УНИВЕРЗИТЕТ СВ.„КИРИЛ и МЕТОДИЈ" - СКОПЈЕ

ФИЛОЗОФСКИ ФАКУЛТЕТ

ИНСТИТУТ ЗА БЕЗБЕДНОСТ, ОДБРАНА И МИР

ДОКТОРСКА ДИСЕРТАЦИЈА

ТЕМА:

НОВИТЕ ПРЕДИЗВИЦИ И ЗАКАНИ НА ВИСОКОТЕХНОЛОШКИОТ КРИМИНАЛ ВРЗ НАЦИОНАЛНАТА БЕЗБЕДНОСТ

МЕНТОР:
Проф. Д-р МИТКО КОТОВЧЕВСКИ

КАНДИТАТ:
М-р МАРИЈА ЃОШЕВА

Скопје, 2017 година

СОДРЖИНА

РЕЗИМЕ

Во ерата на високата технологија, како што многумина го сметаат почетокот на 21 век, нејзината примена најде место во нашите животи со сите нејзини позитивни и негативни придобивки, толку брзо што високата технологија стана тема на денешницата а не нешто што ќе ни го донесе иднината. Во оваа докторска дисертација е направен пристап на влијанието на високотехнолошкиот криминал врз безбедноста и проценките на заканите што ги носи истиот, сите негови видови и облици, при што ќе бидеме во можност да ги утврдиме и мерките кои што на најсоодветен начин ќе допринесат на директната заштита на безбедносната состојба, а самото тоа ќе допринесе на градење на еден ефикасен систем на заштита на националната безбедност.

Се доближвме поблиску до феноменот на високотехнолошкиот криминал кој по своите карактеристики е транснационален и меѓународен. На тој начин се укажа на потребата за превземање на една глобална акција преку поблиска маѓународна соработка како во областа на правната сфера така и во областа на борбата против високотехнолошкиот криминал, затоа што без усогласување на мерките и активностите и без брза и ефикасна размена на докази и информации многу е голема веројатноста поголем број на кривични дела да останат несанкционирани.

И на крај, оваа докторска десертација помогне во разбирањето на тоа дека заштитата од високотехнолошкиот криминал лежи во превенцијата и примената на современи механизми за заштита на системите на софтверско и хардверско ниво како и нивно постојано надградување за да можат да пружат заштита од нови закани кои преставуваатпотенцијална опасност врз системите кои што ја чинат националната безбедност на современите држави.

Клучни зборови: Национална безбедност, високотехнолошки криминал, видови и облици на загрозување, заштита од високотехнолошкиот криминал, законска регулатива, меѓународни институции.

PRATFALL

In an era of high technology, many consider the beginning of the 21st century, its application to find a place in our lives with all its positive and negative benefits, so fast that high technology has become the subject of today and not something that will bring us the future. In this doctoral dissertation is made to access the impact of high-tech crime on security and assessments of threats posed by it, all its kinds and forms, which will be able to determine the measures that the most appropriate way to contribute to the direct protection the security situation, and thus will contribute to building an effective system of protection of national security.

We approached closer to the phenomenon of high-tech crime which by its characteristics is transnational and international. Thus pointed to the need for taking a global action through closer for international cooperation in the legal sphere and in the fight against high-tech crime, because without harmonization of measures and activities without rapid and efficient exchange of evidence and information is very likely greater number of crimes remain unpunished.

Lastly, this doctoral desetacija help in understanding that the protection of high-tech crime lies in prevention and application of modern mechanisms for the protection of systems software and hardware level as their constant upgrading in order to provide protection against new threats which represent potential hazard to the systems that constitute the national security of the modern states.

Keywords: National security, high-tech crime, types and forms of endangerment, protection against high-tech crime, regulation, international institutions.

ВОВЕД

Кога идните историчари ќе ја истражуваат втората половина на дваесеттиот век и почетокот на дваесетипрвиот век најверојатно периодот ќе го наречат „информатичка револуција“. Имено човештвото има напреднато во последниве 50 години како никогаш досега. Една од причините за брзиот развиток е информационата технологија. Односно технолошките можности се зголемени до таа мера што е овозможено конструирање на се поголеми и пософистицирани системи преку доделување на се посензитивни и сложени функции.

Всушност, светот поминува низ втора „индустриска револуција“. Информационата технологија денес допира до секој аспект на животот. Дневните активности кај повеќето луѓе се под влијание на компјутер. Бизнисот, владите, индивидуалците и други ги користат бенефициите од информатичката револуција. Покрај користа во време и пари, компјутерот има влијание во секојдневниот живот, бидејќи компјутерски рутини заменуваат многу човечки задачи. Тие не само што се користат за извршување на некои индустриски и економски функции во општеството, туку на компјутерите им се доверени и многу функции од кои зависат човечки животи. Медицинскиот третман и воздушната контрола се само некој од примерите. Компјутерите, исто така се користат за чување на доверливи податоци од политичка, социјална, економска и лична природа. Тие помагаат во подобрувањето на економијата и на условите за живеење во сите земји. Впрочем комуникациите, науката и индустријата интезивно се развија благодарение на компјутерската технологија, така што нашиот начин на живеење неповратно се смени. Со компјутерот, од порано невозможното, стана возможно. Компјутерот придонесува големи количини на податоци да се сместат на компактен медиум, а големата брзина на работење овозможува и најкомплексните пресметувања да можат да се реализираат во неколку милисекунди.

Информатичката револуција донесе квалитативен напредок во животите на сите луѓе, толку голем, што повеќе е речиси невозможно да се замисли

цивилизација без информатичка поддршка и тоа во сите облици кои што ги пружа информационата технологија.

Информационата технологија е вештачка замисла која бара висока техничка опременост, добра информациона инфрастуктура во која паралелно коегзистираат виртуелното и реалното и каде што комуникацијата е колективна.

Од друга страна, ваквиот експлозивен развој придонесе за појава на пропратни последици од негативен карактер. Имено, дојде до негова поголема злоупотреба во смисла на појава на нови криминални активности и иновирање на начинот на извршување на класичните кривични дела. Односно ја "отвори вратата" на антисоцијалното и криминално однесување на начин што досега бил невозможен. Компјутерските системи нудат нови и високо-софистицирани можности за кршење на законот, со потенцијал да се извршат традиционални типови на криминал на нетрадиционални начини. [1]

Развојот на информационата технологија влијае на зголемување на облици на кривични дела од областа на високотехнолошкиот криминал. Порастот на овие кривични дела посебно се однесува на облици на кривични дела со елементи на прекугранично организиран и трансанационаклен криминал. Во многу држави ширум светот кои имаат развиено информациона структура која по својата природа е многу ранлива на вакви видови на напад, високотехнолошкиот криминал е означен како еден од најштетните.Научната и стручната јавност ја препозна опасноста која прети од високотехнолошкиот криминал.[2]

Со оглед на тоа дека на интернет се поврзани над 200 земји, злоупотребата на информационата технологија стана глобален проблем, кој бара многу големо учество и соработка помеѓу државниот и приватниот сектор во сите земји. Главна компонента на информатичката безбедност е

---

[1] *Магистерски труд под наслов „Видови и облици на злоупотреба на Информатичката технологија" одбранет на 21.10.2009 година на Филозофскиот Факултет Св.„Кирил и Методиј" Скопје – Институт за одбранбени и мировни студии.*

[2] *Policija I visokotehnoloski criminal – Primeri iz prakse I problem u radu MUP-a. pdf. Др Владимир Урошевиќ, Мр Сергеј Улјанов, Радоје Вуковиќ,Министарство унутрашњих послова Републике Србије.*

способноста на нацијата да спречи, открие, истражува и судски да ги гони криминалните активности поврзани со овој вид криминал. Слабоста во која било од овие области може да ја загрози безбедноста не само во одредена земја, туку широм светот. Секоја земја треба да се занимава со злоупотребата на информационата технологија, затоа што во спротивно ќе стане најслаба карика во глобалната компјутерска безбедност.

Главни недостатоци во досегашната борба се неадекватна меѓународна координација и непотполни правни и организациони способности на земјите во развој, каква што е и нашата земја.

Притоа, потребна е мала грешка во работењето на овие системи за да се стават човечки животи во опасност. Брзата експанзија на големите компјутерски мрежи и можноста да се пристапи до многу системи преку обична телефонска линија ја зголемуваат ранливоста на овие системи и ја отвораат можноста за злоупотреба и криминална активност. Последиците од информационата технологија можат да придонесат за сериозни економски кризи, како и нарушување на безбедноста. Безбедноста на мрежата и компјутерот преставува дел од научна дисциплина, наука за компјутерите, а непостоењето на безбедност на мрежата и на централни компјутерски системи представува важно прашање за секој кој користи интернет. За жал злоупотребата на информационата технологија по својата природа, често е невидлива. Поединци, односно организации, во некој случаи не ни знаат дека станале жртви. Но, мал е броот на луѓе кои пријавуваат случаи на хакинг или други кривични дела поврзани со овој вид криминал.

Непријавувањето на злосторство, не значи дека злосторство не постои.

Злоупотребата на информационата технологија преставува една од најголемите закани за користење на информационо-комуникациска технологија низ целиот свет. Било тоа да е во облик на хакинг, економска шпиунажа, упропастување на web страници, саботирање на податоци, вируси, измами, неовластен пристап или откривање на податоци, тоа ги погодува сите – (државата, граѓаните, претпријатијата и други корисници).

Треба да се има предвид и тоа дека ефикасната превенција, откривањето, гонењето и покренување на кривични постапки против сторителите на кривични дела, дополнително е отежнато и поради транснационалниот карактер на овие кривични дела.

Криминалците кои се занимаваат со високотехнолошки криминал не мораат да ги напуштат своите домови или да ја поминат државната граница за да сторат кривично дело во неколку држави низ светот. Нив не им е потребна виза, пасош или авионска карта. Патот на нивната комуникација може да оди преку локални телефонски компании, меѓуградски врски, интернет провајдери кои даваат интернет услуги и безжични сателитски мрежи. Тие можат да поминат низ компјутери кои се наоѓаат во неколку земји пред да ги нападнат целните системи низ светот. Кога еднаш ќе направат упад, овие криминалци може да го користат нападнатиот компјутер како средство за извршување на компјутерско кривично дело по свој избор. За да ситуацијата биде уште покомплицирана, трагите и идентитетот на сторителот често се добро маскирани и анонимни, односно некој може да направи кривично дело „компјутерска измама" истовремено против лица кои се наоѓаат во различни земји, а притоа да остане анонимен. Доказите од овој вид на криминал дури може да бидат меморирани на серверите во земји во кои криминалецот не се наоѓа, а жртвите можат да бидат од повеќе земји.

За разлика од истрага на класично кривично дело, овде е скоро неможно да се сочува доказ. За многу компјутери кои се приклучени на интернет не се води никаков оперативен регистар за промена на податоци кои поминуваат низ нив. Поради тоа може да се случи да клучни докази едноставно не постојат. Дури и кога постојат, може да биде невозможно да се добијат правно и легално. А кога доказите ќе се добијат анализата е сложена и се губи многу време. Затоа овие криминалци забрзано ја унапредуваат техничката стручност и „учат" како да ја користат напредната технологија како што е шифрирање, анонимност и софтвер за стенографија (програм за прикривање податоци, слики или текст во рамка на друг документ или слика, невидливи за око и неприметни за заштитните бариери, при што потребен е посебен софтвер за да се откриат податоците стенографски сокриени).

Комуникацијата често може да поминува низ неколку земји и поради тоа потребна е координација помеѓу полициите. На пример патот на електронската пошта која што сте ја испратиле на некој пријател кој живее на другиот крај на градот, може преку пакети да води низ земји на три континенти, пред да стигне до електронското сандаче на примателот.[3]

[3] *Магистерски труд под наслов „Видови и облици на злоупотреба на Информатичката технологија" одбранет на 21.10.2009 година на Филозофскиот Факултет Св.„Кирил и Методиј" Скопје – Институт за одбранбени и мировни студии.*

МЕТОДОЛОШКА РАМКА

1. ФОРМУЛИРАЊЕ НА ПРОБЛЕМОТ

Безбедносната политика на национално ниво ја поставува перцепцијата на власта за заканите за безбедноста на државата и нејзиното население и нејзините одговори на овие закани.

Притоа, заканите можат да бидат од различна природа и карактер. Со развојот на општеството и развојот на техниката и технологијата, покрај големите придобивки кои што ги има човештвото од нив тие со себе носат се повеќе можности и остваруваат услови за загрозување како на националната безбедност така и на глобалната безбедност.

Сите негативни поведенија поврзани со употребата на новите технолошки достигнувања се имплементирани како општествено опасни деланија и вметнати како кривични поведенија или кривични дела во законодавните рамки на национално ниво како и во рамките на меѓународните договори и спогодби. Оттука, високотехнолошкиот криминал опфаќа збир на кривични дела кадешто како објект на сторување и како сретство за сторување на кривичните дела се појавуваат компјутерите, компјутерските мрежи како и нивните продукти во материјален и електронски облик. Оваа дефиниција опфаќа голем број на злоупотреби на информатичките технологии како и злоупотребата на телекомуникациските технологии.

Развојот на информациските технологии во голема мерка влијае на зголемување на бројот на појавни облици на кривични дела од областа на високотехнолошкиот криминал. Зголемувањето на бројот на кривичните дела од оваа област посебно се однесува на оние облици на извршување на кривични дела со елементи на прекугранични, организиран и тренснационален криминал. Во многу држави во светот, кои имаат развиена информациска структура која пак по својата природа е осетлива на ваков вид на напади,

високотехнолошкиот криминал е означен како еден од најштетните, и борбата против него е ставена на високо ниво.

Брзиот раст и широката распространетост на електронска обработка на податоци и електронски бизнис спроведена преку Интернет, заедно со бројните појавувања на меѓународниот тероризам, ја наметнале потребата од подобри методи за заштита на компјутерите и информациите што ги чуваат, обработуваат и пренесуваат. Академските дисциплини компјутерската безбедност, безбедноста на информациите и осигурување на информациите се појавиле заедно со голем број професионални организации - сите споделувале заеднички цели за обезбедување на безбедноста и сигурноста на информациските системи.

Денес економски развиените земји, постојано вложуваат огромни средства во правец на сузбивање на високотехнолошкиот криминал. Притоа, една работа мора да биде неспорна, а тоа е дека без создавање на безбедно компјутерско опкружување, нема да има ефикасни резултати, ниту пак ќе биде возможно да се оствари ефикасна соработка помеѓу земјите во регионот. Меѓутоа, согледувајки ги актуелните состојби, земјите во транзиција и онака имаат голем број на проблеми а премалку финансиски средства и човечки ресурси за да се сконцентрираат на создавање на одбрамбен систем против високотехнолошкиот криминал, што дополнително ја усложнува борбата против овој вид криминал.

Високотехнолошкиот криминал искористувајќи ја ваквата хибернирачка состојба многу лесно може во блиска иднина во значителна мерка да ја загрози како глобалната така и националната безбедност, поради што потребно е да се посветиме на овој проблем со потребното внимание.

2. ХИПОТЕТИЧКАТА РАМКА

Општа хипотеза

Новите предизвици и закани на високотехнолошкиот криминал преставуваат реална, сериозна, брзо растечка закана за националната безбедност на современите држави.

Посебни хипотези

1. Високотехнолошкиот криминал е специфичен по цела серија свои обележја и како транснационален организиран криминал кој непрестано се развива, создава нови предизвици и закани врз националната безбедност на современите држави;
2. Делата кои потекнуваат од високотехнолошкиот криминал е тешко да се перципираат, истражуваат и процесуираат, и со тоа се откриваат најважните недостатоци на „традиционалното" кривично право, со што се создава атмосфера граѓаните да се чуствуваат незаштитени, несигурни во моќта на државата да ги заштити, а со тоа и губење доверба во системот и самата држава;
3. За успешно спречување на високотехнолошкиот криминал потребна е одлична соработка помеѓу јавниот и приватниот сектор, односно помеѓу судството, полициските служби и интернет провајдерите, телекомуникациските институции, мобилните оператори, пред се поради обезбедување на клучните докази;
4. Координарана активност и соработка на државите и нивните институции, посебно безбедносните, размена на информации помеѓу стручните лица за борба против високотехнолошкиот криминал, формирање база на податоци, води кон успешна борба против предизвиците и заканите на високотехнолошкиот криминал;
5. За националната безбедност до неодамна се сметало дека најважна е воената компонента, денес научно-техничката револуција доведе до формирање на информациско општество во кое информацијата е

главен фактор во управување со светот, и високотехнолошкиот криминал постана меѓународен феномен и најсериозна закана за безбедноста;

6. Глобализацијата на општеството овозможена од современите начини на комуникација преку INTERNET (социјални мрежи) и потенцијалната опасност од нивното користење врз личната, националната и глобалната безбедност;
7. Електронското тргување овозможено со користење на електронски банкарски сметки и опасноста од крадење на лични и доверливи информации и нивна импликација врз економскиот систем и стабилност, а со тоа и врз националната безбедност
8. Користењето на интернет просторот како поле за заработување на нелегално стекнати како и користење на интернетот за прикривање на потеклото на нелегално стекнати пари (перење на пари), со цел употреба на истите при финансирање на терористички организации или современо наречено „интернет тероризам“ и неговото директно влијание врз националната безбедност;
9. Лесната достапност до информациите на интернет поради ранливоста на компјутерските системи од една страна и употребата на компјутерските системи за складирање, обработка и размена на доверливи информации, и дава нови димензии на поимот „шпиунажа“, правејќи го моќна алатка во рацете на современите контраразузнавачки агенции дефинирајќи притоа сосема нов поим наречен „компјутерска или сајбер шпиунажа“.

3. ЦЕЛИ И ЗАДАЧИ

Целта на ова истражување е да се согледаат новите предизвици и закани на високотехнолошкиот криминал врз националната безбедност на современите држави, како трансанационален организиран криминал кој може да се објасни како феномен кој го загрозува идентитетот на една држава, и стана сериозна безбедносна закана, повеќе од кога и да било. Високотехнолошкиот криминал особено е злоупотребен од терористичките групи, глобалните информатички мрежи станаа многу ефикасно средство во рацете на терористите, овозможувајки им нови начини на дејствување, за кои што порано не можеле ниту да замислат.

Основна цел на ова истражување е да се објаснат безбедносните закани и предизвици на високотехнолошкиот криминал врз националната безбедност на современите држави, последиците од истите, влијанието врз нормалното функционирање во секојдневието, пред се поради тоа што високотехнолошкиот криминал се разликува од класичниот криминал во секој поглед, истиот секогаш го извршуваат организирани криминални групи составени од членови од целиот свет, чија соработка рапидно се зголемува и секогаш е инкорпорирано уште некое кривично дело од класичниот криминал. Целта ќе биде да се стави акцент на поврзаноста помеѓу високотехнолошкиот криминал и компјутерскиот тероризам, искористувањето на моќта на компјутерот од страна на терористичките групи, и заштита на компјутерските системи како единствен начин да се спречи злоупотребата на високотехнолошкиот криминал во нелегални цели. Просторната распространетост на високотехнолошкиот криминал е голема, на пример сторителот може да биде во една земја, серверот кој го напаѓа во друга, а жртвата или последиците во трета. Во ваков случај собирањето на доказите е многу тешко од аспект на различни правни системи, јурисдикции итн. Законите, системите на криминалната правда и интернационална соработка не ја одржуваат брзината со која технологијата се менуваше. Високотехнолошкиот криминал е нова форма на меѓународен криминал и за да се разгледува ефективно, неопходна е меѓународна соработка, и тоа може да се случи само

ако постои основа за разбирање кој е проблемот и кои можат да бидат решенијата.

Научна цел на ова истражување е да се даде научен опис, научна рамка за описот на новите предизвици и закани на високотехнолошкиот криминал врз националната безбедност на современите држави, научно објаснување дека феноменот на високотехнолошкиот криминал постои долго време и нема ни да исчезне, престои негов значаен развој. Научната цел би дала објаснување дека сеуште ја немаме видено најголемата величина на високотехнолошкиот криминал, би ги дала начините за спречување бидејќи земјите мораат да бидат запознаени со проблемот и да ги сфатат импликациите за нивниот социјален и економски развој.

Практичната цел на ова истражување е согледување на фактичката состојба, влијанието на брзиот развиток на технологијата, нејзината потреба во секој аспект на животот, сите активности се поврзани со информатичката технологија што говори за зависноста од компјутерот, да се даде објаснување дека високотехнолошкиот криминал преставува закана како за државата така и за граѓаните, и да се нагласи потребата од меѓународна полициска и правна соработка, координирање на истите, користењето на меѓународна правна помош со цел размена на доказите, се во функција на спречување на високотехнолошкиот криминал.

Резултатите и донесените заклучоци на ова истражување може да придонесат иницијатива за подобра интернет безбедност, заштита од интернет заканите, воочување на изворите на интернет заканите, заштита на критичните информациони инфрастуктури, за подобра соработка на државите од регионот и пошироко, да се донесат нови законски или подзаконски акти за да се усогласи Кривичниот закон со цел казните на сторителите да бидат еднакви секаде. Да се согледаат заедничките елементи и разлики во борбата против високотехнолошкиот криминал на современите држави, и државите од регионот.

4. ДОСЕГАШНИ ИСТРАЖУВАЊА

Со наглото развивање на Високотехнолошкиот криминал во последната деценија од 20 век а во 21 век неговата еволуција е се по евидентна, дојде до ситуација дека тој се интернационализира значително побрзо во споредба со некои други облици на транснационален криминал. Во последните години злоупотребата на високотехнолошкиот криминал во глобални рамки добива загрижувачки замав. Со оглед на тоа дека овој вид на криминал непрестано се развива и создава нови појавни облици, како и тоа дека повеќето држави дури во последната деценија реагирале во измена на законодаството, се доаѓа до низа на потешкотии кои се јавуваат во праксата. Соочени како со традиционалните така и со нетрадиционалните безбедносни предизвици, државите делувајќи сами се лошо опремени. Непостојаното управување и контролирање на безбедносните мрежи, а посебно јавно-приватната соработка, преставува се почест одговор. Од друга страна високотехнолошкиот криминал се повеќе станува подрачје на организирано десјствување на корпорации и на криминални структури, декларирани како компании за различни компјутерски услуги. Неговата распростанетост во секој сегмент од животот овозможува вклучување на вакви злоупотреби на широка и неограничена мрежа на учесници од различни краишта на светот.

Во современото постиндустриско, информатичко општество, повеќето економски активности, особено преку компјутеризација на различно производство, трансакции, како што е електронско тргување, банкарството, финасиите, безбедноста и одбраната, но и користењето на социјалните мрежи за комуникација, стануваат зависни од ефикасноста на компјутерите и компјутерските системи и мрежи. Општеството постанува зависник, но истовремено нивното користење создава можност за различни злоупотреби во криминални цели.

За овој феномен имаат пишувани повеќе странски автори, но со оглед на брзиот развиток на информатичката технологија, неговата сериозност, негативните последици врз националната безбедноста на државите и безбедноста на самите граѓани, поради тоа што не постои во технолошка смисла апсолутна заштита, сигурен и ефикасен систем, овие научни

истражувања не се доволни, со што се остава простор за понатамошни научни анализи.

Високотехнолошкиот криминал, дефиниран како злоупотреба на компјутерските системи и мрежи за остварување криминални цели, се надвисува како тешка закана над современото општество, и државите кои сеуште се во транзиција, во мера во која рапидно се зголемува бројот на субјектите што се вклучени или може да пристапат кон таквите системи и мрежи. Во Р.Македонија е истражуван од мал дел од научната заедница, но тоа е недоволно за овој најсовремен вид на криминал кој постојано е во нагорна линија со молскавична брзина. Не се направени доволно анализи за новите предизвици и закани од овој вид на криминал, и како тие ќе делуваат на националната безбедност на современите држави. Не се истражени начините на соработка помеѓу земјите во регионот, сосема е јасно дека битката е однапред изгубена ако и превенцијата и системот на казнената правда и примената на законот не се модернизираат и не се потпрат врз истите достигнувања на современата информатичка ера, кои се злоупотребуваат за криминални цели. Сето ова доведува до засилена потрага по правна регулатива и креирање на едно ново „информациско казнено право".

Во иднина потребно е истражување на заеднички мерки кои ги превземаат меѓународните полициски и правни институции, во спречување на организираниот криминал и новите предизвици и закани на високотехнолошкиот криминал врз националната безбедност на современите држави.

