиците може да бидат катастрофални: оној кој успеал да вметне тројанец, може да ги уништи сите документи на компјутерот или компјутерскиот систем, може да го потроши Интернет сообраќајот за сопствени цели, може да нападне сервер на некоја банка или било каква друга институција. Можни се два начини на уфрлање на тројанци, и тоа: преку надворешна меморија и преку Интернет.

„Генетски заснован вирус“ се заснова на генетскиот алгоритам, кој е настанат како резултат на истражувањата во областа на „вештачкиот живот“. Името, го добил преку механиката на природната селекција, преку природната генетика.

Тој претставува комбинација на најспособните преживеани суштества со организирана, но сепак случајна измена на податоците, чија, главна цел е да се формира посилен вирус.

Овие вируси имаат способност за самопоправање, самоводење и самопродуктирање по истите правила како и биолошките системи. Овој систем може да има сопствен систем за имунитет и техника за избегнување од можното фаќање.

◄ ***„Логичка бомба“***,[83] е вирус кој сам себе се активира на одреден ден, во одредено време, или во моментот кога се одвиваат одредени случувања. Тие претставуваат програма во програма.

Овој вирус може да биде програмиран да биде мирен со недели, месеци па дури и години. Овој вирус не може да се размножува, но може да предизвика резови и да превзема податоци. Типична логичка бомба чека одреден настан , скриена во одредена програма и има деструктивно дејство кога некој ќе ја активира таа програма.

Како и да е, со новите генерации на компјутерски базирани апликации, како на пример Power – builder, SQL Server, Visual Basic и други, кои својата примена ја наоѓаат во големите организации кои сакаат да развијат сопствени апликации, се отвараат голем број на можности во компјутерската средина.

◄ ***„Црв“***,[84] е дел од софтверот кој се движи низ само еден компјутерски систем, или низ компјутерска мрежа и притоа врши манипулирање, менување или уништување на податоците или програмските кодови, онаму каде што ќе се добие пристап. Црвите се многу опасна појава за компјутерите, може да уништат или да сменат било какви податоци.

Црвот не се умножува, туку се движи наоколу предизвикувајќи штета на својот пат. Дури и да се забележи неговото присуство, црвот може да го избегне фаќањето. Голем број вируси имаат вградено црви во себе.

---

[83] http://www.telh-faq.com/logic-bomb.shtml (12.07.2009)
[84] http://www.microsoft.com/security/worms/conficker.aspx (03.09.2009)

◄ ***„Заклопна врата“,*** овозможува посебен пристап до оперативниот систем на хакерот. Може намерно да се постави во оперативниот систем на главниот компјутер, од мрежата компјутери, за да им се овозможи на системските програмери да ги отстранат грешките во оперативниот систем ако работите почнат да се движат погрешно.

„Заклопната врата“ може да се користи за да се постигне незаконски пристап до тајните податоци во базата на податоци или програми во библиотеката на компјутерските програми или да се вметне пенетрациски механизам во оперативниот систем за да се саботираат базите со податоци или библиотеката со програми, било преку тајно модифицирање или бришење.

Претходно споменатите вируси се најчести видови, но бројот на вируси во сајбер светот, е огромен и никогаш неможе точно да се утврди, затоа што секојдневно настануваат нови видови, пософистицирани и потешки за откривање.

Секојдневно се зголемува бројот на компјутерски експерти и хакери, а со самото тоа се зголемува бројот на проблеми во компјутерската технологија. Сите овие, настојуваат да ги истакнат своите знаења и способности во компјутерскиот свет, да навлезат и да срушат компјутерски системи кои се многу добро чувани и обезбедени.

Затоа, во делот што следува ќе се обидеме да ги откриеме различните начини на откривање на коомпјутерски криминал и можностите за заштита на компјутерите и компјутерската технологија, од различните вируси и напади, кои може да предизвикаат огромни штети.

5. Можности и начини за откривање на компјутерски криминал и мерки за заштита

Компјутерскиот криминал е многу сложен процес, затоа што се врши врз компјутери и компјутерски системи и со помош на компјутери и компјутерски системи. Од тука произлегуваат и потешкотиите за негово навремено откривање и превземање на соодветни мерки за негово спречување. Во карактеристиките на компјутерскиот криминал не спаѓаат само типот на нивните извршители.

Во оваа смисла, во прв ред треба да се истакне перманентноста во вршењето на овие кривични дела, односно се повторуваат. Имено, доволна е една манипулација за потем кривичното дело автоматски да се врши, толку долго додека се наоѓа во употреба нападнатата програма.

Следната специфичност е временското несеопфаќање на актот и делувањето. Ако некој програм е долго во употреба, извршувањето на кривичното дело може да трае со месеци и години. Со тоа нужно е поврзана и висината на штетата, која по правило далеку ги надминува штетите кај некои други дела.

Феноменологијата и обемот[85] на овие кривични дела не се докрај познати, зашто не е можно да се утврдат со криминалните статистики, но со оглед на горенаведените начини на поведение може слободно да се каже дека засега се непроценливи. Оттаму, како и поради природата на работите во оваа сфера на криминално делување, во идните криминолошки истражувања мора да се води сметка за тоа дека темната броја е исклучително голема и се покомплицирана за откривање.

Од голема важност е и начинот на обезбедување на правна помош за решавање на проблемите кои се однесуваат на компјутерски криминал. Затоа, мора да постојат и домашни, регионални и меѓународни иницијативи.[86]

---

[85] „Криминологија“,З.Сулејманов,Графос,Скопје,2007,стр.62.
[86] „Medjunarodni vodic za borbu protiv kompjuterskog kriminala“, Amerikanska advokatska komora, 2003,стр.102.

Еден од наједноставните начини да се обезбеди правна помош, е да се одреди делото околу кое се врши истрагата, со што им се овозможува на властите да соработуваат на неформална основа, да заштедат време за успешно откривање на сторителите и нивно казнување. А, со регионалните и меѓународните претреси пак, се избегнуваат долготрајни и комплицирани процеси, кои може да излезат во многу пошироки рамки, отколку што е познато досега во историјата на компјутерите и компјутерската технологија.

5.1. Можности и начини за откривање на компјутерски криминал

Употребата на компјутерите и Интернетот, за извршување на традиционални облици на криминал покренува значајни и тешки проблеми во нивното откривање. До овие проблеми може да дојде поради единствената природа на доказните материјали, кои се меморираат во компјутерите и се пренесуваат во мрежи, и поради леснотијата со која овие податоци се создаваат, меморираат, копираат и се пренесуваат.

Ваквите проблеми бараат од компјутерската форензика и другите истражни можности да се насочат поголеми и посовремени средства и технологии и да се усоврши обуката и образованието на кадрите.[87]

Затоа, најдобро е да се ревидираат закони со кои се регулираат овластувања кои се даваат на органите на редот. Секоја ревизија треба внимателно да се разгледа за да се процени вистинската потреба за таквите дополнителни мерки, можности за нивна злоупотреба и нивното можно влијание на другите важни општествени вредности.

Како начини за откривање на компјутерски криминал ќе ги наведеме начините кои ги користат легитимните органи на редот во една држава. Порастот на компјутерскиот криминал, значајно влијае врз способноста на органите на редот да спроведат истрага за ваквиот вид кривични дела.

Тие мора да бидат во тек со технолошките достигнувања во врска со компјутерскиот криминал, треба да обрнат внимание на влијанието на компјутерските доказни материјали и

[87] „Medjunarodni vodic za borbu protiv kompjuterskog kriminala“, Amerikanska advokatska komora, 2003,стр.205.

информатичко – компјутерската технологија во традиционалните кривични дела, како што се убиства, грабежи, трговија со дрога, оружје, луѓе итн.

Компјутерските кривични дела, пред надлежните органи поставуваат, три главни вида на проблеми:

1. ***Технички проблеми,*** предизвикани со брзи промени на технологијата и невозможноста на органите на редот да бидат во тек и техничките недостатоци кои го отежнуваат пронаоѓањето и кривичното гонење на компјутерските криминалци.
2. ***Правни проблеми,*** предизвикани од пречките на правната постапка, и невозможноста правните облици во целиот свет да ги следат технолошките откритија, како и работната средина која постојано се менува.
3. ***Оперативни проблеми,*** предизвикани од недостаток на опрема, обука и адекватна организациона структура и потребата да се работи со голема брзина без оглед на временската зона, јазикот и културните разлики.

Заради решавање на овие проблеми, државните органи постојано мораат да посветуваат внимание и средства на обука на кадрите во истражните и форензичките техники.

Борбата против компјутерскиот криминал, исто така бара нов партнерски однос помеѓу приватниот и општествениот сектор, за да се овозможи органите на редот да се спротивстават на предизвиците на криминалот со висока технологија. Таквите партнерства треба да се засноваат на размена на информации, соработка и заедничка работа, се со цел одржување минимални стандарди на глобален план.

Органите на власт мора брзо да реагираат за криминалците да не бидат во предност. Потребен е централизиран, координиран пристап во распределбата на ресурсите за технички средства, обука, помош на лице место и истражувачка работа.

Десет најважни приоритетни потреби кои можат да се решаваат на државно ниво, за да се подобри можноста органите на редот да се борат против компјутерскиот криминал се:

1. Да се подигне нивото на свест на јавоста за појавата и влијанието на компјутерскиот криминал;
2. Да се подобри собирањето на податоци, анализи и пријавување на компјутерскиот криминал;

3. Да се истакнат единствени курсеви за обука и сертификација;

4. Да се основаат оперативни единици за електронски криминал, со способности на делување на регионално и на државно ниво;

5. Да се ажурираат правни облици во согласност технологијата и меѓународните закони;

6. Да се оствари подобра соработка со индустријата на висока технологија;

7. Да се постави централен регистар и место каде што можат да се добијат податоци поврзани со компјутерски криминал;

8. Подобро да се запознае раководството со трендовите и потребите на компјутерскиот криминал;

9. Да се дојде до современи истражни и форензички средства;

10. Да се следат најдобри начини на работа во основање на единица за електронски криминал.

Многу земји, активностите на владата на САД, во областа на компјутерскиот криминал ги сметаат како вреден пример и настојуваат колку што е можно повеќе да го следат тој пример, да ги искористат досегашните сознанија. Исто така, многу мултинационални организации се занимаваат со компјутерски криминал, меѓу кои Советот на Европа, Групата 8 и Обединетите Нации, Федералното Истражно Биро, Европската Полиција, имаат водечка улога.

Конвенцијата на Советот па Европа, е првиот мултилатерален договор кој се занимава со многу правни и процедурални бариери и пречки со кои се соочуваат органите на редот и обвинителите во тек на решавањето на проблемите од компјутерски криминал.

Со оваа Конвенција, од земјите потписнички се бара да соработуваат и да пружат навремена правна помош во тек на собирањето и чувањето на доказниот материјал, како и во истрагата и судското гонење на компјутерскиот криминал.

Покрај сите напори, на меѓународните активности им недостасува координација меѓу органите засегнати со ваков вид на проблеми, а постојат и голем број потешкотии во правните системи и непостоење на голбална правна рамка, без која е многу тешко да се продолжат понатамошни ефикасни активности.

5.1.1. Форензички истраги за откривање на компјутерски криминал

Во текот на 1984 година, ФБИ (Федерално истражно биро – САД), започнало со развој на лабораторија и програма за испитување на компјутерски докази, која потоа прераснува во единствената CART (Computer Analysis and Response Team), кој подоцна е формиран во голем број организации на САД.[88]

Во 1997 година, пак е формирана Меѓународна организација за компјутерски докази IOCE (International Organization on Computer Evidence), во чии рамки се дефинира поимот дигитални докази.

Во рамките на оваа организација се формирани две работни групи и тоа: TWGDE (Tehnical Working Group for Digital Evidence), и SWGDE (Scientific Working Group for Digital Evidence), чии членови се судски органи, експерти и научници.

Во 1999 година, ФБИ помогнал во развој на уште една работна група, наречена SWIGT (Scientific Working Group in Imanging Technologies), чија главна задача е олеснување на правосудните органи при собирање на дигиталните докази, складирање, процесирање, анализа, пренос и излезен формат.

Врз база на специфичностите на техниките, алатите и методите на истрагата во форензичката пракса се дефинирани следните главни области на дигиталната форензика:

- форензика на компјутерите (активизација и анализа на хард дискови и разни видови преносни мемории);
- мрежна форензика (упади во мрежи, злоупотреба итн.);
- активна (жива) форензика на системот (компромитирани хостови – сервери, злоупотреба на системи итн.).[89]

---

[88] Milosavljevic.M, Grubor,G. " Istraga kompjuterskog kriminala, metodolosko – tehnoloske osnove", Univerzitet Singidunum, Beograd, 2009, стр.21

[89] Milosavljevic.M, Grubor,G. " Istraga kompjuterskog kriminala, metodolosko – tehnoloske osnove", Univerzitet Singidunum, Beograd, 2009, стр.22.

Корисници на компјутерската форензика, во денешно време се:

- полиција,
- војска,
- правосудни органи,
- фирми кои професионално се занимаваат со опоравување на податоци од компјутерите,
- корпорации за управување со компјутерски инциденти.

Главни поими кои се користат во компјутерската форензика се: дигитални докази, активизација на дигитални докази, објекти на податоци, физички предмет, оригинален дигитален доказ, дупликат на дигитален доказ, копија на дигитален доказ.

Дигиталните докази се сите информации кои имаат докажувачка вредност во компјутерските форензички истраги. Дигиталните докази се или зачувани или пренесени во бинарна (дигитална) форма. Дигиталниот доказ вклучува, дигитални аудио и видео уреди, мобилни телефони, дигитални факс машини и сл. Дигиталниот доказ е информација ускладена и пренесена во бинарна форма на која судот може да се потпре и да ја искористи во докажување на случајот.

Активизација на дигиталните докази, започнува кога податоците и информациите се соберени за потребите на истражувањето. Податоците треба да ги собира некој што е овластен од судот, процесот на собирање да биде легален и во согласност со законските норми и регулативи.

Објекти на податоци, се податоци придружени со физички елементи и имаат докажувачка вредност. Тие може да се појават во различни формати, но не смее да се менува вредноста на информациите.

Физички предмет, предмети во кои може да бидат сместени податоците или предмети со кои тие податоци се пренесени.

Оригинален дигитален доказ, докази придружени со физички материјал, зачувани на хард дискови, различни видови на надворешна меморија и тие имаат докажувачка вредност, одземени во време на истрагата.

Дупликат на дигитален доказ, прецизна дигитална репродукција на сите податоци што ги има во оригиналниот дигитален доказ.

Копија на дигиталниот доказ, прецизна репродукција на информациите кои се содржани во оригиналниот физички предмет, независно од оригиналниот физички предмет.

Кога се формализираат стандардните оперативни процедури во компјутерската форензика, треба да се вклучат следните елементи: [90]

→ Наслов – треба да содржи точно име на процедурата;
→ Намена – зошто, кога и кој ќе ја користи таа процедура;
→ Опрема, материјал, стандарди, контрола;
→ Опис на процедурата;
→ Калибрација – секој чекор што ќе се превземе;
→ Калкулација – секоја математичка операција што ќе се користи во процедурата;
→ Ограничувања;
→ Сигурност – на целата процедура;
→ Референци – сите документи кои ќе се користат.

Генерално, во дигиталната форензика на компјутерскиот систем , потенцијални извори на дигитални докази може да се најдат во бројни хардверски и софтверски компоненти на системот:

◦ Хард диск, магнетна лента, надворешни (подвижни) мемории за складирање на податоци;
◦ лог фајлови на мрежната инфраструктура;
◦ апликации и лог фајлови на безбедносно релевантни случки;
◦ електронска пошта;
◦ содржини од други сервери, заеднички бази на податоци, њеб сервери;
◦ фатен мрежен сообраќај.

[90] Milosavljevic.M, Grubor,G. " Istraga kompjuterskog kriminala, metodolosko – tehnoloske osnove", Univerzitet Singidunum, Beograd, 2009, стр. 26.

Карактеристично е спроведувањето на форензичка компјутерска истрага на активен инцидент, што подразбира фаќање на сторителот на дело. Тоа може да се спроведе додека, напаѓачот е сеуште на мрежата, во тек на директен напад на модемот, во тек на интернет поврзување преку телефонска линија.

Интегрираниот процес на компјутерска, дигитална форензичка истрага се изведува во неколку фази, и тоа:

1. Подготовка (оперативна и инфраструктурна);

2. Фаза на развој:
   - детекција и известување;
   - потврда и авторизација.

3. Истраги на физичкото место на кривичното дело, кои опфаќаат:
   - обезбедување на физичкото место;
   - ревизија на физичкото место;
   - документирање;
   - пребарување и собирање докази;
   - реконструкција на физичкото место;
   - експертско вештачење (анализа).

4. Истраги на дигиталното место на кривичното дело:
   - фиксирање на дигиталното место;
   - пребарување на дигиталното место;
   - документирање на пронајдените податоци;
   - собирање дигитални докази;
   - реконструкција на дигиталните докази;
   - презентација на доказите;
   - проверка на доказите.

Компјутерска форензика на дигитални податоци може да извршуваат само добро обучени експерти од компјутерските и информатичките науки, во најсовремено опремени лаборатории. Форензичката анализа опфаќа, класифицирана анализа на податоците во три

основни дела и тоа: форензичка анализа на софтверот, форензичка анализа на хардверот и форензичка анализа на сајбер просторот и компјутерските мрежи.

При форензичката анализа се користат голем број алати, кои се поделени на софтверски и хардверски форензички алати, кои ги користат форензичките експерти. Овие алатки се многу комплицирани и неможе секој да се служи со нив. Поради тоа и сведочењата и вештачењата на компјутерските кривични дела може да ги изведуваат само компјутерски експерти и лица кои се занимаваат со компјутерска технологија и Интернет комуникации.

5.2. Фактори кои го олеснуваат дејството на компјутерскиот криминал

Компјутерскиот криминал многу тешко се открива поради тоа што сторителите може да бидат илјадници километри оддалечени од местото што е жртва на нивниот напад. Феноменологијата и обемот на овие кривични дела не се докрај познати, па поради тоа неможат да се утврдат криминалните статистики.

Оттаму, како и поради природата на работите во оваа сфера на криминално делување, во идните криминолошки истражувања мора да се води сметка за одреден број фактори што ќе го олеснат дејството на компјутерскиот криминал, а со тоа и да може соодветно да се реагира, за да може овој вид на криминал да се намали или да се спречи во целост.[91]

Како фактори кои го олеснуваат дејството на компјутерскиот криминал ќе ги наведеме: глобализацијата, границите, финансискиот сектор, техничко-технолошкиот сектор, транспорт, измами со идентитет.

- Глобализацијата означува динамичен економски, политички и културен процес, кој е овозможен со развојот на компуникацијата, компјутерската технологија и транспортот, а најчесто е воден од големите корпорации заради освојување на нови пазари. Токму поради развојот на компјутерите и компјутерската технологија и нивното ширење на светско ниво,

[91] „Компјутерски криминалитет“, Н.Тупанчевски, Годишник на правниот факултет, Скопје 1991, стр.210.

односно глобализацијата може да придонесе и до позитивни и до негативни импликации на тој план.

Глобализацијата е процес на осовременување на светот, но овој процес меможат, сите држави да го следат со ист чекор заради нивото на целокупниот развој, што досега е постигнат. Глобализацијата[92] е еден од најважните фактори кој може да допринесе до откривање на различни облици на компјутерски криминал.

- ***.Границите*** во денешниот свет се многу поразлични од порано. Со развојот на компјутерите и компјутерската технологија границите се прошируваат, а во многу области воопшто и не постојат. Со помош на компјутерите и Интернетот, комуникациите се многу полесни и поедноставни, со било кој дел од светот и тоа без разлика дали ке биде пишан текст, аудио или видео пренос. Границите во поголема мера го отежнуваат откривањето на компјутерски криминал, отколку што можат да помогнат. Електронска граница претставува опасност од незаконски дела кои се вршат со употреба на Интернет.

- ***Финансискиот сектор*** е еден од поважните фактори за откривање на кривични дела поврзани со компјутерите и компјутерската технологија.

Финансиите се главната причина поради која се случуваат кривичните дела, па затоа и најчеста жртва на компјутерски напади се банките и големите финансиски корпорации, токму тие треба да бидат многу внимателни во поставувањето на соодветни системи за заштита. Исто така, многу важни се финансиските средства во набавка на современа технологија, со која може успешно да се откриваат и да се спречуваат кривични дела поврзани со компјутери и компјутерска технологија.

- ***Техничко-технолошки сектор,*** исто така е многу значаен фактор за олеснување на откривањето на компјутерскиот криминал, поради фактот дека компјутерскиот криминал се изведува со најсовремена технологија. За изведување на компјутерскиот криминал потребна е најсовремена технологија и технички средства, но истите тие, па дури и поусовршени се потребни за откривање на компјутерскиот криминал.