5. ПРЕДМЕТ НА ИСТРАЖУВАЊЕ

Предметот на ова научно истражување ќе биде фокусиран на високотехнолошкиот криминал, новите предизвици и закани кои потекнуваат од овој вид на криминал и нивното негативно делување врз националната безбедност на современите држави. Во моментов високотехнолошкиот криминал (сите негови видови и облици) се во подем, што може да доведе до сериозни нарушувања на општата безбедност на земјата, како еден од најмодерните и најсофистицирани видови на криминал. При тоа научното истражување има за цел да даде и една слика за тоа како најновите компјутерски програми со нивна примена во интернет-просторот нанесуваат штета во одредени измами како што се перење пари, измама со кредитни картички, интернет трговија (e-commerce), детска порнографија, софтверска пиратерија, компјутерскиот тероризам, а ќе се идентификуваат интернет безбедноста, интернет просторот, приватност во интернет просторот, информацискатa безбедност, информацискoто војување. Дел од овие активности успешно можат да се прикриваат во интернет-просторот.

Најголем број држави во светот немаат изградено адекватна легислатива за справување со ваквите активности.

Феноменолошката слика на организираниот високотехнолошки криминал опфаќа два основни облици: дела што ги имаат за свој објект компјутерите и дела кај кои компјутерите се средство за извршување на други дела, односно употребата на компјутерот како објект на напад и како средство за извршување на делото.Кога се појавува како објект на напад, кај компјутерот може да се нападнат две компоненти хардверот и софтверот. Оштетувањето, уништувањето или злоупотребата на овие две компоненти се остварува со помош на три основни средства, а тоа се компјутески вируси (virus), црви (worms) и тројанци (trojan). За разлика од првите два, кои што нивниот креатор кога ќе ги испрати нема повеќе контрола над нив, третиот тип претставува опасност која за нас е од посебен интерес, со оглед на тоа што претстасвува компјутерски програм, кој што му овозможува на испраќачот да пристапи

на“заразениот” компјутер, а со тоа да има увид во неговите податоци, и да манипулира со истите, без притоа сопственикот и да е свесен за тоа.

Кога се појавува како субјект на напад, односно како средство на извршување на кривичното дело, станува збор за олеснување или овозможување за реализација на одредена кривична активност со негова помош. Тука е многу значајно да се напомене дека компјутерот може да се употребува како средство за планирање односно прикривање на кривични дела или раководење со одредени криминални активности. Се однесува на различни манипулации, како што се: шпионажа, измама, користење услуги на туѓ компјутер или манипулации со банкарски сметки. Оаа функција е значајна поради фактот што во иднина таа ќе биде точка на поврзување помеѓу организираниот криминал и високотехнолошкиот криминал.

5.1 ЗАДАЧИ НА ИСТРАЖУВАЊЕТО

Како задачи на истражувањето ги поставуваме:

1) Да се прикаже историскиот осврт на високотехнолошкиот криминал;
2) Да се прикажат факторите за појава на високотехнолошкиот криминал на национално и регионално ниво;
3) Да се прикаже влијанието на високотехнолошкиот криминал како значаен фактор на загрозување на националната безбедност на современите држави;
4) Да се прикажат негативните последици на новите предизвици и закани на високотехнолошкиот криминал врз националната безбедност на современите држави;
5) Да се испитаат резултатите од меѓусебната соработка на НВО, меѓународни организации и владини институции во превенција и борба противвисокотехнолошкиот криминал;
6) Да се испита улогата и значењето на државните институции задолжени за справување со оваа закана во превенцијата и во борбата против високотехнолошкиот криминал, нивото на меѓународна полициска соработка;
7) Да се прикажат мерките и активностите кои се превземаат во Р. Македонија и во современите држави во борба против високотехнолошкиот криминал и неговите предизвици и закани врз националната безбедност.

6. МЕТОДИ И ТЕХНИКИ НА ИСТРАЖУВАЊЕ

Оваадокторска дисертација поаѓајќи од нејзината цел на истражување ќе има претежно ***експликативен карактер***, поради тоа што ќе биде насочено да го детерминира високотехнолошкиот криминал како најнова закана врз националната безбедност на современите држави, и поради тоа што ќе се заложува кон хармонизирање на веќе донесените теориски, сознанија и генерализираните искуства од современите држави.

Оваадокторска дисертацијаима и ***апликативна цел***од аспект на самиот стратешки проблем на оваа проблематика, а дава и можност да се согледаат проблемите и да се осознае она што е потребно во иднина да се направи со цел да се одговори на современите тенденции.

Дескриптивен карактер – со самото истражување се дава јасна слика за негативното влијание на високотехнолошкиот криминал, неговите предизвици и закани врз националната безбедност на современите држави и недоволната безбедност на самите граѓани и недовербата во информатичката технологија, како и мерките кои се превземаат за сузбивање на истите.

За потребите на ова истражување ќе се применат неколку научни методи: Анализа на содржината на официјално објавени документи и правни пописи, акти, спогодби и извештаи на институции од современите држави, Анализа на податоците од секундарни извори и ***Компаративна анализа*** на податоците од повеќе различни документи.

Техниката на собирање податоци ќе ја опфати анализата на содржина како методолошка постапка.

Постапки и техники кои ќе се користат за анализа на податоците:

- создавање на прегледи
- создавање на листа на податоци

- класификација на податоците
- мерење на податоците
- кодификација на податоците
- техничка и компјутерска обработка

Преку анализирање и компарација на обработените податоци за изминатиот период ќе се добијат резултати кои ќе овозможат да се види дали би биле посигурни со преземените мерки и активности по однос на дадената проблематика.

I ГЛАВА

1. ДЕФИНИРАЊЕ НА ПОИМОТ НАЦИОНАЛНА БЕЗБЕДНОСТ

Прашањето за безбедноста, луѓето и општеството ги окупира уште од почетоците на нивното постоење. Се работи за егзистенционално и вечно прашање. Егзистенцијално е затоа што без способност да се оствари безбедност на егзистицијално ниво не е можен опстанок. Секој жив организам и секоја заедница на живи суштества по природа тежнее кон сопствена безбедност. Тоа важи и за луѓето и нивните заедници. Тоа е израз на природниот нагон во ниеден поглед да не се наруши сопствениот интегритет и да се овозможи и осигура потполн живот.

Поимот безбедност потекнува од латинскиот збор „sinecura" (sine – без, и cura – грижа) што во превод значи сигурен, безгрижен, доверлив, цврст, заштитен.

Безбедноста како поим, во нејзиното традиционално и современо значење, се поврзува со различни активности на поединецот и на државата, насочени кон обезбдување на опстанок.[4]

Безбедноста е еден од основните феномени на човечкото општество во сите фази од неговиот развој. Човекот како поединец, општествените, национални и државни заедници, како и целокупното човечко општество имаат потреба за самоодржување, зачувување и осмислување на своето постоење.

Оттука, безбедноста како поим е битен предуслов за развој на општеството и современите држави. Кога зборуваме за безбедност мислиме пред се на безбедност на човекот како единка. Од безбедноста во голема мерка зависи развојот и функционирањето на една единка, неговите погледи и сваќања за современиот свет, неговата интелектуална и творечка дејност,

[4] *Александар Дончев, Современи безбедносни системи, Скопје, 2007. Стр. 48.*

развојот на односите во едно општество што од своја страна ги претставува темелите на едно современо општество, а со тоа и современите држави.

Меѓутоа, безбедноста на поединецот не можеме да ја разгледуваме како изолирана категорија. Безбедноста на поединецот пред се зависи од имплементирање на мерки и активности и употреба на механизми со кои што ќе се детектираат, превенираат, репресираат или санкционираат одредени објективни и субјективни фактори кои што во голема мерка влијаат на безбедноста на поединецот а со тоа и на заедницата во целина. Притоа, гледајќи на безбедноста од овој агол како гарант за нејзината заштита се појавува државата. Значи државата преку заштита на поединецот ги штити националните интереси.

Од тука доаѓаме до поимот „национална безбедност" којашто во најширока смисла на зборот може да се дефинира како состојба на заштита на темелните вредности на општеството и на институциите засновани на нив, заштита на виталните државни интереси како и интегритетот на државниот сектор и неговите институции.

Поимот национална безбедност во почетокот на неговото појавување немаше доволно јасна содржина, но со текот на времето доаѓа до негово јасно детерминирање и прецизирање. Во фокусот на националната безбедност почнува да се согледува и анализира вкупноста на политичките, воените и економските напори кои ги превземаат владите за остварување на внатрешната и надворешната безбедност на своите држави.

Во меѓународната енциклопедија националната безбедност е дефинирана како способност на државата да ги заштити своите вредности од надворешни опасности. За националната безбедност до неодамна се сметало дека најважна е воената компонента.

Арнолд Волферс (Arnold Wolfers) националната безбедност ја детерминира во објективна смисла со отсуство на загрозување на основните општествени вредности, а во субјективна се однесува на отсуство на страв за општеството дека неговите општи вредности ќе бидат загрозени.[5]

За безбедност на државата традиционално се користи зборот национална безбедност, без оглед на различноста на поимот држава и нација. Се смета дека за првпат поимот национална безбедност го употребил Валтер Липман (Wallter Lippmaun), 1943г.[6]

Националната безбедност е поврзана со поимот држава и нација. Традиционалното сфаќање на националната безбедност не е во состојба да ги објасни сложените безбедносни појави, затоа што денес националната безбедност покрај воените има и невоени аспекти на безбедност.

Националната безбедност подразбира состојба на уживање и оптимална заштита на националните (државни и друштвени) вредности и интереси (првенствено мирот, слободата, правата и безбедноста на луѓето и друштвените групи, квалитетот на живеење, национално единство, достоинство, гордост и идентитет, здрава животна средина, енергетска стабилност, економски и социјален просперитет, информациски ресурси, уставен и правен поредок, територијален интегритет, политичка независност, суверенитет), кој се постигнува, одржува и унапредува на основа на безбедност на граѓаните и национален систем на безбедност.[7]

Друга дефиниција за национална безбедност е од експертот за безбедносни аспекти на современите меѓународни односи Марио Нобило. Тој ја дефинира националната ебзбедност како комплексна интеракција помеѓу политичките, економските, воените, идеолошките, правните, општествените и други внатрешни и надворешни општествени фактори, преку кои индивидуалните држави се обидуваат да обезбедат прифатливи барања за да

[5] *Митко Котовчевски, Национална Безбедност, Филозофски Факултет - Скопје 2013, стр.35,*
[6] *Саша Мијалковиќ, Национална Безбедност – од вестфалког концепта до постхладнограговском, стр.60.*
[7] *Саша Мијалковиќ, Национална Безбедност – од вестфалког концепта до постхладнограговском, стр.69.*

ја одредат нивната сувереност, територијален интегритет, физички опстанок на своето население, политичка независност и можности за брз општествен развој на еднакво ниво.[8]

Амин Хјуди експерт по меѓународни односи и дипломат со долго искуство, ја дефинира националната безбедност како активност на држави-нации со која државите во рамките на нивните општествени капацитети во сегашност и иднината, имајќи ги предвид глобалните промени и развојот, го штитат својот идентитет, постоење и интереси. Оваа активност вклучува:

- Посебни мерки (во трговија, економија, култура итн) да се заштитат и одбранат самите од која било закана од средината;
- Безбедносни мерки на општеството, кои мора да бидат во согласност со капацитетите на општеството (во спротивно тие би можеле да водат до небезбедност);
- Овие мерки мора да бидат планирани (долгорочни и краткорочни);
- И прилагодени на глобалните и регионалните промени во светот.

Според Валтер Липман (Walter Lippmaun) државата е сигурна толку колку што немора да ги жртвува своите основни вредности без војна или со неа.[9]

Бери Бузан е убеден дека безбедноста е поврзана со напорите за слобода од страв. Во меѓународната рамка, безбедноста го опфаќа капацитетот на општествата и државите да се одржи нивниот независен идентитет и нивниот функционален интегритет.

Кен Бут тврди дека стабилна безбедност може да се достигне само од страна на нациите и државите кои не ги лишуваат другите од неа. Сепак, ова може да се достигне само во случај безбедноста да се разгледува како процес на ослободување.

---

[8] *Марина Митревска, Антон Гризолд, Владо Бучковски, Ентони Ванис, превенција и менаџирање на конфликти, Скопје 2009, стр.32.*

[9] *Митко Котовчевски, Национална Безбедност, Филозофски факултет – Скопје 2011, стр. 44.*

Националната безбедност претставува специфичен општествен процес и состојба на одделните општества, при што во нивното секојдневно живеење и функционирање отсуствува било каков страв од надворешен напад, од загрозување на материјалните и духовните вредности и интереси или било каков вид закана од некоја соседна држава или од сојуз на држави.[10]

Поимот национална безбедност сугерира на неговата поврзаност со: воениот, политичкиот, економскиот, социоеталниот и факторот од сферата на внатрешната, социеталната и еколошката безбедност.[11]

Спасески националната безбедност ја дефинира како ,,состојба која се однесува на целината на функционирањето на општеството и државата и на егзистенцијата на сите луѓе во услови на мир и демократија."[12]

Според Лазаревски, остварувањето на националната безбедност не се сведува само на функцијата на вооружените сили на земјата, иако нејзиното значење е неспорно.[13]

Според Дончев под национална безбедност подразбираме не само функционирање на безбедносните сили туку и политичка, економска, воена, социетална, еколошка и информатичка стабилност, меѓународен углед и интегрираноста на земјата во меѓународните структури.[14]

Така, националната безбедност може во најопшти услови да се дефинира како состојба на безбедност на државата- нација. Таа вклучува: безбедност на националната територија (вклучувајќи го и воздушниот простор и територијалните води), заштита на животите и сопственоста на нејзиното население, постоење и одржување на нејзиниот национален суверенитет и практицирање на основните функции на нејзиното општество (економски, социо-политички, културни, еколошки, општествени, итн.).

---

[10] *Ѓорѓи Тоновски ., Меѓународни односи, авторизирани предавања, Факултет за општествени науки, Скопје, 2004, стр. 258.*

[11] *Зоран Нацев., Теориски основи на доктрината и стратегијата на националната одбрана, НИП Ѓурѓа, Скопје 1999 и Зоран Нацев., Ратко Начевски., Војна, мир и безбедност, Македонска ризница, Куманово, 2000.*

[12] *Јордан Спасески .,Македонија столб на безбедноста и мирот на Балканот, Скопје, 2005, стр. 255.*

[13] *Панде Лазаревски „ Стратешки истражувања" Одбрана, бр. 68, Скопје, 2001 стр.14.*

[14] *Александар Дончев, Современи безбедносни системи, Скопје, 2007. Стр. 56*

Денес, националната безбедност е политичко и лично добро, имплементирано како основно човеково право во една либерална демократска држава. Така, разбрана и дефинирана националната безедност покрај политичко-воени, исто така, ги вклучува и гореспоменатите поширок димензии на безбедноста на поединецот, како и на општествените групи на различни нивоа од нивната структура, т.е. на регионални, на национално, на меѓународно и на наднационално ниво.[15]

Политиката на национална безбедност претставува сложен и меѓузависен збир на мерки, активности, планови и програми, кои ги презема Република Македонија заради заштита, одржување и унапредување на безбедноста на Република Македонија и нејзините граѓани, во согласност со расположивите ресурси и со активна соработка со меѓународната заедница.

Во себе системски ги содржи политичката, економската, одбранбената, внатрешно безбедносната, социјалната, еколошката и други области.[16]

Основна и долгорочна цел на политиката на национална безбедност е да ја заштитува, одржува и унапредува безбедносната состојба на државата, создавајќи амбиент за остварување на националните интереси на РМ. Развивањето на безбедносна политика вклучува утврдување пристап кон безбедносните прашања, одредување на приоритетот на заканите за безбедноста и донесувањето на најважните одлуки за безбедносниот сектор. Безбедносните политки на национално ниво, кои опфаќаат политики за национална безбедност и посебни политики за институциите, ги третираат и внатрешните и надворешните закани за безбедноста и се развиваат во

---

[15] *Марина Митревска, Антон Гризолд, Владо Бучковски, Ентони Ванис, Превенција и менаџирање на конфликти – Случај Македонија (нова безбедносно парадигма) Скопје, 2009 стр. 30.*

[16] *Влада на Р.М., Национална концепција за безбедност и одбрана, Скопје.*

рамките на меѓународната и регионалната легислатива кон која пристапила државата.[17]

Влијанието на глобализацијата врз безбедноста не е без последици. Потребата од прилагодувањето на безбедносните служби на промените кои ги постави глобализацијата е евидентно во неколку правци. Така на пример глобализацијата ја интензивираше динамиката во доменот на високотехнолошкиот криминал, разузнавањето, градењето на соодветните стратегии и доктрини, персоналната политика (унапредување и соодветната едукација и потребата од развивање на интерресорски вештини), сервисната поддршка на безбедносниот сектор (во информатичка и логистичка смисла) и секако во доменот на комуникациите.

INTERNET (социјални мрежи), електронското тргување овозможено со користење на електронски банкарски сметки, користењето на интернет просторот како поле за заработување на нелегално стекнати средства, лесната достапност до информациите на интернет носат потенцијалната опасност од нивното користење врз личната, националната и глобалната безбедност;

Успехот во прилагодувањето на овие динамики кои се детерминирани од глобализацијата и техничко-технолошкиот развој кој паралелно се одвива со неа во кумулативна смисла недвосмислено го детерминира успехот во раководењето, командувањето и контролата на безбедносниот сектор.[18]

Едноставно кажано националната безбедност преставува основа за нормалното човеково функционирање, а со тоа и функционирањето на една држава, односно националната безбедност преставува „ахилова пета". Кога националната безбедност е кревка, или пак во најлоша варијанта нарушена, тоа се рефлектира како „домино ефект" врз целото општество, влијае во сите сфери, сите клучни органи, институции и сл.

---

[17] *IPU and DCAF, Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices, (IPU and DCAF: Geneva), 2003, p. 27.*

[18] *Пошироко види во: Wolf, Martin, Why Globalization Works, New Haven, CT: Yale University Press, 2004, стр. 173-212.*

Од поширока перспектива за што ќе зборуваме и во овој труд е дека современите држави се соочуваат со голем број на закани по нивната национална безбедност кои се многу различни од традиционалните закани, затоа што природата и барањата на националната безбедност се менуваат брзо. **Најважните имликации на овие промени се заканите на високотехнолошкиот криминал врз националната безбедност.**

Националните политики на современите држави мора да се променат, односно мора да се прилагодат на зголемена меѓународна соработка на економски план, така се нагаласува и потребата од соработка и меѓусебна координација во справување со заканите кои ги носи високотехнолошкиот криминал, како би ја заштитиле својата национална безбедност, а со тоа и мирот, спокојот, безбедноста на самите граѓани.

Високотехнолошкиот криминал е специфичен по цела серија свои обележја притоа создава нови предизвици и закани врз националната безбедност на современите држави. Бидејќи делата кои потекнуваат од високотехнолошкиот криминал е тешко да се перципираат, истражуваат и процесуираат, за успешно справување со високотехнолошкиот криминал потребна е одлична соработка помеѓу јавниот и приватниот сектор како и координарана активност и соработка на државите и нивните институции.

2. ОБЛИЦИ И ИЗВОРИ НА ЗАГРОЗУВАЊЕ НА НАЦИОНАЛНАТА БЕЗБЕДНОСТ

„Од кого и од што треба да се штити општеството“ преставува вечен проблем за сите општества, феномен од чии одговори зависи судбината на конкретните општества, нивниот живот или нивната смрт. Одговорот на овие посложени прашања преставува фундамент за сите дејствувања во безбедносна смисла, бидејќи преку нив во најголема мера се врши дефинирање, класификација и објаснување на настанокот, траењето и разорното делување на општествено штетните и опасни појави од аспект на неговата интегрална безбедност.[19]

Листата на доминатни облици и извори на загрозување на националната безбедност се менуваат во текот на историјата, и зависат од многу фактори, од кои најистакнати се технологијата и политиката. Продлабочувањето на старите и појавата на нови облици и извори на загрозување се шират на внатрешни и меѓународни односи кои се изразени во разликите, во зависност од економскиот, политичкиот и културниот развој на одделни земји и региони. Какко доминантен извор на загрозување на националната безбедност во изминатиот период важеше нуклеарното оружје, но денес луѓето оваа закана ја стават во позадина, и се повеќе стравуваат од тероризмот, миграцијата, граѓански војни, климатските промени, и благодарение на брзиот развој на технологијата се појавуваат и извори на загрозување кои доаѓаат од информацискатa технологија.[20]

Соочени како со традиционалните така и со нетрадиционалните безбедносни облици и извори на загрозување, државите делувајќи сами се лошо опремени. Непостојаното управување и контролирање на безбедносните мрежи, а посебно јавно-приватната соработка, преставува се почест одговор.

---

[19] *Митко Котовчевски, Национална Безбедност, Скопје 2013, стр.152.*

[20] *Хатиџа Бериша, Концепт Велике Албаније као претња националној безбедности Република Србија, Београд 2014, стр.24.*

Од друга страна високотехнолошкиот криминал се повеќе станува подрачје на организирано десјствување на корпорации и на криминални структури, декларирани како компании за различни компјутерски услуги. Неговата распростанетост во секој сегмент од животот овозможува вклучување на вакви злоупотреби на широка и неограничена мрежа на учесници од различни краишта на светот и како транснационален организиран криминал кој непрестано се развива, создава нови предизвици и закани врз националната безбедност на современите држави.

Во современото постиндустриско, информатичко општество, повеќето економски активности, особено преку компјутеризација на различно производство, трансакции, како што е електронско тргување, банкарството, финансиите, безбедноста и одбраната, но и користењето на социјалните мрежи за комуникација, стануваат зависни од ефикасноста на компјутерите и компјутерските системи и мрежи. Општеството постанува зависник, но истовремено нивното користење создава можност за различни злоупотреби во криминални цели. Денес научно-техничката револуција доведе до формирање на информациско општество во кое информацијата е главен фактор во управување со светот.

Меѓутоа, согледувајки ги актуелните состојби, земјите во транзиција и онака имаат голем број на проблеми а премалку финансиски средства и човечки ресурси за да се сконцентрираат на создавање на одбрамбен систем против високотехнолошкиот криминал, што дополнително ја усложнува борбата против овој вид криминал. Високотехнолошкиот криминал искористувајќи ја ваквата хибернирачка состојба многу лесно може во блиска иднина во значителна мерка да ја загрози како глобалната така и националната безбедност, поради што потребно е да се посветиме на овој проблем со потребното внимание.

❖

Современата информатичка и компјутерска технологија внесоа нови и драстични промени во сите сфери на општествениот живот. Тие промени покрај позитивните и корисните импликации донесоа и низа на проблеми

поврзани за појавата и ширењето на компјутерскиот криминалитет од најразлични облици, форми, видови и начини на исполнување. Сите овие промени може да се сведат на следното: се создава нова форма на вредности, се врши концентрација на податоците, се создава нов амбиент на дејствување и работење, нови методи и техники на дејствување, ширење на географскиот простор на дејствување, стабилност на ризикот и сл.

Како што споменавме погоре во текстот постојат повеќе облици и извори на загрозување на националната безбедност. Но свесни сме дека заканите по националната безбедност на современите држави се од менлив карактер, а најмногу сме свесни за климатските промени и последиците од нив по националната безбедност, почнувајќи од природни катасрофи кои ја зголемуваат потребата од хуманитарна помош, а со тоа и бран на бегалци, затоплувањето кое ќе доведе до топење на поларните мразови, зголемување на нивото на водата а со тоа и нови конфликти.

Исто така транснационалниот криминал е закана по националната безбедност, односно преку коруптивни влијанија ги искористува државните институции, самите влади, а со тоа се зголемува нелегалната трговија со дрога, оружје, трговија со луѓе, органи, и др., расте сивата економија, а со тоа се намалува нормалниот напредок на една современа држава.

Но најновиот бран на закани по националната безбедност кој се очекува во иднина е од технички аспект, односно од сите видови и облици на високотехнолошкиот криминал. **Мрежните упади се сметаат за едни од најсериозните закани по националната безбедност, а со тоа и врз јавната безбедност како и врз економските предизвици.**

Современата информатичка технологија, мемориските капацитети, компјутерските мрежи и глобалната дистрибуција на податоци и информации дополнително ја отежнува можноста за откривање на овие кривични дела и пронаоѓање на нивните извршители.[21]

---

[21] *Милошевиќ М., Урошевиќ В.: Крађа идентитета злоупотребом информационих технологија, Безбедност у постмодерном амбијенту, Зборник радова књига VI, Центар за стратешка истраживања националне безбедности, Београд, 2009, стр. 53.*

Се нудат голем број на производи кои нудат заштита од високотешнолошкиот криминал, но софистицираноста на нападите кои доаѓаат од напредната информациска технологија бара решенија кои се надвор од традиционалните.

Бидејќи делата кои потекнуваат од високотехнолошкиот криминал е тешко да се перципираат, истражуваат и процесуираат покрај државните институции со кои Министерствата за внатрешни работи имаат соработка сметаме дека е потребно да се вклучат и додатни институции, бидејќи недостига ефикасен систем за надгледување на Интернетот со цел за откривање на кривични дела од областа на високотехнолошкиот криминал, како и ефикасна платформа за пријавување на овие кривични дела во On-line окружувањето.

Како посебен проблем се јавува и потребата за подобра соработка со факултетите, невладините организации итн. Сметаме дека е потребно да се воспостави ефикасен CERT тим Computer Emergency Responce Team)[22] за спречување на овие кривични дела и да се одредат институции чии претставници би требало да се ангажираат во оваа насока. Воспоставувањето на ваков тим во голема мера би допринел за ефикасно спречување на овие кривични дела, би се овозможила брз пристап во истражувањето на оваа појава и заеднички одговор на предизвикот и заканата кои оваа појава ги носи.

[22] *Лидија Комлен Николић et.al: Сузбијање високотехнолошког криминала, Удружење јавних тужилаца и заменика јавних тужилаца Србије, Београд, стр. 231.*

II ГЛАВА

1. ВИСОКОТЕХНОЛОШКИОТ КРИМИНАЛ – ЗАКАНА ПО НАЦИОНАЛНАТА БЕЗБЕДНОСТ НА СОВРЕМЕНИТЕ ДРЖАВИ

Високотехнолошкиот криминал преставува една од најголемите закани за националната безбедност, од страна на непознати напаѓачи може да се предизвика огромна штета и огромни загуби.

Високотехнолошкиот криминал преставува брзо растечка закана за националната безбедност на современите држави. Тој е специфичен по цела серија свои обележја и како транснационален организиран криминал кој непрестано се развива, создава нови предизвици за националната безбедност на современите држави.

Во современото општество високотехнолошкиот криминал постана меѓународен феномен. Се поголемата достапност и употреба на информатичката технологија во општеството, како и глобализација на економијата се карактеристики на нашата ера. Технолошкиот развој и растот на користење на отворените мрежи како што се интернетот, во иднина ќе обезбеди многу нови можности и ќе придонесе за нови предизвици.[23]

Високотехнолошкиот криминал е дефиниран како криминал во кој компјутер е предмет на кривично дело (хакирање, фишинг, спам) или се користи како алатка за да изврши кривично дело. Компјутерските криминалци може да ја користат информационата технологија за пристап до лични информации, деловни трговски тајни, или го користат интернетот за злонамерни цели. Криминалците исто така може да ги користат компјутерите за комуникација и документ или складирање на податоци.[24]

---

[23] *Chik B. Waren, "Challenges to Criminal Law Making in the New Global Information Society", 2011, p. 123*
[24] *https://www.techopedia.com/definition/2387/cybercrime, (27.10.2015).*

Високотехнолошкиот криминал во мултилатералните меѓународни договори се сваќа како поим во потесна и поширока смисла. Така на пример, во официјалните документи на Обединетите Нации под високотехнолошки криминал во потесна смиска се подразбира ,,секое незаконито однесување насочено на електронски безбедносни операции и податоци обработени во нив", додека во поширока смисла се подразбира ,,секое незаконско однесување поврзано за или во однос на компјутерски систем и мрежа, вклучувајќи и таков криминал како што е илегално работење, нудење и дистрибуирање информации преку компјутерски систем и мрежа".

За полесно да се сфати влијанието на високотехнолошкиот криминал врз националната безбедност, треба да се дефинира и поимот на **информациона безбедност.**

1.1 ИНФОРМАЦИОНА БЕЗБЕДНОСТ

Под **ИНФОРМАЦИОНА БЕЗБЕДНОСТ** се подразбира заштита на информациите и информациските системи од неовластен пристап, искористување, откривање, прекин, модификација, проучување, испитување, снимање или уништување. Информационата безбедност станува еден од виталните национални интереси. Поимот информациона безбедност честопати погрешно се поистоветува со компјутерска безбедност со која несомнено има допирни точки. Областите меѓусебно се поврзани и споделуваат заеднички цели кои се насочени кон заштита на доверливоста, интегритетот и достапноста на информациите, меѓутоа меѓу нив постојат значајни разлики. Разликите се најочигледни во пристапот на одреден предмет, методот кој се користи и областите на кои се сконцентрирани.

Информационата безбедност се занимава со доверливост, интегритет и достапност на податоците независно од нивната форма: електронска, печатена или некоја друга форма. Компјутерската безбедност се фокусира на обезбедување достапност и правилно дејствување на компјутерскиот систем без оглед на зачуваните или обработени податоци во компјутерот.

Владите, војската, корпорациите, финансиските институции, болниците и приватните бизниси имаат многу доверливи информации за нивните вработени, потрошувачите, производите, истражувањата и финансиската состојба. Најголем дел од информациите денеска се собираат, обработуваат и зачувуваат на електронски компјутери и се пренесуваат преку мрежите до други компјутери. **Со нелегално добивање на овие податоци и нивно злонамерно искористување директно се влијае врз националната безбедност, што ја покажува спрегата помеѓу информационата и националната безбедност**.

Информационата безбедност се дели на:

1. Компјутерска Безбедност;
2. Безбедност на мрежите и
3. Интернет безбедност

Компјутерска безбедност

Компјутерската безбедност на една држава преставува обезбедување на сигурност на националниот компјутерски простор од закани кои може да имаат различен облик. Безбедноста на компјутерските мрежи е многу значаен процес, без кој во денешно време, незамисливо е функционирањето на една мрежа. Кражбата на тајни информации од национални компании (јавни претпријатија, но и приватни) и органите на државната управа, напад на инфрастуктури од витално значење за функционирање на државата или напад на приватноста на самиот граѓанин, може да се посматраат како екстремни примери на големи закани. Денес напаѓачите на компјутерскиот простор се професионалци кои работат за Владите на државите, за хакерски организации или криминални организации, пред поединци или групи кои во потрага за краткотрајна слава поради лична афирмација, извршуваат напади на компјутерски простор на некоја земја.

Сложеноста дека компјутерскиот простор треба да се направи безбеден, се претвара во проблем кој не е само технички, туку пред се социјален, правен и економски. Унапредувањето во знаењето за компјутерска безбедност, со унапредување на вештините и способностите, се од суштинско значење за давање на подршка на средината и заштита на виталните инфрастуктури, како што се телекомуникациските мрежи, електро мрежите, индустријата, финансиската инфрастуктура и сл.

Во денешно време, во време на информационата ера разузнавачките активности се одвиваат низ компјутерскиот простор, со цел да се проучат слабостите на една држава. Унапредувањето во компјутерската безбедност е од суштинско значење за давање подршка на општеството и заштита на виталните инфрастуктури, како што се телекомуникациските мрежи, електро

мрежи, индустрија, финансиската инфрастуктура, а со тоа и да се намали негативното влијание на високотехнолошкиот криминал на националната безбедност на современите држави.[25]

Компјутерската безбедност е активност за заштита на информации и информациски системи (мрежи, компјутери, бази на податоци, центри за податоци и апликации) со соодветни технолошки мерки за безбедност. Во таа смисла поимот компјутерска безбедност е генерички и ги опфаќа сите мерки за заштита.

Компјутерската безбедност се поистоветува со националната безбедност. Во последно време јачината на безбедноста на една држава се гледа по јачината на компјутерската безбеднсот на таа држава. Компјутерската безбедност е алатка за постигнување на посакуваната цел.

Современите држави дефинираат стратешки цели на една безбедна компјутерска средина во која можат да постигнат целосен економски потенцијал и да ги заштитат граѓаните од различни компјутерски напади и ризици. Решавањето на потребите на компјутерската безбедност за една држава не е лесна задача.

Секоја држава се соочува со постојано зголемување на нивото на опасност од компјутерски напади, а со тоа се бара и државата да утврди цели и стратегии за заштита, и да вложува во компјутерската безбедност.

Безбедност на мрежите

Безбедноста на мрежите преставува сет на мерки и процедури кои ќе ја гарантираат безбедноста на мрежата и податоците кои се процесираат преку истата мрежа. Исто така примената на технички средства и софтверски решенија за мониторирање и обезбедувањето на безбедноста на мрежата преставува една од клучните мерки за подобрување на безбедноста на мрежите и податоците.

---

[25] *http://www.odbrana.mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/VD_3-2015/67-2015-3-11-Nedelikovic.pdf (19.04.2016)*

Развивањето и примената на процедури за соодветно и безбедно користење на сервисите кои се понудени од одредена мрежа е основниот чекор за безбедноста на мрежата и податоците преку кои истите се процесираат.

Правилната имплементација на софтверски и хардверски решенија за безбедност на мрежа е исто така важен сегмент од безбедноста на мрежата. (хардвер за енкрипција, софтвер за енкрипција, софтверски решенија за мониторинг и алармирање на одредени злоупотреби, софтверски решенија за ефикасна автентикација и авторизација на корисниците итн).

Третиот сегмент од безбедноста на мрежи преставува корисникот и неговото однесување на мрежа, односно неговото ниво на свесност за безбедноста и обезбедената обука за безбедно користење на мрежата и заштита на податоците.

Со самата заштита на мрежата, со вложување во истата, ги заштитуваме информациите од неовластено превземање, го заштитуваме протокот на сите информации кои поминуваат низ мрежите, го правиме безбеден компјутерскиот простор во кој се наоѓаат информациите.

Заштитата на информациите е од суштинско значење, затоа што доколку чуствителни податоци, информации од национален карактер, дојдат до одредени криминални структури или до некоја друга држава, можат да предизвикаат последици и несакани дејствија од огромни размери, а со тоа и да се влиаје на националната безбедност.

Интернет безбедност

Интернетот и неговите придружни компликации станаа составен дел од нашите животи. Со оглед на огромното влијание на интернетот врз нашите секојдневни активности, како и продорното влијание што го има врз сите сегменти на компјутерската индустрија, системите кои се користат во

домовите, образованието, бизнисот, Владини институции, сите се подложни на интернет инвазијата, се поставува и прашањето за безбедноста на интернетот.

Интернет безбедноста е широк поим, и истата опфаќа безбедност на податоците внесени на интернет, како и целокупната проверка и заштита на податоците кои се испратени преку интернет протокол.

Преку интернет може неовластено да се навлезе во компјутерски системи, банкарски сметки, електронска пошта, бази на податоци, при што може да се инсталира одреден вирус и да се украдат сите податоци. Со тоа се доаѓа до огромен број на лични податоци на лица, се краде нивниот идентитет, податоци од нивните банкарски сметки или платежни картички, а со тоа се крадат нивните парични средства, се доаѓа до класифицирани информации, податоци и информации од државен карактер кои се државна тајна и сл.

Исто така заштитата на личните податоци е голем приоритет на секој поединец, кој кога ќе биде сигурен дека неговите лични податоци се безбедни на интернет се повеќе ќе го користи интернетот а со тоа се зголемуваат можностите за негова лична надградба, се зголемуваат неговите погледи и сл.

Добра интернет безбедност го штити финансискиот пазар, како и интернет трговијата која е во се поголем подем во секоја современа држава, дава сигурност на населението за користење на интернет банкарство, вршење на интернет трансакции.

Поради тоа потребно е интернет безбедноста да стане врвен приоритет на секоја современа држава која се стреми да има безбедно интернет општество, да се создадат правила и постојано да се превземаат активности за да интернетот се заштити од напади односно неовластен пристап.

Компоненти на Информационата Безбедност се следниве:

- Заштитна, одбранбена безбедност во која спаѓаат:
    - Лична, физичка и безбедност на документите;
    - Безбедност на комуникациите (Comsec),

Emcom, Copusec итн;

- Камуфлажа
  прикривање
  намалување на потписите;
- Контраприслушкување
  Контраиспрашување
  Безбедносна едукација;

- Откривање, неутрализација и непријателски напад во кој спаѓаат:
  - Физичка елиминација на прибирачите на разузнавање
  - Контрашпионажа
  - Контраразузнавање

- Измама во која спаѓаат:
  - Двојни агенти
  - Доставување на лажен и фалсификуван материјал до странските сензори[26]

Концептот на информационата безбедност не е нов. Развиен е така наречен концепт „Комуникациона Безбедност" (COMSEC – communication security). Со појавата на компјутерите во седумдесетите години развиен е и концептот „Компјутерска Безбедност" (COMPUSEC – computer security). Кон крајот на осумдесетите години COMSEC и COMPUSEC се обединили во „Информациона Безбедност" (INFOSEC – information security).

Акцентот на Информационата безбедност е ставен на спречување на неовластен пристап на информационите системи, со што се гарантира довербата, интегритетот, и расположивоста на информациите.

Информационата безбедност е интегрална компонента на националната безбедност, која подразбира заштита на животно важните вредности и интереси на поединецот, друштвото и државата во информатичката сфера, од надворешни и внатрешни закани и ризици, односно

[26] *Мајкл Херман, Моќта на разузнавањето во Мир и во Војна, Академски печат Скопје, 2009, стр.194.*

заштита на информационата средина која овозможува нејзино формирање, користење и развој во интерес на граѓаните, организациите и самата земја.[27]

Конкретно информационата безбедност преставува заштита на националните информациони ресурси и потенцијали од физичко загрозување, во отсуство на опасност што може да ја загрози стабилноста на информациите, што ја покажува корелацијата на Информационата Безбедност и Националната Безбедност.

Информационата безбедност како еден вид на безбедност е дел од информационото друштво. Современото информационо друштво е незамисливо без сериозно третирање на информационата безбедност. Со тек на времето информационата безбедност стана основна компонента на националната безбедност.

За поединецот, информационата безбедност значително влијае на приватноста, што во различни култури различно се толкува.

Во тој контекст Информационата безбедност се дели:

- *Доверливост;*
- *Интегритет и*
- *Достапност.*

Доверливост – преставува етички принцип на одлучување, сигурност дека информациите се достапни само на авторизирани луѓе. Кога информацијата ќе се прочита или ископира од некој кој не е овластен тоа да го прави, резултатот на тое е губење на доверливост. За некои видови на информации доверливоста е многу важен атрибут. Се поприсутни се во медицинита, правото, но важат и за деловни тајни што значи дека се применуваат и во бизнис сферата. Исто така се однесува и на личните податоци и сите други податоци кои не смеат да станат достапни до лица за кои не се наменети, како

---

[27] *Корелација Информационе и Националне Безбедности, Др Саша Мијалковиќ, Др Вера Арежина-Ќериќ, Др Горан Бошковиќ, стр.8. пдф.*

и во коорпоративни инвестициски стратегии. Ова е особено важно за банки и кредитни компании, наплата на долгови, агенции кои нудат услуги како што се психолошки советувања, третман со лекови и сл. Доверливоста денес во работењето се базира на принцип на минимум информации кои треба да се знаат, односно службените тајни кои се достапни на вработените се одредени на минимум, онолку колку што им е потребно за извршување на работните задачи.

Интегритет – преставува заштита на точноста и интегритетот на информацијата, како и на самиот процес. Информациите можат да бидат оштетени кога се ставени на несигурна мрежа. Во поширока смисла интегритетот одредува временски лимит, точност и валидност на информацијата, што подразбира дека за дадените услови за информација нема да бидат променети во однос на оригиналната форма. Интегритетот е нарушен доколку дојде до намерна или ненамерна промена на релевантни податоци или информациски систем. Интегритетот е особено важен за критични безбедносни и финансиски податоци кои се користат за активности како што се електронски трансфер на средства, контрола на воздушниот сообраќај, сметководство и сл.

Достапност – преставува сигурност дека само овластените лица имаат пристап до информацијата. Доколку информацијата не е достапна до крајниот корисник, постои веројатност дека ќе дојде до загрозување на задачата за која била потребна. Достапноста е често најважниот атрибут во бизниси кои зависат од информации како на пр: авиокомпании, online системи и сл. Достапноста на самата мрежа е важна за секој чиј бизнис или образование се базира на мрежна конекција. Кога корисниците неможат да пристапат на мрежата или специфичните услуги обезбедени на мрежата, тие имаат одбивање на услугата. За да ги стават на располагање информациите до оние на кои им се потребни, организациите користат проверка на автентичност и авторизација. Автентикацијата и авторизацијата одат заедно „рака под рака". Корисниците мора да бидат заверени пред извршување на дејноста, дека се овластени да ја извршуваат таа дејност.[28]

---

[28] *Introduction to Information Security, Linda Pesante, 2008 Carnegie Mellon University, pdf, pp.2.*

Овие концепти на безбедност на информации исто така се однесуваат на безбедност на терминот информација. На интернет корисниците сакаат да бидат сигурни дека:

- Тие може да веруваат на информациите кои ги користат;
- Информациите за кои се одговорни да се делат само на тој начин на кој тие очекуваат;
- Информациите ќе бидат достапни тогаш кога ќе биде потребно;
- Системите кои тие ги користат ќе ги обработуваат информациите навремено и на доверлив начин.

Покрај тоа информациите се прошируваат на сите системи, како системи за контрола, вградени системи, опфаќаат системи со хардвер, софтвер и човечки компоненти.

Вредноста на информациите доаѓа од карактеристиките кои ги поседува самата информација, и според тоа вредноста на информацијата или се зголемува или се намалува. Некои карактеристики влијаат на вредноста на информацијата, може да зависи од навременост на информацијата која може да биде критичен фактор, бидејќи информацијата која се губи и е дадена премногу доцна, губи од својата вредност. Примери на важни информации се лозинки, контрола на пристап на датотеки, енкрипција, алгоритам, информации за персонал. **На интернет никој не имун.** Оние кои се засегнати се банки, финансиски компании, осигурителни компании, брокерски куќи, владини изведувачи, владини агенции, болници, даватели на мрежни услуги, универзитети и сл.

Доколку една држава има информациона моќ, односно развиена информациона технологија, тоа значи дека истата ја унапредува технолошката моќ, овозможува развој на економијата, модернизација на вооружените сили, унапредување на животниот стандард на населението, како и контрола на транснационалниот електронски и комуникациски сообраќај, и на тој начин ја зголемува политичката моќ на државата.

Глобалните компјутерски мрежи овозможуваат создавање на нов облик на криминал. Научно-техничката револуција доведе до формирање на информациско општество во кое информацијата е главен фактор во управување со светот, и високотехнолошкиот криминал постана меѓународен феномен и најсериозна закана за националната безбедност.

На крајот од 20 век и почетокот од 21 век бил забележан значителен напредок во областа на телекомуникациите, компјутерскиот хардвер и софтвер, и кодирањето на податоци. Достапноста на помала, помоќна и помалку скапа компјутерска опрема ја става електронската обработка на податоци на дофат на малите бизниси и на приватните корисници. Овие компјутери многу брзо станаа меѓусебно поврзани преку мрежа генерички наречена Интернет или World Wide Web (Светски распространета мрежа).

Високотехнолошкиот криминал е во рапиден пораст, а според најновите истражувања штетата од нападите на глобално ниво изнесуваат повеќе од 400 милијарди долари. Како резултат на финасискиот високотехнолошки криминал, Австралија во 2003 година се соочи со загуба од 3,5 милиони долари, а вирусите, црвите и тројанците преку два милиони. Следната година финасискиот компјутерски криминал се намалува на два милиони долари, но последиците од вирусите се зголемуваат преку седум милиони. Исто така и Британците не поминуваат ништо подобро, бидејќи во 2003 година, финасискиот компјутерски криминал ги чинел 120 милиони фунти, а вирусите 27,8 милиони.[29]

Приватниот сектор и корисниците почнуваат да преставуваат значаен фактор во создавањето на услови за заштита на приватните компјутерски мрежи и нивната поврзаност со глобалната интернет мрежа, размената на информации помеѓу стручните лица за борба против високотехнолошкиот криминал. Развојот на безбедна интернет инфраструктура не може да се

[29] *Југослав Ачкоски, Сигурност на компјутерски системи, компјутерски криминал и компјутерски тероризам, Скопје, 2012, стр.23.pdf.*

замисли без заеднички активности на секој од овие актери, бидејќи високотехнолошкиот криминал постана меѓународен феномен и најсериозна закана за безбедноста.

Постоечките и потенцијални предизвици во областа на високотехнолошкиот криминал се меѓу најсериозните предизвици на 21-от век. Заканите произлегуваат од широк спектар на извори, а се насочени кон Влади, поединци, национални инфрастуктури. Нивните ефекти носат значителен ризик за националната безбедност, јавната безбедност, како и стабилноста на државите.

Злоупотребата на високотехнолошкиот криминал и заканите кои доаѓаат од него лесно може да бидат сокриени. Потеклото, мотивот, идентитетот на сторителот тешко може да се утврди. Сторителите може да работат од различни места на светот, и да поминат неказнето. Тоа се некои од најважните недостатоци на „традиционалното" кривично право, кои придонесуваат граѓаните да се чувствуваат несигурни во моќта на државата да ги заштити. Мотивите се различни, во најголема мера е едноставно демонстрација на техничка моќ, кражба на пари или информација, или како продолжение на државен конфликт. [30]

Во моментов високотехнолошкиот криминал (сите негови видови и облици) се во подем, што може да доведе до сериозни нарушувања на општата безбедност на земјата, како еден од најмодерните и најсофистицирани видови на криминал.

Вклучување на малициозни софтвери и скриени функции во информационата технологија ја поткопува довербата на луѓето во услугите и производите, ја нагризува довербата во трговијата а со тоа се влијае на растот на економијата, и се влијае на националната безбедност.

---

[30] *Department Of Information Technology National Cyber Security Policy "For secure computing environment and adequate trust & confidence in electronic transactions "*, Department of Information Technology Ministry of Communications and Information Technology Government of India Electronics Niketan, Lodhi Road New Delhi – 110003 *pdf.*

Добро организиран и распореден напад со помош на високотехнолошкиот криминал може да доведе до витални информации, комуникации, шифри за енкрипција и сл. Зголемувањето на софистицираноста на нападите се усложнува се повеќе, и напорите за собирање на вредни разузнувачки информации се ефиктивни заштитни и превентивни мерки.

Нападите на високотехнолошкиот криминал кои се насочени кон критични информации и критичната инфрастуктура (телекомуникациски објекти, објекти за пренос и производство на електрична енергија, складишта и транспорт на нафта, гас и други деривати, водоснабдување, сообраќај, владини државни институции и др.) се од витално значење за националната безбедност на секоја држава, и се класифицираат како масовни напади кои ја оневозможуваат инфрастуктурата и ја прават неупотреблива.

Поради тоа современите држави даваат големо внимание за заштита на националната безбедност од заканите предизвикани од високотехнолошкиот криминал. Врвната технологија, софистицираните системи, огромната брзина – на компјутерските системи за складирање, обработка и размена на доверливи информации, тоа се само дел од многуте силни атрибути на високотехнолошкиот криминал.

Времето на потценување на важноста на информационата технологија, како и ставање во позадина на незапирливото брзо напредување на информационата технологија, заврши.

Економијата на секоја земја се потпира на информационите системи и мрежната поврзаност, и на тој начин се обезбедува просперитетот на една држава, а со тоа се заштитува и безбедноста на компјутерскиот простор од криминални активности кои влијаат на националната безбедност. Кражбата на тајни информации од национални компании, напад на инфрастуктури од витално значење за инфрастуктури од витално значење за функционирање на државата, или напад на приватноста на

граѓаните, се сметаат како екстремни примери на закани на високотехнолошкиот криминал врз националната безбедност.

Со оглед на транснационалниот карактер на високотехнолошкиот криминал, техничките и правните предизвици во обезбедувањето на националната безбедност, информационите системи и мрежи, безбедноста на информациите, како и поврзани влијанија врз социо-економскиот живот во земјата, вклучува серија на овозможување на процеси, соработка и заеднички напори во земјата и надвор од неа.

Една од најдобрите заштити на националната безбедност од заканите на високотехнолошкиот криминал е соработката помеѓу владиниот и приватниот сектор, односно јавно-приватното партнерство е клучна компонента. Оваа соработка може значително да ја подобри размената на информации, ќе ја подобри свеста помеѓу луѓето, ќе има технички подобрувања, обуки и сл. Исто така клучни активнсоти за заштита на националната безбедност од заканите на високотехнолошкиот криминал се користењето на безбедносни услуги, протоколи, доверливи мрежи и дигитални системи за контрола, успешна соработка и координација со Интернет сервис провајдерите (ISP) во однос на обезбедување на податоци, обезбедување на безбеден проток на информации.[31]

Како најдобра заштита е формирање на Национален безбедносен тим за справување со компјутерски инциденти (CERT). Ова национално тело ќе превзема проактивни мерки со цел да се делува за да се спречат или ублажат

[31] *Department Of Information Technology National Cyber Security Policy "For secure computing environment and adequate trust & confidence in electronic transactions ",* Department of Information Technology Ministry of Communications and Information Technology Government of India Electronics Niketan, Lodhi Road New Delhi – 110003*pdf.*

последиците од можни штети, како и реактивни мерки за делување на компјутерски инциденти.