- *Транспортот* е тесно поврзан со сите претходно наведени фактори, односно тој има влијание и во изведувањето на кривичните дела, но и во откривањето на истите. Како посебен вид транспорт, ќе го споменеме транспортот на податоци и документи, кој со

[92] "Globalizacija ili diktiranje buducnosti", LJ.Bezberovic, Sarajevo,1996, str 65.

современата технологија е олеснет и поедноставен, но постојат огромни ризици при самото вршење на овој вид пренос на информации. [93]

- *Измами со идентитет* се најчести примери на компјутерски криминал. Со помош на компјутерите и компјутерската технологија се откриваат шифри и тајни податоци со помош на кои се зема нечиј идентитет, се пробиваат пин кодови од банкарски сметки, се влегува во витални институции и со сите овие активности се прават огромни штети, како за поединците, така и за општеството во целина.

Најчест пример се фалсификуваните картички, преку кои од банкоматите се вадат милионски суми, со што се предизвикуваат материјални штети, но и се предизвикува чувство на страв и несигурност кај граѓаните при користење на ваков вид на услуги.

5.3. Превенција и заштита од компјутерски криминал

Борбата против компјутерскиот криминал е многу тешка, комплицирана и долготрајна. Голем број од ваквите кривични дела останат и нерасветлени, а криминалците воопшто и не може да се откријат.

Доказниот материјал може да се наоѓа на голем број компјутери и компјутерски системи, кои може да се наоѓаат во повеќе земји. [94]

Исто така, компјутерските криминалци може да користат технологија на шифрирање и друга технологија која ги надминува можностите на државата. Многу е тешко да се докаже вината на криминалецот, а според тоа, тешко е и соодветно да се казни. Како и да е, органите на редот мора да реагираат, тие мора да знаат да одговорат на проблемот предизвикан со компјутерски криминал.

Некои почетни чекори, кои треба да се превземат при превенција и навремена заштита од компјутерски криминал, го опфаќаат следново:

---

[93] http://www.bs.wikipedia.org/wiki/globalizacija

[94] „Medjunarodni vodic za borbu protiv kompjuterskog kriminala“, Amerikanska advokatska komora, 2003,str.163

● Предвидувања за компјутерски криминал може да се откријат во компјутерските оперативни регисми, доколку се чуваат, кои обучениот службеник на органите на редот ќе може да ги искористи за следење.

Доколку хакерот не направил измени во оперативниот регистар, тогаш тој ќе ја покаже точната адреса на компјутерот преку кој е извршен неовластениот пристап. Хакерот може да направи и скокови преку компјутери, за да ја покрие трагата. Податоците за корисникот на компјутерот ги има компанијата која ги дава услугите, односно телекомуникациските и Интернет услугите.

● Можеби ќе има потреба од повици за сведочење, судски *налози*, налози за претрес на давателите на телекомуникациски услуги, односно на напаѓачот, доколку е идентификуван.

● Доколку се установи дека комуникациите ги поминуваат државните мерки, тогаш треба да се превземат соодветни мерки.

● Барањата што се поставуваат мора да бидат јасни и прецизни, да се знае точно што се бара.

● Да се бара од давателот на услуги да ги чува податоците кои може да се искористат како доказен материјал.

● Да се бара помош при утврдување на сведоци и разговор со нив.

● Мора да се добие согласност од жртвата, за доказните материјали што може да помогнат во истрагата.

● За активен надзор потребно е да се добие судски надзор, за прислушкување на телефонски линии, регистрирање повици и фаќање и следење на влезни комуникации.

● Ако е откриен идентитетот на хакерот , треба да се обезбеди налог за претрес на хакеровиот компјутер и друг релевантен материјал.

Од голема важност е пресретнувањето на податоците во промет, во реално време, кое мора да биде под правна контрола поради идентитетот и други податоци на корисниците. Исто така, важно е да се дефинира непосредниот пристап до меморираните податоци со помош на претреси и заплени.

Освен традиционалните компјутерски кривични дела, компјутерските превари и злоупотреби, постојат и многу класични кривични дела кои многу полесно се изведуваат со

помош на компјутер и Интернет. Токму поради овие факти треба да се превземат соодветни методи и техники за заштита од компјутерски криминал.[95]

До проблеми и компликации доведува природата на доказниот материјал, кој се меморира во компјутерите и се пренесува преку мрежите и од леснотијата со која податоците се создаваат, меморираат, користат и се пренесуваат.

Секоја постапка треба внимателно да се разгледа, поради можноста за злоупотреба на одредени податоци и информации и нивното влијание врз важни општествени вредности.

Активностите на органите на редот треба да бидат насочени кон вистинската цел, така што откривањето и спречувањето на компјутерски криминал ќе биде ефикасно и навремено. Интернетот сам по себе не е сигурен, поради тоа што најголемиот број на персонални компјутери користат нелегални оперативни системи кои имаат ниско ниво на заштита.

Во денешно време, Интернет револуцијата, поставува огромни барања пред органите на редот во следење на ваквите кривични дела и нивно откривање, без разлика дали е тоа во локални или меѓународни рамки.[96]

Компјутерите може да бидат вмешани во компјутерски криминал на три начини:

- Може да бидат цел на напад;
- Може да бидат средство, со кое е направено кривичното дело;
- Може да бидат случајно вмешани во кривичното дело и потоа се користат како доказен материјал.

Најважна активност која треба да се превземе за заштита на компјутерските системи е донесувањето на соодветни закони. Земјите кои настојуваат да допринесат за соодветна заштита на компјутерските системи, информатичките средства и критичната инфраструктура, најчесто ги дополнуваат постоечките кривични закони со делови за компјутерскиот криминал, со дополнителни закони и прописи со кои се уредуваат безбедни и електронски трансакции и пренесување на пораки за проверка на идентитет.[97]

---

[95] http://www.cybercrime.gov/unlawful.htm (mart,2007)

[96] „Medjunarodni vodic za borbu protiv kompjuterskog kriminala“, Amerikanska advokatska komora, 2003,стр.124.

[97] http://www2.epic.org/reports/cripto2000

Најчеста грешка, што се прави во ваквите случаи е тоа што, земјите во развој мислат дека ваквите закони имаат сложена структура која ја контролира владата. Сите закони според ОН, ЕУ и САД бараат неутралност во поглед на користење на технологијата, и проверките на идентитетот да се вршат во согласност со законите.

Земјите во развој посебно треба да обрнат внимание и средства кон насочување на информациско-комуникациската технологија кон примена и развој на индустријализацијата, економијата и напредок на општеството.

Најдобри мерки за заштита на компјутерите и компјутерската технологија од недозволени дејства, а што треба да се превземат се:

- Привлекување дирекни странски инвестиции во изградба на инфраструктурата;
- Приватизација и либерализација на провајдерите;
- Привлекување на апликации за обработка на податоци;
- Привлекување нови Интернет компании;
- Користење на информациско-комуникациската технологија за учење од далечина;
- Модернизација на финансиските сектор;
- Унапредување на развојот на мали и средни претпријатија и слични мерки.

На планот на криминалитетот, главна заштита е превенцијата. Притоа, се разбира дека апсолутна заштита од компјутерскиот криминалитет не е можна, како што впрочем не е можна и кај останатите криминални поведенија.

Меѓутоа, со посериозно преземање чекори за заштита на компјутерски системи, особено таму каде што однапред се знае дека со било какво навлегување во нив може да се предизвика огромна штета, може да се претпостави дека последиците можат значително да се ублажат.

Борбата против овој вид на криминално однесување меѓутоа, несомнено мора да се води и на планот на репресијата. Тоа особено се однесува на нашата земја која во поглед на

инкриминациите на неговите појавни облици се уште не заостанува за вистинската заштита од овие дела.[98]

За да не се доведе еден систем во опасност од разни видови закани, криминални дејствија или пак натрапници, подобро е прво тој систем добро да се заштити. Следуваат некој од најраспространетите видови процедури и методи за заштита на компјутерски систем или пак мрежа во рамки на една организација.

Потребна е соодветна класификација на информациите, според соодветното ниво на пристапност, заради заштита на информациите. Според безбедносните правила и прописи, секое нелегално влегување и инцидент би требало да се документира. Потребно е да се изработи и соодветен прирачник, кој ќе содржи упатства за активности и мерки кои треба да се превземат во случај на инцидент.

За успешната заштита на информациите, важно е да се стекнат добри основни работни навики и да се воспостават процедури за оддржување на работните навики. Затоа е потребно да се одберат луѓе кои се потполно адекватни и сигурни за таа работа. Пристапот до информациите, исто така треба да е ограничен и адекватен на доверливоста.

За заштита на компјутерите или пак на цел систем од нелегални и неавторизирани влегувања во нив се користат системи за идентификација и авторизација на корисниците.

Пристапот до компјутер може да биде ограничен, со контролни процедури кои се базираат на различни типови на системи за идентификација и авторизација.

1. Идентификацијата е процедура во два чекора: да се идентификува корисникот и да се потврди идентификацијата. Најпростите системи се базираат само на лозинки. Пософистицираните системи користат картички или биометриски методи во комбинација со лозинки.

- **Системи со лозинки.** Овие системи даваат мерки на заштита од повремени побарувања на податоци, но ретко запираат посериозни напади. Лозинките имаат улога на клуч на компјутерот. Лозинките се креираат по одредени правила, односно треба да се разликуваат од корисничкото име, да биде алфанумеричка и со најмалку 6 карактери.

[98] "Taking up tehnology",Financial Timer,april,2008.

- Систем со картички и нивна поделба. Картичките може да бидат: магнетни со магнетна лента, која содржи доверливи податоци и чип картички кои наместо магнетна лента содржат чип.

2. Авторизацијата е процес кој следува по процесот на идентификацијата, односно со авторизацијата се врши контрола на пристапот до податоците од одреден компјутер или компјутерски систем.

Компјутерските криминалци можат да користат силна технологија на шифрирање и други технологии кои можат да ја надминат моќта на државите. Многу е тешко да се обвини некој за компјутерски криминал, уште потешко е да се соберат соодветни докази за одредено дело. Токму поради овие факти, органите на редот во државата мора да знаат како да одговорат на опасности од компјутерски криминал, посебно кога ќе се утврди дека тој криминал вклучува комуникации или активности на државно ниво или пошироко.[99]

Некои почетни чекори, при откривање на компјутерски криминал, а кои треба да се превземат го опфаќаат следново:

- Заканите од компјутерски кривични дела, најчесто можат да се забележат во компјутерските регистри, кои ги следат органите на редот, почитувајќи го Интернет Протоколот.[100] Идентитетот на корисникот на одреден компјутер може да се најде во Американскиот регистар на броеви на Интернет;
- Да се повикаат соодветни сведоци;
- Доколку случајот ги надминува границите на една држава, соодветно на тоа треба да се превземат соодветни мерки;
- Кога се бара некоја информација, многу важно е користењето на соодветна терминологија и тоа посебно да се внимава од која земја се бараат информации, дали термините се соодветни во таа земја;
- Доколку информациите не се избришани, се бара од давателот на тие информации да ги зачува истите;

[99] „Medjunarodni vodic za borbu protiv kompjuterskog kriminala“, Amerikanska advokatska komora, 2003,стр.77.

[100] http://www.orin.net/tools/whois_help.html

• Потребна е согласност од жртвата за да се добие доказниот материјал, кој може да биде од голема корист;

• Ако е потребен активен надзор, односно секојдневно прислушкување и следење на комуникациите, мора да постои судски налог и голема тајност за спроведувањето на таа постапка;

• Ако е утврден идентитетот на хакерот мора да се добие соодветен налог и да се најде неговиот компјутер и друг доказен материјал што бил користен во криминални дејства;

• Мора да се обрне внимание и на тоа дали е потребна екстрадиција или не, односно дали сторителот на кривичното дело поврзано со компјутери и компјутерска технологија е од државата во која е сторено делото или од надвор.[101]

Непосредни активности за заштита на персонален компјутер или на цела мрежа компјутери се: инсталирање антивирусни програми, back up, огнен ѕид (firewall), систем за детектирање натрапници и сл.

- **Антивирусни програми.** Овие програми го спречуваат инфицирањето на компјутерот и ги уништуваат вирусите. Тие функционираат на тој начин што ги скенираат постоечките фајлови во потрага по код и доколку најдат некој таков да го спречат неговото активирање.

Антивирусните програми имаат база на вирусни кодови, која што ја пронаоѓаат производителите на антивирусната програма. Исто така, потребно е постојано обновување на таа база на вирусни кодови, односно update на програмата. Во денешниот свет, секојдневно се појавуваат огромен број на антивирусни програми, некои поефикасни, способни да детектираат огромен број на вируси, а некои послаби кои се способни да детектираат само одредени вируси.

- **Back up** – Компјутерските системи се осетливи, може да доведат до уништување до важни податоци. За заштитата на системот од целосно губење на податоците, неопходно е да се превземат процедури за правење на регуларни копии на податоците. Копиите од податоците се чуваат на back-up медиум, кој компјутерите најчесто го поседуваат и автоматски ги копираат податоците, или да се копираат на надворешна меморија.

[101] „Medjunarodni vodic za borbu protiv kompjuterskog kriminala“, Amerikanska advokatska komora, 2003,str.170.

- Огнен ѕид (firewall), се користи за заштита на внатрешните мрежи од натрапници и неавторизирано испраќање и примање на информации. Огнен ѕид претставува систем или група од системи кои го контролираат пристапот помеѓу две мрежи. Тој не само што треба да врши контрола на специфични операции, превземање електронска пошта, итн., туку треба и да му отежне или оневозможи на натрапникот или напаѓачот однадвор да пристапи кон внатрешната мрежа. Ваквите системи се реализираат со машински или програмски техники. Рутерите во компјутерските мрежи, ја имаат улогата на машински техники за остварување на огнениот ѕид. За реализација на програмски техники, потребно е поставување на специјални компјутери и специјални програми на истите.

- Систем за детектирање на нелегални влегувања – Покрај огнениот ѕид, има потреба и од систем за детектирање на нелегални влегувања, затоа што огнениот ѕид штити само од надворешни влегувања. Постојат два типа на системи за детектирање: - Статичко детектирање кое бара навлегување на статички податоци за да се детектира необичното однесување во системот; - Детектирање по шема или потпис преку кој се гледаат активности кои се случуваат по некоја шема или прекршување на некои правила.

5.3.1. Заштита од различни видови на компјутерски вируси

Постојат огромен број на вируси и нивниот број е во постојан пораст. Секојдневно се појавуваат нови и се покомплицирани вируси. Нивната точна бројка не е позната, ниту може да биде, затоа што секојдневно се додаваат се понови видови на вируси.

Најчести и најопасни се вирусите наречени тројанци (troyan horse), потоа црви, логички бомби и сл.

◦ ***Тројанците*** се програми, кои доколку се уфрлат во нечиј компјутер, сите шифри ги праќаат преку електронска пошта, или преку надворешна меморија, притоа му се овозможува на испраќачот да може да чита, пишува, брише, менува фајлови на заразениот компјутер, што значи дека може да го користи заразениот компјутер за секакви дозволени или недозволени цели, а сето тоа ќе биде направено без знаење на сопственикот на компјутерот.

Тројанците своето име го добиле по познатиот коњ од опсадата на Троја, која Грците ја напаѓале 10 години, безуспешно. После некоја битка, оставиле дрвен коњ, во кој имало скриени војници пред портите на Троја, во знак на признавање на поразот. Тројанските војници, воодушевени од победата го внеле коњот внатре. Ноќта кога војниците заспале, еден војник излегол од коњот и го отворил портите на Троја, по што таа била поразена.

Името потекнува од огромната сличност со навлегување во туѓ компјутер, да се превземаат фајлови, шифри и слично.

Тројанците[102] се злонамерни програми кои се „маскирани“ како корисни и се прошируваат во компјутерите и компјутерските системи како корисни програми. Тие обично вршат несакани акции во компјутерот и тоа тајно и прикриено. Најчесто такви несакани дејства се: откривање лозинки, откривање банкарски сметки и други податоци, прислушување, навлегување во важни документи и доставување на истите до корисникот на тројанскиот коњ.

Постојат и тројански коњи кои се користат во служба на полицијата за собирање на податоци од корист на службата. Тие во некои држави се легитимни и се користат со судски налог, во некои држави се уште се разгледува ваквата можност, а во некои е одбиено и се смета дека ги нарушува човековите основни слободи и права.

Тројанските коњи се појавуваат во различни форми и облици. Некои од попознатите се: Back Orifice, Netbus, SubSeven, Zenux и уште голем број други видови на тројански коњи.

Последиците може да бидат катастрофални: да се уништи повеќегодишна работа, да се потроши Интернет сообраќајот за сопствени цели, да се навлезе во строгодоверливи организации и институции и да се влијае врз нивната работа, да се вршат различни типови на шпионажа, да се навлезе во серверот на некои банки и да се вршат недозволени трансакции.

◦***Црви.*** Црвите се софтвер кој делува само на еден компјутерски систем и притоа манипулира, менува или уништува податоци. Црвите се мали програми кои најчесто се користат за крадење на доверливи и скриени податоци. Тие вршат огромен број разновидни инфекции на постоечките програми во компјутерот.

[102] http://sr.wikipedia.org/wiki/%D0%A2%D1%80%D0%BE%D1%98%D0%B0%D0%BD%D1%81%D0%BA%D0%B8_%D0%BA%D0%BE%D1%9A_(%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)

Црвот не се размножува, туку се движи наоколу предизвикувајќи штета насекаде по својот пат. Дури и да се открие неговото присуство, црвот може да го избегне фаќањето.

Како најпознат пример, односно користење на црв (worm), за нелегални активности е кражбата на лозинки од Facebook[103]. Со помош на црвот наречен RAMNIT, биле украдени преку 45 илјади шифри на корисници и тоа главно од Англија и од Франција. Оваа случка била во 2010 година, а била откриена од страна на истражувачи на Израелската компанија *Seculert.* Шифрите биле крадени уште при самото вклучување (логирање) на оваа страница.

Овој црв инфицира извршни фајлови на Windows, Microsoft Office, HTML фајлови, каде што се вршат недозволени активности. Овој црв многу брзо се движи низ компјутерските системи и мрежи, така што некои статистики покажале дека за два месеци успеале да се заразат дури 800 000 компјутери.

Социјалните мрежи се најчеста мета на ваквиот вид на вируси. Затоа сите експерти препорачуваат користење на ефикасни антивирусни програми.

◦ ***Логички бомби[104].*** Логичките бомби се кодови кои се внесени во софтверот и влијаат на одредени активности. Овие бомби претставуваат програми во програми кои вршат деструктивни акти врз активен настан. Тие ретко се среќаваат сами, а почесто се стават во комбинација со тројански коњ или со црв.

Најчесто се препознаваат по деструктивната природа. Типичната логичка бомба чека одреден настан, за да може да врши измени во одредена програма. Програмерот може да внесе логичка бомба која постојано ќе брише одредени податоци и апликации за кои смета дека не му се потребни на корисникот. Кај логичките бомби е специфично тоа што може да се определи времето кога и како тие да почнат да дејствуваат.

Поради ефикасна заштита на компјутерите и компјутерските системи од различните видови вируси најважна е превенцијата и навремената заштита на компјутерите и компјутерската технологија од можни напади, затоа што во секој случај е подобро да се заштитат отколку подоцна да се поправаат штетите кои може а бидат катастрофални.

[103] http://www.informacija.rs/Virus/Kompjuterski-crv-Ramnit-ukrao-45000-lozinki-korisnika-Facebooka.html
[104] http://en.wikipedia.org/wiki/Logic_bomb

Заштитата од тројанци опфаќа користење на заштитни програми, односно антивирусни програми, кои мора навремено да се освежуваат, затоа што секојдневно се појавуваат се понови облици на тројанци. Доколку не бидат освежени антивирусните програми може да дојде до непрепознавање на новите видови на вируси и нивно слободно навлегување во компјутерите и компјутерските сиситеми.

Заштитата од тројанци, најчесто и најефикасно се спроведува во три чекори:

- Да не се отвара ниту еден фајл со сомнително потекло;
- Заштита преку STRAT UP, Catalog, MSCONFIG;
- Користење на огнен ѕид – firewall.

Многу важно е да споменеме кои активности треба да се превземат, доколку дојде до инцидент предизвикан од било каков вид на вируси. Иако на системот има инсталирано и огнен ѕид и систем за детектирање натрапници, сепак некој треба да се грижи за него во случај на инциденти. Да се биде подготвен на инциденти, е најдобар начин да се справи со нив.

Некои познати методи за справување на инциденти се состојат од следниве фази: подготовка, детектирање, запирање на ширењето, поправка и проследување на инцидентот.

Најважно е тоа што сите важни податоци во компјутерот мора да се зачуваат на одреден вид на надворешна меморија, за да недојде до штети и нивно губење доколку тој компјутер или компјутерски систем биде нападнат од било каков компјутерски вирус. Секој компјутер, посебно оние што се поврзани на Интернет, мора да имаат инсталирано најнови изданија од било која антивирусна програма, за да можат успешно да се борат со сајбер нападите.