Меѓу ***проактивните мерки*** кои ќе ги превзема телото се:

- Континуирано следење на состојбите во областа на информацискатa безбедност и времено објавување на предупредување (security alerts), во насока на превенција од настанување на штета;
- Континуирано следење на развојот на технологиите за информациска безбедност и дисеминација на собраните информации;
- Подигнување на јавната свест за значењето на информацискатa безбедност;
- Обезбедување едукативни обуки за специфични групи на корисници.

Реактивни мерки кои ќе ги превзема телото се:

- Координација во решавањето на поголеми компјутерски инциденти;
- Подготвување и дистрибуирање безбедносни предупредувања (security alerts), врз основа на добиени информации;
- Собирање, обработување, подготвување и дистрибуирање на безбедносни препораки за ранливост на информациските системи.

Воспоставувањето на Националното тело за справување со компјутерски инциденти истовремено ќе значи и подршка за градење на национална култура за информациска безбедност и подршка на иницијативи за подигнување на свеста помеѓу корисниците и граѓаните.[32]

Во Р.Македонија веќе е формиран CERT Тимот кој е во рамките на Агенцијата за Електронски Комуникации – АЕК, и во фаза на развивање.

Можеме да заклучиме дека бројните и разновидни потенцијални закани кои ги загрозуваат информационите системи во институциите, организациите и компаниите, а посебно оние кои имаат карактер на криминални дела,

[32] *http://it.mk/k-e-se-formira-natsionalno-telo-za-spravuvan-e-so-kompjuterski-intsidenti/ (21.04.2016).*

недвосмислено ја наметнуваат потребата за изградба на соодветни системи за заштита на дигиталните податоци во компјутерските мрежи. Во ниеден момент не смее да се заборави на фактот дека не постои апсолутна заштита и дека секој информационен систем е изложен на ризици, но со навремено дејствување, големината на постоечкиот ризик, можно е да се доведе во прифатливи граници.

III ГЛАВА

1. ВИСОКОТЕХНОЛОШКИ КРИМИНАЛ

1.1 ПОИМ И ВИДОВИ НА ВИСОКОТЕХНОЛОШКИОТ КРИМИНАЛ

Промените предизвикани со информатичката технологија, кои се очигледно видливи, се однесуваат на начинот на прибирање, складирање, обработка и презентирање на информации, при што информацијата станува стратешки ресурс кој во постиндустриската ера може да се покаже вредна и влијателна во мерка во која тоа претставува капитал во индустриската ера. Благодарејќи на тоа, современиот информационен и комуникациски систем, користен на вистински начин може да ја зголеми ефикасноста на голем број активности.[33]

Свесни сме за брзината со која напредува светот како и новата технологија. Новите технологии им овозможуваат на криминалците нови можности и полиња на делување. Начинот на извршување на кривичното дело во минатото и денес е многу различен. Денес криминалците со многу помали ризици остваруваат голема финансиска корист и многу други придобивки.

Развиената технологија во модерното информациско општество се користи за извршување или олеснување на разни криминални активности. Во рацете на лица кои се криминогени, информацискатa технологија може да стане алатка за загрозување или повреда на животот, имотот или достоинството на поединецот. *Пристапот на класичната безбедност само ги доведува во застој новитетите во однос на високотехнолошкиот криминал.* Тоа веќе не е изводливо во овој дигитален свет, бидејќи обработката на инфорациите се дистрибуира многу брзо. Иновативните решенија се поптираат

[33] *Никола Тупанчевски и Драгана Кипријановска „Основи на македонското информатичко казнено право" МРКПК бр. 2 - 3, Скопје, 2008, стр. 523.*

на новите технологии, се променува традиционалниот пристап кон безбедноста.[34]

Делата кои потекнуваат од високотехнолошкиот криминал е тешко да се перципираат, истражуваат и процесуираат, и со тоа се откриваат најважните недостатоци на „традиционалното" кривично право, со што се создава атмосфера граѓаните да имаат намалена доверба во системот. За успешно спречување на оваа појава потребна е соработка помеѓу, полициските служби и интернет сервис провајдерите, телекомуникациските институции и мобилните оператори. Координарана активност и соработка на овие институции води кон успешна борба против заканите на високотехнолошкиот криминал.

Дали злоупотребата на информатичката технологија е само логичен продолжеток на секојдневниот криминалитет, како негов подвид или пак се работи за сосема нов и посебен облик на криминогено однесување кој бара посебен пристап и третман?

Поставената дилема треба да се гледа во контекст на следниве факти а во функција на разликување на злоупотреба на информатичката технологија во однос на добро познатите облици на класичен криминал и се однесува на следново:

- потребен е релативно краток период за да се стекнат неопходни вештини за извршување на кривични дела од оваа област;
- релативно се мали вложувањата во однос на направената штета или остварената противправна имотна корист, кои може да се направат без физичко присуство на местото на сторување на кривичното дело;
- често не е јасно дефинирано дали се работи за кривично дело или не, поради недостатоците на правниот систем; и
- тешкото откривање и уште потешкото докажување.

Меѓутоа, и покрај искажаното, сите класични елементи кои се применуваат при откривање и гонење на класичниот криминал се применливи и тука, без

[34] *Creating a Safer Information Society byImproving the Security of Information Infrastructures and Combating Computer-related Crime, Europe 2002, pp. 7, pdf.*

оглед на наведените разлики, затоа што на крајот на краиштата, компјутерите и компјутерските мрежи како и интернетот се само орудие во рацете на вештите криминалци.

Имено, првичното дефинирање на високотехнолошкиот криминал било дека тоа е:,,било кој незаконски акт за чие успешно извршување е пресудно познавањето на компјутерската технологија".[35]

Високотехнолошкиот криминал е криминал овозможен од страна, или од друг таргетиран компјутер. Некои тврдат дека не постои утврдена дефиниција за Високотехнолошки криминал, бидејќи „компјутерскиот простор" е нов специфичен инструмент кој се користи да им помогне во извршувањето на кривичните дела. Високотехнолошкиот криминал вклучува намерни напади на други компјутери со цел да уништи процеси, тука се вклучува и компјутерската шпионажа. Ако терористичката група требаше да започне компјутерски напад за да предизвика штета, таков чин се вклопува во дефиницијата на високотехнолошки криминал. Примарната разлика е во намерата на напаѓачот, и возможно е дејствијата од двете етикети да се преклопат.[36]

Во моментов високотехнолошкиот криминал (сите негови видови и облици) се во подем, што може да доведе до сериозни нарушувања на општата безбедност на земјите, како еден од најмодерните и најсофистицирани видови на криминал.

Во теоријата за кривично право, криминологија и криминалистика може да се најдат повеќе дефиниции за поимот на високотехнолошки криминал, но и меѓународните документи имаат свои дефиниции за овој вид криминални дејствија.

Дон Паркер го одредува високотехнолошкиот криминал како злоупотреба на компјутерот во смисла на секоја активност која е поврзана со

---

[35] Светлана *Николоска Компјутерски кривични дела против слободите и правата на човекот и граѓаните во Република Македонија, Хоризонти бр. 6, Битола, 2010, стр. 243.*

[36] *Clay Wilson Specialist in Technology and National Security Foreign Affairs, Defense, and Trade Division, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, pdf.*

употреба на компјутерската технологија во која жртвата трпи загуба или би можела да има загуби, а сторителот делува со намера за себе да прибави или би можел да прибави корист.[37]

August Bequai го дефинира високотехнолошкиот криминал како вршење на кривични дела кај кои компјутерот се јавува како средство или објект на заштита, односно како употреба на компјутерот при вршења на измами, затајувања или злоупотреби при што целта е присвојување на пари или услуги или вршење на политичка или деловна манипулација која вклучува и дејствија насочени кон компјутерот.[38]

Бого Брвар има своја дефиниција за високотехнолошкиот криминал и тоа дека тоа се кривични дела кај кои компјутерот се појавува како средство (орудие), предмет или објект за чие извршување или обид е неопходно одредено знаење од информатиката или компјутерите.[39]

Ѓорѓе Игњатовиќ под високотехнолошки криминал подразбира посебен вид криминални однесувања кај кои компјутерскиот систем (сфатен како единство на хардвер и софтвер) се појавува или како средство на извршување или како објект на кривичното дело, доколку делото на друг начин или спрема друг објект воопшто не би можело да се изврши или би имало други карактеристики.[40]

„Под компјутерски криминал се подразбира секое дејствие во кое компјутерот е средство и цел за извршување на кривично дело, според Сулејманов". [41]

Треба да се прави разлика помеѓу високотехнолошкиот криминал и компјутерскиот „cyber" криминал. Високотехнолошкиот криминал ги опфаќа кривичните дела кои се извршени на компјутер, материјалите содржини во него (софтвер и податоци) и притоа компјутерот се користи како средство или се со цел за извршување на кривични дела.

---

[37] *Don Parker, Computer abuse, Springfild, 1973, str. 70.*
[38] *August Bequai, Computer crime, Lexington, 1978, pg. 4.*
[39] *Brvar Bogo, Pojavne oblike zlorabe računalnika, Revija za kriminalističko in kriminologijo br. 2/1982, Ljubljana*
[40] *Đ. Ignjatović, Pojmovno određivanje kompjuterskog kriminaliteta, Anali Pravnog fakulteta u beogradu, Beograd, br. 1 - 3/1991, str. 142.*
[41] *Зоран Сулејманов „Криминологија" Скопје, 2003, стр. 631.*

Високотехнолошкиот криминал опфаќа, навлегување во друг компјутерски систем, кражбата на компјутерски податоци, или користењето на on line системите за извршување или помош во извршувањето на измами. Тука спаѓаат хакирањето, напад на сервисите за одржување и функционалност, неовластено користење на податоците и сајбер вандализмот.

Додека пак од друга страна компјутерскиот „cyber" криминал ги опишува криминалните активности кои се извршени со користење на електронски медиуми за комуникација. Во најширока смила компјутерскиот „cyber" криминал е секоја криминална активност која се извршува преку употреба на компјутери и компјутерски системи и мрежи.[42]

Оттука, логички произлегува да ги рекогницираме основните карактеристики на високотехнолошкиот криминал. Како негови најосновни обележја се употребата на компјутерот како објект на напад и како средство за извршување на делото. Покрај големиот број на различни криминални постапки, дури невозможно е да се одреди заедничка цел на високотехнолошкиот криминал. Меѓутоа, може да се заклучи дека сите активности кои што имаат карактеристики на инкриминарани дејства се сведуваат на уништување, оштетување, отуѓување, неовластена измена, објавување или употреба, оштетување и навлегување во компјутерски системи или нивни делови.

Кога се појавува како објект на напад, кај компјутерот може да се нападнат две компоненти хардверот и софтверот. Оштетувањето, уништувањето или злоупотребата на овие две компоненти се остварува со помош на три основни средства, и тоа: компјутески вируси (virus), црви (worms) и тројанци (trojan). За разлика од првите два, кои што нивниот креатор кога ќе ги испрати нема повеќе контрола над нив, третиот тип претставува опасност која за нас е од посебен интерес со оглед на тоа што претстасвува компјутерски програм кој му овозможува на испраќачот да пристапи на „заразениот" компјутер, да има увид во неговите податоци и да манипулира со истите, без притоа сопственикот и да е свесен за тоа.

[42] Drakulic, Mirjana, Drakulic, Ratimir, „Cyber kriminal", Fakultet organizacionih nauka, Begorad, 2009, str. 56

Кога се појавува како субјект на напад, односно како средство на извршување на кривичното дело, станува збор за "олеснување" или овозможување на реализација на одредена кривична активност со негова помош. Тука е многу значајно да се напомене дека компјутерот може да се употребува како средство за планирање односно прикривање на кривични дела или раководење со одредени криминални активности. Оаа функција е значајна поради фактот што во иднина таа ќе биде точка на поврзување помеѓу организираниот криминал и високотехнолошкиот криминал. Односно веќе спомнавме дека сите фази на компјутерски операции се осетливи на криминална активност, како цел на криминал или како инструмент за изведување криминал, а операциите за внесување, обработка на податоци, операциите за излез и комуникациите се користат за забранети цели.

Користење на интернетот за прикривање на потеклото на нелегално стекнати пари (перење на пари), со цел употреба на истите при финансирање на терористички организации, ранливоста на компјутерските системи од една страна и употребата на компјутерските системи за складирање, обработка и размена на доверливи информации, и дава нови димензии на поимот „шпиунажа", правејќи го моќна алатка во рацете на современите контраразузнавачки агенции дефинирајќи притоа сосема нов поим наречен „cyber или компјутерска шпиунажа", електронското тргување и неговото директно влијание врз националната безбедност, како и глобализацијата се потенцијалната опасност за личната, националната и глобалната безбедност.

Со оглед на фактот што високотехнолошкиот криминал не е во потполност феноменолошки заокружен, постојат повеќе други поделби спрема различни критериуми, но за ниту една не може да се рече дека е универзално прифатена.

Но, според една од најприфатените класификации, разликуваме повеќе видови и тоа:

- **економски компјутерски криминалитет** (компјутерска измама, саботажа, кражба, хакинг, правење и внесување вируси, софтверска пиратерија и сл);

- **политички компјутерски криминал** (компјутерски тероризам и шпиунажа);
- **нарушување на сајбер приватноста** (нелегално прибирање на податоци за личноста, кражба на идентитет, користење на лажни податоци, навлегување во е-маил, фишинг, прислушкување, снимање и сл.);
- **производство и дистрибуција на недозволени содржини** (детска порнографија, педофилија, верски секти, ширење на идеологијата на рацистички, нацистички и слични идеи и ставови, злоупотреба на жени и деца);
- **манипулација на забранети производи, супстанци и стока** (дрога, човечки органи и оружје);

Но, според ***Конвенција за компјутерски криминал***[43], наведени се следниве појавни облици и начини на извршување на кривичните дела од областа на високотехнолошкиот (компјутерскиот) криминал:

1. **Компјутерска измама;**
2. **Крадење на идентитет (phishing, pharming и spam);**
3. **Финансиски кражби и злоупотреби;**
4. **Фалсификување на податоци и документи;**
5. **Компјутерски вандализам;**
6. **Изработка и употреба на компјутерски вируси (вируси, црви и тројанци);**
7. **Компјутерска саботажа и шпионажа;**
8. **Хакерство (креирање и злоупотреба на botnet мрежи);**
9. **Неавторизирана репродукција на легално-заштитени компјутерски програми (софтверско пиратство);**
10. **Компјутерски тероризам.**

---

[43]*Конвенцијата за компјутерски криминал е донесена од Советот на Европа на 23.11.2001 година во Букурешт, а влезена во сила на 01.07.2004 год. Република македонија ја има ратификувано Конвенцијата со Закон за ратификување на Конвенцијата за Компјутерски криминал донесен на 16.07.2004 год.*

1.1.1 КОМПЈУТЕРСКА ИЗМАМА

Компјутерската измама е кривично дело кое го врши одредено лице со внесување на одредени неточни податоци, или невнесување на одреден важен податок со цел тоа да влијае на резултат на електронската обработка или на преносот на податоците и така за себе или за друг противправно да прибави одредена имотна корист или да нанесе штета на друг.

Компјутерските измами можеме да ги дефинираме и како измами кои се извршуваат со намера за стекнување за себе или за друг со протиправна материјална корист, со тоа што кај нив во заблуда не се доведува или одржува некое лице, како што се случаите со обичните измами, како материјалните кривични дела со кои се предизвикува штета, туку заблудата се однесува на компјутер во кој се внесуваат неточни податоци, или се пропушта внесувањето на точни податоци, или на било кој друг начин, компјутерот се користи за остварување на измами во кривично – правна смисла. Компјутерските измами представуваат најраширен облик на компјутерски криминал.[44]

Компјутерската измама претставува специфичен облик на класичниот облик на измама каде што жртвата се доведува во заблуда од страна на сторителот кој може да има директен (непосреден) контакт или индиректен

[44] *Југослав Ачкоски, Сигурност на компјутерски системи, компјутерски криминал и компјутерски тероризам, Скопје, 2012, стр.30,пдф*

(посреден) контакт со жртвата која ја доведува во заблуда презентирајќи и лажни факти или состојба, со цел да извлече одредена материјална корист.

Кај компјутерската измама карактеристично е тоа дека сторителот и жртвата не стапуваат во директен физички контакт, нивниот контакт е директен, но електронски.

Исто така, компјутерските измами се извршуваат и со внесување на неточни податоци, или со пропуштање на внесување на точни податоци со што се користи компјутерот за стекнување на некаква корист или нанесување на некаква штета.[45]

Информации за платежни картички, како и лични и финансиски информации за лицата-поседувачи на истите, се секојдневна мета на организираниот криминал. Продажбата на овие информации на фалсификатори на платежни картички и патни документи претставува голема опасност.

Компјутерската измама преставува најраширен облик на високотехнолошки криминал. Бројот на облици на измама и нивната реализација е практично неограничен.

Можноста за продажба на стоки и услуги на огромни растојанија и меѓународни граници само со допир на тастатурата или клик на глувчето, создаде бескрајни можности за бизниси. Со напредната технологија границите станаа безбначајни, и се создадоа нови можности за измами.

Она по што ја карактеризира компјутерската измама е тоа што таа е распространета насекаде, во различни облици како на пример: лажни огласи, подразбира фиктивна продажба на секаков вид на стоки, и при уплата на парични средства од страна на жртвата, истите се измамени и не ја добиваат стоката за која уплатиле, потоа неовластено навлегување во електронската пошта и менување на фактури за уплати кои ги користат компаниите а се однесуваат на промени на „iban code“ односно промена на вистинската сметка

---

[45] *Светлана С. Николовска,Методика на итражување компјутерски криминалитет, Скопје, 2013, стр. 29.*

на која треба да се уплатат паричните средства, со лажна сметка, која промена е минимална и неприметна за жртвата. На тој начин паричните средства одат на сметката која ја контролираат криминалците и се стекнуваат со огромна финансиска добивка.

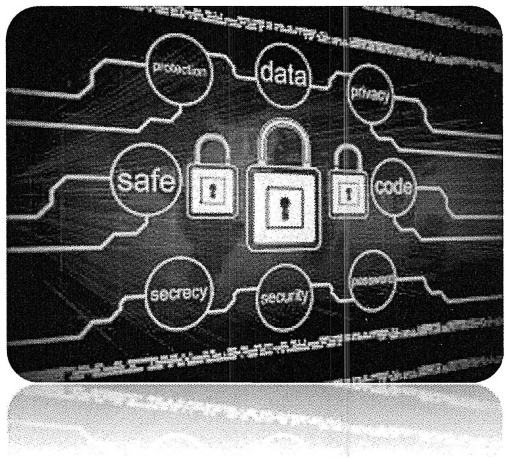
Компјутерските измами може да имаат големо влијание, загубите се значајни, криминалците овие нелегално стекнати парични средтсва можат да ги пренасочат и да ги користат во други области и за извршување на други кривични дела, кои директно влијаат на националната безбедност.

❖

Борбата против компјутерската измама е тешка битка. Со секоја нова технологија, криминалците кои вршат компјутерски измами имаат се поголема можност за извршување на кривичното дело, да иновираат нови модуси, да се заштитат подобро, и секогаш да бидат понапред. Повеќето од компјутерските измами се извршени од срана на меѓународни организирани криминални групи, кои делуваат во различни држави во светот, и поради тоа гонењето против истите е многу тешко.

Покрај малите бизниси така и големите организации треба да ја подобрат својата заштита, да инвестираат во соодветни ресурси, да развијат посилни контроли на нивните мрежи и дигитални податоци. Како еден вид на заштита од компјутерските измами може да биде биометриската технологија која вклучува препознавање на глас. Овој начин на заштита би спречил милијарди долари да завршат во рацете на криминалците, затоа што загубите на глобално ниво се огромни, затоа што се почестите компјутерски измами придонесуваат за огромни финансикси загуби.

1.1.2 КРАДЕЊЕ НА ИДЕНТИТЕТ



Крадење на идентитет е сложен проблем кој е распространет насекаде низ светот. Многу аналитичари истакнуваат дека терминот „крадење на идентитет" најчесто се користи за да се означи терминот „измама на идентитет", па затоа сметаат дека термините „крадење" и „измама" треба да бидат одделени.[46] Постојат повеќе дефиниции за тоа кривично дело кое, всушност е крадење на идентитет за да се изврши измама. Извршителите можат да дејствуваат сами, но се почесто формираат мрежи, како би можеле да оперираат низ светот, со што бројот на нивните жртви станува повеќе милионски.

Според некои процени, годишните парични загуби изнесуваат милијарди долари. Компјутерски криминалци може да ги надминат безбедносните мерки за заштита, да пробијат одредена база на податоци (детални финансиски податоци како на пример банкарски сметки, медицински податоци за лица, и други чуствителни информации), како и да украдат податоци од лични документи: патни исправи, лични карти, возачки дозволи и сл.

Исто така, многу лесно можат да дојдат до идентитетот на секој корисник на платежни картички како еден од видовите на високотехнолошки криминал кој се во подем, на пример со инсталирање камери над банкоматите,

[46] *Wendy Parkes, Thomas Legault, "Identity Theft: Introduction and Background", CIPPIC Working Paper No.1 (ID Theft Series), March 2007, Ottawa: Canadian Internet Policy and Public Interest Clinic, pdf.*

поставување „скимер уреди“ за читање на податоци од платежни картички, кои многу лесно можат да се набават преку интернет. Исто така, на интернет може да се најдат и броеви на платежни картички кои се продаваат на одредени форуми, на кои членството во тие форуми е лимитирано и неможе едноставно да се зачлениш.

Овие криминалци се софистицирани, делуваат организирано и имаат соработка во групи, и истите се неконкурентни. Претпазливи се и не вклучуваат лица од надвор.

Главна цел им е финансиската добивка. Со сите овие прибавени лични податоци на лицата преку нелегално крадење на идентитетот, компјутерските криминалци може со истите да ги компромитираат лицата, да ги продадат нивните лични податоци на други криминалци од сите видови и нивоа, кои пак може да ги искористат за извршување на сериозни кривични дела како (финансирање на тероризам, перење пари, трговија со луѓе, нелегална миграција, компјутерски тероризам и сл.), кои директно би ја загрозиле на националната безбедност на државата.

Како најпознати и најзастапени начини на кражба на идентитет преку информатички систем со цел злоупотреба на истиот, во денешно време се т.н. Фишинг (phishing), фарминг (pharming) и спам (spam).

❖

Кражбата на идентитет првенствено преставува сериозно нарушување на приватноста на поединецот. За да се намали ризикот и да се заштити поединецот потребно е да се идентификуваат потенцијалните ризици и да се работи на нивно отстранување, да се заштитат безбедносните системи како и да се зголеми безбедноста на интернет. Со самото тоа ќе се зголеми довербата на поединецот во информатичката технологија, во новитетите и довербата помеѓу клиентите и давателите на услуги.

1.1.3 ФИШИНГ (Phishing)

Иако постојат неколку различни дефиниции за phishing нападите, во основа тие многу не се разликуваат. Phishing напад подразбира активност на неовластени лица преку користење на лажни пораки-електронска пошта, креирање лажни web страници на финансиски организации со цел наведување на корисникот да ги открие своите доверливи податоци. Притоа се мисли на податоци како што се банкарски сметки, броеви на кредитни картички, кориснички имиња, pin кодови но и други пристапи.

Терминот фишинг доаѓа од англискиот збор "fhishing" кој метафорички ги опишува постапките на неовластените корисници кои ги мамат корисниците на интернет доброволно да ги откријат своите податоци. Иако терминот phishing прв пат се појавил уште во 1996 година, дури последните години се прошири во поширокатa јавност и тоа најмногу поради порастот на неовластени активности од овој тип. Phishing напад во развиените земји станал прилично актуелен и се поголемо внимание се посветува на едукација на корисниците и превземање на сигурносни мерки кои можат да помогнат во спречување на такви напади.

Овие напади може да се поделат во три групи, односно лажни напади, со кои што жртвата, преку лажни пораки, се наведува да даде лични податоци, злонамерни напади, каде што напаѓачот употребува злонамерни софтвер со цел да дојде до посакуваните информации, како и DNS базирани напади, во кои се врши измена на доменот, при што корисникот се упатува на лажна интернет страна.[47]

Најголем проблем кај phishing нападите е тоа што тој не се базира исклучиво на технички елементи, туку користи се посложени и понапредни техники на социјалното инжинерството (social engineering), кое што го искористува неискуството и незнаењето на корисниците на интернет. Со креирање специјално смислени и лажирани пораки на електронска пошта, се

[47] *Aaron Emigh ,Radix Labs „Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures" October 3, 2005.pdf*

обидува да се навести корисникот доброволно и несвесно да ги даде сопствените доверливи информации на неовластениот корисник.

На напаѓачите додатно им олеснува напредната технологија за изработка на web страници (java script, dhtml, activex, flash итн.), кои освен својата легитимна намена се повеќе место наоѓа во неовластените активности како што е на пр.Phishing. Користењето на наведените технологии овозможува да се осмисли многу сложен напад кој ќе ги измами и најискусните корисници. Додатен проблем преставуваат и бројните ранливости во внатрешноста на различни web прегледувачи и e-mail клиенти, кои во комбинација со некој од наведените технологии преставува многу моќно оружје во рацете на неовластените корисници. Се претпоставува дека префиксот **ph** доаѓа од терминот phreaking, денес веќе заборавена техника со која неовластените корисници го компромотирале телефонскиот состав. Спојувањето на овие две фрази (fishing + phreaking) се добива нова кованица под терминот **phishing**.

Текот на phishing нападот можно е да се подели во неколку фази:

- осмислување и подготвување на нападот;
- спроведување на нападот;
- собирање доверливи информации и нивно искористување.

Во фазата на осмислување подготвување на нападот, напаѓачот собира информации за организацијата која сака да ја компромитира, односно за корисниците кои се потенцијални мети на нападот. Успешноста на нападот во голема мерка зависи од тоа колку внимателно и детално е планиран нападот. Искусните неовластени корисници на оваа фаза и посветуваат многу време и ресурси.

Првиот чекор на смислување, односно подготовката за нападот подразбира идентификација на целната организација, детална анализа на содржината и воочување на сигурносните пропусти во внатрешноста на web страницата, идентификација на ранливоста на непознатите клиенти. На темелите на собраните информации напаѓачот креира лажирана копија на web страницата на целната организација, смислува содржина на phishing пораката која ќе ја проследи потенцијалната мета на нападот. Начинот на креирање лажирани web страници првенствено зависи од искуството и вештините на

неовластениот корисник, слично како и за лажирањето на порака по електронска пошта. Досегашните искуства покажуваат дека phishing нападите може прилично да се разликуваат во сложеноста и софистицираноста. Пораките на електронската пошта се настојува да се обликуваат така да делуваат службено, при што содржината на пораката кај корисникот треба да создаде чуство кое што ќе ја намали можноста за реална проценка на ситуацијата (страв, несигурност и сл.).

Во фазата на осмислување и подготовка исто така спаѓа и постапката на идентификација на ранливите e-mail корисници кои ќе се искористат за проследување на пораката на електронска пошта. Тогаш најмногу се користат незаштитените e-mail или proxy, а се почесто се користат и компромитирани компјутери на кои се инсталирани специјални програми кои овозможуваат праќање на e-mail порака. Откако ќе бидат подготвени сите опишани елементи, напаѓачот може да продолжи со следната фаза на спроведување на напад.

Во фазата на спроведување на нападот, напаѓачот праќа спремна порака на електронска пошта на адреса на корисници кои се избрани како потенцијални мети на напад. Освен преку електронска пошта, пораката може да се прати и по пат на news grupa, icq-аи други слични инстант messagingсервиси, огласување на web страници и сл. Освен корисниците кои се целни мети на нападот, напаѓачите многу често користат и додатни канали преку кој може да привлечат поголем број корисници. Така на пример, напаѓачите на лажирани web страници многу често на интернет пријавуваат дека бараат нешто и на тој начин се обидуваат да привлечат корисниците кои за да дојдат до адресата на web страницата користат алатки како што е на пр.google пребарувач. Откако пораките се пратени на припремените адреси, напаѓачот се прикрива и ја очекува првата жртва на нападот.

Во финалната фаза на нападот, напаѓачот по пат на лажирани web страници собира доверливи информации од крајните корисници и ги чува за покасно користење. Собраните податоци може да се искористат за остварување на финансиска корист или е можно да ги продаваат на заинтересирани личности. Крајната цел на оваа фаза е секако финансиска корист.Еве како изгледа една фишинг страна:

Слика

Покрај основните поими и појаснувања за самиот термин phishing, во продолжеток ќе биде накратко опишан типичен пример на спроведување phishing напад. Слично како и кај други малициозни активности, методите на спроведување напад секојдневно напредуваат. Во случај на phishing напад, забележани се неколку различни техники кои накратко ќе бидат опишани.

МАСКИРАЊЕ НА URL АДРЕСА

Една од најчестите техники која ја користат phiseri при лажирање порака на електронска пошта е маскирање url адреса. Со користењето на специјални техники, url адресата наведена во внатрешноста на пораката на електронската пошта, го преусмеруваат корисникот на web страни кои со својот изглед се многу слични (идентични) на web страниците на финансиски установи, кои лажно се прикажуваат. Верувајќи дека се работи за службена web страна на таа установа, корисникот во предвидената web форма ги внесува своите доверливи податоци, а притоа не е свесен дека се работи за измама. Техниките на маскирање на url адреса најчесто зависат од искуството и вештината на неовластениот корисник, но во повеќето случаи доволно се сложени и можат да ги измамат и искусните корисници. Повеќето техники на маскирање на url адреса се базираат на користење напредни својства htmljазик

и други сродни технологии (javascript, dhtml, activex, и сл.), што значи дека користењето на вакви техники не е можно кај порака во чист текстуален облик.

НАЈПОПУЛАРНИТЕ ТЕХНИКИ НА МАСКИРАЊЕ НА URL АДРЕСА СЕ:

Користење домен со слично име. Најчест и наједноставен пример на url маскирање е користење име на доменот кој на прв поглед не се разликува од легитимното име на доменот на организацијата која се импресонира. На пример доколку се сака да се компромитира банка чија легитимна страница се наоѓа на адресата http://www.banka.mk, користењето име на доменот како што е www.banka.city.mk, www.banka.private.mk, www.banka.biz, ќе измами изненадувачки голем број корисници. Познати се случаеви каде се користени и многу посложени методи, кои додатно ја отежнувале можноста на детекција на нападот. На пример регистрација на домен со користење специјални знакови од одредено јазично подрачје, потоа замена на буквата о со бројот 0, или голема буква і со мала буква lи сл. Искуствата покажуваат дека вакви едноставни техники на маскирање се многу ефикасни во смисла на збунување на корисникот.

Користење url адреса со корисничко име и пасворд. Познато е дека поголем број модерни web претражувачи содржат можност да како дел од url адреса наведат корисничко име и пасворд на корисничкиот компјутер од кој се пристапува на web содржината. Формат на urlадреса во тој случај е http://username:password@ www.example.com.

Слично како и во бројни други случаи, вештиот напаѓач ваквата конструкција на urlадреса може да ја искористи за насочување на корисниците на адреса на која се наоѓа web страница поставена за собирање доверливи корисни информации. На пример Urlадреса http://banka:internetbankarstvo @malicious. Com/login.phpнеискусен корисник ќе го преусмерат на web послужател на адресата malicious.com, иако тој е уверен дека се работи за службена webстраница на банката.

Поради тоа што web страниците често користат сложени и прилично долги urlадреси, се појавиле организации кои нудат бесплатни услуги со кои долгите адреси се скратуваат на прифатлива должина. Една од таквите услуги е и онаа која може да се најде на адресата http://www.tinyurl.com.

Користејќи техники од социјално инжинерство и својства на одделни клиенти за прегледување на електронската пошта, кои долгите url адреси ги дели во повеќе редови, phiserite многу често користат токму вакви сервиси за пренасочување на прометот на свој давател на услуги. Наместо да се бара од корисникот делови од долгата адреса неколку пати да ги копира во adressbar поле на web пребарувач, лажираната порака на корисниците им нуди можност да користат скратен облик кој корисниците ќе ги пренасочи на малициозни даватели на услуги. Во тој случај phishing пораката на електронска пошта содржи информации кој го наведуваат корисникот да посети скратен облик на url адреса. Неискусните корисници многу често прифаќаат таква можност, при што на напаѓачите им го олеснува нападот.

За да се осигура подршка на различни јазични подрачја, поголем број нови програмски пакети подржуваат различни типови кодирања со кој е возможно да се прикажат специфични знакови. Таков е сучајот и со модерните web пребарувачи, при што некој од основни техники на кодирање на url адреса се:

1. **Url кодирање** – класичен облик кодирање на url адреса специфичен по знакот % кој се става пред знакот кој се кодира. (на пр.знакот / се прикажува во облик %2f);
2. **Unicod кодирање** – ова е интернационален стандард за кодирање на знакови, кој при користење 16 битни запис оозможува приказ на речиси 50.000 знакови од различни јазични подрачја. Стандардот е развиен поради ограниченият број знакови кој е можен да се прикаже во ascii формат, поради што различни јазични подрачја користат различна имплементација на ascii кодирање. Со оглед на проблемите со компатибилноста со старите состави, развиени се модифицирани од кои најпознат е utf-8 стандард;
3. **Utf-8 кодирање - utf-8** стандард подржува кодирање на знакови користени од една до шест бајтови. Тоа значи дека еден ист знак

може да се прикаже на неколку различни начини, а додатна погодност е тоа што овој стандард е компактибилен со традиционалниот ascii кодирање.

На пример на користење на utf-8 стандард прикажан е на кодиран знак точка (“.“). 8-битни приказ 2e, 16-битни приказ coae, 24 битни приказ 80 ae, 32 битни приказ f0 80 80 aeитн.

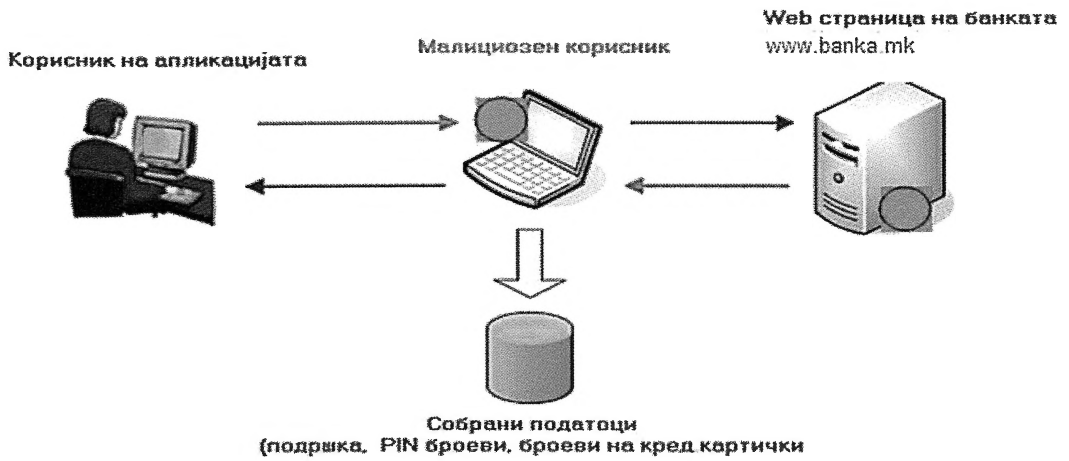
Хексадецимални, октални и децимални прикази кај url адресите можно е секогаш да се користи и поинаков формат на запис на ip адресата со што би се измамил корисникот. На пример децимален приказ на адреса http://192.168.1.1 може да се прикаже на следниве начини: *Хексдецимален приказ* – http://0xc0.0xa8.0x1.0x1 и *Октален приказ* – http://0300.0250.0001.

На сличен начин може да се користи и приказ на користење знакови и точки на кои им се додаваат поедини делови на адресите, (на пример Http:// 3232235777 во децимален облик или http:// coa80101 во хексадецимален облик).

Пресретнувањето на комуникација помеѓу клиентот и давателот на услуга (**Main in the middle attack**) е една од најчестите техники на доаѓање до доверливи корисни информации. Навлегувањето во комуникациски канал воспоставен помеѓу клиентот и давателот на услуга, на напаѓот му овозможува да го анализира комплетно прометот кој се разменува помеѓу овие две точки, дири и кога се користи криптирана комуникација. Самата примена на main in the middle (mitm) напад е идеален за спроведување на phishing напад.

За успешна реализација на нападот потребно е клиентот да се пренасочи на малициозна адреса, а прометот понатаму ќе се пренасочи на легитимен web пребарувач на финансиска установа која сака лажно да се прикаже. Нападнатиот компјутер во тој случај ја извршува proxy функцијата, и ги бележи сите податоци кои се неопходни за понатамошно спроведување на нападот.

Илустрацијата на овој напад е прикажана на шема бр.1.

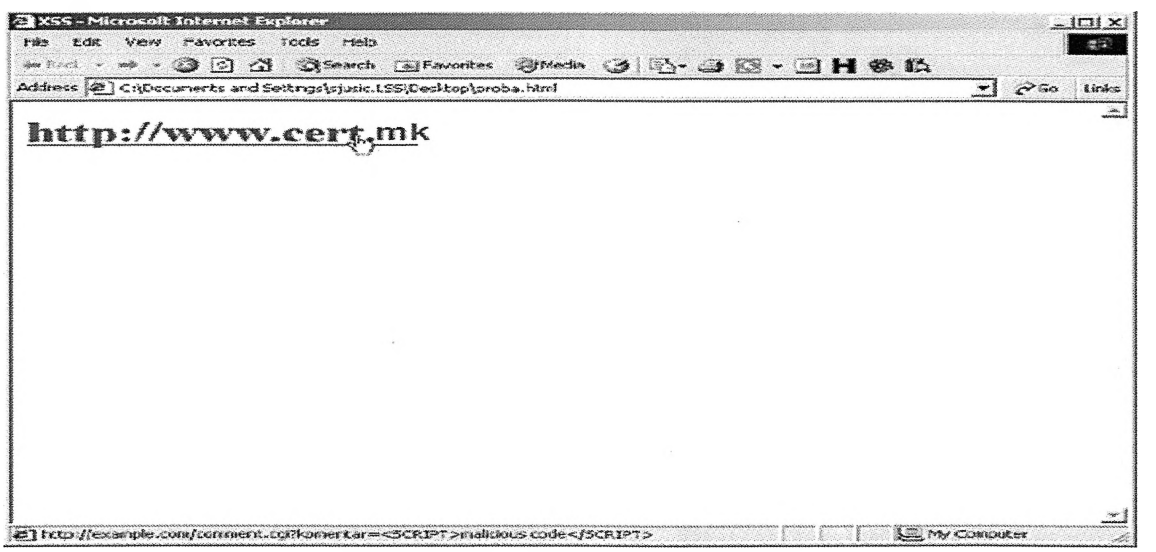


Шема 1: *пресретнување на комуникации помеѓу клиенти и сервери*

Техниките со кои се наведуваат корисниците на малициозни proxy пребарувачи варираат. Освен техниката на маскирање на url адреса може да се користат и посложени напади кои додатно ќе ја отежнат детекцијата на нападот. (Прикажана илустрација подолу)

Една од можностите е **користење dns cache poisoning напади**. Во тој случај напаѓачот во dns базата на некоја банка или финансиска институција, вметнува малициозна адреса која е под контрола на неовластениот корисник. Основен проблем на овој метод е тој што неовластениот корисник мора да биде во можност да го компромитира dns услужувачот на целната институција, што често бара дополнително знаење и искуство.

За доаѓање до доверливи податоци на корисникот напаѓачот може да ги искористи и сигурносните пропусти во web апликацијата на институцијата чии корисници сакаат да се компромитираат. Доколку апликацијата е ранлива на *cross site scripting* (xss) напади, на напаѓачот му се отвараат дополнителни можности за спроведување на нападот. Тоа е врста на напад со кој внатре во web прегледувачот на корисникот се обидува да се изврши малициозен скриптен код (најчесто java script или vbs script), кој на напаѓачот ќе му овозможи реализирање на злонамерни постапки. Xss ранливоста најчесто се појавува како последица на недоволно филтрирање на содржината која апликацијата ја испишува на web страницата. До колку апликацијата без никаква проверка на страницата испишува податоци кои корисникот може произволно да ги уредува, многу е голема веројатноста дека апликацијата е ранлива на xss напади. Доколку корисникот на апликацијата, наместо легитимните податоци го пренесе малициозниот скриптен код кој апликацијата без проверка ќе го испише внатре во страницата, тој код ќе се изврши внатре во web прегледувачот на последниот корисник. На следната шема е прикажан основниот концепт на xss напад.



Односно во првиот чекор легитимниот корисник се пријавува на web пребарување и продолжува со работа во внатрешноста на апликацијата. Во тој момент напаѓачот на истиот корисник му проследува малициозна порака на

електронска пошта во која е содржана url адреса со вграден малициозен код, кој сака да се приклучи на компјутерот на корисникот. Малициозниот код се извршува во внатрешноста на web страницата и извршува малициозна работа одредена од вчитаниот код.

Ова ни укажува на се поголемата опасност од phishing нападите, материјалните загуби кои тие ги нанесуваат, а најмногу треба да бидеме загрижени доколку доверливи информации и податоци со помош на phishing напад дојдат до криминалците. Со оглед на опасноста која доаѓа од овој вид на напад, станува јасно дека треба се повеќе да се вложува во компјутерската сигурност, за да не се дојде до несакаи последици. Да се идентификуваат аномалиите на системите, со цел навремено да се реагира на новите закани.

1.1.3-а Заштита од Phishing напади

Заштитата од phishing нападите требада се имплементира на повеќе нивоа. Бидејќи се работи за напад кој што комбинира технички елементи со социјален инженеринг, потребно е заштитата да се насочи во двата правци. Потребно е техничките аспекти да се решат со соодветни сигурносни контроли кои ќе оневозможат спроведување на нападот (сертификати, сигурно програмирање, редовна инсталација на сигурносна заштита и сл.), додека проблемите на социјалниот инженеринг можно е да се решат првенствено со едукација и подигање на свеста на крајните корисници.[48]

Слично како и во останатите сфери на компјутерска сигурност контролите можат да се поделат во детекциски и превентивни. *Детекциските* контроли се врзани за можноста на навремено откривање и спречување на нападотот ако истите се појават, додека *Превентивни* контроли се врзани за активностите кои ги спречаваат самите појави на напад. Секако, најдобри резултати се добиваат со комбинирање на двата пристапи.

Со имплементација на соодветни *анти-phishing* сигурносни контроли давателите на услуги можат многу да го подигнат нивото на сигурност кое го нудат на своите корисници. Превентивен пристап во решавањето на проблемите многу ќе ја намали можноста на спроведување на *phishing* напади, а корисниците ќе имаат повеќе доверба во услугите кои ги користат. Постојат повеќе превентивни мерки за заштита на корисникот и апликациите на пребарувачот.

Еден од нив е едукација на корисникот. Еден од најважните чекори во нивното спречување е едукација на корисниците преку навремено и редовно информирање за потенцијалните сигурносни проблеми и начините на нивното спречување. Потребно е корисниците јасно да се запознаат со начините на комуникација кои институцијата ги користи и да се нагласи дека било кој друг

---

[48] *Aaron Emigh ,Radix Labs „Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures" October 3, 2005.pdf*

облик на комуникација е несоодветен. Некој од методите кои можат да помогнат во подигањето на свеста и едукација на корисниците се:

- редовно известување на корисниците за актуалните измени и новости во самата институција. Секогаш е можно да се наведат и примери за недозволени активности како корисниците би се запознале со основните техники на залажување кои неовластените корисници ги применуваат;
- оневозможување на пријава на *phishing* нападите. Навремена детекција на *phishing* нападите многу ќе го намали бројот на нејзините жртви. Секако, институцијата мора да вложи доволно средстава во обработка на таквите предупредувања и во соработка со законодавните тела да се овозможи истражување на таквите случаи;
- истакнување на елементи на проверка со кои е можно да се процени легитимноста на службените web страници на организацијата (https конекција, исправност на сертификати, проверка на url адресата и сл.);
- креирање на сигурносната политика и правилници во врска со работењето на институцијата и односите со корисниците. Со креирање и воведување на вакви документи на корисниците им се олеснува детекцијата на сите постапаки кои одстапуваат од дефинираните правила.

Слична автентичност на корисникот. На сите банки и други слични организации им се препоручува користење на силни механизами со кои ќе се оневозможат спроведувања на *phishing* напади, дури и ако напаѓачот дојде до доверливи кориснички информации. Во тој случај се препоручува користење на **token и smart card** аутентикациски механизами во комбинација со пин број или лозинка. Двојната автентичност од корисникот побарува да два пати го докаже својот идентитет, со што додатно се подига нивото на сигурност. Освен познавањето на пин бројот кој е потребан за пристап на составот, корисникот мора и физички да поседува сам token уред за да би остварил пристап.

Ваквиот облик на автентичност на давателот на услугата, но и на крајниот корисник, му даваат поголемо чувство на сигурност, што е многу важно кај критичните состави кои процесираат осетливи информации. Основен недостаток на ваквите решенија се нешто поголеми трошоци на давателите на услугите по корисникот, поголема потреба за едукација, подршка и сл.

Сигурен развој на web апликациите. Сигурен развој на програмскиот код е еден од темелните услови за воспоставување на сигурносен и сигурен информациски состав. Бидејќи *phishing* нападите се усмерени кон институции кои нудат финансиски услуги, овој проблем е додатно нагласен.

Основно правило кое важи при развојот на информациските состави со високо ниво на сигурност е да сигурносните аспекти мораат да се вклучат во што порана фаза на проектот. Последователното решавање на сигурносните проблеми, откако апликацијата е веќе довршена, најчесто ќе резултира со голем број на грешки и слабости кои преставуваат потенцијална опасност. Со оглед дека сигурноста на web апликациите е многу широко подрачје овде ќе бидат наведени некои од основните препораки до кои програмерите би требало да се придржуваат:

- рестриктивно да се филтрира корисничкото внесување;
- рестриктивно да се филтрираат сите податоци кои се испишуваат на страницата, да се користат моќни и проверени криптографски алгоритами, да се користат проверени состави за управување, при испишувањето на грешки да не се откриваат податоци за работата на апликацијата, да се спроведе детално тестирање на апликацијата пред воведувањето во продукциско опкружување, да се користат сигурни механизми за автентичнот и контрола на пристапот.

Сигурност на mail корисникот.

Бидејќи во склопот на спроведување на ***phishing*** нападите за залажување на корисниците најчесто се користат лажирани пораки во електронската пошта, сигурноста на mail услугата исто така игра многу важна улога во заштита од вакви напади. Со оглед дека smtp протоколот, на кој се базира e-mail сервисот, не подржава сигурносни контроли кои би го осигурале интегритетот, доверливоста на автентичноста на пораката во електронската пошта, всушност тоа е еден од основните причини зошто e-mail сервисите најчесто се користат за спроведување на малициозни активности. Дополнително, пораките на електронската пошта многу лесно се лажираат,

што напаѓачите многу често го користат да би ги залажале корисниците и ја зголемат ефикасноста на своите напади.

За да се реши проблемот со лажирање на пораките во електронската пошта досега се предложени неколку решенија, но ниедно од нив не заживеало во потполност.

Едно од решенијата е она од microsoft под име *callerid* односно *senderid.* Основна идеа на овој концепт е организациите во своите dns услуги, освен дојдовните mx услуги задолжени за примање на пораки во електронската пошта, да ги наведат и оние појдовните, кои се користат за испраќање на пораки во електронската пошта. Примателот на пораката на темелот на полето: from, дојдовните пораки би можел да ги провери дали тие истите се испратени од легитимниот e-mail услужувач кој е регистриран како појдовен mx услужувач на domenot чие име е наведено во пораката. На овој начин за секоја порака би било можно да се провери дали навистина доаѓа од domenot кој е наведен во самата порака.

Подетални информации за sender id концептот можно е да се пронајдат на страниците на microsoft

http://www.microsoft.com/mscorp/twc/privacy/spam/senderid/default.mspx

и во carnet cert документот под име „идентификација на пораката на испраќачот на електронската пошта" (http://www.cert.hr/filehandler.php?did=168).

Сличен концепт е предложен и под името rmx (*Remotemailexchanger)* забелешки (http://www.mikerubel.org/computers/rmx records/).

Дигитално потпишување на пораките во електронската пошта

Со дигиталното потпишување на пораките можно е многу да се подигне нивото на сигурност на e-mail составот. Со користење на асиметрична криптографија и сертификат се осигурува автентичност, интегритет и доверливост на пораката што е темелно сигурносно побарување кај модерните информациски состави. Како пример на стандард кој може да се користи за дигитално потпишивање на пораката во електронската пошта можат да се наведат s/mime и pgp, односно open pgp. Важно е да се напомене дека иако овие два стандарди на корисниците им нудат скоро идентична

функционалност, постојат одредени разлики кои овие две технологиии ги прават меѓусебно некомпатибилни. S/mime оригинално е замислен од страна на фирмата rsa data security. Запишувањето на пораката е базиран на pkcs #7 форматот, додека за сертификат се користи x.509v3 стандардот. За разлика од s/mime сервисот, pgp ги користи своите сопствени формати што овие два сервиси ги прави меѓусебно некомпатибилни. Исто така, дигиталното потпишивање и проверка на пораката во електронската пошта можно е да се имплементира или на ниво на клиентот на електронската пошта или на ниво на mail услужувачот преку кој пораките се испраќаат или примаат. Денес на пазарот постојат голем број на алатки кои ги нудат овие функции и фирми кои се занивааат со финансиско работење секако би требало сериозно да ја разгледаат можноста за нивно користење.