Последиците може да бидат катастрофални: да се уништи повеќегодишна работа, да се потроши Интернет сообраќајот за сопствени цели, да се навлезе во строгодоверливи организации и институции и да се влијае врз нивната работа, да се вршат различни типови на шпионажа, да се навлезе во серверот на некои банки и да се вршат недозволени трансакции.

6. Компјутерскиот криминал и неговите импликации врз безбедноста во современиот свет

Компјутерите и компјутерската технологија се иднината на современиот свет. Во современи услови неможе да се замисли било кој дел од општественото живеење без употреба на компјутерите. Тие се движечка сила на сите држави, институции и организации во светот. Со самото тоа што се застапени во сите области на општественото живеење, ги прават тие области поосетливи на било какви надворешни влијанија.

Компјутерскиот криминал се однесува на компјутерски системи во сите области во животот, од воздушна, железничка, автобуска контрола, до координација на медицински сервиси и национална безбедност. Само мала грешка во работењето на овие системи може да предизвика огромни штети за општеството во целина, па дури и по цена на човечки животи.

Интернетот е многу ранлив поради огромниот број на корисници, отвореноста и слободниот пристап, нерегуларноста, е идеално место за развој на криминалот од секаков вид, затоа што контролата е на ниско ниво или воопшто неможе да се спроведе.

Компјутерскиот криминал е специфичен облик на криминал, затоа што освен во одредени индивидуални компјутери и компјутерски сиситеми, може да се одвива во повеќе институции во државата, но најголемата специфичност е во тоа што овој вид на криминал многу често ги поминува државните граници и добива карактеристики на транснационален криминал. [105]

Овој криминал предизвикува слабости во повеќе области од секојдневното живеење. Овие слабости вклучуваат:

- светски поврзани компјутери и нивни корисници, што ќе предизвика многу поголеми жртви, за разлика од истите активности во компјутерскито систем на една држава;
- широко распространети диспаритети, помеѓу државите и политичкото опкружување, вклучувајќи и компјутерски криминал и недостаток на висок степен на научност на интернационална кооперација за сузбивање и одвраќање на ваквиот вид на криминал.

[105] http://media.hoover.org/sites/default/files/documents/0817999825_1.pdf

Безбедноста на граѓаните, државите и на општествата во современиот свет, се почесто ќе биде загрозувана од криминални дејства чие остварување е поврзано со компјутер и компјутерска технологија.

Тенденциите за во иднина се уште поголема и покомплексна компјутеризација на општеството во целина, меѓу сите институции и организации. Токму поради ваквата меѓузависност и поврзаност меѓу сите институции и организации, истите ги прави уште поранливи и поосетливи на компјутерски криминални дејства.

Институтот за право, наука и глобална безбедност[106], во серијата од годишни сосотаноци во 2008 -2009 година, бил фокусиран на правните, политичките и безбедносните импликации на заканите од компјутерски криминал. Покрај тоа што компјутерската безбедност е важна за секоја држава, таа има големо влијание и во одржување на безбедноста на интернационално ниво, односно глобалната безбедност.

Глобалната пролиферација на компјутерското поврзување, посебно забележувајќи се со порастот на користењето на Интернетот, ги револуционализираше работите на владите, на општествата, на светските комуникации и на спроведувањето на бизнисите.[107]

Во исто време, забрзаниот развој на информатичката технологија, се појавуваат и бројни можности за појава разни облици на компјутерски криминал и компјутерски војни.

Компјутерските оружја[108] (вируси, црви, логички бомби и сл.), најчесто може да доведат до катастрофални резултати доколку бидат користени од криминалци или терористи, како што се на пример:

- Компјутерските натрапници ги пренасочуваат фондовите на банкарските компјутери и корумпираат податоци во банкарските бази на податоци, предизвикувајќи нарушување и паника, па дури до исклучување на банкарските компјутерски сиситеми за да можат да се справат со проблемит;

- Компјутерските натрапници крадат или откриваат доверливи лични, медицински или финансиски информации, за да ги користат како алат за уцени или изнудување и предизвикување на социјална неприфатливост и срам;

- Крадење класифицирани информации од сигурно владини бази на податоци и да се здобијат со податоци витални за националната безбедност, и

---

[106] http://lsgs.georgetown.edu/programs/CyberProject/Cyberwarfare/
[107] http://lsgs.georgetown.edu/programs/CyberProject/Cyberwarfare/EJIL.LotrionteJoyner.pdf, стр. 840
[108] http://lsgs.georgetown.edu/programs/CyberProject/Cyberwarfare/EJIL.LotrionteJoyner.pdf, стр.846

- Терористите бираат авиони за да ги нападнат и со тоа да предизвикаат страв привремено завземајќи го неговиот компјутерски систем, без кој тој не би можел безбедно и нормално да функционира.

Раелните закани од сајбер напади мора фундаментално да биде разработено од интернационалните правни правила. Современите интернационални закони на секоја држава и даваат слобода на интернационалната арена – тоа е сигурно право да бидат слободни, независни и без надворешна контрола и насилно влијание.

Компјутерскиот криминал често води кон разновидни напади на инфраструктурни објекти, со што се предизвикува страв и паника кај населението, но и огромни материјални штети. Некои инфраструктурни објекти може да имаат витално значење во општеството, со самите напади може да се уништат важни документи, податоци, книги, до кои е дојдено со долгогодишен напорен труд и работа и трошење на непроценливи средства. [109]

● Импликациите на компјутерскиот криминал врз безбедноста во современиот свет, посебно се забележуваат преку влијанието на компјутерскиот криминал во ***економскиот сектор.*** Компјутерските напади се реален ризик и потенцијал за криминал кој ќе има огромни размери.[110]

Како илустрација на ова тврдење ќе ја наведеме споредбата со ураганот Ендру во САД, кој бил најскапа катастрофа во историјата на САД, а изнесувала околу 11 билиони долари. Додека пак, „love bug" вирусот, нанел штети на компјутери и компјутерски системи меѓу 3 и 15 билиони долари. Од тука треба да се свати сериозноста на тоа што еден обичен студент од Филипините, користејќи обична, не многу скапа опрема успеал да огромни штети и ја ставил на ризик целосната глобална економија.

Освен од финансиски аспект, сајбер нападите во свои рамки вклучуваат и интелектуална сопственост, финансиски измами, рушење на репутацијата, намалување на продуктивноста и одговорност на трети страни.[111]

Компјутерскиот криминал е сериозна и растечка закана, но штетите и опасностите може да бидат поголеми од можностите на било која држава во светот. Вековен труд во градењето на огромни светски пазари, соработка меѓу разни земји во светот може да бидат срушени за многу кратко време.

---

[109] http://www.steptoe.com/publications/231a.pdf, стр.2.
[110] http://www.steptoe.com/publications/231a.pdf стр.3
[111] http://www.steptoe.com/publications/231a.pdf стр.10

Економскиот сектор, воедно е и најпривлечен сектор во активностите на хакерите, односно на компјутерските криминалци. Најголем број од хакерските активности се планираат и се изведуваат поради економски и финансиски придобивки.

Финансиите се главната причина поради која се случуваат кривичните дела, па затоа и најчеста жртва на компјутерски напади се банките и големите финансиски корпорации, токму тие треба да бидат многу внимателни во поставувањето на соодветни системи за заштита. Исто така, многу важни се финансиските средства во набавка на современа технологија, со која може успешно да се откриваат и да се спречуваат кривични дела поврзани со компјутери и компјутерска технологија.

● ***.Границите*** во денешниот свет се многу поразлични од порано. Со развојот на компјутерите и компјутерската технологија границите се прошируваат, а во многу области воопшто и не постојат. Со помош на компјутерите и Интернетот, комуникациите се многу полесни и поедноставни, со било кој дел од светот и тоа без разлика дали ке биде пишан текст, аудио или видео пренос.

Границите во поголема мера го отежнуваат откривањето на компјутерски криминал, отколку што можат да помогнат. Електронска граница претставува опасност од незаконски дела кои се вршат со употреба на Интернет. Границите во многу наврати се цели на напад на хакерите, програмите што нивните службеници ги користат, со цел да се употребат за одредени цели на хакерите.

● ***Техничко-технолошки сектор,*** исто така е многу значаен фактор за олеснување на откривањето на компјутерскиот криминал, поради фактот дека компјутерскиот криминал се изведува со најсовремена технологија. Имплицираноста на компјутерскиот криминал во овој сектор е посебно забележителна по тоа што може да предизвика нарушување на безбедноста и да доведе до огромни промени во нормалното функционирање на општествените функции.

За изведување на компјутерскиот криминал потребна е најсовремена технологија и технички средства, но истите тие, па дури и поусовршени се потребни за откривање на компјутерскиот криминал. Во минатото работата во фабриките не можела да се изведува без човечки труд, додека во современи услови голем дел од работите се заменти со компјутери и компјутерски машини. Компјутеризацијата на техничко – технолошкиот сектор го прави секторот многу поранлив и осетлив на хакерски напади.

● Компјутерскиот криминал и неговите импликации врз безбедноста, исто така може да се забележат преку неговото влијание врз различните видови ***сообраќај.*** Најосетлив, од

сите видови сообраќај е воздушниот, а потоа следат и железничкиот, водниот па на крај патниот сообраќај.

Во современи услови постојат голем број примери на компјутерски напади, кога цел на напад на хакерите се одредени авиони, кои се претходно добро изберени за остварување на одредена цел. Ваквите напади се изведуваат со цел да се предизвика страв и паника кај населението за да се остварат одредени барања на хакерите. Тие своите напади ги вршат преку превземање и блокирање на оперативните сиситеми на авионите, без кои авионот неможе нормално да функционира.

Штетите за нападнатите авиони и авионски компании може да бидат огромни и тоа во поглед на материјални штети во моментот на напад, но и подоцна затоа што ќе дојде до губење на доверба и чувство на сигурност кај граѓаните при користење на услугите на таа компанија,а во краен случај може да дојде и до губење на човечки животи како најголема штета.

- *Транспортот* е тесно поврзан со сите претходно наведената имплицираност на компјутерскиот криминал врз безбедноста, односно тој има влијание и во изведувањето на кривичните дела, но и во откривањето на истите. Како посебен вид транспорт, ќе го споменеме транспортот на податоци и документи, кој со современата технологија е олеснет и поедноставен, но постојат огромни ризици при самото вршење на овој вид пренос на информации. [112]

- *Измами со идентитет* се најчести и најмногу застапени примери на компјутерски криминал. Со помош на компјутерите и компјутерската технологија се откриваат шифри и тајни податоци од чиповите на разни видови картички, со помош на кои се зема нечиј идентитет, се пробиваат пин кодови од банкарски сметки, се влегува во витални институции и со сите овие активности се прават огромни штети, како за поединците, така и за општеството во целина.

Кражбите на идентитет се користат и за разновидни други криминални дејствија, за нелегални преминувања во други држави, за разновидни измами и слични други дејства.

Најчест пример на измами со идентитет се фалсификуваните картички, преку кои од банкоматите се вадат милионски суми, со што се предизвикуваат материјални штети, но и се предизвикува чувство на страв и несигурност кај граѓаните при користење на ваков вид на услуги.

[112] http://www.bs.wikipedia.org/wiki/globalizacija

Според импликациите на компјутерскиот криминал врз безбедноста во современиот свет мора да се спроведат и соодветни мерки за заштита на компјутерите и компјутерските системи заради нормално функционирање на виталните функции во општеството.

Во ерата на компјутеризација и развој на информатичкото општество нема сектор ниту област во општеството која не е поврзана со компјутер и компјутерска технологија и Интернет и од тие причини осетливоста од хакерски влијанија е многу голема. Поради тоа потребно е да се превземат и соодветни мерки за заштита и и превенција, а потребна е и соодветна обука на персоналот за соодветно и најбезбедно работење со компјутерите и компјутерската технологија.

Размената на информации меѓу сите сектори во општеството е неопходна поради ефикасна превенција и гонење на компјутерскиот криминал. Размената на информации и сознанија од областа на компјутерскиот криминал, на регионално и на меѓународно ниво, може да помогне и ублажи понатамошен компјутерски напад, да помогне во примена на законите во гонење на криминални активности и олеснување на активности кои подржуваат подобри и поефективни начини за безбедна работа на сите корисници на информатичко – комуникациската технологија.

Компаниите, државните органи и поединците во целиот свет ги користат предностите на Интернетот преку електронска трговија, електронска влада и електронска пошта. Но, покрај позитивните можности, Интернетот е подложен и на разновидни напади. Ниту државниот, ниту приватниот сектор не можат да ги решаваат сами ваквите проблеми. Координацијата и соработката меѓу овие организации и институции се најважните елементи за борбата со компјутерскиот криминал и за превенција од било какви криминогени активности.

Поради јасно прецизирање на импликациите на компјутерскиот криминал врз безбедноста во светски рамки, ќе наведеме некои покарактеристични примери на компјутерски криминал и штетите што притоа се нанесени. Нема земја во светот која не се соочила со било каков пример на компјутерски криминал од посериозни размери при кој биле доведени во прашање безбедноста и нормалното функционирање на поголеми компании и витални институции во државата.

Па така, Шпанската полиција ја разбила најголемата хакерска мрежа во светот, која заразила со вируси, околу 13 милиони компјутери низ целиот свет, а во операцијата се уапсени три лица. Хакерите ги заразувале компјутерите на физички лица и фирми од сите

делови на светот, крадејќи им податоци од кредитни картички, корисничките имиња, лозинки и други доверливи информации. Таканаречената мрежа, Марипоса, за првпат била откриена во мај 2009 година, од државна канадска фирма за заштита на информации. А, тројца приведени биле шпански државјани на возраст од 25 и 31 година. Интересно е што, припадниците на оваа група, воопшто не биле стручни во компјутерските вештини, туку хакерските програми ги купиле на црниот пазар.[113]

Исто така, како карактеристичен ќе го наведеме случајот кога во САД биле уапсени 80 хакери, поради ограбување банки. Хакерите биле од Источна Европа, а краделе кориснички имиња и лозинки и здружувајќи се со странски студенти, кои отворале сметки во САД, успеале да украдат најмалку три милиони долари. Тука, ја цитираме и изјавата на јавниот обвинител Прет Барара, кој рекол дека „ глушецот и тастатурата може да бидат, далеку поефикасни од пиштол и маска на глава“, споредувајќи ги злонамерните сајбер криминалци, со класичните ограбувачи на банки.

Најголем дел од демократските земји, имаат развиено системи за откривање на сомнителни финансиски трансакции и имаат усвоено закони за пронаоѓање, замрзнување и запленување на криминални средства.[114] По терористичките напади на Соединетите Американски Држави на 11 септември, 2001 година, беше заклучено дека подобар увид во врските помеѓу тековите на капитал и терористичките активности е од огромно значење за борбата против тероризмот и против организираниот криминал, а со тоа и против компјутерскиот криминал.

Во 1993 година во Холандија, биле усвоени нови закони, за да се зголемат законските овластувања на полицијата и законодавната власт, за да можат да ги „исчистат“ или да ги „соголат“ криминалците и нивните организации.

Овие промени во холандскиот кривичен законик, претставуваат важна промена во истражната пракса и во судското гонење; стариот пристап што го става обвинетиот на централното место сега мора да биде придружен од пристап, базиран на профитот.

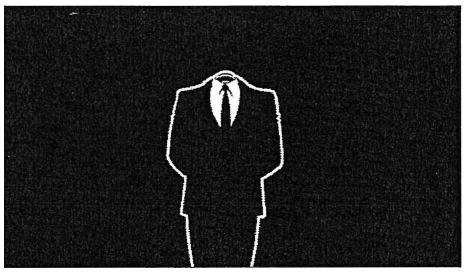
---

[113] http://www.naslovi.net/20-03-03/b92/razbijena_velika_hakerska_mreza/157894

[114] „Глобален организиран криминал-трендови и случувања“,Д.Зигел,Х.ван де Бунт, Д.Зоур, Магор, Скопје,2009,стр.141.

Од овие примери, можеме да заклучиме дека, компјутерскиот криминал е мошне сериозна и опасна појава, која може да предизвика огромни последици. Исто така, многу очигледно е дека во светски рамки опасностите се огромни, односни станува збор за огромни суми на пари, додека во Република Македонија се уште нема појава на толку ефектни хакери и толку опасни хакерски напади.

Во пошироки рамки хакерите се поголеми организирани групи, кои имаат претставници низ целиот свет, додека во Република Македонија станува збор од организирани групи, од најмногу десет луѓе. Во секој случај, потребно е огромно внимани за откривање и спречување на секаков вид на компјутерски напади.



Најпознатата хакерска група Anonymous, во последно време е се поактуелна, односно на 26 јануари 2012 година, го нападнале сајтот на Европскиот Парламент, поради тоа што биле револтирани од потпишувањето на договорот за заштита на интелектуална сопственост од повеќе земји членки.

Нападот беше извршен во знак на револт поради договорот со кој се регулира заштитата на интелектуална сопственост или "Договорот за заштита на авторските права на Интернет, наречен скратено (АКТА)[115]", што го потпишаа Европската Унија и земјите членки, кој според критичарите ги загрозува граѓанските слободи, правото на приватност и интернетската иновација.

Со овие закони во голема мерка се ограничуваат досегашните граници на Интернетот, се стекнуваат права за регулирање на работата на Интернет страните, можности за ограничување или дури и забрана на работата на некои Интернет стани, строго регулирање на податоците што се објавуваат на било која Интернет страна, за кои земјите потписнички на овие договори ќе сметаат дека не постапуваат правилно.

[115] АКТА- (*Anti-Counterfeiting Trade Agreement),* е меѓународен договор, кој има за цел да воспостави меѓународни стандарди за заштита на интелектуалната сопственост, потписан на 11 октомври, 2011 година, од страна на САД, Канада, Сингапур, Мароко, Нов Зеланд и Јужна Кореја, а во почетокот на 2012 кон договорот се приклучува и Европската Унија.

Ваквите договори се одржуваат уште од 2005 година, но во тајност, а јавно биле откриени со аферата Викиликс во 2008 година, сите потписнички ги држеле овие преговори во тајност, од свои причини.

Портпаролот на Европскиот Парламент го потврдил нападот, но нагласи дека хакерите не успеале да стигнат во внатрешната мрежа на институцијата.[116]

Потоа седуваа и на нападите на страницата на ФБИ, на 3 февруари, 2012 година. На 10 февруари 2012 година, била нападната страницата на ЦИА- централна разузнавачка агенција, а на 11 февруари, 2012 година, била нападната и страницата на ИНЕТРПОЛ – Меѓународната полициска агенција.

Сите овие напади се во знак на протест, а оваа хакерска група најавува и други напади на значајни државни и меѓународни институции, меѓународни организации, политички партии ширум светот, револтирани од задушувањето на слободата и демократијата на Интернетот. [117]

Во оваа област интересна е и изјавата на рускиот експерт Eugene Kaspersky, кој рекол дека - "Земјите во развој ќе страдаат најмногу, поради тоа што повеќе од другите земји се зависни од компјутери и компјутерски мрежи. Хакери денес може да сопрат се што сакаат, не само фирми и корпорации, туку и цели држави, а сето тоа благодарение на оружјето во областа на информатичките технологии кое е релативно лесно да се развие и имплементира."

Тој, исто така смета дека во иднина, хакерите може да се претворат во терористи и да дојде до водење на сајбер војна. Дали е тоа можно, останува да видиме што ќе се случува во иднина.

Неговите ставови ги поддржува и поранешниот шеф на ЦИА, Мајкл Хајден. [118]Тој на конференцијата во Минхен потсети на компјутерски вирус Stuxnet, кој ја инфицира центрифугата на нуклеарната програма на Иран. "Тоа доведе до самоуништување на машините, и од тогаш ништо не е исто како пред тоа, бидејќи со тоа беше докажано дека

[116] http://www.daily.mk/cluste3/19b0e0a11b6c5..97865878a3a31f62/1114225/anonimusi-go-napadnaa-sajtot-na-evropskiot-parlament
[117] http://www.time.mk/read/296a19ca5c/02bf046012/index.html
[118] http://www.fakulteti.mk/news/12-02-19/na_povidok_e_sajber_vojna.aspx

вирусот може да предизвика физичка штета по пат на новите технологии", предупредува Хајден.

Активностите на хакерите, во денешно време, се многу олеснети со големиот процент на поврзаност на сите држави во светот со помош на компјутерите и компјутерската технологија.

Тие, комуницираат меѓу себе, разменуваат мислења, идеи и искуства, а притоа лично воопшто и не се познаваат, се среќаваат само во виртуелниот свет и тоа под тајни имиња, псевдоними, што сами си ги смислуваат.