Заштита на клиентот

Освен заштитата на услужувачот и апликацијата од страна на давателот на услугата, потребно е да се води сметка и за заштита на персоналните компјутери кои корисниците ги користат за пристап на интернет. Сигурносните пропусти во оперативните состави и различните програмски пакети како што се cems office, internet explorer и сл., неовластените корисници многу често ги користат за спроведување на своите активности. Доколку не се води сметка за сигурносните подесувања во редовната надоградба на составот, корисниците на персоналните компјутери остануваат многу лесни мети за неовластените корисници. На интернет денес е можно да се пронајдат голем број на малициозни програми преку кои е многу лесно да се оствари пристап до персоналните сметачи доколку истите не се редовно одржувани. Проблемот стана дополнително нагласен со појавата на технологии кои овозможуваат постојана врска на интернет *(cablemodem,*xdsl и сл.). Слично важи и за *phishing* нападите кои многу често користат сигурносни пропусти во програмите како што се internet explorer, ms outlook, opera, mozzila firefox и сл. Во продолжение ќе бидат споменати некои од мерките кои ќе го подигнат нивото на сигурност кај персоналните компјутери.

❖

Со следење на овие мерки за заштита значително се намалува ризикот од напад. Но секако треба да бидеме свесни дека никогаш неможеме да бидеме целосно сигурни дека неможе да ни се случи phishing напад. Со следење на новитетите во технологијата и постојано вложување во компјутерската безбедност, драстично го намалуваме ризикот од напад.

1.1.3-b МЕРКИ ЗА ЗАШТИТА НА ПЕРСОНАЛНИТЕ КОМПЈУТЕРИ

Антивирусна заштита, антиспам, персонални „огнени зидови" (Antivirus protection, antispam, personal "firewalls"). Во првата линија на одбрана кога се зборува за персоналните компјутери сигурно спаѓаат алатките како што се антивирусна заштита и персонални огнени зидови, а се почесто во таа категорија се вбројуваат и antispam и antispyware алатките и состави за детекција на неовластени активности (англ. *Intrusion detection sysetm, ids). Исправното користење и редовно ажурирање на овие алатки се темел за одржување на задоволително ниво на сигурност на персоналните компјутери.*

Нивната употреба во повеќето случаи ќе ја спречи појавата на малициозни програми како што се вируси, црви, тројански коњи и сл., ќе ги блокира малициозните конекции од интернет, ќе ги детектира обидите на нелегитимен пристап на составот и другите многубројни слични малициозни активности. Исто така, со комбинирање на наведените алатки автоматски се постигнува и задоволително ниво на заштита на составот.

Инсталација на сигурносни заштити. Слично како и на ниво на услугата, редовното инсталирање на сигурносни мерки, игра важна улога кај одржувањето на компјутерите на клиентите. Користењето на алатки кои ги автоматизираат постапките за инсталација на сигурносни алатки е се популарно и на секого се препорува нивно користење, посебно кај поголемите состави со голем број на компјутери на клиенти и персонални компјутери.

Сигурност на електронската пошта на клиентите. Со оглед на се понапредните функционалности кои доаѓаат од клиентите за прегледување на електронската пошта, се зголеми и бројот на можности кои напаѓачите можат да ги искористат за спроведување на неовластени активности. Со цел подигање на сигурноста на клиентите за прегледување на пораките на електронската пошта се препорачува оневозможување на прикажувањето на пораката во html формат, извршавање на скриптни јазици како што се vbs, javascript и сл., блокирање на потенцијално малициозните привезоци (*Attachment),* користење на алатки за детекција на spam пораки и сл. *Со*

оневозможувањето на html прикажување ќе се спречат повеќето phishing напади кои користат маскирање на url адресата.

Сигурност на web прегледувачите. Слично како и кај клиентите за прегледување на пораките на електронската пошта, воведување на напредните функционалности и кај web прегледувачите носат нови сигурносни пропусти кои неовластените корисници можат да ги искористат за спроведување на малициозни активности. Со цел на зголемување на нивото на сигурност на персоналните компјутери и превенција на *phishing* нападите се препоручуваат следните постапки:

- оневозможување на pop-up функционалностите;
- оневозможување на подршка за java апликации;
- оневозможување на activex подршка;
- забрана на автоматско извршување на сите датотеки земени од интернет;
- минимална подршка за мултимедијални формати;
- редовна инсталација на сигурносни алатки;
- користење на алтернативни web прегледувачи (opera, google, mozzila и сл.).

Доколку некои од наведените постапки можеби се престроги за индивидуални корисници, во работните организации тие би требало да бидат стандард на кој сите корисници треба да се придржуваат.[49]

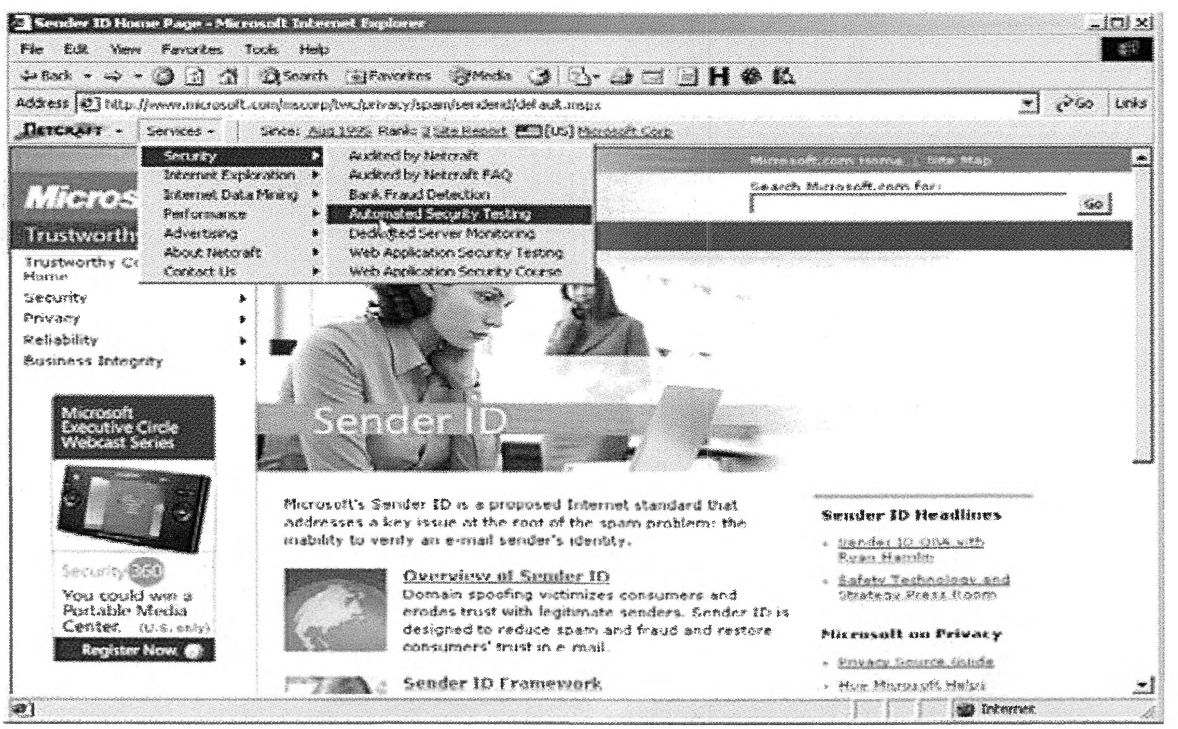
Со оглед на исклучително големиот број на сигурносни проблеми кои во последно време се појавија во (ie) web прегледувачите, се поголем број на корисници преоѓаат на алтернативни решенија како што се mozzila firefox, opera и сл. Анализите покажуваат дека (ie) web прегледувачот моментално е најсофистициран web прегледувач на интернет, иако повеќето корисници користат само 5% од неговата функционалност. Проблемот дополнително е нагласен со фактот дека компонентите на (ie) web прегледувачите се интегрирани во самиот операциски состав, што значи дека искористувањето на

[49] *Магистерски труд под наслов „Видови и облици на злоупотреба на Информатичката технологија" одбранет на 21.10.2009 година на Филозофскиот Факултет Св.„Кирил и Методиј" Скопје – Институт за одбранбени и мировни студии..*

сигурносните пропусти автоматски можат да овозможат потполно превземање на контролата над составот.

Во смисол на заштита од *phishing* напади стануваат се популарни и специјалните додатоци за web прегледувачи кои вклучуваат специјални сигурносни контроли наменети за детекција и спречување на *phishing* напади. Во повеќето имплементации на овие алатки се проверува дали одредена адреса е позната како извор на *phishing* напади. Еден од таквите алатки е netcraft toolbar кој може да се земе од следната адреса http://toolbar.netcraft.com/install. Алатката после успешната инсталација се интегрира во web прегледувачот, а потоа е можно да се користитат неговите функции. [50]

Тоа е прикажано на следната слика.



Вградениот додаток на корисникот му овозможува едноставно и брзо доаѓање до бројни информации за web страниците кои ги посетува, врз основа на што е можно поквалитетно да се процени нивниот интегритет и легитимност.

[50] *Подетални информации за начинот на работа на netcraft toolbar додатокот можно е да се пронајде на web страниците на производувачот (http://news.netcraft.com/).*

Внимателност на корисниците. Во повеќето случаи корисниците со својата внимателност и промислени постапки можат да ја намалат можноста да станат жртва на *phishing* напади. Еве некои препораки како да се препознае *phishing* нападот или некоја друга слична малициозна активност:

- На сите службени известувања кои корисникот преку електронска пошта го известуваат за чуствителни прашања како што се затворање на сметката, потреба од промена на кориснички податоци и сл., се препорачува да се реагира преку телефон или усмено. Никако да не се одговара на примената порака или да се користат адресите наведени во содржината на пораката;

- Сите службени пораки од финансиските институции би требало да бидат дигитално потпишани. До колку тоа не е направено, се препорачуваат дополнителни мерки на претпазливост;

- Строго да се избегнуваа презентација на доверливи финансиски информации преку пораки во електронската пошта. Smtp протоколот податоците преку мрежата ги праќа во чист текстуален облик што го прави ранлив на нападите со следење на мрежниот промет (англ. *Sniffing);*

- Доколку доверливите информации се внесуваат преку web пристап, се препоручува посебна претпазливост и дополнителни проверки со кои ќе се утврдити легитимноста и интегритетот на тој што ја нуди услугата. Потребно е да се провери дали се користи криптирана комуникација (https://ознака во полето *address* bar или во долниот десен агол на web прегледувачот);

- Детално да се анализира ssl сертификатот понуден од страна на давателот на услугата. Да се провери дали сертификатот е важечки и дали е издаден од организацијата. Информациите за сертфикатот можат да се добијат во било кој момент со двојно кликање на глушецот на иконата во облик на катанец во долниот дел на прозорецот;

- Доколку на web страниците на организацијата се забележат „чудни" промени во однос на претходно познатиот изглед, се препоручува дополнителна претпазливост. *Phiseri* многу често при лажирање на страницата прават ситни грешки, со кои лажираните страни можат да се разликуваат од оригиналните.

Детекциски контроли

Многу важан аспект на заштита од *phishing* нападите е нивната навремена детекција, врз основа на што е можно да се превземат соодветни сигурносни мерки кои ќе ги минимизираат последиците од нападите. По детектираниот напад организациите можат на своите корисници да им пратат известување кое ќе ги предупреди на потенцијалната опасност, а можни се и многу построги мерки како што е привремено оневозможување на услугите за сите корисници на составот.

Регистрација на домен со слично име. Со цел на детекција на *phishing* напад финансиските институции би требало редовно да ги следат регистрациите на domen чие име е слично со имињата на domen на организацијата. Во рамките на спроведување на *phishing* нападите, напаѓачите многу често регистрираат имиња на domen кои се слични со имињата на domen на организацијата која сака да се искористи за *phishing* напад. На пример доколку web страницата на организацијата се наоѓа на адресата http://www.gradskabanka.com, пожелно е да се следи регистрацијата на сите домени чие име во одредена мерка е слично на ова. На пример додавање на цртичка: gradska-banka.com; користење на domen: други држави: gradskabanka.mk; исфрлање на знакови: gradska-bank.com; слични имиња: grad-banka.com и.т.н., иако секогаш постои можност дека се работи за легитимен домен, ваквите регистрации на домени секако е пожелно да се имаат под контрола.

На сличен начин потребно е да се води сметка и за истекот на регистрираните домени како навремено би се продолжила нивната исправност. Денес на интернет постојат организации кои водат сметка за истекот на регистрациите на домените и ги нудат на другите корисници кои се заинтересирани за нивно купување. Организациите кои имаат регистрирано неколку различни домени посебно треба да водат сметка за овој проблем, бидејќи со невнимание некој од тие имиња може да се заборави.

Користење на анти спам сервисот и алатки

Постојат комерцијални алатки сервиси кои овозможуваат препознавање на пораката од електронската пошта кои во себе садржат карактеристики на *phishing* напад. Со користењето на вакви алатки можно е да се препознаат обидите за напад и да се пријави проблемот на одговорните лица на организацијата за која нападот е поврзан. Врз основа на детектираните пораки исто така е можно да се креираат соодветни потписи кои ќе се дистрибуираат на останатите производувачи на анти спам алатки со цел да се детектираат нови обиди за напад.

Пријави од страна на корисниците

Детекцијата на *phishing* нападите може да се направи попродуктивна доколку на корисниците им се овозможи едноставен и брз механизам за пријава на воочените инциденти. Во основа на пораката во електронската пошта за која корисникот мисли дека е поврзана со спроведување на *phishing* напад, можно е да се известат одговорните лица доколку за тоа постои соодветен механизам. Во овој случај одговорноста е на страна на банките и останатите слични институции, корисниците да ги известат за можностите за пријава на напади и начини на кои тоа може да се спроведе.

❖

Phishing нападите се нови закани за корисниците на интернет. Со комбинирање на техники на социјален инженеринг и лажирање на web страници и пораки на електронската пошта, неовластените корисници се обидуваат да дојдат до доверливи кориснички информации, банкарски сметки кои ќе им овозможат остварување на финансиска корист. Како што е детално објаснето во документот, техниките кои неовластените корисници ги користат во оваа цел многу се сложени што резултира со многу голем број на жртви на *phishing* напади.

Фактот дека денес секој корисник на мобилен телефон, компјутер, преносен компјутер, платежна картичка, може да биде потенцијална жртва, особено дека овој вид на криминал не познава граници и широко е распростанет.

Откако криминалците ќе дојдат до доверливи информации од безбедносен карактер, истите можат да ги продаваат на други влади, на приватни компании, на кој начин може да предизвика сериозно нарушување на безбедноста.

ПРИМЕР: Во 2012 година за време на претседателските избори во Франција, кабинетот на претседателот бил заразен со малициозен софтвер, меѓу компромитираните компјутери бил и на Генералниот Секретар на Саркози, Ксавиер Муска. Нападот е извршен преку Социјалната мрежа „Facebook" и ширел малициозен софтвер. Напаѓачите споделиле линк од заразена web страна која страна била фишинг страна на оригиналната страна на Elysee's, на која пристапиле голем број на лица и на тој начин превземале голем број на кориснички имиња и нивните ингеренции пристапувајќи на нивните компјутери без тие да бидат свесни. Сите компјутери во рамките на претседателската мрежа, вклучувајќи ги и оние на неговите најблиски соработници биле заразени.

Напаѓачите со фишинг напад не само што успеале да стигнат до срцето на Француската политичка моќ, туку тие ја имале командата на сите компјутери кои биле во претседателската мрежа, биле во можност да пребаруваат во компјутерите и на тој начин да дојдат до информации од висок безбедносен карактер, државни тајни и сл.[51]

Гореизнесеното јасно ја објаснува заканата и сериозноста на Phishing нападите како еден од облиците на високотехнолошкиот криминал врз националната безбедност на современите држави.

[51] *http://resources.infosecinstitute.com/phishing-dangerous-cyber-threat/ (16.12.2016г.).*

1.3.1-в ФАРМИНГ(Pharming)

Pharming е облик на оддалечен напад кој е насочен кон ранливата web страница и истиот се пренасочува кон злонамерно обликованата web страница. Овој напад може да се изведе со измена на датотеката со информации на нападнатиот компјутер или со искористување на сигурносните недостатоци dns (domain name system). Задачата на dns е поврзување на имиња со стварни адреси на интернет, а за компромитираниот dns се кажува дека е „затруен". [52]

Pharming е измамничка пракса во која злонамерен код кој е инсталиран на персонален компјутер или сервер, кој погрешно ги упатува корисниците да лажни веб сајтови без нивно знаење или согласност. Хакерите се обидуваат да го сокријат вистинскиот идентитет, преку користење на лажни адреси или лажно се претставуваат. Pharming е наречен "фишинг без мамец."[53]

Името на овој напад настанал од игра на зборови од англиската фраза *farm* што значи фарма, и phishing (password fishing), израз кој означува вид на напад од собрани напади на социјален инжинеринг, а целта му е стекнување на кориснички веродостојни шифри и кориснички имиња. Два вида на напад, pharming i phishing, се користат за кражба на идентитет и банковни web страници, банкарски сметки, пасворди и лозинки и др. Сложената техника на pharming нападот неможе да ја спречи вообичаен антивирус, туку бара примена на посебни анти- pharming мерки.

Односно Pharming е назив за техника која криминалците ја користат за кражба на идентитет и изведување на измами, а се темели на искористување на ранливоста во постапките за лоцирање и поврзување на корисникот на различни услуги на интернет. Phishing и pharming нападот за цел имаат наоѓање корисник кој посетува злонамерно обликувана web страна, а се разликува во користените техники. Phishing нападот користи излажани

---

[52] *Магистерски труд под наслов „Видови и облици на злоупотреба на Информатичката технологија" одбранет на 21.10.2009 година на Филозофскиот Факултет Св.„Кирил и Методиј" Скопје – Институт за одбранбени и мировни студии.*

[53] *Кенет К.Лаудон, Џејн П.Лаудон, Менаџмент информациски системи : Управување со дигитална компанија, Скопје : Арс Ламина, 2010 стр.300.*

корисници, додека pharming нападот се темели на манипулирање на различни компоненти за компјутери на интернет.

Pharming нападите злоупотребуваат механизми на поврзување на повеќе услуги, кој корисниците секојдневно ги користат како стварни услуги. За разбирање на pharming нападот потребно е познавање на тие механизми. Па така, Dns составот преставува еден од основните механизми кои овозможуваат сестрано користење на интернет. Може да се каже дека овој состав делува слично како телефонски именик, поврзува имиња на мрежни уреди (англ.hostname), на пр. www.primer.mk, со ip (eng. Internet protocol) адреса на пр. 208.77.188.166.[54]

Повеќе протоколи, кои на компјутерите им овозможува комуникација по пат на интернет, за разликување на достапни мрежни уреди се потпира на IP адреса. Овие адреси се многу ефикасни за комуникација помеѓу повеќе уреди, но луѓето даваат предност на лесно помливите псевдоними.

Во почетоците на интернет, и пред неговата брза популарност, секој компјутер имал своја ip адреса придружена со псевдоним.

Опишаниот начин на пристапување на компјутер добро функционоира во внатрешноста на малите мрежи, но поседува значајни недостатоци поврзани со одржувањето. Dns составот е осмислен со цел одстранување на споменатите недостатоци.

Основата на dns составот е хиерархиска структура на корисникот. Преку корисниците на повисоко ниво, можат да пристапат корисниците на пониско ниво кои даваат детални информации. Ова може да се илустрира со пирамида каде податоците се движат од повисок корисник, преку TLD (Top level domain) корисник се до авторитетни корисници на доменот (англ. Authoritative domain server - ad).

Со таква структура на корисниците им се овозможува пристап до услугите било каде во светот, со истовремено локално управување на компјутерите. Поради тоа пред пристапот на одделни услуги, потребно е да се пристапи на dns корисник кој содржи податоци за нивната ip адреса, при што самото пристапување на овој корисник се прави во повеќе чекори и со помош

[54] http://us.norton.com/cybercrime-pharming (04.03.2016).

на различни други корисници. (На пример ако корисникот сака да посети страна на одредена банка, чија ip адреса е на dns корисник кој е под контрола на банката, потребно е прво да се пристапи на тор корисник).

Иако е можно спроведување на потполно dns пребарување од страна на секој компјутер присутен на интернет, со секое посетување на некоја страница или користење на услуга, постојат методи кои со постапка на преведување на ip адреса се убрзува, и истовремено се намалуваат потрошените мрежни ресурси.

Во големи организации, како што се корпорации или сите корисници кои на интернет пристапуваат преку ист давател на услуга (англ. Internet Service Provider - ISP), можно е да се пренасочат dns прашања према dns корисниците на таа организација, наместо према високите корисници. Такви корисници dns пребарувањето го поминуваат за сите придружни клиенти, а можно е и претходно побараните имиња на доменот во прирачната меморија.

Зависно од постапката на корпоративни или ISP, DNS корисници, наместо спроведена потполна DNS претрага можно е информацијата за доменот да се побара од поголем или подобро позициониран корисник. Во случај да таков корисник веќе постои во бараните податоци во сопствената меморија, времето за пребарување значително се намалува.

Ако бараната информација не е пронајдена, се праќа барање до повисокиот корисник и се спроведува потполно dns пребарување. Резултатите од оваа потрага можно е да се хранат, во траење кое е одредено од TTL (англ. Time to live) параметри од страна на сопственикот на доменот.

Dns корисникот кој спроведува привремено собирање податоци собрани од други Dns корисници се нарекува прирачен Dns корисник (англ. Dns cache server). Корисници кои незнаат многу адреси, до саканата услуга доаѓаат со впишување на одредени клучни зборови на некој од пребарувачите. Овие методи корисниците поради брзина и практичност ги употребуваат дури и кога им е позната адресата. Резултатите од пребарувањето се рангираат према различни критериуми, како што се бројот на појавување на клучни зборови, зачестено посетување и др. Притоа составот за преведување на IP адреса потребно е редовно да се одржува и подесува, така да нивниот интегритет и

сигурност во голема мера зависи од администраторот. Поради сложеноста на овие состави на злонамерните корисници кои имаат пристап им овозможува спроведување на измени кои тешко, или речиси е невозможно да се откријат.

При напад на Dns корисник, на напаѓачите обично им се интересни следниве категории:

- Dns корисник во внатрешноста на мрежата – составен администратор може лесно и неприметно да измени или додаде записи во прирачната меморија која влијае само на Dns пребарувањето на корисникот во внатрешноста на мрежата;
- ISP, Dns корисник – со краткотрајната измена на Dns внесувањето резултира со голем број „жртви";
- корпоративен Dns корисник – измената на dns внесувањето на ова ниво на напаѓачот, осигурува пренасочување на својот промет кон алтернативната ip адреса со повисок ризик на откривање;
- глобален Dns корисник – доколку напаѓачот на некој начин успее да ја измени постапката на Dns пребарувањето на глобално ниво големи се шансите брзо да се открие измамата.

За изведување pharming напад злонамерните корисници можат да користат различни услуги кои им олеснуваат пронаоѓање на domein. Така напаѓачот може кај фирмата која го одржува пребарувачот да купи така наречена спонзорирана врска (англ. Sponsored link) и така да се осигура дека неговиот домејн ќе се најде на врвот на пребарувањето со одредени клучни зборови. Притоа успешната манипулација на резултати на web пребарувањето е појдовна точка за изведување на pharming напад.

❖

Сериозноста и тежината на овој вид на напад е голема. Овие напади се сконцентрирани на специфични индустрии, како што се финансиските и безбедосните. Опасноста од овој вид на напад е универзален проблем, а тоа е мотив плус да се спроведат мерки за контрола на ризикот, да се минимизира

потенцијалното оштетување. Бидејќи pharming нападот содржи и технички и социјални елементи, заштитата од истиот треба да биде технички многу добра.

Со се поголемата популарност на интернет банкарството и електронската наплата на сметки, подразбира дека има се поголема опасност од кражба на доверливи информации, а тоа може да предизвика колапс на финансискиот систем.

Последиците може да придонесат економски кризи како и да предизвикаат нарушување на безбедноста.

Исто така, доколку преку pharming напад се дојде до здраствени информации, истите може да бидат променети, односно да се промени одредена терапија или крвна слика на пример на Претседател на држава или Премиер, значи извршен атентат врз таа личност, со што би се предизвикале немири во таа држава, а со тоа директно се влијае на националната безбедност на државата.