Тие користат различни начини на меѓусебно комуницирање и функционирање кои се многу тешки за откривање и за следење од страна на обичните работници и обичната и недоволно развиена технологија. За нивно следење потребна е соодветна обука, која ќе биде на нивно, но и на многу повисоко ниво.

7. Компјутерски криминал во Република Македонија

Компјутерскиот криминал е облик на криминална активност која која се појавува во современи услови, а претежно ги зафаќа и се распространува во недоволно развиените земји и во земјите во транзиција.

Република Македонија спаѓа во групата со овие земји и секојдневно се соочува со проблеми кои може да се вбројат во облици на компјутерски криминал. Ваквите облици на криминалана активност се се позачестена појава и жртва може да биде секој граѓанин на Република Македонија, без разлика дали користи компјутер или не. Најчесто, цел на напад се банкоматите, трансакциските сметки на граѓаните и различните апарати за неготовинска наплата, односно наплата со картички.

Република Македонија е држава, кој настојува и со законите и со активностите да се бори со сите облици на организираниот криминал. Но, во Република Македонија, се уште, многу малку внимание се посветува за осознавање на негативното влијание на компјутерите и компјутерската технологија, врз безбедноста во сите области на секојдневното опстојување и функционирање.

Исто така, многу ниско е нивото на сознанија за можните штети што може да настанат од несоодветна примена на компјутерите и компјутерската технологија, а посебно за штетите од нелегални дејства кои се извршуваат со помош на компјутерите.

Компјутерскиот криминал[119] е појава на современото време и појава која зема се поголем замав во сите аспекти на човековото живеење. Компјутерскиот криминал може да се појави во повеќе облици, и тоа: компјутерски измами, компјутерски фалсификати, неовластено навлегување во компјутерски систем и слично.

Во Република Македонија честа е појавата на неовластено навлегување во компјутерски систем и тоа најчесто од страна на помлади корисници и тоа на возраст од 16 до 30 годишна возраст. Исто така, често се случуваат и разни кражби кои се изведуваат со помош на компјутер. Кражбите пак, најчесто се вршат од страна на малку постари лица, од

[119] http://www.mvr.gov.mk/ShowAnnouncements.aspx?ItemID=10637&mid=1367&tabId=358&tabindex=0

претходно споменатите и често лица кои потекнуваат од странски држави или пак се потпомогнати од лица од странски дрґави.

Врз основа на тоа дека е ниско нивото на сознанија на опасностите од несоодветна примена на компјутерите и компјутерската технологија и дека нема доволно сознанија за можните штети, значи дека и нивото на заштита е на прилично ниско ниво.

Заштитата главно се сведува на примена на антивирусни програми, по желба на корисниците на компјутерите, а чие ниво на заштита не е доволно проверено, ниту пак доволно безбедно.

Во Република Македонија со компјутерскиот криминал, со негово настанување, навремено откривање и спречување и со последиците се занимаваат: Министерството за внатрешни работи, Министерството за економија, Министерството за финансии, Министерството за информатички технологии, Министерството за правда со судовите и Јавното Обвинителство и други органи и институции кои имаат можности и ингеренции за да се занимаваат со ова прашање.

7.1. Законска рамка на компјутерскиот криминал во Република Македонија

Компјутерскиот криминал ги опфаќа сите облици и форми на криминални поведенија, поврзани со злоупотреба на компјутерските и на информатичките системи, кои се општествено опасни и се со основна намера да се постигне одредена материјална корист за сторителот, а да се нанесат огромни штети на жртвите и тоа за многу кратко време и со начин на кој тешко може да се откријат или да останат неоткриени.

Во Република Македонија, во поново време почнува повеќе внимание да му се посветува на компјутерскиот криминал, како се позачестена и се поопасна појава, која му се заканува на општествениот развој од секој аспект.

Секојдневно се појавуваат се поголем број на случаи на компјутерски криминал од било каков облик. Тие може да бидат поситни екцеси и испади на несериозни хакери, но може да бидат и напади од витална важност за државата па и од меѓународ аспект.

Одредени поими, кои се користат за појаснување на компјутерскиот криминал, се опфатени во Кривичниот Законик на Република Македонија, а тоа се поимите „компјутерски систем“ и „компјутерски податоци“.

- Кривичен Законик на Република Македонија

Имено, во член 122, т.22 - е наведено дека:

„ Под ***компјутерски систем*** се подразбира, каков било уред или група на меѓусебно поврзани уреди од кои еден или повеќе од нив, врши автоматска обработка на податоци според одредена програма“.

Додека пак, во член 122, т.23, од Кривичниот Законик на Република Македонија – е наведено дека: „под ***компјутерски податоци*** се подразбира презентирање на факти, информации или концепти во облик, кој е погоден за обработување преку компјутерски систем, вклучувајќи и програма подобна компјутерскиот систем да го стави во функција“.

Како кривични дела од областа на компјутерскиот криминал се предвидени следниве кривични дела:

- Оштетување и неовластено навлегување во компјутерски систем

Во член 251, се вели дека тој што неовластено ќе избрише, измени, оштети, прикрие или на друг начин ќе направи неупотреблив компјутески податок или програма, или уред за одржување на информатичкиот систем, или ќе го оневозможи, или отежне користењето на компјутерскиот систем, податокот или програмата или на компјутерската комуникација, ќе се казни со парична казна или со казна затвор до три години.

Понатаму, стои дека со казната од став 1, ќе се казни и тој што неовластено ќе навлезе во туѓ компјутер или систем со намера за искористување на неговите податоци или програми, заради прибавување противправна имотна или друга корист, за себе или за друг или предизвикување имотна или друга штета, или заради пренесување на компјутерските податоци што не му се наменети и до кои неовластено дошол, на неповикано лице.

Потоа, следи дека тој што делата од ставовите од претходните членови ќе ги стори спрема компјутерски систем, податоци или програми што се заштитени со посебни мерки за заштита, или се користат во работењето на државните органи, јавни претпријатија или јавни установи или во меѓународните комуникации, или како член на група создадена за вршење такви дела, ќе се казна затвор од една до пет години.

Ако со делото од првите два става, од членот 251, е прибавена поголема имотна корист или е предизвикана поголема штета, сторителот ќе се казни со казна затвор од шест месеци до пет години.

Ако со делото од став 3, е прибавена поголема имотна корист или е предизвикана поголема штета, сторителот ќе се казни со затвор од една до десет години, тој што неовластено изработува, набавува, продава, држи или прави достапни на друг посебни направи, средства, компјутерски програми или компјутерски податоци наменети или погодни за извршување на делата од ставовите 1 и 2, ќе се казни со парична казна или со казна затвор до една година. [120]

- Правење и внесување на компјутерски вируси

Во членот 251 –а, се наведува дека тој што ќе направи или ќе превземе од друг компјутерски вирус со намера за внесување во туѓ компјутер или компјутерска мрежа, ќе се казни со парична казна или со казна затвор до една година.

Тој што со употреба на компјутерски вирус ќе предизвика штета во туѓ компјутер, систем, податок или програма, ќе се казни со затвор од шест месеци до три години.

[120] Кривичен Законик на Република Македонија, (Сл.весник на РМ,бр.19, 30.03.2004)

Ако со делото од став 2, е предизвикана поголема штета или делото е сторено во состав на група создадена за вршење такво дело, сторителот ќе се казни со казна затвор од една до пет години.

- Компјутерска измама

Компјутерската измама се регулира со членот 251- б, во кој се регулира дека, тоа што тој со намера за себе или за друг ќе прибави противправна имотна корист со внесување во компјутер или информатички систем, невистинити податоци, со невнесување на вистинити податоци, со фалсификување на електронски потпис или на друг начин ќе предизвика невистинит резултат, при електронската обработка или преносот на податоците, ќе се казни со парична казна или со казна затвор до три години.

Тој што неовластено изработува, набавува, продава, држи или прави достапни на друг посебни направи, средства, компјутерски програми или компјутерски податоци наменети за извршување на делото од став1, ќе се казни со парична казна или со казна затвор од една година.

- Компјутерски фалсификат

Во член 379 – а, се вели дека тој што со намера ќе ги употреби и 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, ќе се казни со парична казна или со казна затвор до три години.

Ако делото од став 1, е сторено во однос на компјутерски податоци или програми што се користат во работењето на државните органи, јавни установи, претпријатија или други правни и физички лица кои вршат работи од јавен интерес или во правниот сообраќај со странство или ако со нивната употреба е предизвикана значителна штета, сторителот ќе се казни со казна ззатвор од една до пет години.

Тој што неовластено изработува, набавува, продава, држи или прави достапни на друг посебни направи, средства, компјутерски програми или компјутерски податоци наменети или погодни за извршување на делото од став 1, ќе се казни со парична казна или со казна затвор до три години.

Со Законот за изменување и дополнување на Кривичниот Законик на Република Македонија[121], извршени се и измени во следниве кривични дела, а се однесуваат на компјутерската технологија:

- Прикажување порнографски материјал на малолетник

Во член 193, стои дека тој што на малолетник кој не наполнил 14 години, прикаже или со јавно излагање на друг начин ќе му направи достапни слики, аудиовизуелни и други предмети со порнографска содржина или ќе му прикаже порнографска претстава, ќе се казни со затвор од шест месеци до три години.

- Производство и дистрибуција на детска порнографија преку компјутерски систем

Во член 193-а, се утврдува дека тој што произведува детска порнографија со цел нејзина дистибуција, дистрибуира или пренесува или нуди или на друг начин прави достапна детска порнографија преку компјутерски систем, ќе се казни со затвор од три до пет години, а тој што набавува детска порнографија преку компјутерски систем за себе или за друг или поседува детска порнографија во компјутерски систем или медиум кој служи за чување на компјутерски податоци со намера за покажување на друг или за дистрибуција ќе се казни со затвор од шест месеци до три години.

[121] Сл.весник на РМ, бр.139, 04.11.2008, изменување и дополнување на Кривичен Законик на РМ.

- Закон за кривична постапка на Република Македонија

Во 2004 година, во Република Македонија, донесени се измени на Законот за Кривична Постапка,[122] во делот на примена на посебни истражни мерки, со цел примена на софистицирани техники за прибирање на докази и нивна употреба пред суд.

Па така, во член 146 од овој закон, се вели дека, заради обезбедување податоци и докази неопходни за успешно водење на кривичната постапка кои на друг начин не можат да се соберат, или нивното собирање би било сврзано со поголеми тешкотии, за кривични дела за кои е пропишана казна затвор од најмалку четири години и за кривични дела, за кои е пропишана казна затвор до пет години, за кои постои основано сомнение дека се извршени од страна на организирана група, банда или друго злосторничло здружение, може да се нареди преземање на посебни истражни мерки:

1) следење комуникации и влез во дом и други простории или во превозни средства, заради создавање на услови за следење на комуникации, под услови и постапки утврдени со закон;

2) увид и пребарување во компјутерски систем, одземање на компјутерски систем или дел од него или базата за складирање на компјутерски податоци;

3) тајно набљудување, следење и визуелно-тонско снимање на лица и предмети со технички средства;

4) привиден откуп на предмети, како и привидно давање поткуп и привидно примање поткуп;

5) контролирана испорака и превоз на лица и предмети;

6) користење на лица со прикриен идентитет за следење и собирање на информации или податоци;

7) отворање привидна банкарска сметка, на која може да се вложуваат средства што потекнуваат од сторено кривично дело;

8) регистрирање на привидни правни лица или користење на постојни правни лица заради собирање податоци.

[122] http://www. jorm.org.mk/docs/zakon-krivicna.rtf

- Закон за заштита на лични податоци

Законот ја уредува заштитата на личните податоци како една од основните слободи и права на граѓаните, а особено правото на приватност во врска со обработка на личните податоци.[123]

Главни начела, на кои се заснова Законот за заштита на лични податоци и кои треба да се почитуваат во секојдневниот живот се следните: законитост и праведност при обработка на личните податоци, спецификација на целта заради која е формирана збирката на личните податоци, слободен пристап до збирката на лични податоци од страна на субјектот на лични податоци, посебна заштита на посебните категории на лични податоци, пренос на личните податоци во други држави и создавање на одговорни контролори и обработувачи на збирки на лични податоци

Со Законот за заштита на лични податоци, се заснова и ***Дирекција за заштита на лични податоци***, како самостоен и независен државен орган со советодавни и контролни надлежности во оваа област.

- Закон за класифицирани информации

Со Законот[124] за класифицирани информации, помеѓу другото, се уредуваат мерките и активностите за информатичката безбедност во Република Македонија, односно со овој закон се уредуваат:

- сертификација на комуникациско – информатички системи и процеси;
- проценка на можно нарушување на безбедноста на комуникациско– информатичките системи (КИС);
- утврдување на методи и безбедносни процедури за прием, обработка, пренос, чување и архивирање на класифицирани информации во електронска форма;
- заштита на информациите при процесирање и чување на КИС;
- дистрибуција на крипто – клучеви и друг крипто – материјал;

[123] Закон за заштита на лични податоци, Сл.Весник на РМ, бр.7/05 и 103/08
[124] Закон за класифицирани информации, Сл.весник на РМ, бр.9, 27 февруари, 2004.

-криптографска заштита на КИС;

- определување на зони и простории заштитени од компромитирачко електромагнетно зрачење;

- инсталирање на уреди за чување на класифицирани информации.

Целта на овој Закон е, обезбедување на законско користење на класифицирани информации и оневозможување на секаков вид на незаконски пристап до информациите.

Под информација од интерес за Република Македонија, се подразбира секоја информација или материјал изготвен од државните органи и институции, но и други домашни и странски правни и физички лица, кои се однесуваат на безбедноста и одбраната на државата, на нејзиниот територијален интегритет и суверенитет, уставниот поредок, јавниот интерес, слободите и правата на човекот и граѓанинот.

За обезбедување на доверливост, интегритет и достапност на класифицираните информации во КИС, се спроведува процес на безбедносна акредитација, кој опфаќа: акредитација, сертификација и евалуација.

Со овој Законот се воспоставува, ***Дирекција за безбедност на класифицирани информации***, како самостоен орган на државната управа со бројни надлежности во оваа област.

- Закон за слободен пристап до информации од јавен карактер

Овој Закон [125] ги уредува условите, начинот и постапката за остварување на правото на слободен пристап до информациите од јавен карактер со кои располагаат органите на државната и локалната власт и други установи, институции и претпријатија.

За информации од јавен карактер, се сметаат информации кои може да бидат од корист за граѓаните во остварување на нивните секојдневни активности, а кои немаат на нив назнака за доверливо или строго доверливо.

[125] Закон за слободен пристап до информации од јавен карактер, Сл.весник, 1 септември,2006.

Целта на Законот е да се обезбеди јавност и отвореност во работењето на имателите на информации, а на физичките и правните лица да им се овозможи да го остваруваат правото на слободен пристап до информации од јавен карактер.

Општото правило кое овој Закон го воспоставува, е дека слободен пристап до информациите имаат сите правни и физички лица, а само со закон се определуваат исклучоците од ова правило.

Заради почитување на законските одредби од оваа област, Законот воспоставува независна ***Комисија за заштита на правото за слободен пристап до информациите од јавен карактер***, чија главна надлежност е да одлучува по жалбите против решението и заклучокот со кои имателот на информацијата го одбил барањето за пристап до информации на барателите.

7.2. Примена на компјутери и компјутерска технологија во Република Македонија (институционална рамка)

Република Македонија е во фаза на компјутеризација на државните служби и постепено поврзување во една единствена мрежа на информации.[126]

За тоа постојат многу примери, како што се: компјутеризација на Управата за јавни приходи, Македонски телекомуникации, Фонд за пензиско и здравствено осигурување, банки, министерствата и други, при што сето ова поврзување е интерно, само за сопствени потреби, без пристап за други корисници кои сакаат да дознаат било какви информации за овие служби.

Откако оваа компјутеризација ќе биде зацршена во целост, ќе следува поврзување на сите органи во еден единствен систем, за да се скрати времето и да се поедностави пристапот до одредени информации и вадењето на потребни документи.

Исто така, од многу голема важност е и поврзувањето судовите, со што нивната соработка ќе биде на повисоко ниво. Во фаза на изработка е архива во која ќе бидат сместени сите предмети.

---

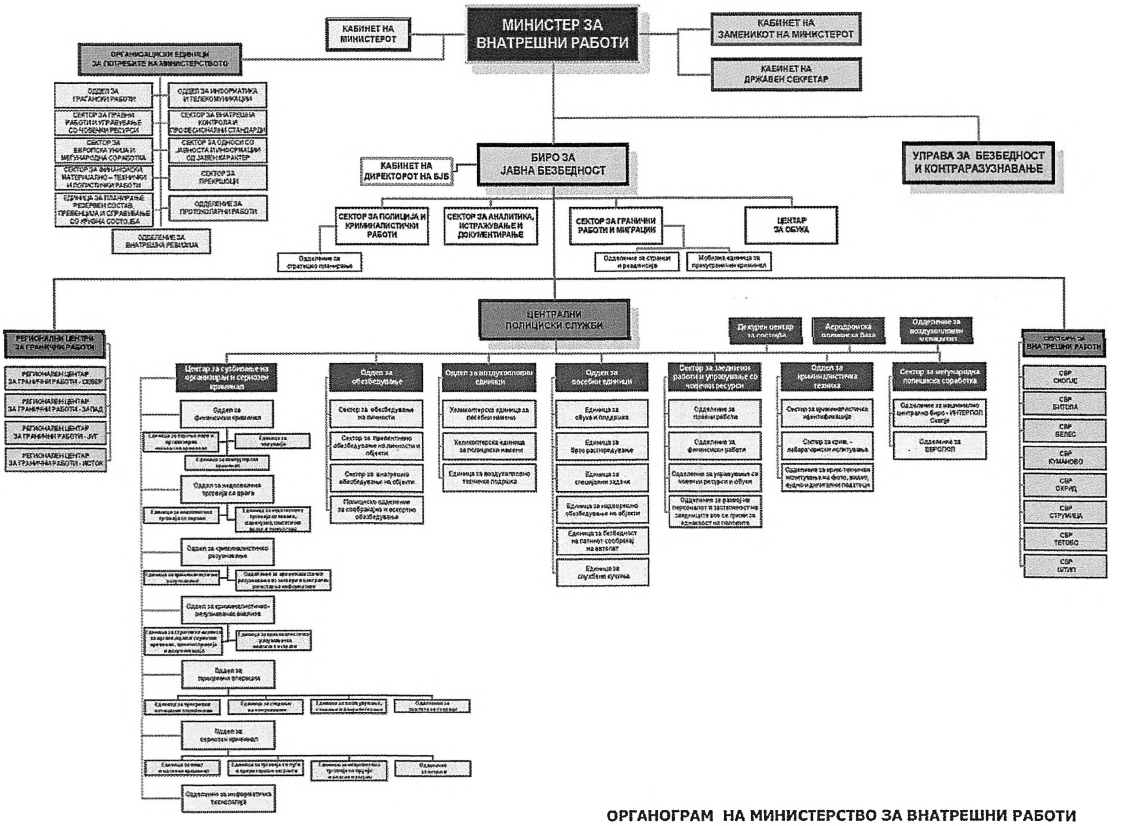
[126] „Сајбер-криминалитет- нови можности за криминално однесување“,Legal journal Lawyer, mart,2003.

Дефинирајќи ја компјутерската технологија и компјутерскиот криминал, како општествено кривично поведение, гонењето на сторителите го вршат одредени институции, првенствено, Министерството за Внатрешни Работи и Јавното Обвинителство на Република Македонија, како и други институции кои се дирекно или индирекно вклучени во борбата против компјутерскиот криминал.

7.2.1. Министерство за Внатрешни Работи на Република Македонија

Министерството за Внатрешни Работи на Република Македонија, во рамките на своите надлежности и овластувања, врши континуирана примена на мерки и активности во правец на откривање и гонење на сторители на кривични дела и поднесување на кривични пријави пред правосудните органи.

Сите мерки и активности; Министерството ги превзема врз основа на Кривичниот Законик на Република Македонија.



ОРГАНОГРАМ НА МИНИСТЕРСТВО ЗА ВНАТРЕШНИ РАБОТИ
ОКТОМВРИ 2011

Во јануари 2005 година, е формиран Одделот за Организиран Криминал, при Министерството за внатрешни работи на Република Македонија, во чии рамки постои посебна Единица за борба против компјутерски криминал, која е специјализирана и обучена за справување со компјутерски напади и со случаи на недозволена употреба на компјутерите и компјутерската технологија.

Надчежностите на Единицата за борба против компјутерски криминал, е работа на случаи поврзани со компјутерски криминал и фалсификување и употреба на вредносни картички (платежни, вредносни, дебитни и др.).

Како една од најзначајните мерки и активности што ги превзема Единицата за борба против компјутерскиот криминал, е борба со организираниот криминал преку употреба на посебни истражни техники и водење на проактивни истраги (водење на истраги пред да биде сторено кривично дело).

Исто така, во јануари 2005 година, при Одделот за крим-техника во Министерството за Внатрешни Работи, е формирано посебното, Одделение за анализа и вештачење на компјутерска опрема и компјутерски системи, чија што цел е анализа на опремата со цел за обезбедување на квалитетни докази потребни за докажување на делото и водење на кривичната постапка. Ова Одделение е задолжено за извршување на компјутерска форензика, односно за собирање на докази при откривање на кривични дела извршени со помош на компјутер и компјутерска технологија или врз компјутер или компјутерска технологија.

Покрај досега наведените, една од позначајните улоги на Министерството за внатрешни работи, е и превентивната функција, што значи спречување на извршување на кривични дела. Ова се постигнува со благовремено детектирање на одредени појави од областа на криминалот и нивно спречување на различни начини, пред да настанат штетните последици од извршувањето на кривичното дело и пред воопшто да настане кривичното дело (на пример, информирање на јавноста преку јавни гласила, директна соработка на полицијата со граѓаните и сл.).[127]

[127] http://www.mvr.gov.mk/DesktopDafault.aspx?tobindex=0&tabid=98

7.2.2. Јавно Обвинителство на Република Македонија;

Јавното Обвинителство е единствен и самостоен државен орган, кој ги гони сторителите на кривични дела и на други, со Закон утврдени казниви дела, раководејќи се според Законот за кривична постапка.[128]

Во финкција на зајакнување на позицијата на Јавниот Обвинител, за да може поуспешно да одговори и соодветно да постапи на предизвиците кои ги носи времето, во остварувањето на поефикасната борба против организираниот криминал, корупцијата и другите сериозни казниви дела, во месец декември 2007 година, е донесен Закон за Јавно Обвинителство и Законот за Совет на Јавни Обвинители на Република Македонија, со што започнува, во суштинска смисла, реформата во казнено процесниот систем.

Јавното Обвинителство, според Законот, е организирано по принципот на хиерархија и субординација и тоа како Јавно Обвинителство на Република Македонија, Вишо Јавно Обвинителство, Основно Јавно Обвинителство и Основно Јавно Обвинителство за организиран криминал и корупција.

Со новите измени, Одделението за гонење на сторителите од областа на организираниот криминал и корупција, основано според поранешниот Закон во рамките на Јавното Обвинителство на Република Мкдонија, прераснува во посебно Обвинителство и тоа како Основно Јавно Обвинителство за организиран криминал и корупција, основано за целата територија на Република Македонија, со седиште во Скопје.

Во рамките на ова посебно обвинителство е гонење на сторители на кривични дела од областа на организираниот криминал. Затоа, многу важна е и улогата при спроведување на посебните истражни мерки, како еден од начините за водење на предистражната постапка.

Според мене, најпрвин би требало да се изготви научна експертиза за работата на било кој од наведените органи во Република Македонија. На пример, за судовите треба првин да се изготви веб страница, која ќе биде достапна за јавноста и на која ќе се

[128] http://www.jorm.org.mk/docs/brosura.pdf

презентира работата на секој суд поединечно, но и на повисоките судови, како и на Врховниот суд.

Најважно е да се внимава на сигурноста на целата мрежа, дали таа ќе биде заштитена од упади на хакери и од различни видови вируси.

Инвестицијата за изработка на единствениот софтвер за било кој од наведените органи е многу скапа, но и заштитата на компјутерите и на целата компјутерска мрежа од разни недозволени упади и вируси ќе биде уште поскапа.

Затоа, најдобро е да се согледаат искуствата од Европските земји, или земји кои веќе користат вакви системи, така што ќе се избере најсоодветен начин на компјутеризација на целокупното општество, кој ќе биде најдобар и најевтин систем за условите што ги има Република Македонија.

Република Македонија настојува да ги компјутеризира сите сфери од секојдневното функционирање на општеството. Така што, поставени се компјутери во сите основни и средни училишта, во катастарот, во локалната самоуправа, Министерството за здравство, Министерството за внатрешни работи и во голем број други државни субјекти, но целосната компјутеризација се уште не е завршена.

7.3. Досегашни истражувања во Република Македонија, во областа на компјутерите и компјутерската технологија

Многу важно за целокупниот компјутерски развој на една земја, е употребата на компјутерите во домаќинствата и тоа да бидат опфатени сите возрасни групи. Во поново време се поретко има домаќинства кои не поседуваат било каков компјутер и кои немаат пристап до Интернет, без разлика дали е тоа дома или во специјализирани објекти.

Во тек е забрзан информатичко – комуникациски развој кој мора а биде следен во чекор за да може да се функционира нормално во едно вакво високо-технолошки развиено општество.

Со цел да се одредат достапноста и начинот на користење на одредени информатичко-комуникациски технологии, Државниот завод за статистика на Република Македонија, од 2005 година, ги спроведува следните статистички истражувања, според типот на корисниците:

- Употреба на информатичко - комуникациски технологии, во деловните субјекти, од нефинансискиот и финансискиот сектор, (годишно истражување);
- Употреба на информатичко - комуникациски технологии, во домаќинска и кај поединци, (годишно истражување);
- Употреба на информатичко - комуникациски технологии, во јавниот сектор, (двегодишно истражување).

Како илустрација на сите претходно наведени констатации и факти ќе ги разгледаме и анализираме анкетите на Државниот завод за статистика на Република Македонија,[129] спроведени во 2007, 2008 и 2009 година, на територија на целата држава, во областа на компјутерите и Интернетот и нивната примена во домаќинствата, фирмите, јавниот и приватниот сектор.

Истражувањето што е спроведено од Државниот Завод за Статистика на Република Македонија е многу опширно и сеопфатно, но во овој труд ќе бидат наведени само соодветните резултати.

Од аспект на овој труд, многу е важно истражувањето спроведено од Државниот завод за статистика, а се однесува на – Употребата на информатичко-комуникациските технологии во деловните субјекти од финансискиот сектор, спроведувано секоја година и тоа во временски период од 2007, па до 2011 година.

Истражувањето многу прецизно ги опфаќа и мрежите, врските, технологијата што се користат во секојдневното функционирање на деловните субјект без оглед на тоа колку вработени имаат истите.

Во оваа анализа, ние подетално ќе ги разгледаме само елементите што се од аспект на ова истражување, односно бројот на компјутери, според бројот на вработените, пристапот до Интернет, користењето на Интернет услугите и сл..

[129] http://www.stat.gov.mk/Publikacii/MakBrojki2010web.mac.#

Предмет на ова истражување се опременоста и користењето на информатичко-комуникациските технологии од страна на деловните субјекти од финансискиот сектор во Република Македонија, почнувајќи од 2007 година, според бројот на вработени.

Единици на набљудување, кои се користени во овие истражувања се деловните субјекти, кои се регистрирани во Деловниот регистар на Република Македонија, чија што основна дејност е финансиско посредување и финансиско работење (банки, штедилници, кредитни институции и осигурителни компании).

Според бројот на вработените, деловните субјекти се класифицирани на:

- мали претпријатија, кои имаат од 10 до 49 вработени во свои рамки,
- средни претпријатија од 50 до 249 вработени,
- големи претпријатија кои имаат 250 и повеќе вработени, и
- дополнителна група од 1-9 вработени.

Во ова истражувањето се користени методолошките основи и препораки на Еуростат, кои се во согласност со Регулативата на ЕУ 1099/2005.[130]

Сето ова подетално ќе го разгледаме и ќе го разјасниме, преку неколку табели, кои се скратени и прецизирани и во кои се извадени само податоците кои може да бидат од интерес на ова истражување.

Овие табели би можеле да дадат реална слика за употребата на компјутерите и компјутерската технологија во Република Македонија, употребата на Интернетот во секојдневниот живот и во професионалното функционирање и тоа следено во период од 2007 година, до 2011 година. Преку нив се добива реална слика за целосната состојба во Република Македонија и може да се прецизираат плановите, целите и задачите на полето на компјутерите и компјутерската технологија за во иднина.

Од разгледувањето на овие истражувања ќе можеме да видиме во која насока се движи развојот на државата, односно дали ги следи светските трендови на компјутеризација и информатичка револуција, односно дали се осовременува на технолошки, информатички, комуникациски, а со тоа и на образовен план.

[130] http://www.eur-lex.europa.eu/lexUriServ.do?uri=OJ:L:2005:183:0047:0062:EN:PDF

Табела, бр.1. ***Употребата на информатичко-комуникациските технологии во деловните субјекти од финансискиот сектор, 2007 година, во проценти (%).***

	Вкупно	Број на вработени				
		1-9	10+	10-49	49-249	250+
Деловни субјекти	100	100	100	100	100	100
Компјутери	100	100	100	100	100	100
Интернет	97.8	91.7	100	100	100	100
ИТ Систем управување со нарачки	31.1	25.0	33.3	33.3	37.5	20.0
Веб страни	81.8	36.4	97.0	91.7	100	100
Рекламирање на веб-стр.	75.0	36.4	87.9	83.3	87.5	100

Од оваа табела, ќе забележиме дека во 2007 година, сите деловни субјекти од финансискиот сектор користеле компјутер, а 97.8 % имале пристап до Интернет, 31.1 % од деловните субјекти имале пристап до системот за управување со нарачки, а 33.3 % од деловните субјекти со над 10 вработени имале пристап до системите за управување со нарачки.

Исто така, забечежуваме дека во 2007 година 81.8 % од деловните субјекти имале своја веб страна, а 75.0 % од деловните субјекти на веб страните ги рекламирале своите услуги.

Како важен сегмент од ова истражување ќе ја разгледаме бројната состојба на домаќинствата во однос на користењето на компјутери, компјутерска технологија и пристапот до Интернет во Република Македонија, во 2009 година.

Според Државниот завод за статистика, во 2009 година, 54,1 % од домаќинствата во Република Македонија користеле компјутер, додека пак 81,0 % од населението имале пристап на Интернет и тоа најчесто преку ADSL поврзување.

Табела бр.2. ***Користење на компјутери и компјутерска технологија во домаќинствата во Република Македонија, според населено место.***

	Вкупно	Тип на населено место	
		Градско	Останато
Домакинства	200	100	100
Домакинства што користат компјутер	54.1	64.4	38.0
Домакинства со пристап до Интернет	41.8	52.6	24.6
Тесноопојасно	9.0	9.8	7.8
Модем ISDN	8.5	9.2	7.5
Моб.телефон GPRS	0.5	0.6	0.3
Широкопојасно	33.8	43.9	17.9
ADSL	19.7	23.5	13.7
Други начини	15.1	21.9	4.4

Во овој контекст ќе направиме и анализа за користењето на компјутер и Интернет според пол и возраст на населението во Република Македонија, според истражувањето спроведено во 2009 година.

Табела бр.3. ***Корисници на компјутер и Интернет според пол во 2009 година;***

	Вкупно	Пол	
		Машки	Женски
Возраст од 15-74 год.	200	100	100
Компјутер	59.6	61.9	57.2
Интернет	52.7	54.4	50.9

Според оваа табела, можеме да заклучиме дека во Република Македонија, компјутер и Интернет, во поголем процент користи машко население, така што 61.9 % машко население, користи компјутер и компјутерска технологија, наспроти 57.2 % женско население. Приближен е и односот при користење на Интернет, така 54.4 % машко население има пристап до Интернет, наспроти 50.9 % женско население.

Следното истражување на кое ќе посветиме внимание, се однесува на вработените во финансискиот и нефинансискиот сектор, користењето на информатичко-комуникациски технологии според одредени дејности, застапеност на електронската трговија во Република Македонија, користење на автоматска размена на податоци, итн.

Според податоците од Државниот завод за статистика [131], во 2009 година, дури 94,7 % од деловните субјекти од финансискиот и нефинансискиот сектор со десет и повеќе вработени биле опремени со компјутери и компјутерска технологија, 71,8 % користеле компјутерска мрежа LAN, а 31,9 % користеле безжичен пристап.

Најраспространето поврзување на Интернет е преку таканаречените DSL (Digital Subscriber Line) технологии, од кои најзастапено е ADSL поврзувањето, односно 71,8 % од деловните субјекти во Република Македонија, со пристап на Интернет имале ваков тип на поврзување.

Од деловните субјекти со пристап на Интернет, 70,8 % најчесто го употребувале за банкарски и финансиски услуги, а 55,9 % од деловните субјекти во Република Македонија, имале своја веб страна. Тука ќе забележиме дека кај деловните субјекти, развојот на компјутерската технологија се уште не е на доволно високо ниво.

Автоматска размена на податоците, со други деловни субјекти имале само 29,1 %, а внатрешна автоматска размена на информации на рамките на деловниот субјект извршувале 48,4 % од деловните субјекти.

[131] http://www.stat.gov.mk/publikacii/MakBrojki2010web.mac.p#

Табела бр.4. ***Користење на информатичко-комуникациски технологии, по дејности, во 2009 година;***

	Дејност според Националната класификација на дејности							
	Прерабо-тувачка индус-трија	Градеж-ништво	Трго-вија	Хотели	Сооб-раќај	Деловн и Актив-ности	Филм, видео, радио, ТВ	Банки и осигур-ување
Деловни суб	100	100	100	100	100	100	100	100
Компјутер	93.9	89.4	97.3	100	91.8	97.4	100	100
Интернет	83.8	79.2	89.8	90.5	83.2	96.2	100	100
Сопствена Веб страна	40.1	47.7	48.1	63.5	61.1	66.9	78.3	97.3

Исто така, од голема важност е да го знаеме и соодносот на користењето на Интернет по одредени дејности, спроведено во 2009 година и тоа опфаќајќи ги банките, финансиски сектор, образование, е-влада, е- набавки, и е-продажба.

Табела бр.5. ***Користење на Интернет во деловните субјекти во 2009 година;***

	Деловни субјекти според број на вработени			
	10+	10-49	50-249	250+
Деловни сунјекти со пристап на Интернет	100	100	100	100
Банкарски и финансиски услуги	70.8	70.3	71.9	75.6
Обука и образование	38.2	38.0	37.6	45.5
Е – Влада	75.8	74.5	77.5	90.3
Е – набавки	8.2	8.0	8.6	9.2
Е – продажба	5.0	4.9	5.2	5.0

Во ова истражување примерокот е стратифициран врз основа на случаен примерок. Стратификацијата на примерокот, е по стратум од 14 групи на дејности и по 5 групи од вработени (1-4 вработени, 5-9, 10-49, 50-249, 250 и повеќе, значи вкупно 70 стратуми.

Рамката на примерокот е Статистичкиот деловен регистар, избрани се 2051 деловни субјекти, од кои 1965 припаѓаат во нефинансискиот сектор, а 86 субјекти се од финансискиот сектор (банки, штедилници и осигурителни компании).

Во 2009 година, пристап до интернет имале 99,4 % од ентитетите кои се во јавниот сектор, (од централната и од локалната власт). Своја веб страна имале 84,2 % од субјектите од јавниот сектор со интернет пристап. Од субјектите со интернет пристап, 98,2 % интернетот го користеле за добивање разни информации, а 92,7 % за давање информации за своето работење. Исто така, 78,8 % интернетот го користеле за интеракции со органите на власта, односно јавната администрација.

Табела бр.6. ***Користење на информатичко-комуникациски технологии во јавниот сектор во 2009 година;***

	Вкупно	Министерства	Државни агенции	Јавни претпријатија	Локална самоуправа
Ентитети	100	100	100	100	100
Компјутер	100	100	100	100	100
Интернет	99.4	100	97.8	100	100
Систем за електронско пополнување на документи	47.6	40.0	44.4	36.0	54.3
Систем за доверливи идентификациони податоци	12.7	20.0	20.0	4.0	9.9

Во продолжение на оваа табела, ќе го разгледаме и за кои намени се користи Интернетот во јавниот сектор, во 2009 година.

Единици на ова истражување се органите на јавната администрација (министерства и други државни органи, судовите, управите, државните агенции, бироа, заводи), јавните претпријатија и локалната самоуправа во сите општини во Република Македонија.

Во истражувањето биле вклучени 191 статистичка единица, од нив одговориле 166, односно процентот е 87 %.

Податоците кои се опфатени во овие табели, се однесуваат на субјектите во јавниот сектор кои одговориле на прашалникот, а тоа се: 14 министерства и Владата на Република Македонија, 45 државни агенции, институции, организации, 25 јавни претпријатија и 81 единица на локалната самоуправа – општините.

Табела бр.7. ***Намена на користење на Интернет во јавниот сектор, 2009 година;***

	Вкупно	Министер-ства	Државни агенции	Јавни претпријатија	Локална самоуправа
Пристап до Интернет	100	100	100	100	100
Добивање информации	98.2	93.3	100	98.0	98.8
Давање информации за своето работење	92.7	100	93.2	84.0	93.8
Давање информации за легислативата	67.9	86.7	56.8	44.0	77.8
Давање податоци за состојбата во државата	43.6	73.3	43.2	36.0	40.7
Целосно електронско оперирање	29.1	33.3	25.0	36.0	28.4
Банкарски и финансиски услуги	28.5	20.0	25.0	48.0	25.9
Образование и обука	44.8	66.7	52.3	48.0	35.8
Набавки	23.0	40.0	13.6	28.0	23.5
Продажба	2.4	/	4.5	4.0	1.2
Веб страни	84.2	100	84.1	64.0	87.7

Податоците на Државниот Завод за Статистика на Република Македонија, од 2011 година, го покажуваат следново:

- 55 % од домаќинствата во Република Македонија, во 2011 година, имале пристап до Интернет;
- 56,7 % корисници на Интернет во Република Македонија (на возраст од 15 до 74 години), во 2011 година;
- 88,6 % деловни субјекти со 10 или повеќе вработени со пристап на Интернет, во 2011 година.

Табела 8. ***Користење информатички и комуникациски технологии во домаќинствата, според типот на населено место (во %)***

	Вкупно	Тип на населено место	
		Градско	Останато
Домаќинства	100	100	100
Домаќ. со компјутер	61.2	69.1	48.4
Пристап до Интернет	55.0	63.3	41.5

Од оваа табела, можеме да забележиме дека 61.2 % од испитаните домаќинства користат компјутер, а 55 % користат Интернет на било каков начин. Овој процент на користење и на компјутери и на Интернет, во споредба со претходните години е во постојан пораст, а се очекува така да биде и во иднина. Исто така, важен е и податокот дека градското население во доста поголем број користи компјутер и Интернет, за разлика од останатото.

Табела 9. ***Информатичко – комуникациски технологии во деловните субјекти,според бројот на вработен, во 2011 година (во %)***

	Вкупно	Според број на вработени		
		10-49	50-249	250+
Вкупно дел.субјекти	100	100	100	100
Компјутери	93.0	88.3	96.2	99.1
Интернет	88.6	82.3	92.7	97.6

Според бројот на вработени, можеме да забележиме дека најголем процент на користење на компјутери има во поголемите компании, односно во оние кои имаат 250 и повеќе вработени.

Табела 10. ***Користење на информатичко – комуникациски технологии, во јавниот сектор во 2011 година (во %)***

	Вкупно	Државни органи	Локална самоуправа
Ентитети, вкупно	100	100	100
Користење компјутер	100	100	100
Користење Интернет	100	100	100

Најспецифична е табелата, на која е прикажана состојбата кај државните органи и локалната самоуправа. Од оваа табела, можеме да видиме дека сите државни органи и сите сегменти од локалната самоуправа користат и компјутер и Интернет. Тоа се должи на напорите на државата за компјутеризација и осовременување на сите сегменти во општеството, со цел да се следат современите светски текови и состојби.

Табела 11. ***Вработени во јавниот сектор кои употребувале компјутер и Интернет, во 2011 година***

	Вкупно	Државни органи	Локална самоуправа
Вкупно вработени	100	100	100
Употребувале компјутер	82.8	83.7	79.3
Употребувале Интернет	71.7	70.1	77.8

Во оваа табела, која е поврзана со претходната, можеме да видиме дека околу 80 % од вработените во државните органи и локалната самоуправа користат компјутери, иако застапеноста на компјутерите е 100 %, а уште помал процент, односно околу 70 % од вработените користат Интернет, иако достапноста до оваа услуга е 100 %.

Проблемот е во тоа што вработените се уште не се доволно обучени и упатени за користење на оваа технологија.

Во Република Македонија, доста зачестена е и злоупотребата на компјутерите и компјутерската технологија за постигнување на одредени лични цели, за постигнување на материјална и имотна корист.

Најчести примери на компјутерски криминал во Република Македонија се во областа на економскиот криминал. Според Кривичниот Законик на Република Македонија, член 251, оштетување и неовластено навлегување во компјутерски систем, Министерството за внатрешни работи спровело статистичко истражување[132].

Во тоа истражување се опфатени податоците во период од 2001 година, до 2010 година и може да се забележи постојан пораст на кривичните дела поврзани со компјутер во тек на секоја наредна година.

Од спроведеното истражување на Министерството за внатрешни работи, ќе ги издвоиме оние податоци кои се од интерес за ова истражување и тоа регистрираните кривични дела и пријавените сторители ово однос на оштетување и неовластено навлегување во компјутерски системи.