1.1.3-г ЗАШТИТА ОД ФАРМИНГ (PHARMING) НАПАД

Од Pharming напад е многу тешко да се заштитиме споредено со традиционален phishing напад поради нивната дистрибуирана природа и поради користењето ресурси кои не се под контрола на нападната организација. Додатна потешкотија е во тоа што нападите главно се изведуваат на многу ниско ниво на Dns, па постојат релативно многу малку методи кои можат да откријат злонамерни измени.

Многу од техниките за заштита од phishing напад може да се применат и на pharming напад.

Од страна на клиентите овие методи опфаќаат:

- користење вообичаени алатки за заштита на сигурноста на компјутерот;
- користење прикладни, помалку софистицирани, комуникациски поставки;
- користење алатка за надзор на разни кориснички апликации;
- заклучување на web пребарувач (англ. *browser lock-down*) и
- дигитално потпишување и проверка на валидноста на електронските писма.

Од страната на пребарувачот се препорачува:

- овозмоување и користење технологија за проверка на валидноста;
- развој на сигурни web апликации кои не содржат лесно искористување на сигурносните недостатоци;
- одржување едноставни и разбирливи состави на името на доменот.

Методи кои отежнуваат phishing i pharming напади на разни организации се:

- автоматска проверка на пребарувачот на електронската пошта на примени пораки;

- дигитално потпишување на електронските писма;
- надзор на корпоративниот domen и воочување регистрација на слични domen-и;
- заштита на пристапувачот (*gateway*).

Поради големата опасност од злонамерни измени внатре во Dns составот од страна на вработени, се советува:

- пристап до конфигурациските дадотеки и прирачната меморија да се овозможи само на овластени вработени лица при измена на Dns составот;
- сите промени во Dns составот да се бележат во дневен запис;
- надзор на записите за измени во Dns составот треба да ги води тимот кој е одвојен од останатите вработени;
- редовен надзор и компаративна анализа на секундартните прирачни Dns пребарувачи.

Заштита од pharming напад можно е со имплементирање на посебни датотеки на web пребарувачите кои вршат проверка на веродостојноста на доменот. Одделни алатки прикажуваат IP адреса на посетен домен, потполни податоци за нејзиното име, така што корисникот може да ја воочи изменетата web страна.

Некој од расположливи додатоци за откривање на pharming напад, се преку правење на сопствена листа на IP адреси и придружни имиња на домени. Кај поновите посети на доменот се проверува дали IP адресата е еднаква со последно забележаната посета. Доколку се воочи разлика на корисникот му се испраќа сигнал. Проблеми може да се јават ако сосптвеникот на доменот ја промени IP адреста на доменот на кој му е доделен поголем број на IP адреса.

На располагање се и алатки кои овозможуваат одредување на земјата каде се наоѓа доменот врз темелите на IP адесата, со што се олеснува откривањето на pharming страница, на пример кај посета на страница која се наоѓа во Русија, а се преставува како Австралиска банка.

Додатни начини на заштита се сертификати на пребарувачите преку кои се докажува идентитетот. Поголем број web пребарувачи овозможуваат читање и проверка на споменатите сертификати. За имплементација на таков состав за заштита на организацијата во чија сопственост е доменот, треба да се побара и да се добие сертификат од овластено тело за доделување сертификати (англ. Certificate authority).

Како и кај сите интернет услуги, така и кај Dns составот задолжителни се подесувања на сите поставки и правовремени надградби. Покрај тоа се советува користење на актуелни програмски пакети кои во повеќе случаи содржат најпотполна заштита од нови напади.

Dns пребарувачот е ранлив доколку е подесен да одговара на секакви прашања. Напаѓачот може да прати прашање за адреса од доменот кој е придружен со dns пребарувач под негова контрола и така да ги направи некои од опишаните напади.

Dns пребарувачот на оние организации кои го користат, односно на администраторите кои го одржуваат, им дава голем број конфигурациски можности. Поради тоа е потребно да се посвети посебна внимателност при нивно сигурно поставување а во согласност со следниве препораки:

- оневозможување на секакви прашања, доколку е тоа можно;
- ограничување на адреси на кои пребарувачот ќе праќа одговори на прашања;
- кога на пребарувачот му се ограничени ресурсите тој делува со пасивен начин на работа, не праќа односно Dns прашања на други пребарувачи.

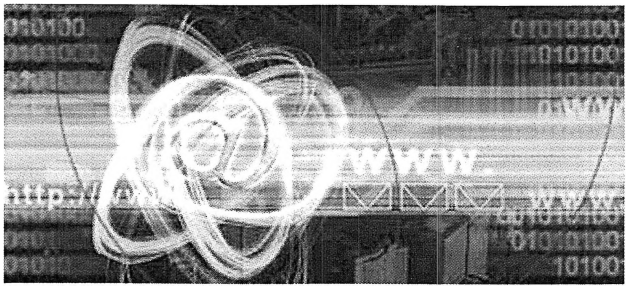
❖

Нападите кои се темелат врз злоупотреба на постапките на преведување на имиња со цел остварување на финансиска корист или кражба на идентитет во иднина веројатно ќе станат се почести. Недостатокот на разбирање на последните постапки кои се прават со поврзување на ip адреси со имиња на компјутери или услуги од страна на корисникот, но и на бројни

организации, често резултира со неоткриени напади кои се темелени на измени на dns составот.

Во борба против pharming нападот е разбирањето на глобалните dns услуги и можните начини на нивна злоупотреба. Со такви знаења организациите може да имплементираат подобри методи на надзор и рано воочување на опасноста.

1.1.3- д СПАМ (Spam)



Спам, е непосакувана електронска пошта. Тоа е проблем кој веќе повеќе години создава загриженост кај корисниците на интернет. Без разлика дали се работи за крајни корисници, големи компании или провајдери на интернет, спамот освен што задава проблеми на корисниците тој влијае и на финансиските загуби. И покрај големите обиди за спречување на спамот со различни информатички алатки, законски регулации, несаканата електронска пошта претставува и понатаму нерешен проблем во информациските системи. Слободно може да се каже дека голем број на корисници се навикнати на спам пораките и го прифаќаат како нешто неизбежно.

Освен вознемирувачкиот карактер кој го има спамот кај крајните корисници, проблемите кои ги создава спамот имаат поширока важност. Имено, тој може да влијае на нарушување на угледот и интегритетот на компаниите или поединците, искористувајќи го времето на туѓиот компјутер за извршување на дејствието, просторот на хард дискот, мрежните можности итн. Време и енергија кој секој корисник ги троши за бришење и пронаоѓање на спам пораката исто така влијае на нивната продуктивност.

Еве пример како изгледа една СПАМ порака - *Изглед на спам порака*

РЕГИСТРАЦИЈА ЧЕКОР ❷ ОД 3

Потребна е активација на Вашиот профил! На вашата електронска пошта vase_eposta@yahoo.com е испратена порака со линк за активација.

Доколку сè уште не сте ја добиле оваа порака, причекајте извесно време и проверете повторно во Inbox, Spam и Junk папките, или кликнете на следниов линк:

ИСПРАТИ ПОВТОРНО Е-ПОРАКА СО ЛИНК ЗА АКТИВАЦИЈА

Статистичките податоци покажуваат дека дневно во интернет системот кружат околу 30 милијарди пораки на електронска пошта. Од нив на спам пораки отпаѓа околу 40-60%, што значи околу 15–18 милијарди пораки. Доколку тој број се помножи со времето кое е потребно корисникот да препознае спам порака и да ја избрише (околу 4-5 секунди) излегува дека за тоа е потребно вкупно околу година дена. Според последните проценки направени во САД, трошоците за спам заштита се движат околу 250 милиони долара за обичните корисници и до девет милијарди долари за компании. Иако ублажување на проблемот може делумно да се реши со anti-spam заштита, која варира од производ до производ сепак сеуште е присутна борбата за искоренување на појавата.

Интересите на **„спам индустријата“** се очигледно големи. И покрај превземените законски и технички мерки, бројот на спам пораките не се намалува. Во последните неколку години спам индустријата е напредната и проширена на целиот свет. Таа е најразвиена во САД, но и во останатите земји како што се Јужна Кореја, Кина и Бразил.

Спам индустријата условно може да се подели на три меѓусебно поврзани ангажмани. **Првиот дел** се однесува на собирање на адреси, преку секојдневно пребарување на интернетот со цел добивање на нови адреси кои подоцна би се искористиле за испраќање на спам пораки. За оваа работа се користат доста софистицирани програми кои со напредни техники вршат пребарување на различни подрачја на интернет на кои се добиваат mail адресите. Овие адреси покасно се продаваат на заинтересирани личности, најчесто на самите спамери кои ги користат за масовно испраќање на пораки.

Следен важен елемент се самите спамери, односно личности кои вршат испраќање на спам пораки. Во овој поглед спам индустријата значајно е напредната, за да денес постојат спам организации, па дури и интернет услуга за испраќање на спам порака. За разлика од легалните интернет провајдери кои водат сметка да од нивната адреса не се испраќа спам порака, спам организациите се регистрираат како такви и преку нив се овозможува незабележително да се ловат електронските пошти. За испраќање на порака се користи најчесто mass mailing program каде една иста порака се испраќа на

повеќе различни места, при што се користи техника на лажирање на порака со што е отежнато пронаоѓањето на изворот на испраќање.

Последен елемент се луѓето кои го користат ова со цел да прибават финансиска корист. Карактерот и содржината на спамот тргнува од интересот на спамерот, но најчесто се работи за порака од рекламен карактер преку која се нуди одредени производи или услуги.

1.1.3-ѓ ВИДОВИ НА СПАМ

Зависно од видот на пораката, начинот на кој е испратена и типот, спам пораката може да се подели на неколку категории. Наједноставната категорија се спам пораките од комерцијален тип (Unsolicited commercial e-mail или uce). Следат некои типични категории на спам пораките, заедно со нивните основни карактеристики.

- **E-mail spam**

- Несакана комерцијална електронска пошта (Unsolicited commercial e-mail или uce), подразбира порака од електронска пошта која рекламира производи или услуги, а да самиот корисник не барал да добие таква пошта. Оваков тип на порака уште се вика и junk e-mail;
- Несакана bulk електронска пошта (unsolicited bulk e-mail или ube) се однесува на порака од електронска пошта која се од одредени интереси се испраќа на повеќе, па дури и до еден милион корисници. Најчест карактер на овој вид порака е политичко лобирање и вознемирување на корисниците;
- Make money или mmf пораки, најчесто во вид на последователни писма или пирамидални маркетинзи, се тип на спам пораки кои на корисниците им нудат брза и лесна заработувачка доколку на одредена адреса испратат одредена сума на пари. Многу од пораките имаат опција самата порака да се испрати и на други корисници од страна на веќе злоупотребениот корисник. Иако ова е многу примитивно и воочливо, сепак овој тип на пораки сеуште измамува поголем број на корисници, посебно оние кои се помалку искусни;
- Напад на репутација (Reputation attacks) се лажирани пораки по електронска пошта испратени во име на поединец или организација. Основна улога на таква порака е загрозување на репутацијата или кредибилитетот на субјектите во чие се име испраќа пораката.

- **Usenet spam**

- Excessive multi-posting (emp), се однесува на ситуација кога иста news порака индивидуално се испраќа на поголем број на news група. Секоја копија на вести има различни идентификационен број (message-id) и тој се појавува во различни news групи. На тој начин секоја порака се испраќа на сите компјутери поврзани со usenet провајдерот.
- Excessive cross-posting (ecp) spam, се однесува на вести кои се испратени на голем број на групи;
- Spew, се појавува кога неправилно сетирани програми испраќаат една иста порака на голем број на нови групи. Поставување на вести со различна тема на места каде несоодвестува со другите вести, (на пример извадок за спорт не одговара да биде поставен во извадок во кој се вестите за компјутери, автомобили итн.);
- Бинарни пораки, се оние кои содржат бинарно кодирани датотеки, како што се слики, музика, видео итн.;

1.1.3-е ТЕХНИКА ЗА ИСПРАЌАЊЕ НА СПАМ

За испраќање на спам порака спамери најчесто користат специјапни алатки, кои најчесто сами ги развиваат. Но и на оние постоечки кои ги прилагодуваат за испраќање на спам порака. Тоа се програми за менување на заглавје на електронска пошта, со додавање на елементи за заобиколување на anti spam филтерот, прикривање на изворот на испраќачот, автоматизирано пронаоѓање и чистење на спам пораката и сл. Тие алатки постојано се развиваат во согласност со новите потреби и побарувања на спамерите.

Бидејќи голем број интернет провајдери не дозволуваат испраќање на спам пораки преку нивни mail услуги, спамерите морале да пронајдат нови механизми за испраќање на порака. Најпознати се три методи кои на спамерите им овозможуваат да испратат порака по електронска пошта, а притоа во голема мера останат анонимни. Се работи за следниве:

- **Open relay** опслужувачи со незаштитени mx (mail exchanger), односно опслужувачи кои овозможуваат испраќање порака на електронска пошта било каде на интернет. Овакви mail опслужувачи се неприфатливи за сигурноста на корисниците, бидејќи на спамерите им се овозможува многу едноставно испраќање на порака и прикривање на испраќачот. Секој mail опслужувач мора да има авторизиран пристап за испраќање на порака кон корисник, што е најчесто ограничено со внатрешните вмрежени компјутери во организацијата. Доколку е дозволено испраќање на порака со непозната адреса (случај со модемски влез) се користат сервиси за smtp автентикација како што е smtp auth.
- **Web site mail-form hijacking.** За испраќање на порака спамерите многу често искористуваат несигурни скрипти кои се поставени на незаштитени web пребарувачи. Со поставување на специјални web форми, спамерите многу едноставно ја автоматизираат постапката на испраќање на порака при што тие целокупно остануваат анонимни;
- **Open proxy.** Со оглед на улогата и начинот на работата незаштитените proxy даватели на услуги тие се идеални за спам порака. Со користење на отворени прокси даватели на услуги спамерите можат многу лесно и едноставно да остварат конекција

према било кој компјутер поврзан на интернет, а да притоа како извор на испраќач се види само адресата на провајдерот. Како отворени прокси опслужувачи можат да се искористат погрешно сетирани програмски пакети како што се squid и со него слични, а почести се и примери каде неовластени корисници користат туѓи компјутери инсталирајќи прокси сервери кои покасно се користат за испраќање на спам пораки. Самите корисници на компјутерите многу често не се ни свесни дека дека нивната „машина" се користи како нелагална, што на спамерите им овозможува континуирано испраќање на порака за подолг временски период. *Загрозените компјутери кои се користат за испраќање на спам се нарекуваат зомби компјутери*.

Освен претходно опишаните техники за масовно испраќање на спам пораки и прикривање на нивните извори, спам пораката редовно содржи бројни елементи со кои врши заобиколување на anti-spam филтерите. Некои од популарните техники кои спамерите ги користат за заобиколувае на anti-spam филтерите, се следниве:

- Намерно погрешно напишана содржина. Бидејќи anti-spam филтрите се состојат од едноставни пребарувачки системи на клучни зборови во електронската пошта, на овој начин тие едноставно се излажани преку проверката на anti-spam пребарувачот;
- Поставување на html порака внатре (vi>gra). Кога клиентот на електронска пошта ја интерпретира текст пораката, тој ја интерпретира и содржината на html ознаката, така да пораката би се прикажала на правилен начин. Во тој случај на корисник би се покажала пораката во зелено пола и поради поставениот html ознака филтерот би бил заобиколен. Многу често во пораките се поставува и непостоечки html код кој клиентот би го прифатил и би бил прикажан како зелен текст, а филтерот би бил заобиколен;
- Додавање на специјално формиран текст на крај од пораката на електронска пошта со цел да се излаже анти-спам филтерот. Овој текст многу често се пријавува и прилагодува како порака за да биде невидлив;
- Користење на различен начин кодирана порака.

1.1.3-ж ТЕХНИКА ЗА СОБИРАЊЕ НА АДРЕСИ НА ЕЛЕКТРОНСКА ПОШТА

Едно од основните обележја на спам пораката е да се испраќа на голем број на корисници, односно адреси. На тој начин се зголемува веројатноста некој од корисниците да отвори спам порака и да ја изврши постапката која ја бара содржината на пораката. Еден од темелните чекори на спамерите е да се добијат повеќе адреси на електронски пошти на кои подоцна би биле испраќани спам пораките. Следат повеќе примери како спамерите доаѓаат до кориснички адреси:

- Со купување на готова листа на адреси од електронска пошта за неколку десетина долари. Цените на оваквата листа може да варира зависно од тоа дали адресите се проверени како постоечки или непостоечки;
- Со користење на таканаречени e-mail extractors програми кои вршат пребарување на интернет барајќи адреси на електронска пошта на web страниците, форумите, новинските групи и други интернет сервиси. Просечен програм од овој тип може да пронајде и до 15 000 адреси за еден час. За оневозможување на ваквите програми на различни web страни се применуваат специфични методи за прикажување на електронските адреси во различни формати при што самата програма не ја пронаоѓа како адреса за електронска пошта;
- Рачно пребарување на интернет и собирање на адреси за електронска пошта. Иако претставува спор процес во споредба со другите методи, се повеќе се применува со оглед на тоа дека голем број на страници користат техники на одбегнување на автоматско собирање на адреси;
- Користење на т.н. Newsgroup harvesters програми кои автоматски собираат адреси од newsgroups. Таков програм може да собере десетици илјади адреси за многу кратко време;
- Поставување на различни интернет услуги кои од корисникот побаруваат оставање на адреса за електронса пошта;
- Крадење на готова листа со адреси за електронска пошта од интернет провајдери;

- Користење на специјализирани програми кои користат brute-force и dictionary техника која овозможува погодување постоечки адреси на одредени domein-и. При генерирање на случајни адреси се користат вообичаени имиња, поими и знакови, при што можноста за добивање на валидни адреси е голем на одреден domein. За да се провери дали една адреса е валидна на самата неа се испраќа спам порака со цел да се утврди нејзината валидност. Оваквите напади се многу проблематични за системските администратори на mail серверите, бидејќи за мал временски период пристигнуваат голем број на невалидни и валидни адреси на самиот domein.

При испраќање на спам порака спамерите користат бројни техники на лажирање на електронската пошта за да го прикријат вистинскиот извор на испраќање. Освен од полето **from**, со кое се опишува испраќачот, најчесто се врши и лажирање на полето **recived** за да се прикрие вистинскиот тек на комуникација помеѓу изворниот и крајниот smtp опслужувач. **Recived** полето се додава од секој меил опслужувач на пат од испраќач до примачот на пораката, при што од нивната анализа може да се утврди од каде е испратена пораката (при тоа се мисли на ИП адреса на маил серверот или компјутер од кој е испратена пораката, а не на идентитетот на корисникот).

Затоа спамерите многу често во заглавјето на пораката додаваат лажирана **recived** информација така да корисникот го наведува на погрешен пат кога сака да го утврди изворот на пораката. Со иста цел за испраќање на пораката се користи и незаштитен open relay и open proxy давател на услуги кој во заглавјето на пораката го додава сопственикот на изворот на пораката, лажиран.

Од сето наведено може да се заклучи дека лажирањето на пораката на електронска пошта е еден од поважните сегменти во постапката на креирање и испраќање на спам пораката. Кога не би се применувале техниките на лажирање на заглавјето на пораката и прикривање на изворот на испраќачот, испраќачите на спам пораките би било многу лесно да се утврдат а нивните адреси би можеле да се постават на глобалната црна листа со која се оневозможува понатамошно испраќање на спам пораки.

Бидејќи сегашната специфичност на smtp протоколот не содржи сигурносна контрола која би попречила испраќање на лажирана порака, проблемот со спамот е дополнително отежнат. За попрецизни идентификации на изворот потребно е подетално да се разгледа структурата на заглавјето на електронската пошта и да се знае како да се анализира. Кога се зборува за анализа на спам порака најважно е правилно разбирање на **recived** заглавјето и исправно препознавање на елементите кои се намерно ставени во пораката за лажирање на корисникот.

Recived полето содржи важни информации за mail послужувачите преку кои пораката поминала, временски информации и сл., а тие се позначајни елементи во постапката на индетификација на изворот на пораката.

Подолу е даден пример за заглавје на спам порака каде е покажано значењето и смислата на посебните елементи на заглавјето на пораката. Содржината на пораката не е толку значајна во овој пример на разгледување.

```
Return-Path: <kevinwww@po.zzn.com>
From: kevinwww@po.zzn.com
Received: from h2.mail.home.com ([24.2.2.28]) by mail.rdc1.ab.home.com
          (InterMail v4.01.01.07 201-229-111-110) with ESMTP
          id
                    <19990728164203.WNNS19181.mail.rdc1.ab.home.com@h2.mail.
                    home.com>
          for <someuser@mail.ssdt1.sk.wave.home.com>;
          Wed, 28 Jul 1999 09:42:03 -0700
Received: from mx3-e.mail.home.com (mx3-e.mail.home.com [24.2.2.26])
       by h2.mail.home.com (8.9.3/8.9.0) with ESMTP id JAA29657
       for <someuser@home.com>; Wed, 28 Jul 1999 09:42:02 -0700 (PDT)
Received: from bftoemail10.bigfoot.com (bftoemail10.bigfoot.com
[208.156.39.200])
       by mx3-e.mail.home.com (8.9.1/8.9.1) with SMTP id JAA25058
       for <someuser@home.com>; Wed, 28 Jul 1999 09:42:02 -0700 (PDT)
Received: from relay.somedomain.com ([126.33.246.159])
          by bftoemail9.bigfoot.com (Bigfoot Toe Mail v1.0
          with message handle 990728 124133 6 bftoemail9 smtp;
          Wed, 28 Jul 1999 12:41:33 -0500
          for someuser@bigfoot.com
Received: from knusun.kangnung.ac.kr ([202.30.48.2])
       by relay.somedomain.com (8.9.3/8.9.0) with ESMTP id FAA294657
       for <someuser@home.com>; Wed, 28 Jul 1999 09:41:22 -0700 (PDT)
Received: from chem.kangnung.ac.kr (chem.kangnung.ac.kr [203.255.218.45]
        by knusun.kangnung.ac.kr (8.8.8H1/8.6.9) with SMTP id BAA29317;
        Thu, 29 Jul 1999 01:41:58 +0900 (KST)
Received: from chem.kangnung.ac.kr by chem.kangnung.ac.kr (SMI-8.6/SMI-SVR4)
        id BAA03348; Thu, 29 Jul 1999 01:40:04 +0900
        Date: Thu, 29 Jul 1999 01:40:04 +0900
Message-Id: <199907281640.BAA03348@chem.kangnung.ac.kr >
Received: from localhost [127.0.0.1]} by mx.aol.com (8.8.8H1/8.6.9) with
SMTP id BAA935176; Wed, 28 Jul 1999 23:55:32 +0900 (KST)
To: kevinwww@po.zzn.com
Subject: Findout About Anyone Fast (499651)
X-UID: 1510
```

Важно е да се каже дека заглавјата на пораката се ставени како пораката која поминува низ давателот на интернет. Тоа значи дека првата **recived** линија на врвот од заглавјето е последен опслужувач кој ја проследил пораката и така по ред. Оваквата структура на заглавјето на пораката

подразбира дека може да се измени со додатни **recived** линии вметнати од страна на спамерот, кои се наоѓаат на долниот дел на заглавјето.

Подолу е прикажано објаснување на посебни заглавја на дадената порака:

```
Return-Path: <kevinwww@po.zzn.com>
From: kevinwww@po.zzn.com
```

Овие линии се поставени од испраќачот на електронска пошта на основата на оној кој ја испраќа електронската пошта. Притоа со анализа на заглавјето ова поле може и да го нема бидејќи многу лесно може да се измени.

Следен дел од заглавјето ја означува патеката по која се движела пораката низ интернет опслужувачите додека ја достигнала крајната цел. Во овој случај се работи за компјутерска мрежа **home.com** домеин.

```
Received: from h2.mail.home.com ([24.2.2.28]) by mail.rdc1.ab.home.com

          (InterMail v4.01.01.07 201-229-111-110) with ESMTP
          id
<19990728164203.WNNS19181.mail.rdc1.ab.home.com@h2.mail.home.com>
          for <someuser@mail.ssdtl.sk.wave.home.com>;
          Wed, 28 Jul 1999 09:42:03 -0700 (PDT)
```

На примерот е даден детален опис на **recived** полето при што корисникот лесно може да изврши анализа на електронската пошта.

Првиот дел од записот означува име, односно ИП адреса на опслужувачот од кој е пораката примена.

```
from h2.mail.home.com ([24.2.2.28])
```

Потоа следи адреса на опслужувач кој ја примил подоцна пораката, заедно со натписот и mail опслужувачот (intermail v4.01.01.07 201-229-111-110) и ознака на испраќачки протокол (esmtp).