Табела 12. ***Оштетување и неовластено навлегување во компјутерски систем;***

Оштетување и неовластено навлегување во комп.јутерски систем	2001		2002		2003		2004		2005		2006		2007		2008		2009		2010	
	Р	П	Р	П	Р	П	Р	П	Р	П	Р	П	Р	П	Р	П	Р	П	Р	П
	/	/	2	2	1	3	7	7	2	1	2	4	7	11	20	30	63	73	36	43

Во оваа табела кратенките Р и П означуваат:

- Р - регистрирани кривични дела;
- П - пријавени сторители.

[132] http://www.mvr.gov.mk/DesktopDefault.aspx?tabindex=0&tabid=395

Од оваа табела можеме да забележиме дека, со текот на годините бројот на регистрирани кривични дела е во постојан пораст, а исто така во пораст е и бројот на пријавените сторители на вакви кривични дела.

Посебно драстичен е порастот на ваквите кривични дела од 2007 година, кога и расте бројот на пријавување на сторителите. Ова се должи најмалку не развојот на компјутерската технологија и на целокупната компјутеризација на општеството, но и на свеста на граѓаните. Граѓаните се повеќе свакаат дека нивните компјутери се нападнати и дека нивните податоци се во опасност.

Од овие статистички податоци, можеме да заклучиме и дека и во иднина ќе се случува истото, односно ќе има пораст на кривичните дела и исто така се повеќе ќе се пријавуваат сторителите, што ќе се должи на се поголемиот и побрзиот развој на компјутерите и компјутерската технологија.

7.4. Начини на откривање на компјутерски криминал и сторители на компјутерски криминал во Република Македонија

Еден од најчестите начини за дознавање на кое било кривично дело, па така и на кривичните дела кои се поврзани со информатичката технологија и компјутерскиот криминал, е секако пријавата од страна на оштетениот, односно жртвата, а потоа следува следењето на сомнителни случаи и личности. Следење на работата на серверите и навремено забелењување на било каков недозволен пристап до нив, без разлика дали е сериозен напад или само хакерска игра.

Во оваа смисла, под поимот оштетен, може да бидат физички и правни лица, државни органи, јавни или приватни институции, групи или поединци. На пример, кога стручните лица кои ги одржуваат и администрираат информатичките системи ќе забележат дека дошло до неовластено навлегување во системот, кој тие го одржуваат однадвор и дека настанала одредена штета во смисла на губење податоци или на целокупното работење на системот, секако дека ова неовластено навлегување треба да го пријават до соодветен државен орган,

кој што е надлежен понатаму да постапи, со цел пронаоѓање и санкционирање на сторителот на ваквиот вид кривично дело.

Стручните овластени лица имаат функција да вршат проценка на видот и обемот на настанатата штета во компјутерот или компјутерскиот систем и превземаат понатамошни мерки.

Истражувачите на овој вид криминал најчесто користат оригинална апликациска програма, а понекогаш се случува да користат и специјален софтвер за анализа и алатки за истражување, но во најголем број случаи користат програми или апликации кои што сами ќе ги изработат и ќе ги искористат или во соработка со други хакери насекаде во светот, разменувајќи мислења и искуства на ист план.

Истражувачите имаат пронајдено различни начини за собирање траги од оддалечен компјутер, до кој немаат непосреден физички пристап, спроведувајќи пристап преку телефонска линија,мрежна или интернет конекција.

Овие процедури формираат дел од она што е наречено, компјутерска форензика, термин кој се користи при употреба на компјутерот за анализа на комплексни податоци.

Друга употреба на терминот е кога компјутерите се искористени во судот во форма на компјутерска графика, за да илустрираат комплексна ситуација, или како замена на голем волумен на листови – базирани на истражувања и состојби.

Инаку, компјутерска форензика[133] е доказ од компјутер, кој треба да биде издржан убедлив и доволен за судот да може да го прифати. Во форензичко – информатичките постапки, без разлика колку и да се внимателни лу]ето кои имаат за цел да крадат електронски информации, оставаат траги од нивните активности. Исто така, и сторителите на ваквиот вид кривично дело оставаат траги, така што сите тие траги и докази може да се искористат во постапката за кривичното гонење.

Компјутерските форензички специјалисти, прават многу сложени и комплексни истражувања, односно „ evidence recovery procedures“, со вештина и експертиза, која ќе го држи го држи кредибилитетот на електронските докази пред судот.

Во основа, овие постапки опфаќаат: копирање на податоци, барање на докази од електронска пошта и друга интернет комуникација, враќање на податоци, пребарување на документи и други податоци.

---

[133] Хрватска академска и истражувачка мрежа, CARNET/C, http://www.cert.hr/documents.php?long=hr&page=11

Во спроведувањето на борбата со организираниот криминал, освен оние единици и рогани формирани специјално за борба против компјутерскиот криминал, активно учество треба да земат и други институции и правни лица, директно засегнати со проблемот на компјутерскиот криминал.

Тоа, во главно, се државните комисии и агенции и тоа: Управа за финансиска полиција при Министерството за финансии,[134] која има за цел да спречува кривични дела поврзани со финансии, да спроведува финансиска контрола, да спроведува предистражни мерки за откривање на кривичното дело, соработува со други државни органи на тој план, соработува со сродни органи од други земји и сл. Потоа следува, Државната комисија за спречување корупција,[135] Дирекцијата за безбедност на класифицирани информации,[136] основана со Закон за класифицирани информации од 2004 година. Агенција за електронски комуникации,[137] банки, интернет провајдери, меѓународни компании, здруженија на граѓани, невладини организации, итн.

Искуствата на другите држави во светот во борбата со компјутерски криминал и справување со проблемите настанати како последица од компјутерски криминални дејства се од голема важност за формирање на ефикасен систем за превенција и сузбивање на кривични дела настанати со помош на компјутер и компјутерска технологија.

Како какрактеристичен и многу поучен пример за заштита од фалсификување и недозволено користење на платежните картички, ќе го разгледаме со Велика Британија и начинот со кој тие се справуваат со овој проблем.[138] Нејзиното значење е во развојот и имплементирањето на „чип и пин“ проектот, кој е земен за пример од повеќе земји во светот.

Заедно со огромните финансиски инвестиции кои се инвестирани за осовременување и подобрување на безбедноста во електронското функционирање на општеството, односно во развојот на „чип и пин“ и пилот - проектот на Единицата за криминал со чекови и електронски картички (иновативна единица, финансирана и од државниот и од приватниот сектор), во многубројните иницијативи, кои досега се превземени на тој план (некои од нив

[134] http://finance.gov.mk/node/103
[135] http://www.dksk.org.mk/index.php?option=com_content&task=view&id=32&id=32&itemid=51
[136] http://dbki.gov.mk/files/pdf_files/Zakon_za_klasificirani_informacii.pdf
[137] http://www.aec.mk/index.php?option.com_content&view=category&id=48&itemid=91&Long=ml
[138] „Глобален организиран криминал-трендови и случувања“,Д.Зигел,Х.ван де Бунт, Д.Зоур, Магор, Скопје,2009,стр.140

се дел од сеопфатни и комплицирани програми чијашто реализација е се уште во тек, во поголем број држави во светот), спаѓаат:

- претставување на контролниот систем со адреса и безбедносна шифра (која ќе ја знае само корисникот на картичката и која нема да се повторува) за да се намалат измамите со неприкажаните картички;

- огромна програма за обучување на „продавачите“ како да можат да препознаат фалсификувани картички;

- потикнувачки шеми, со цел да се охрабри пријавувањето на фалсификувани картички, (над 19 милиони фунти биле дадени како награди во 2002 година, како награди за забележување на вакви активности);

- развој на проект за целата индустрија, за да се спречи измамата со крадење идентитет;

- зголемување на бројот на трансакции овластени во места за малопродажба, со вклучена дополнителна обука заради воочување на сомнителни трансакции и препознавање на фалсификувани картички;

- користење картички на кои се впишани деталите на изгубени и украдени картички;

- воведување на поширок спектар на безбедносни методи за достава на картичките, со обезбедена тајност и заштита при транспортот и доставување на картичките до рацете на вистинските корисници;

- развој на системите, како што се „дозволено од *Visa*“ на „*Visa*“ и „безбедносен код“ на „ MasterCard“, за борба против измамите што се прават преку Интернет.

8. Компјутерскиот криминал и негови импликации врз безбедноста во Република Македонија

Со сеопфатниот и брз развој на компјутерите и компјутерсктата технологија се појавуваат големи закани во сите сфери на секојдневното живеење и функционирање во современото општество. Компјутерскиот криминал е современа појава која постепено навлегува во сите сегменти на општеството. Фактот дека компјутерите се главниот дел од сите сфери на општеството, допринесува и до голема ранливост и осетливост на општествените институции и поединци.

Компјутерите и компјутерската технологија, освен предностите имаат и големи негативни импликации врз целокупниот развој на државата, а со тоа негативно влијаат и врз безбедноста на граѓаните во државата.

Негативните импликации на компјутерскиот криминал врз безбедноста најдобро може да се разгледаат преку посебните области на негово влијание. [139]

- ***Индустрија на информациска технологија***

Компаниите на информациски и компјутерски технологии, вклучувајќи даватели на Интернет услуги (Интернет провајдери), компании за уредување и дизајнирање на страници на Интернет и компании за електронска трговија, се најчестите жртви на компјутерски криминал и разни видови на компјутерски напади.

Нападите, вклучувајќи хакирање, вируси, црви, спречување на пристапот до Интернет, и сл. бараат нагласена потреба од ефикасни мерки за компјутерска безбедност и заштита на компјутерите, компјутерската технологија и огромниот број на податоци кои се наоѓаат во нив, а кои имаат големо општествено значење.

[139] „Medjunarodni vodic za borbu protiv kompjuterskog kriminala“, Amerikanska advokatska komora, 2003,стр.222

Информацискатa технологија, посебно е осетлива кога станува збор за преносот на точни и навремени информации, за задржување на тајноста и доверливоста на податоците, заштита на финансиските средства и информациите во врска со безбедносните шифри.

- ***Комуникации***

Како и давателите на Интернет услуги, така и преносителите на телекомуникации се во голема мерка се поврзани и користат информациона технологија. Комуникацискиот сектор уште во најраната историја на негово постоење бил цел на различни напади.

Порано нападите биле за крадење на телефонски импулси, со цел да се разговара бесплатно било каде во светот и без ограничување на времето. Но, во денешно време нападите не се однесуваат само на телефонските импулси. Комуникациите често се цел на напади заради ширење на различни дезинформации, за прислушување и навлегување во доверливи подрачја, па дури потоа заради бесплатни услуги.

Значењето на комуникациските системи бара политика на спречување на компјутерски криминал и чување на услуги во случај на напад, посебно на најважните владини служби и групи за итни интервенции.

- ***Финансиски услуги и банкарство***

Финансиските превари се најчест и најопасен облик на компјутерски криминал, со кој се кочат способностите на земјата да привлече директни странски инвестиции и сериозни вложувања, затоа што со криминалот во оваа област остава лош впечаток и неможност да привлече сериозни инвестиции.

Високата технологија ја унапредува ефикасноста и ги смалува цените на работа, но ги изложува компаниите на надворешни пречки по безбедноста и сигурното и ефикасно работење.

Државните органи треба да превземат посебни мерки за да спречат употреба на своите банкарски системи за перење пари. Да се обезбедат што посигурни и побезбедни услуги за граѓаните, без разлика дали станува збор за граѓани на Република Македонија или за странски граѓани.

- ***Хемиска, биолошка и нуклеарна безбедност***

Потребно е огромно внимание од страна на државните органи посебно во оваа област, каде што штетите може да бидат големи, но и катастрофални, затоа што тоа се ресурси од витално значење. Во оваа област доволно е со само едно кликнување на глувчето да се направат огромни штети, без разлика дали се материјални и финансиски или дури и човечки жртви.

Сите закани во современиот свет и сите напади настануваат или со некој од овие видови оружје или со користење на закани дека ќе биде употребено некое од овие оружја. Република Македонија се уште нема нуклеарно оружје, затоа пак, посебно внимание треба да се посвети на другите два вида, на хемиското и биолошкото оружје, производството, чувањето и транспортирањето и користењето на истото.

- ***Комунални услуги и сообраќај***

Со компјутерски напад може да се сруши енергетска мрежа, системи за контрола авионски сообраќај, железнички системи, и други системи за управување со сообраќај, системи за водоснадбување, за метеоролошки услуги и сл.

Сите од претходно споменатите области имаат витално значење во секојдневниот живот во современиот свет. Нефункционирањето на било која од споменатите услуги доведува до големи штети во домаќинствата, градовите и државата.

- ***Информациони системи на државните органи***

Државните органи одржуваат бази на податоци и имаат обврска кон граѓаните безбедно да управуваат со податоците кои се меморирани во нив. Нападите на државните органи го нарушуваат кредибилитетот на државните органи и ја намалува довербата на граѓаните која е од витално значење за ефикасна државна управа.

Информационите системи на државните органи се најинтересна мета за напад на хакерите. Главната цел за напад на овие органи е хакерите да ја докажат својата способност и ефикасност во компјутерските вештини.

- ***Обични корисници на компјутери и компании***

Секој корисник на компјутер е подложен на вируси, хакирање и други видови на компјутерски криминал. Затоа е потреба соодветна обука за да се спречат или намалат ваквите напади.

Исто така, давателите на Интернет услуги треба да ги предупредат своите корисници за слабите точки и можните опасности. Штетите на индивидуалните корисници главно се во рамките на крадење на телефонски импулси, Интернет сообраќај или само едноставно внесување вируси вво компјутерот заради пробивање на лозинки или откривање на доверливи податоци и фотографии.

Може да се предизвикаат и штети на софтверот и хардверот на индивидуалниот компјутер. Тие штети може да бидат од кочење и бавно работење на одредени програми во компјутерот, до негово целосно блокирање и уништување.

Негативните импликации на компјутерскиот криминал врз безбедноста на граѓаните во Република Македонија , најдобро ќе ги согледаме преку секојдневните примери со кои се среќаваме во секојдневниот живот.

Прво, ќе го наведеме примерот, кој беше објавен од Македонската информативна агенција, на 16 ноември 2009 година, според соопштение на Министерството за внатрешни работи, кога биле забележани фалсификувани платежни картички на територијата на СВР Штип.[140] Првин била направена сомнителна трансакција на бензинска станица и тоа од страна на вработен на истата бензинска станица, а случајот бил забележан и пријавен од банката преку која била вршена трансакцијата, а при претресот кај сомнителното лице биле најдени уште пет фалсификувани картички. Тој ја открил и соработката со уште две лица, од истиот град и сите заедно во период од околу два месеци, противправно се стекнале со сума од околу 650 000 денари. Карактеристично за случајот, е што пронајдените платежни картички: Американ Експрес, Маестро, Мастер Кард и Виса, се издадени од домашни банки, но од страна на групата, оригиналните податоци биле бришани, по што електронски биле внесувани податоци од странски државјани, односно нивни сметки во Барклис банката од Лондон, Националната банка на Кувајт и други.

[140] http://www.mia.com.mk/default.aspx?mid=31&IId=1

На 12.07.2009 година, од страна на Министерството за внатрешни работи, било објавено соопштение, врз основа на шестмесечна анализа за компјутерскиот криминал, во текот на која биле откриени дури, 29 случаи. Од вкупниот број случаи, дури 20 дела се "оштетување и неовластено навлегување во компјутерски систем", потоа три дела се „издавање чек без покритие и злоупотреба на кредитна картичка", две дела „компјутерска измама" и по две дела се „соизвршителство" и „помагање" извршени со „оштетување и неовластено навлегување во компјутерски систем".[141] Исто така, во истото соопштение е направена и анализа за местото на извршување, односно главниот град се појавува како најчесто место за извршување на ваков вид на кривични дела, а што се однесува до сторителите, тоа се најчесто бугарски државјани и останатиот дел се македонски државјани. Најчесто, биле вршени трансакции и плаќања со фалсификувани платежни картички или со оригинални картички на кои компјутерски им биле менувани податоците, најчесто биле внесувани податоци на странски државјани, но имало и случаи со податоци на македонски државјани. Исто така, имало случаи и на неовластено користење на електронски и комуникациски услуги.

Карактеристичен е и примерот за „комјутерска измама" забележан во една спортска обложувалница во Скопје, кога двајца вработени преку специјална програма, која ја инсталирале на службените компјутери, недобитните тикети ги преправале и ги печателе како добитни и со тоа успеале да се стекнат со околу 500 000 денари.

Сопружници од Бугарија, биле осомничени дека со фалсификувани кредитни картички, украле околу 12.000 евра, од банкомати на банка во Скопје и во Софија. Тие на банкомат на домашна банка поставиле апарат наречен „скимер", со кој ги копирале, односно краделе податоците од сопствениците на платежни картички. Украдените податоци потоа ги вметнувале на празни пластични картички, со кои подигале пари од други банкомати. Сопружниците со лажните картички, направиле 191 трансакција, со кои украле околу 720.000 денари.

[141] „Medjunarodni vodic za borbu protiv kompjuterskog kriminala", Amerikanska advokatska komora, 2003,str.215

9. Соработка на државно и меѓународно ниво при откривање и спречување на компјутерскиот криминал

Соработката и координацијата меѓу институциите, се многу потребни при откривање и спречување на појава на компјутерски криминал, без разлика дали станува збор на соработка на локално, регионално, државно или меѓународно ниво.

Соработката меѓу институциите во една држава подразбира, превземање на мерки и активности за поквалитетна и попродуктивна работа и боефикасно решавање на проблемите предизвикани со криминална употреба на компјутерите и компјутерската технологија.

Важни компоненти за соработка во областа на безбедноста на компјутерските информации, се:[142]

- Помош на софтверската индустрија и размена на информации за клиентите;
- Работни упатства на база на учинокот;
- Заеднички критериуми: важен стандард за безбедност;
- Безбедносна ревизија и надзор на управувањето;
- Осигурување;

Поради тоа што, компјутерскиот криминал се смета за светски проблем, важно е да се разгледа и нивото на меѓународна соработка во оваа област.

Соработката на државно и меѓународно ниво во областа на компјутерскиот криминал, посебно е регулирана од Европската Унија, Групата 8 (Канада, Франција, Германија, Италија, Јапонија, Русија, Велика Британија, САД), посебно од Подгрупата за криминал од висока технологија, Советот на Европа, Организацијата за европска соработка и развој, Азиско – Пацифичка економска соработка, Унија на меѓународни телекомуникации.

Исто така, мора да постои соработка и меѓу навладините организации, како што се: Меѓународна трговска комора, Глобален работен дијалог за електронска трговија,

[142] „Medjunarodni vodic za borbu protiv kompjuterskog kriminala“, Amerikanska advokatska komora, 2003,str.242

Американско здружение на информациска технологија и Советскиот сојуз на информациони технологии и услуги, Глобален проект за Интернет, Комисија за глобална информациона инфраструктура.

Земјите од регионот го прават првиот чекор во борбата со компјутерскиот криминал, но се уште треба многу да работат на ова пол,е се вели во извешатј од Советот на Европа, со чија поддршка се одржала регионалната конференција за обука на судии и јавни обвинители во Охрид. Земјите во регионот се на почеток. Тие се уште немаат стратегија за борба со компјутерскиот криминал.[143]

Земјите имаат законска легислатива, тоа е првиот чекор, но се уште им треба многу обука за да може комплетно да се посветат на решавањето на овој проблем, вели Катерина Шулман, од Советот на Европа. Експертите од регионот, на Конференцијата на тема - Компјутерски криминал - треба да разработат стратегија за заедничко совладување на овој вид криминал.

9.1. Компјутерски криминал во меѓународната заедница

Компјутерскиот криминал е мошне комплексен поим, кој зема се поголем замав во сите држави во светот, без разлика на нивниот развој. Затоа, на кратко ќе ги разгледаме законските регулативи на некои од соседните земји и пошироко во врска со компјутерскиот криминал.

Сето ова е со цел, да се направи споредба со состојбите во тие држави и состојбата на ова поле во Република Македонија.

Превентивните мерки често не се доволни, за борба со различните видови на злоупотребата на компјутерите за различни цели, затоа логично е дека сите современи кривични законодавства во системот за инкриминација познаваат едно или повеќе кривични дела, за кои се пропишани различни видови санкции.

[143] http://www.daily.mk/cluste3/19b0e0a11b6c5..97865878a3a31f62/1114225/anonimusi-go-napadnaa-sajtot-na-evropskiot-parlament

Меѓународната правна помош, е важна како за развиените земји, така и за земјите во развој. Затоа, потребни се посебни договори за взаемна помош, потоа процедури за службени барања и начини на осудување и изрекување казни.[144] Исто така, потребно е да се предвидат постапки во случаи кога земјата, чија помош се бара, нема одговарачки закони, случаите кога органите на редот немаат доволна техничка стручност, случаите кога традиционалните начини се премногу бавни и големи.

Многу земји имаат закони кои се однесуваат на кривични дела против компјутерите. Прифаќајки го фактот дека прв чекор кон компјутерски криминал, е пристап и користење компјутер од страна на криминалците, хакерите и останати злонамерни лица, државите донеле закони за компјутерски криминал кои содржат неколку заеднички елементи:

◇ Законот предвидува дека кривично дело е добивање пристап до компјутер без одобрување или пристап до заштитени компјутерски системи;

◇ Законот предвидува казнени мерки за дела направени по пристап до компјутер, како што се неовластен пристап до податоци, менување и уништување податоци или софтвери неовластено користење компјутерско време и ресурси.

Најголем придонес во борбата против компјутерскиот криминал, и подетално објаснување на овој поим, има Советот на Европа и тоа преку Конвенцијата на Советот на Европа за превенција од тероризам и Европската конвенција за Сајбер криминал,[145] со што се предвидува легална одговорност за заштита на човековите права и индивидуални слободи.

Врз основа на овие два важни документи, се раководат, скоро сите европски држави без разлика дали тие се членки на Советот на Европа, или не. Тие настојуваат својата легислатива да ја насочат во тој правец, за што поефикасно и понавремено справување со проблемите поврзани со компјутерите и компјутерската технологија. Исто така, посветено е внимание и на казните и санкциите, кога ќе бидат фатени сторители на компјутерски кривични дела.

---

[144] „Medjunarodni vodic za borbu protiv kompjuterskog kriminala“, Amerikanska advokatska komora, 2003,str.88

[145] “Cyberterrorism:the Use of the Internet for terrorist purposes”, by Council of Europe, 2007, http://book.coe.int

Според Советот на Европа, наведени се три феномени, во областа на компјутерите и компјутерсктата технологија:

1. Напади преку Интернет кои предизвикуваат штети не само на електронските комуникации или на компјутерската инфраструктура, туку и на други системи, легални интереси, дури и човечки животи.

2. Дистрибуирање на илегална содржина, како закани со терористички напади, финансирање на недозволени активности, и ширење на расистички и ксенофобичен материјал.

3. Други логистички употреби на компјутерите и компјутерската технологија.

Нападите кои се изведуваат преку Интернет се карактеристични, по тоа што тие може да се изведат било каде во светот, тие се многу брзи и многу е тешко да се следат и да се најдат докази за нив.

Најсоодветен интернационален документ за компјутерскиот криминал е ***Конвенцијата за Сајбер криминал*** (COE – Convention on cybercrime).[146] Во која детално е посветено внимание на дефинирање на компјутерски систем, компјутерски податоци, даватели на услуги.

Глава 1, од Конвенцијата, која е наречена Кривично материјално право, е разработено следново - Во првиот дел, се разгледуваат кривичните дела против тајноста, целосноста и достапноста, вториот дел, е за компјутерските кривични дела. Третиот дел од Конвенцијата, е посветен на делата во врска со содржината, а четвртиот дел е за дела во врска со кршење на авторски и сродни права. Петтиот дел, се однесува на одговорност и санкции.

Глава 2, е Процесно право, која е посветена на процесните одредби, услови и заштитни мерки, итна заштита на нападнати податоци, налог за достава на податоци, претресување и одземање на компјутерски податоци.

Во Глава 3, е опфатена судската надлежност. Исто така, во Конвенцијата е посветено големо внимание и на Меѓународната соработка.

[146] Конвенција за сајбер криминал, Соверт на Европа, Будимпешта, 2001

Конвенции кои ја дополнуваат, оваа Конвенција, се:

1. Европска Конвенција за екстрадиција, отворена за потпишување на 13 декември, 1957 година, во Париз;

2. Европска Конвенција за взаемна помош во кривични дела, отворена за потпишување на 20 април, 1959 година, во Стразбур;

3. Дополнителен протокол на Европската Конвенција за взаемна помош во кривични дела, отворена за потпишување на 17 март, 1978 година, во Стразбур.

Врз основа на Конвенцијата за Сајбер криминал е донесена и „ Одлука на Советот на Европската Унија за напади на информациони системи “, која се однесува на државите членки, а со цел да се осигура илегалниот пристап до информатичките системи и илегалното мешање во податоци, кои се казнуваат како кривични дела.[147]

Во Германскиот Кривичен Законик,[148] во 1987 година, немало кривични дела поврзани со компјутер, но тоа не значи дека не биле казнувани недопуштените дејства. Во 1986 година во Германија, бил донесен Кривичен Закон за сузбивање на општествен криминал, кој е предизвикан со компјутер, и тоа во облик на компјутерска шпионажа, чл.202а, компјутерска саботажа, чл.303а, фалсификување податоци, чл.269, попречување при правна обработка на податоци, чл.270, и промена на податоци, чл.302а.

Кривичниот Законик на Австрија,[149] предвидува кривично дело предизвикано од компјутери и компјутерска технологија уште во 1989 година. Ваквото кривично дело е наречено оштетување на податоци и е опфатено во член 126а.

Во Велика Британија, во 1990 година, е донесен посебен Закон за злоупотреба на компјутерите, кој се однесува на сите компјутерски системи. Овој Закон е кривичен закон и предвидува поголема низа од кривични дела, поврзани со злоупотреба на компјутери и други информациони системи, за кои се пропишани многу строги казни.[150] Законот за злоупотреба на компјутерите е значаен по тоа што излегува надвор од рамките на злочинот против компјутерскиот систем, опфаќајки и дела како што се перење пари и детска порнографија.[151]

---

[147] "Cyberterrorism:the Use of the Internet for terrorist purposes", Council of Europe, 2007, стр.54 http://book.coe.int

[148] Schanke-Schroder,Strafgesetzbuch,Munchen,1978,str.76.

[149] E.Foregger-E.Serini, Stratgestzbuch,Wien,1989,str.92.

[150] Martin Wasik, The computer misuse act, The Criminal review,1990,str 767.

[151] „Medjunarodni vodic za borbu protiv kompjuterskog kriminala", Amerikanska advokatska komora, 2003,str.57

Велика Британија е прва земја која се занимавала со проблемот на вонтериторијална судска надлежност за компјутерските злосторства.

Во Кривичниот Законик на Република Српска, има сличен пристап кон овој вид кривично дело, како и пристапот во Република Македонија, со таа разлика што во нашиот Законик овој поим е внесен во 1996 година, а во Република Српска е внесен дури во 2000 година .Односно кривичното дело предизвикано со комп-јутер и компјутерска технологија е дефинирано како: Упад во компјутерски систем, член 260. [152]

Ќе ја споменеме и Ерменија [153], каде не е доволно разработена анализата, детекцијата и превенцијата на сајберкриминалот, затоа што компјутерските технологии не се доволно развиени. Злоупотребите на сајбер просторот не се дефинирани во Кривичниот Законик на Република Ерменија, како посебен corpus delicti. Но, во тек е изработка на Закон за информатички технологии и информатичка безбедност.

Кривичниот Законик на Република Словенија, ги препознава следниве кривични дела, поврзани со компјутери и компјутерска технологија: Противзаконски влез во заштитени компјутерски бази на податоци, член 225, и Упад во компјутерски систем, член 242.[154]

Кривичниот Закон на Република Хрватска во членот 223, препознава кривично дело под називот: Оштетување и употреба на туѓи податоци (кое се однесува на автоматски обработени податоци или компјутерски програми). [155]

Кривичниот Законик на Руската Федерација, разликува повеќе компјутерски кривични дела во посебната глава 23, којашто носи назив: Кривични дела во сферата на компјутерските информации. Овде се пропишани следните кривични дела: Противправен пристап до компјутерски информации, во членот 272, правење, користење и ширење на штетни компјутерски програми, во чл.273 и повреда на прописите за експлоатација на компјутерите, компјутерските системи или нивни мрежи во член 274. [156]

---

[152] Sluzbeni glasnik R.Srpske,Banja Luka, br.22, 2000.
[153] "Cyberterrorism:the Use of the Internet for terrorist purposes", Council of Europe, 2007, http://book.coe.int,str109.
[154] B.Penko,K.Stralig,Korenski Zakonik,z.uvodnim pojasnili,Ljubljana,1999.
[155] Narodne novine R.Hrvatske,Zagreb,br.110/1996
[156] J.i.Skuratov,V.M.Lebedov,Kommentari u glavnom u kodeksu Rossijskoj federaciji,Moskva,1996.

Во Кривичниот Закон на Република Србија, компјутерските кривични дела се воведени во 2005 година, и тоа како, кривични дела против компјутерските податоци и основано е посебно, Одделение за борба против високотехнолошкиот криминал.

Во Кривичниот Законик на Канада, основните федерални одредби поврзани со компјутерски криминал се: член 342.1 Неовластено користење на компјутер и член 430.1.1 Штета поврзана со податоците.[157]

Со неовластеното користење на компјутер се подразбира – забрана за кражба на компјутерски услуги, - да се штити приватноста, - да се прогласи прекршок користење на компјутерски систем во различни престапи, насочен е кон лица кои се занимаваат со трговија на програми за лозинки и шифрирање и притоа да предизвикаат престап со таа дејност. А, со штетите поврзани со податоци се регулираат штетите нанесени на податоците и се предвидуваат казнени мерки за престапите за лица кои уништуваат или менуваат податоци, ги прават податоците бессмислени, бескорисни и неефикасни, спречува или прекинува проток и законско користење на податоците, спречува или ограничува пристап на овластени лица до податоците.

Најкарактеристичен и најдобар, е примерот со Соединетите Американски Држави, каде што е посветено најголемо внимание, на овој вид кривични дела.[158] Во Соединетите Американски Држави се донесени поголем број закони и подзаконски акти во врска со кривичните дела предизвикани со помош на компјутер и компјутрска технологија. Во овие закони со прецизност и деталност се разгледани сите видови на кривични дела кои може да се остварат со помош на компјутер и компјутерска технологија.[159]

Во овој контенст ќе споменеме дека законите се поделени во две групи и тоа суштински и процедурални закони.

Како *суштински закони* ќе ги споменеме следниве: заштита на online идентитетот, хакерство, недозволено навлегување во компјутерски системи, детска порнографија, интелектуална сопственост, online коцкање.

А, како *процедурални*, ќе ги споменеме: авторитет за пристап и користење на електронски податоци од трета страна, вклучувајќи провајдерски Интернет услуги; авторитет

[157] Кривичен Законик на Канада, http:// lois.justice.gc.ca/en/C-46/39387.html
[158] http://cybercrime.gov.cc.html, Department of Justice
[159] http://www.oas.org/juridicio/spanish/us_cyb_laws.pdf

за интервенирање во електронски комуникации; авторитет да се пребаруваат и користат електронски податоци.

Најзначаен закон за компјутерски криминал, во Соединетите Американски Држави е – Законот за компјутерски превари и злоупотреби (CFAA), кој бил видно изменет и дополнет, како одговор на терористичките напади од 11 септември, 2001 година, со усвојување на Законот за соединување и јакнење на Американските одговарачки инструменти за спречување и сузбивање на тероризмот (PATRIOT ACT 2001). [160]

Во овој контекст, ќе наведеме и примери за кривични дела поврзани со компјутер и компјутерска технологија, освен за земјите од Европа и САД, ќе наведеми и примери од азиско – пацифичкиот регион, односно ќе ги разгледаме Австралија и Јапонија како поспецифични примери, кои исто така не се имуни на кривични дела предизвикани со компјутер и компјутерска технологија.

Австралија донела сеопфатен Закон за компјутерски криминал, во 2001 година. Иако, во него не постои поим „заштитен" компјутер, има некои сличности во пристапот со американскиот Закон за компјутерски превари и злоупотреби.

Поголем број од членовите на овој закон се однесуваат на компјутерите на државните органи или на компјутерите до кои се пристапува во посредство со службите за телекомуникации. Обвинетите, за дело од Законот за компјутерски криминал се осудуваат на казна затвор од две до десет години.

Јапонија, исто така има специфичен пристап кон компјутерскиот криминал, дефиниран во Законот за неовластен пристап во компјутери, донесен во 1999 година., во кој се опфатени слични области како и во американскиот закон.

Содржи членови кои се однесуваат на неовластен пристап до компјутерите, трговија со лични податоци, намерно мешање во компјутерски системи, компјутерски превари и стекнување на незаконски добивки со воведувањето на погрешни информации во компјутер кој се користи за работа.

[160] „Medjunarodni vodic za borbu protiv kompjuterskog kriminala", Amerikanska advokatska komora, 2003,стр.51.

9.2. Соработка меѓу државниот и приватниот сектор за откривање и спречување на компјутерски криминал

Соработката помеѓу јавниот и приватниот сектор во однос на прашањето за користењето на Интернетот и активностите на компјутерскиот криминал, е многу значајна.

Кога приватниот и јавниот сектор разменуваат и координираат информации кои се однесуваат на ваков вид кривични дела, можат подобро да увидат како да реагираат и да ги ублажат негативните влијанија.[161]

Безбедноста на компјутерите и компјутерските мрежи, претставува дел од академската дисциплина во компјутерските науки, а непостоењето на безбедноста на компјутерите и компјутерските мрежи е од посебна важност за тие што користат Интернет. Ниту државните органи, ниту приватните неможат сами да решат ваков вид на проблем.

За успешно откривање и спречување на појава на компјутерски криминал или било каков вид да недозволена примена на компјутерскта технологија, од голема важност е соработката меѓу институциите во една држава.

Соработката меѓу институциите, главно се заснова на Кривичниот Законик на Република Македонија, и тоа, попрецизно се заснова на примената на Законот за заштита на лични податоци, Законот за слободен пристап до информации од јавен карактер, Закон за класифицирани информации и сл.

Институционалната соработка, пред се подразбира превземање на мерки и активности меѓу различните служби во една инистуција. Ваквиот вид на соработка најчесто е регулиран со правилници и упатства за работа. Таков е примерот со Министерството за внатрешни работи и Одделот за организиран криминал.

Меѓуинституционалната соработка, подразбира превземање на мерки и активности во борбата против злоупотребата на компјутерите и компјутерската технологија, со цел гонење на сторителите на ваквите дела и спроведување на законите.

---

[161] „Medjunarodni vodic za borbu protiv kompjuterskog kriminala“, Amerikanska advokatska komora, 2003,стр.215

Високо ниво на соработка, најдобро може да се постигне со почитување на одредбите од Конвенцијата за сајбер криминал, која е донесена од Советот на Европа.

При спроведувањето на истрага за одредено кривично дело поврзано со компјутерите и компјутерската технологија, активно учество би требало да земат повеќе институции, надлежни за спроведување на законите, и тоа Министерството за внатрешни работи, Царинската Управа, Финансиската полиција и сл.

Оваа соработка, која што пред се, произлегува од законските дефиниции, најчесто се остварува преку склучување на протоколи за соработка помеѓу различни институции.

Меѓународната координација и соработка се значајни исто колку и правните и законските облици.[162] Со законите за компјутерски криминал малку се постигнува, без соодветни владини структури и обучен персонал кои се неопходни за делотворно решавање на прашања за надлежностите, меѓународните барања за помош, како и претрес и заплена на електронски доказен материјал.

Иако државите имаат граници, Интернет просторот ги нема, затоа државите треба да поседуваат правна надлежност да помагаат на странски земји во истрага, дури и ако таа држава не претрпела никаква штета, туку само е место на престој и транзит на сторители на компјутерски кривични дела.

Јасно е, дека е потребен координиран и постојан пристап меѓу државите во истрагите и кривичното гонење на компјутерскиот криминал, за да се следат трагите и електронските комуникации расфрлани по различни временски зони и области на судска надлежност со различни правни системи и нивоа на техничка обученост.

Изработен е и Меѓународен водич за борба против компјутерскиот криминал, кој претставува проект на Комитетот за заштита на приватност и бобра против компјутерскиот криминал на Американската адвокатска комора, а е посветен на меѓународната соработка и координација во борбата против компјутерскиот криминал, проширување на Групата 8 и Советот на Европа и други мултинационални организации и индустриски земји.

162

„Medjunarodni vodic za borbu protiv kompjuterskog kriminala“, Amerikanska advokatska komora, 2003,стр.41

Овој Водич, во најголема мерка има врска со компјутерскиот криминал на земјите во развој, а е изработен со цел да се забрза:

- усвојување закони за компјутерски криминал;
- почитување на човекови права, приватност и безбедност;
- соработка во оваа област;
- соработка меѓу органите на редот, давателите на услуги во комуникациите, компаниите кои се занимаваат со електронска трговија;
- прифатливи начини за претрес и запленување на компјутери и електронски доказни материјали;
- соработка меѓу органите на државниот и приватниот сектор во борбата против компјутерскиот криминал.

9.3. Ниво на меѓународна соработка и потребите од нејзино зајакнување заради успешно откривање и спречување на компјутерски криминал

Компјутерскиот криминал е таков вид на криминално однесување, кое често пати ги поминува границите на дејствување на една држава.

Времето и местото на извршување, често се на различни страни на светот. Затоа, многу е важна меѓународната соработка во оваа област, ако не и најважна за откривање и спречување на кривични дела од оваа област.

Основата за овој вид на соработка, најчесто се Меѓународните Конвенции,[163] како и различни билатерални договори (меѓу две држави), и мултилатерални договори (меѓу повеќе држави).

Република Македонија е активна членка на овие институции и тела и тоа со свои делегирани претставници во седиштата, како и канцеларии во нашата земја.

[163] Конвенција за сајбер криминал, Соверт на Европа, Будимпешта, 2001

Меѓународната соработка најдобро е регулирана преку одредбите од Конвенцијата за Сајбер криминал. Разработени се општите принципи на меѓународна соработка, потоа подетално е разработена екстрадицијата. Опфатени се и општите принципи кои се однесуваат на взаемна помош меѓу две и повеќе страни засегнати со проблем.

Оваа Конвенција, е отворена за потпишување на државите членки на Советот на Европа, но и држави кои не се членки, но учествувале во нејзината изработка, а на барање на Советот на Министри, може и други држави да пристапат на Конвенцијата, но само со согласност на сите членки.

Земјите, потписнички на Конвенцијата, ќе соработуваат во согласност со одредбите, ќе применуваат меѓународни инструменти за соработка во врска со вакви кривични дела, договори потпишани врз основа на меѓународното и домашното законодавство и тоа за собирање на податоци за кривичните дела и водење на постапките против сторителите на вакви кривични дела.

Во Конвенцијата се вели дека страните потписнички, една на друга ќе пружат взаемна помош во најширок можен обем, во спроведувањето на истрагите или постапките во врска со кривични дела поврзани со компјутерските системи и податоци, или во собирањето на докази за кривичното дело во електронски облик.

Најчест и најизразен вид на меѓународна соработка е соработката која се остварува преку ИНТЕРПОЛ, односно меѓународна полиција, потоа преку ЕУПОЛ, европска полиција и СЕКИ ценатрот, координативно тело за полициска и царинска соработка на земјите од југоисточна Европа.

Во рамките на ИНТЕРПОЛ, при Министерството за внатрешни работи на Република Македонија, функционира дежурниот центар кој е достапен 24 часа, седум дена во неделата, во кој Република Македонија од 2008 година, е активно вклучена. Со тоа, се олеснува меѓународната соработка и борбата против различните облици на високо – технолошкиот криминал, брзата и навремена размена на информации.

Значајни се активностите што НАТО ги превзема за борба против компјутерскиот криминал и нападите од ваков вид. [164] Формирајќи ја NCSA (NATO Communications and Information Sistem Services Agency), односно Агенција за комуникациски и информатички услуги, ја имплементирале програмата за сајбер одбрана.

Оваа агенција функционира во Технички Центар (NATO Information Assurance Tehnical Centre), кој се грижи за безбедноста на сите компјутери и компјутерски системи што ги користи НАТО, преку посебни процедури и директиви. Исто така, се грижи за пренос на криптографски материјали и безбедна размена на каков било друг вид на информации.

Исто така, од голема важност е да се спомене меѓународната соработка што ја остварува Јавното Обвинителство. Активностите на Обвинителството се остваруваат преку, укажување на правна помош по барања од надлежните органи, странски органи, одржување на работни средби заради запознавање со состојбите, особено во организираниот криминал, размена на искуства и договарање на натамошните активности, со јавните обвинителста на други држави, работни средби со претставници на меѓународните организации и асоцијации и учество на меѓународни советувања, едукативни курсеви и студентски посети.

Освен укажувањето на меѓународна правна помош, со превземање на дејствијата што се барани со молбите, значајни се и активностите на Јавното Обвинителство за организиран криминал и корупција, во реализацијата на повеќе истражни мерки во заеднички акции со Обвинителствата на другите држави по предмети од меѓународниот криминал.

Потребата од ваквата соработка е интензивирана поради зачестени случаи на кривични дела извршени или подготвувани на територии на повеќе држави.

Врз основа на меморандумот за разбирање, на Јавното Обвинителство на Република Македонија, Државното Обвинителство на Република Албанија, Обвинителството на Босна и Херцеговина, Државното Обвинителство на Република Хрватска, Државното Обвинителство на Република Србија, Врховниот Државен Обвинител на Црна Гора за регионална соработка против организираниот криминал, воспоставена е мрежа на обвинители преку кои се остварува побрза и полесна соработка.

Исто така, Обвинителството остварува соработка и поврзување со Јавните Обвинителства на земјите од Југоисточна Европа.

---

[164] http://www.ncsa.nato.int/topics/Cyber_Defence.html

Спроведено во пракса, при сите видови на наведени соработки и координација, за успешно спроведување на истраги од областа на компјутерскиот криминал, потребно е соработката да биде подигната на ниво на тимска работа, со формирање на тимови составени од експерти од различни области од горенаведените институции.

9.4. Можен модел на соработка за сузбивање на компјутерски криминал

Со оглед на тоа што компјутерскиот криминал е мошне комплициран облик на криминал, потребен е и соодветен пристап за негово навремено откривање и спречување. Затоа во Република Македонија, е потребна уште поголема ангажираност за осовременување на институциите и за обучување на соодветни кадри.

Компјутерскиот криминал, посебно е опасен во областа на економијата и на финансиите, каде што има и најголеми штети, токму затоа е потребно посебно внимание во овие области.

Во спроведувањето на борбата со организираниот криминал, најголема улога имаат Министерството за внатрешни работи, Јавното Обвинителство, и Агенцијата за разузнавање, но мислам дека од голема важност за откривање на компјутерски криминал е вклучувањето на други органи, односно државни агенции во негово навремено откривање и спречување. Тоа се главно државните агенции: Агенција за спречување перење пари и финансирање тероризам, Антикорупциска Комисија, Дирекција за безбедност на класифицирани информации, Агенција за електронски комуникации.

Потребно е поголемо ниво на соработка, размена на информации, координирање на активностите, а исто така од голема важност и поседување на висока технологија, односно вложувања во осовременување на компјутерите и компјутерската технологија со која работат споменатите органи.

Најефикасно и најбрзо откривање и спречување на секаков облик на компјутерски криминал и недозволени дејства со помош на компјутер, може да се остварат само со меѓусебна соработка и координација меѓу сите претходно споменати институции и агенции и тоа со примена на најмодерна и најсовремена технологија, за да може да се биде во чекор со криминалците.

За жал, поради предностите на комуникациската технологија, како што се ниските цени, лесната употреба, можности за анонимност, кривичните дела може да се изведуваат со поголема леснотија, а во спротивност е откривањето на сторителите што е во голема мера отежнато.

Република Македонија, превзема значителни мерки и активности за подобрување на нивото на образование за борбата против компјутерскиот криминал.

Посебно интересен е примерот за учеството на најпознатиот светски хакер во одредени предавања во нашата земја. Порано бил озлогласен хакер, а денес предава како да се заштитат од таквите како него. Тој им предавал на македонските IT инженери како да го спречат интернет криминалот. Се барал со потерница, зошто влегол во системите на ФБИ, Нокиа, Моторола, Фуџитсу. Одлежал 5 години затвор, а по излегувањето во 2000-та, три години му било забрането да користи интернет, дури немал ни мобилен телефон. За неговите сајбер авантури е снимен филм, а денес има сопствена консултантска куќа за компјутерска заштита.

Тој рекол дека парите не биле причина да стане хакер, туку љубопитството било главната причина за тоа, интелектуален предизвик, истражување на науката.

Тоа е еден вид опасна игра. Тој Република Македонија ја вброил во помалку безбедните земји и примамливи за сајбер криминалците. Но, тоа не е само компјутерски проблем, туку и луѓето треба да бидат претпазливи дека некој им ги демне парите на сметка, тајните документи на e-mail и податоците во мобилните телефони.

Рапублика Македонија и во иднина треба да организира вакви и слични предавања, да се организираат гостувања во странство за поголемо образование на информатичките експерти, да се организираат размени на студенти од оваа облласт, со цел да се разменат досегашните достигнувања и начините на кои би можеле да се спречат криминални дејства со компјутер и компјутерска технологија.

Главната цел на ова истражување е да се дефинира поимот компјутерски криминал, да се објаснат неговите својства, да се изнесат сите негови форми и облици. Компјутерскиот криминал е појава која ги засега сите земји во светот. Од тука, се јавува потребата да да се посвети поголемо внимание на овој проблем.

Република Македонија не е имуна на било каква појава, а посебно не е имуна на современите технологии и на нивните негативни влијанија. Компјутерскиот криминал има влијание врз сите земји во светот, вклучувајќи ја и Република Македонија. Затоа, можеме да заклучиме дека ова истражување, ќе биде од големо значење, затоа што прецизно ја разработува оваа појава, факторите кои допринесуваат за појава, но нуди и одговори за превенција и можна заштита на компјутерите и компјутерската технологија.

Овој труд може да биде многу корисен, во најголема мера, за студентите кои се посветени на безбедносните науки, потоа студенти од информатичките науки. Исто така, трудот може да биде од корист и во безбедносните структури, посебно на секторите кои се занимаваат со оваа тематика.

10. Заклучок

Од овој труд можеме да заклучиме дека е корисно да се стекне увид во моделите и пристапите во законите и прописите на земјите и мултилатералните организации што се разгледани во него. Потребна е детална разработка на законите и прописите за полесно совладување на проблемите што настануваат од ваквиот вид кривични дела и можности за превентивно дејствување, со цел да се намалат или да се спречат нападите од ваков вид.

Не е предоцна да се прифатат искуствата кои досега не биле прифатени, посебно безбедносните режими на информациско – комуникациските системи.

Кога се во прашање надлежностите, посебно во случаи на компјутерски криминал, тие зависат од соработката меѓу сите земји и правни системи. За да може да соработуваат, тие треба да бидат посебно оспособе, да имаат соодветно образовани кадри, да бидат опремени со најсовремена компјутерска технологија. Треба да имаат можност брзо да одговорат на барањата за помош при пресретнување, конверзација, пребарување и заплена на електронски податоци.

Преку одреден број меѓународни иницијативи направен е обид за ефикасно и навремено решавање на ваков вид проблеми.

Најзначајна е Конвенцијата за компјутерски криминал на Советот на Европа.Која е потпишана од земјите од Европската Унија и голем број други држави, кои настојуваат што поефикасно да се справат со проблемите од ваков вид.

Постои и цело богатство на ресурси, модели и мрежи на располагање за помош на земјите. Меѓутоа и понатаму постои сериозен недостаток на координација на меѓународно ниво за важни прашања. Јасно е дека компјутерскиот криминал претставува глобален проблем кој бара решавање на глобално ниво.

Појавата и брзиот пораст на компјутерскиот криминал имаат значајни импликации за владите и граѓаните ширум светот.

Потребно е постојано внимание на државните органи и обезбедување ресурси за обука за водење истраги и форензика во области на висока технологија, основање организации во земјите и активно ангажирање на меѓународен план.

Тоа, исто така бара соработка на повисоко ниво меѓу државниот и приватниот сектор, за да може соодветно да се одговори на компјутерскиот криминал.

Таа соработка треба да се заснова на размена на информации, соработка во заедничката работа со цел постигнување минимални стандарди на глобално ниво. Органите на редот се повеќе мора да се занимаваат со компјутерскиот доказен материјал, како и улогата на информациско – комуникациската технологија и во кривичните дела како што се: убиства, силувања, трговија со дрога, детска порнографија и сл.

Размената на информации меѓу приватниот и јавниот сектор е неопходна поради ефикасна превенција и гонење на компјутерскиот криминал. Размената на информации на регионално и на меѓународно ниво, може да помогне и ублажи понатамошен компјутерски напад, да помогне во примена на законите во гонење на криминални активности и олеснување на активности кои подржуваат подобри и поефективни начини за безбедна работа на сите корисници на информатичко – комуникациската технологија.

Компаниите, државните органи и поединците во целиот свет ги користат предностите на Интернетот преку електронска трговија, електронска влада и електронска пошта. Но, покрај позитивните можности, Интернетот е подложен и на разновидни напади. Ниту државниот, ниту приватниот сектор не можат да ги решаваат сами ваквите проблеми.

Не е доволно што земјите од Групата 8, заеднички ќе се борат против компјутерскиот криминал, ниту тоа што Советот на Европа ја донел Конвенцијата за компјутерски криминал, туку потребно е секоја земја да се занимава со проблемит енастанати поради компјутерски криминал, затоа што во спротивно ќе стане најслаба алка во глобалната кибернетска безбедност.

Според импликациите на компјутерскиот криминал врз безбедноста во современиот свет мора да се спроведат и соодветни мерки за заштита на компјутерите и компјутерските системи заради нормално функционирање на виталните функции во општеството.

Во ерата на компјутеризација и развој на информатичкото општество нема сектор ниту област во општеството која не е поврзана со компјутер и компјутерска технологија и Интернет и од тие причини осетливоста од хакерски влијанија е многу голема. Поради тоа потребно е да се превземат и соодветни мерки за заштита и и превенција, а потребна е и соодветна обука на персоналот за соодветно и најбезбедно работење со компјутерите и компјутерската технологија.

Република Македонија спаѓа во земјите во развој и компјутерско и информатичко осовременување и таа во многу голема мерка е осетлива на дејствата на компјутерскиот криминал.

До сега во Република Македонија е посветено само основно внимание на проблемите од компјутерскиот кримина, но се настојува кон детализирање и усовршување на оваа област.

. Тој како појава е дефиниран во Кривичниот Законик на Република Македонија, опфатен е во законите, но сепак е потребно уште по длабоко и попрецизно дефинирање и утврдување, за да може и соодветно да се одговори, за штетите да бидат минимални или пак воопшто да ги нема.

Недостатоци во борбата против компјутерскиот криминал се: неадекватната меѓународна координација и крајно непотполна рамка и организациона способност во земјите во развој кои се неопходни за борба против компјутерскиот криминал.

Целта на овој труд е да се разгледаат законите во поголем број земји во светот, а со тоа да се направи споредба со законите во Република Македонија и да се утврди во која насока тие треба да се движат.

Исто така, треба да се разгледаат прашањата од судска надлежност, соработката во меѓународните истраги. Потребно е да се развијат и прифатат начини за претрес и заплена на електронски доказен материјал. Посебно внимание треба да се посвети за остварување на соработка меѓу општествениот и приватниот сектор.

11. Користена литература

1. Americka advokatska komora (Chikago) , Komitet za zastita privatnosti I borbu protiv kompjuterskog kriminala, Odeljenje za naucno I tehnolosko pravo, *„Medunarodni vodic za borbu protiv kompjuterskog kriminala"*, Produktivnost, Beograd, 2004.

2. Бакрески, Оливер. *„Најсилно оружје досега"*, Современа македонска одбрана, бр.9, стр.165. Скопје, 2004.

3. Бункер, Ц. Бункер. *„ Не-државни закани и идни војни" ,*превод Анита Костовска, Нампрес, Скопје, 2009.

4. Георгиева, Л. „Творење на мирот – Мирот, безбедноста и конфликтите по студената војна", Виладорф,Скопје, 2004.

5. Гинтер, Кајзер. *„Криминологија - вовед во основите",* Александрија, Скопје, 1996.

6. Гоцевски, Трајан. *„Основи на системот на национална безбедност"*, Филозофски факултет, Скопје, 2006.

7. Dimitrijevic, P. *"Kompjuterski criminal"*, Beograd, 2007.

8. Denning, E. Dorothy. "Cyberterrorism - Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, Georgetown University, 2000.

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

10. Зигел, Д. Х.ван де Бунт, Д.Зоур. *„Глобален организиран криминал-трендови и случувања",* превод - Николина Утковска, Магор, Скопје,2009.

11. *"Kompjuterski kriminalitet I potreba koncipiranja krivicnog dela kompjuterske zloupotrebe"*, JRKKP, Beograd, 1991.

12. Котовчевски, Митко. *„Национална безбедност“* (прв дел), Македонска Цивилизација„ Скопје, 2000.

13. Котовчевски, Митко. *„Извори на загрозување на мирот и националната безбедност“*, Балкански центар за мир, Напредок, Тетово, 1999.

14. Котовчевски, М. *„Национална безбедност“* (трет дел), Македонска Цивилизација, Скопје, 2000.

15. Кревелд, В. Мартин. *„Трансформација на војната“*, превод Дејан Делев, Табернакул, Скопје, 2009.

16. Kurbalija,Jovan. "Uvod I upravljanje Internetom"- 2 izdanje, Albatros Plus, Beograd, 2011.

17. Malyuk, A. Antony, Pogozhin, S. Nikolai, Tolstoy, L.Aleksey, " Computer Security Training for Professional Specialists and Other Perosnnel Associated with Preventing and Responding to Computer Attacks", Moscow Engineering Physics Institute, Moscow, 2002.

18. Milosavljevic.M, Grubor,G. " Istraga kompjuterskog kriminala, metodolosko – tehnoloske osnove", Univerzitet Singidunum, Beograd, 2009.

19. McCallister, Erica. Tim Grance and Karen Scarfone. *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* U.S. Department of Commerce, National Institute of Standards and Technology , Gaithersburg, 2009.

20. Moore, R. "Cybercrime: Investigating High - Tehnology Computer Crime", Anderson Publishing, Cleveland, Mississippii, 2005.

21. Патоски, С. *„Сајбер криминалитет - нови можности за криминогено однесување“*, Legal yournal - Lawyer, март 2003.

22. Сулејманов, Зоран. *„Криминологија“*, Графос, Скопје, 2007.

23. Stephenson, P. *"Investigating Computer-related Crime",* CRC PRESS, USA, 2002.

24. Тупанчевски, Никола. *„Компјутерски криминалитет“*, Годишник на правниот факултет, Скопје, 1991.

25. *„Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders”*, Виена, 10 – 17 април, 2000.

26. Colaric M. Andrew. *„Cyber terrorism - Political And Economic Implications“*, Idea group publishing, London, 2006.

27. “Cyberterrorism:the Use of the Internet for terrorist purposes”, by Council of Europe, 2007.

28. *“Cyber-crime and cyber-terrorism. Security Electronic Business Processes”* , Highlights Of The Information Security Solutions Conference, јануари 2004.

29. Clark,A.Richard, “ CyberWar – The Next Threat to National Security and What to do About it”, Harper&Collins Publishers, 2010.

30. Хју, Питер. *„Поим за глобална безбедност“*, превод Дејан Делев, Табернакул, Скопје, 2009.

31. MEPs Debate Cyberterrorism and Islamic Radicalisation in Europe, with EU Counterterrorism Coordinator, 31.03. 2008.

32. Making Strides to Improve Ciber Security in the Chemical Sector, American Chemistry Council, 2009.

33. Smart Grid Cyber Security Strategy and Requirements – The Smart Grid Interoperability Panel – Cyber Security Working Group, February 2010.

- Документи:

1. Кривичен Законик на Република Македонија, (Сл.весник на РМ,бр.19, 30.03.2004). http://www. jorm.org.mk/docs/zakon-krivicna.rtf

2. Конвенција за сајбер криминал, Совет на Европа, Будимпешта, (European Committee on Crime Problems,Convention on Cyber Crime, april 2000).

3. Резолуција на Генерално Собрание на ООН, 1974 година.

4. Кривичен Законик на Република Македонија, член 251, Скопје, 2003.

5. Закон за заштита на лични податоци, Сл.Весник на РМ, бр.7/05 и 103/08

6. Закон за класифицирани информации, Сл.весник на РМ, бр.9, 27 февруари, 2004.

7. Закон за слободен пристап до информации од јавен карактер, Сл.весник, 1 септември,2006.

8. Кривичен Законик на Канада, http:// lois.justice.gc.ca/en/C-46/39387.html

9. Skuratov, V.M.Lebedov, Kommentari u glavnom u kodeksu Rossijskoj federaciji, Moskva, 1996.

10. Narodne novine R.Hrvatske, Zagreb, br. 110/1996

11. Sluzbeni glasnik R.Srpske, Banja Luka, br.22, 2000.

12. B.Penko, K.Stralig, Korenski Zakonik, z.uvodnim pojasnili, Ljubljana, 1999.

13. Закон за кривична постапка
< http://www.jorm.org.mk/docs/zakon-krivicna.rtf >

14. Закон за внатрешни работи на Република Македонија, (Службен весник на РМ. бр.92, 24.09.2009).

15. Krivicni zakonik Republike Srbije (glava 27), Sluzbeni glasnik 85/05 Beograd 2005
< http://www.parlament.sr.gov.yu/content/lat/akta/akta_detalji.asp?!d=285&t=Z >

16. Zakon o organizaciji I nadleznosti drzavnih organa za borbu protiv visokotehnoloskog kriminala,Sluzbeni glasnik 61/05,Beograd,2005,
< http://www.parlament.sr.gov.yu/content/akta_detalji.asp?!d=233&t=Z >

17. Karenski zakonik Republike Slovenije, Uradni list RS, st. 95/2004

- Извори од Интернет:

1. Posredovanje u resavanju racunalnih incindenata, Хрватска академска и истражувачка мрежа, CARNET/C.
< http://www.carnet.hr/posredovanje_u_rjesavanju_racunalnih_incidenata >

2. Computer Crime & Intellectual Property Section, United States Department of Justice
< http://www.cybercrime.gov/unlawful.htm >

3. Bright Hub, Computer Training Online, Computer Security,
< http://www.brighthub.com/engineering/civil/articles/47197.asph >

4. Tech – faq, Certified Information Security Manager,
< http://www.telh-faq.com/logic-bomb.shtml >

5. Microsoft - Safe & Security Center, Computer Security, Digital Privacy and Online Safety
< http://www.microsoft.com/security/worms/conficker.aspx >

6. Федерално Истражно Биро, Internet Crime Complaint Center,
< http://www.ic3.gov/media/annualreports.aspx >

7. Official Site of European Union, Central Library,
< http://ec.europa.eu/libraries/doc/index_en.htm >

8. Webopedia, Online Computer Dictionary for Computer and Internet Terms and Definitions,
< http://www.webopedia.com/new_terms.asp >

9. Science Daily – Your source for the latest research news,
< http://www.sciencedaily.com/articles/computers_math/ >

10. Eur – Lex, access to European Union Law
< http://www.eur-lex.europa.eu/lexUriServ.do?uri=OJ:L:2005:183:0047:0062:EN:PDF >

11. Nacionalni CERT +, Croatian Nacional Computer Emergency Response Team,
< http://www.cert.hr/documents.php?long=hr&page=11 >

12. Organization of American States, Democracy for Peace, Security and Developmnt
>< http://www.oas.org/en/default.asp >

13. Wasik, Martin. *Crime and the Computer*, Oxford University Press, Oxford, 1991.
< http://bjc.oxfordjournals.org/content/33/1/149.extract >

14. Македонски портал за вести
< http://www.daily.mk/cluste3/19b0e0a11b6c5..97865878a3a31f62/1114225/anonimusi-go-napadnaa-sajtot-na-evropskiot-parlament >

15. Министерство за финансии на Република Македонија, Управа за финансиска полиција
< http://finance.gov.mk/node/103 >

16. Министерство за внатрешни работи на Република Македонија
< http://www.mvr.gov.mk/DesktopDafault.aspx?tobindex=0&tabid=98 >

17. Државна комисија за спречување корупција
< http://www.dksk.org.mk/index.php?option=com_content&task=view&id=32&id=32&itemid=51 >

18. Агенција за електронски комуникации на Република Македонија
<http://www.aec.mk/index.php?option.com_content&view=category&id=48&itemid=91&Long=ml >

19. Интститут за информатика, Природно – математички факултет, Скопје.
< http://www.ii.edu.mk >

20. Државен завод за статистика на Република Македонија
< http://www.stat.gov.mk/OblastOpsto.aspx?id=27 >

21. Македонска страна за споделување информации и знаења
< http://www.fakulteti.mk/news/12-02-19/na_povidok_e_sajber_vojna.aspx >

22. Слободна енциклопедија, Wikipedia
< http://www.bs.wikipedia.org/wiki/globalizacija >

23. Јавно обвинителство на Република Македонија
< http://www.jorm.org.mk/docs/brosura.pdf >

24. Македонска информативна агенција
< http://www.mia.com.mk/default.aspx?mid=31&IId=1 >

25. Совет на Европа
< http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp >

26. Дирекција за заштита на лични податоци
< http://www.dzlp.mk/files/uploads/global/ZZLP_Precisten%20tekst.pdf >

27. ИНТЕРПОЛ – Internacional Criminal Police Organization
< http://www.interpol.int/Public/TechnologyCrime/default.asp >

28. NATO – Security of communications network
< http://www.ncsa.nato.int/topics/Cyber_Defence.html >

29. Официјална страна на Белата Куќа
< http://www.whitehouse.gov/issues/technology >