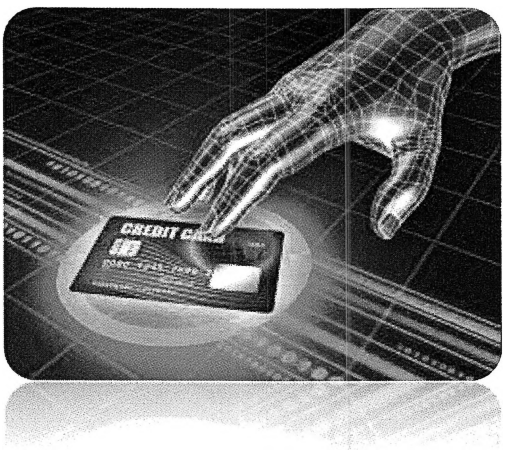
❖

Интернетот, можностите кои ги нуди тој, размената на пораки, се важни методи на комуникација и размена на деловни информации. Свесни дека придобивките од развојот на технологијата се огромни, овозможувајќи ни да комуницираме непречено, да разменуваме информации со секој кој ни е потребно, треба да постанеме свесни и дека сето ова преставува вистинска закана за нашата лична безбедност, продуктивноста, профитабилноста, како и за националната безбедност на секоја држава. Со самиот факт дека милијарди спам пораки се испраќаат секој ден, тоа ни кажува дека опасноста од овие пораки секојдневно прераснува во сериозна закана за националната безбедност.

Секоја пристапна точка во компјутерската мрежа преставува потенцијална закана за безбедноста на системот. Во некој случаеви спам пораката може да содржи скрипта со која се собираат сите информации кои ги поседувате во компјутерот, мрежата, или пак на серверот. Исто така спам пораките може да содржат и малициозен код, вградени макро вируси, кои одкако ќе се активираат на уредот или на мрежата, исто така ги превземаат сите информации, слики, документи кои ги поседувате.

Овој вид на спам пораки е особено сериозна закана за националната безбедност, поради тоа што ако се дојде до осетливи, доверливи информации од безбедносен карактер, класифицирани информации, може сериозно да се наруши националната безбедност, а последиците да бидат огромни.

1.1.4 ФИНАНСИСКИ КРАЖБИ И ЗЛОУПОТРЕБИ



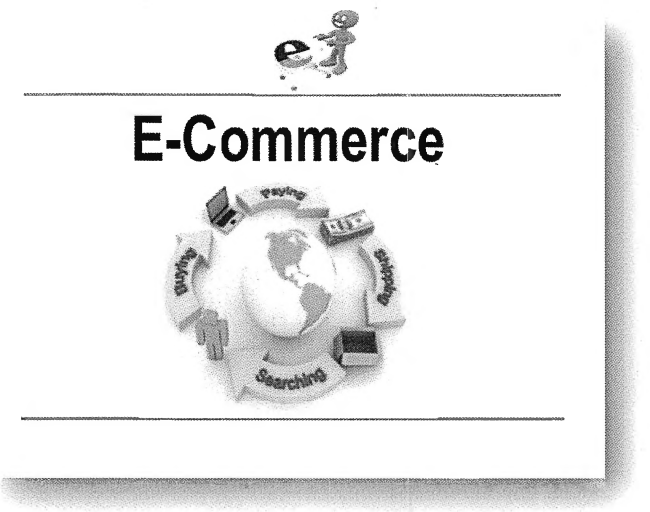
Финансиските кражби и злоупотреби се едни од најчестите компјутерски кривични дела, а се однесуваат на неовластено навлегување во системи на финансиски институции, како на пример системи на банки, процесинг центри кои опслужуваат банки и имаат огромни бази на финансиски податоци вклучувајќи и лични податоци на клиентите, пробивање на банкарски сметки, податоци од платежни картички, злоупотреба на платежни картички.

Злоупотребата на платежните картички е во подем.

Со кражба на податоци на сопствениците на платежни картички, нивните пин кодови, се прават големи злоупотреби со тоа што им се повлекуваат парични средства, се прават фалсификувани платежни картички со нивните податоци кои се злоупотребуваат во различни земји низ светот, како на АТМ (банкомат), така и на ПОС Терминали при што се вршат и нелегални трансакции во продажни места. Има појава на разни форуми на интернет, кои за одредена сума нудат на продажба целосни податоци од платежни картички (броеви од платежни картички, податоци од сопствениците на платежните картички, пин кодови како и CVV 2 кодот кој најчесто се употребува за вршење на трансакции на интернет).

Злоупотребата на платежните картички е едно од најчесто извршуваните кривични дела, и тоа во сите облици како злоупотреба на банкомати, злоупотреба на ПОС Терминали, но тоа во последно време е многу намалено,

а за разлика од тоа во поново време се почесто е злоупотреба при купување на интернет, односно e-commerce (интернет трговија).



Што се однесува до ***Интернет трговијата*** или „e-commerce" можеме да констатираме дека во последно време е во развој, односно настапува ерата на интернет трговијата која овозможува размена на производи било кога, било каде со брзина на светлоста.

Под терминот електронска трговија се подразбираат трансакции кои се спроведуваат преку интернет, и тоа исклучиво преку веб-базирани апликации за трговија (трансакциите преку електронска пошта се исклучени), и кои опфаќаат стоки и услуги како во материјална, така и во нематеријална форма.[55]

Интернет трговијата е начин да се доближи понудата на стоки и услуги на купувачите и истите да станат достапни без притоа воопшто да се напушти домот. За таа цел постојат ВЕБ сајтови кои преставуваат виртуелни продавници каде може да се купат стоките и услугите со плаќање преку виртуелни ПОС терминали со употреба на платежни картици. Оваа погодност

[55] *USAID, Анализа на состојбата со електронската трговија во Република Македонија, Скопје, Ноември, 2010 стр.12*

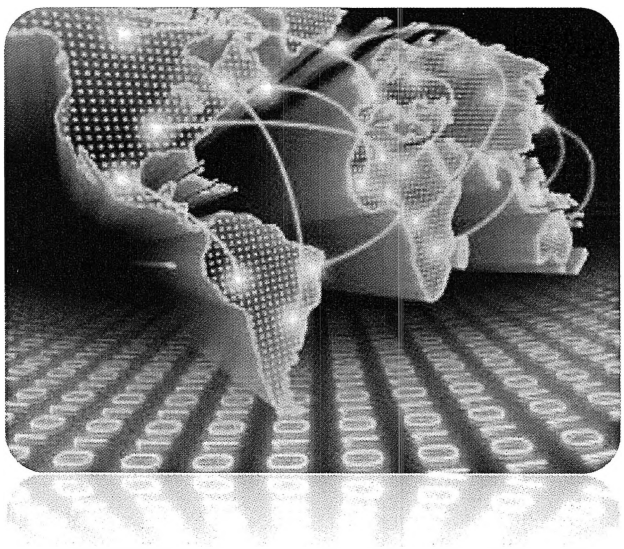
самата по себе дава големо поле на злоупотреби од страна на криминалците како прибирање и пресретнување на податоци од платежни картици со помош на лажни ВЕБ страни (fishing), како и злоупотреба на истите за купување на разни стоки и услуги повторно он лајн.

Олеснителна околност во интернет трговијата е намалениот ризик за откривање на криминалците, пред се затоа што немаат потреба да се појавуваат во продажни места, немаат потреба да поставуваат „скимер уреди" (уреди за кражба на податоци од платежни картички) на банкомати, немаат потреба да изготвуваат фалсификувани платежни картички и да вадат парични средства од банкомати. За извршување на нелегални трансакции на интернет на криминалците доволни им се податоци од платежните картици, и CVV 2 кодот кој се наоѓа на задната страна на платежната картица (во одредени случаеви не е потребен, тоа зависи од интернет страната), и секако пристап на интернет.

Најчесто при извршување на овие нелегални трансакции се купува техничка стока, скапи часовници, компјутерски производи, кои подоцна е полесно да бидат продадени, секако за помала вредност од вистинската, а со тоа криминалците се стекнуваат со противправна имотна корист, благодарение на податоците од фалсификувани платежни картички, кои тие нелегално ги прибавиле и ги поседуваат.

Исто така интернет трговијата со податоци од фалсификувани платежни картички се користи и за резервација на туристички аранжмани, купување на авио билети, потоа за наплаќање на разни видови на сметки, надополнување на мобилен кредит „e-voucher"и др.

Како една од најголемите финансиски кражби и злоупотреби кој исто така е во пораст е Интернет банкарството.



Интернет банкарството стана едно од најпознатите и најраширените електронски услуги. Исклучително удобен финансиски сервис кој нуди услуга 24 часа без дополнителни трошоци, и поради тоа голем број на банки ги нудат предностите од интернет банкарство на клиентите. Сепак, интернет банкарските измами се во пораст. Интернет банкарството треба да биде сигурно. Заштитата на личните податоци на корисникот е приоритетна. Интернет банкарските сајтови се многу примамливи за компјутерските криминалци, пред се затоа што им се профитабилни, може да наведат голема бројка на луѓе, а тоа значи голем број на украдени информации за банкарски сметки, платежни картички, лични податоци на жртвите, пасворди и лизинки и сл.

Исто така интернет економијата стана една од најсилните економии во светот. поголемиот дел од нашиот живот сега се врши „online“. Компјутерските криминалци гледаат голема можност за финансиска измама, кражба, приходи од украдените податоци и други вредни информации.

Овие компјутерски напади се директно таргетирање на бизнис системи, големи синџири за снабдување, како и на големи бизнис компании.

Со овие напади пред се загрозува индивидуалната безбедност на човекот, потоа директно се загрозува финансискиот сектор, се влијае на економската стабилност на државата, се губи вербата во сигурноста на системот на државата, а со тоа се намалуваат финасиските добивки на

државата а поради тоа таа станува економски слаба, а кога една држава е економски слаба таа е отворено поле за многу видови на организиран криминал и корупција, и сето тоа влијае на националната безбедност на државата.

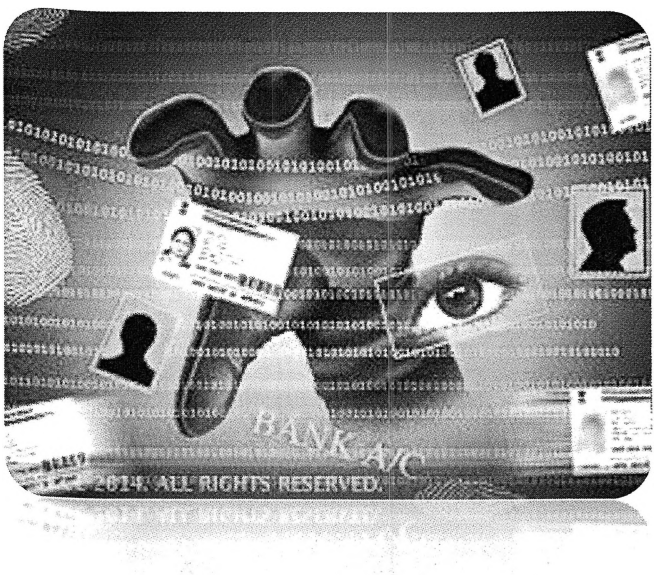
❖

Во иднина треба да се посвети огромно внимание на финансиските кражби и злоупотреби, пред се поради тоа што тие ги користат благодетите на високотехнолошкиот криминал, односно сите негови предности, а тоа се можностите за успешно прикривање на било какви докази, односно прикривање на трагите, користење на proxy сервер кој овозможува маскирање на ИП адресата и давање податоци како да овие кривични дела да се вршат од сосема трето место кое нема никава поврзаност, користење на zombie компјутери кои исто така ги прикриваат трагите и доказите.

Сето тоа говори дека треба да се следат сите новитети кои доаѓаат со технологијата, да се биде во чекор со истите, и успешно да се одговори на заканите и предизвиците кои произлегуваат од нив.

Самата безбедност бара сите оние ке се вклучени да бидат проактивни и постојано да продуцираат решенија согласно со безбедносните закани и предизвици.

1.1.5 ФАЛСИФИКУВАЊЕ НА ПОДАТОЦИ И ДОКУМЕНТИ



Сегашниот степен на развој на компјутерите дозволува дигитализација и менување на содржината на разни акти и документи кои се користат при правниот сообраќај, како и на *фалсификување на податоци* кои се во електронска форма. Кога неавторизирано се менуваат податоци во компјутерска форма, овој тип на криминал се нарекува фалсификување. Подемот на оваа активност е врзана со појавата на компјутеризираните колор ласер печатачи. Овие печатачи имаат можност за печатење со висока резолуција, модификација на документи, дури и креирање на лажни документи.

Квалитетот на тие документи многу често не се разликува од квалитетот на автентичните, а честопати постојат и обиди за фалсификување и на банкноти со помош на компјутер и периферни уреди.

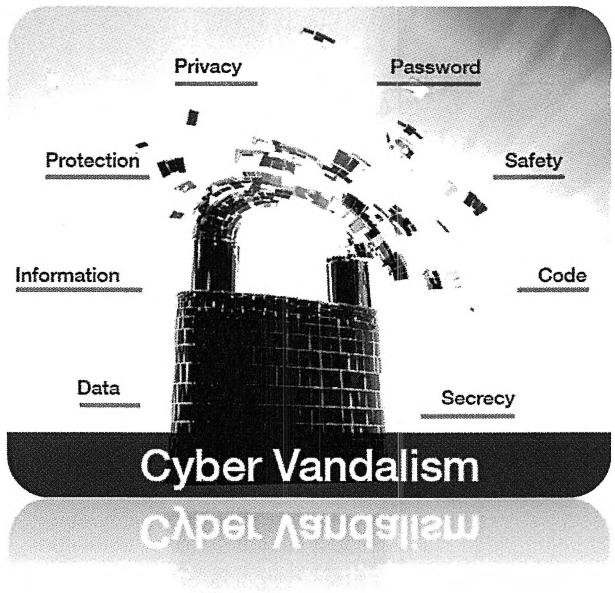
Посебен акцент треба да се стави на фалсификувањето податоци и документи. Треба да сме свесни колку е голема опасноста и колкава штета може да се нанесе на државата, општеството, системот со користењето на информатичката технологија за фалсификување податоци и документи. Најпопуларно е фалсификување на лични документи (лични карти, патни

исправи, возачки дозволи, здраствени картици и сл.), потоа фалсификување на дипломи за завршено образование, фалсификување на разни документи за економски цели, за здраствени цели и сл. Користењето на фалсификувани документи во гласачки процес на избори во некоја држава преставува голема закана

Како што кажавме развојот на технологија покрај нејзината позитивна улога, има многу негативни влијаниа, односно овозможува истата да се користи за нелегални односно криминални активности. Во минатото криминалците за да извршат некое кривично дело користеле отров, камен, нож, пиштол, денес не мораат да ги валкаат своите раце, поради тоа што развиената технологија ги реализира нивните идеи.

Ризикот и опасноста е голема, и затоа акцентот и вниманието треба да се посвети на сузбивање и отривање на овие криминални активности, пред се за да не дозволиме вакви „нечисти умови" кои со лажирање и фалсификување на документи и податоци ќе го разорат системот на нечие општество, а со самото тоа ќе нанесат штета на државата, граѓаните, поединецот, и со тоа директно ќе влијаат на националната безбедност на државата.

1.1.6 КОМПЈУТЕРСКИ ВАНДАЛИЗАМ



Под компјутерски вандализам се подразбира намерно навлегување во туѓи компјутери и заштитени компјутерски системи, бришење и уништување на податоци без некоја посебна цел туку само заради предизвикување на одредена штета кај системите кои се објект на напад во поглед на нивно правилно функционирање.[56]

Исто така компјутерскиот вандализам претставува злонамерно дело на хакерите со што извршуваат нарушување на фукционирањето, изменување, па дури и уништување на страната.[57]

Компјутерскиот вандализам се карактеризира и како website defacement (уништување на интернет страна) или напади Dos (Denial of service). Ако во минатото вандализмот се изразувал со пишување или исцртување графити на зидови на јавни места, или уште поодамна со испишувања во пештери, кој несомнено се користел како средство за комуникација ,,денес тоа се прави со напад на интернет страни".

---

[56] *Магистерски труд под наслов „Видови и облици на злоупотреба на Информатичката технологија" одбранет на 21.10.2009 година на Филозофскиот Факултет Св.„Кирил и Методиј" Скопје – Институт за одбранбени и мировни студии.*

[57] *Кенет К.Лаудон, Карол Герсио Травер, Електронска трговија: бизнис, технологија, општество, Скопје:Арс Ламина, 2010 стр.278.*

Нападнатите интернет страни мораат привремено да бидат затворени за да се острани направената штета, и да се врати во нормална првобитна состојба. Огромните можности кои ги нуди интернетот, како и неговиот досег насекаде во светот, без граници, односно компјутерскиот простор им овозможува на овој тип на криминалци да шират пораки на интернет, кои најчесто се со говор на омраза, како и од економски аспект при што се нанесува штета на економијата и индустријата.

Компјутерскиот вандализам има големо влијание и врз владините сајтови како и врз верските сајтови, а тоа може да биде од политички причини или само од забава. **На пример:** доколку на официјална интернет страна на Влада, Претседател на држава, неовластено се промени содржината и се стават закани од верска и национална природа кон одредена нација, или е напишан говор на омраза, тоа може да предизвика протести, немири од страна на припадниците од таа нација, кои лесно може да ескалираат и со тоа преставуваат закана на националната безбедност на државата.

Во 2009 година на официјалната страна на Претседателот на Р.Македонија д-р Ѓорѓе Иванов било извршено компјутерски вандализам односно defacement, и била променета содржината како на сликата прикажана подоле:

58

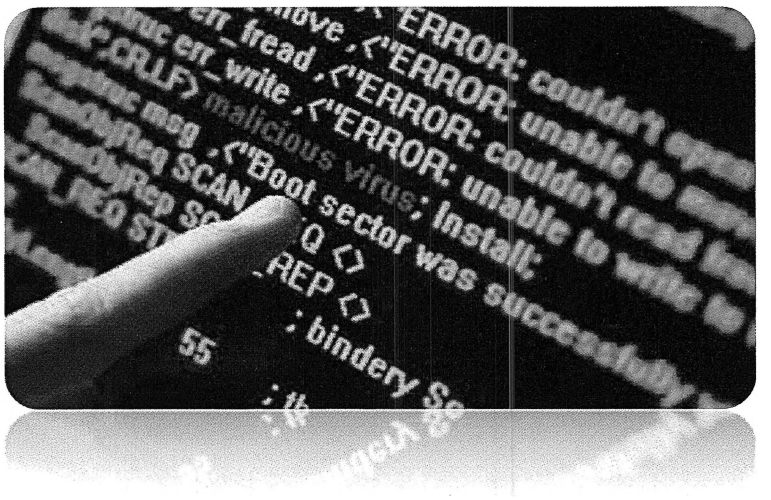
[58] http://www.zone-h.org/mirror/id/8798808 (20.12.2016г.)

❖

За да во иднина се спречи или пак намали компјутерскиот вандализам, потребно е да се вложува повеќе во безбедноста на компјутерските системи, односно безбедноста на самите интернет страни, се со цел да не бидат лесна мета за напад, односно да не се изврши компромитирање врз нив.

Вложувањето во компјутерската безбедност е еднакво на вложување на безбедноста на самата држава.

1.1.7 ИЗРАБОТКА И УПОТРЕБА НА КОМПЈУТЕРСКИ ВИРУСИ



Злонамерните софтвери претставуваат софтвери кои се создадени за да нанесуваат штета на крајниот корисник, а кои вклучуваат мнозинство од закани и тоа различни видови на компјутерски вируси, црви, тројанци и роботски мрежи.[59]

Под поимот компјутерски вируси се мисли на програми кои несовесни поединци ги пишуваат за да нанесат што поголема штета на многу компјутери врзани во мрежа (на пример на глобалната интернет мрежа). Вирус е серија на програмски кодови што ја поседуваат можноста да се „прикачат" на легални програми и да се прошират и на други програми во системот.

Потенцијалните намери на вирусите се различни, од прикажување на безопасни пораки на неколку компјутерски терминали до неповратно уништување на компјутерски податоци.

Оваа категорија на криминална активност вклучува директен или скриен неавторизиран пристап до компјутерски систем со воведувањето на нови програми познати како вируси, „црви" или „логички бомби".

Поимот компјутерски вирус за првпат е користен во 1984 година кога F.Kohen така ја нарекол програмата која не правела ништо штетно, но успешно

---

[59] *Кенет К.Лаудон, Џејн П.Лаудон, Менаџмент информациски системи : Управување со дигитална компанија, Скопје : Арс Ламина, 2010 стр.301*

се ширела низ сите компјутери до кои дошла во контакт. Компјутерскиот вирус е програм, точен компјутерски код кој се преставува дека е нешто друго, има за цел да направи неочекувани, незгодни и често непожелни ситуации, а може да направи мала или голема штета на компјутерот, (на пример губење на податоци од хард дискот). Активираниот вирус може не само да ги инфицира остатанатите програми и документи на компјутерот, туку може да се умножи и пренесе на останатите поврзани компјутери, на ист начин како што и биолошкиот вирус се пренесува од една личност на друга.

Денес вирусите најчесто се шират преку интернет, во случај кога се превземаат (download) разни програми или преку e-mail. Вирусите преку e-mail се шират преку незнаење на сосптвеникот на компјутерот, праќаат лажни е-маил пораки. За да се зашти од компјутерските вируси потребно е на сопствениот компјутер да се инсталира антивирус програм.

Денешните вируси се многу помоќни, отколку што биле во почетните верзии. Вирусите можат да бидат активирани со отворање електронска пошта (attachment), со тоа што ќе кликнете на спам, со посета на сомнителни сајтови, со отворање на работни табели (excel). Сепак денес интернетот преставува главен "автопат" за пренос на вируси.

Некои агресивни вируси како што е на пример Melissa, автоматски се копира и се праќа на електронски адреси на првите 50 личности пронајдени во e-mail адресарот. Таа застрашувачка можност да го отворите е-маилот добиен од страна на некој ваш пријател и да бидете наградени со вирус, е точно она на што смета авторот на вирусот.

Штетата од присуство на вирусот може да варира од мали доцнења на работата на компјутерот, па се до комплетно уништување на податоци. Во однос на поединци, штетата на фирми може да биде многу поголема. На пример оштетена страница може компанијата да ја чини милион долари дневно.

Компјутерските вируси се делат на неколку главни категории и тоа:

- Boot сектор вирус кој претставува вирус кој се накачува на master boot record (MBR) во boot секторот на тврдиот диск, единствената локација на тврдиот диск, каде се сместени основните влезен-излезен систем (BIOS) на компјутерот и програмата за подигнување на оперативниот систем.

- Макровируси кои се наменети за апликации и тој вирус влијае само на апликацијата за која што е напишана.[60]

- Вируси кои инфицираат фајлови претставуваат вируси кои се прикачуваат на exe. фајлови, на компресирани фајлови како zip фајловите и на драјвер фајловите

- Мрежен вирус - овој вид на вирус се пренесува преку мрежата и тоа преку локална мрежа и преку интернет.

- Е-маил вирус – овој вирус како што кажува и неговото име, се пренесува преку електронска пошта.

- Мултипарт вируси - оние кои го добиле називот мултипарт вируси се типовите на компјутерски вируси кои истовремено се и фајл вируси и вируси од boot секторот. Тие влегуваат во компјутерот преку различни видови на уреди, и потоа се прикачуваат самите себе во систем меморијата.[61]

Како да се препознае вирусот на компјутерот? Во случај на помалку значајни вируси може да се приметат чудни пораки, слики и звуци на компјутерот. Инфицираниот компјутер може да има помалку достапна меморија или може да се забележи промена на имињата на фајловите.

Од компјутерот кој е инфициран може да исчезнат програми или одредени фајлови или да не работи како што треба. Ако се забележат било кој од овие карактеристики, веројатно компјутерот е под удар на вирус.

Основна заштита од вируси е инсталирање на антивирусен софтвер, за неделно скенирање на присуство од вируси. Да не се отвара електронска

---

[60] *Gojko Grubor, Milan Milosavljevic, Osnove zastite informacija: metodolosko-tehnoloske osnove, Univerzitet Singidunum, Beograd, 2010 str.106.*

[61] *Кенет К.Лаудон, Карол Герсио Травер, Електронска трговија:бизнис, технологија,општество , Скопје:Арс Ламина, 2010 стр.272.*

пошта од непознати, потребно е да се биде претпазлив кога се отвара attachment и кога доаѓа од луѓе кои ви се познати. Редовно да се прави back-up на податоците во случај вирус да го нападне хард дискот. Уште подобро е да се подеси компјутерот да прави автоматски back-up еднаш неделно. Некој од најпознатите производители на антивируси се: Kaspersky, McAfee, Norton, Avira, Avast итн.

Основни правила за заштита од вируси, црви и тројанци се:

- Треба да се скенира секој програм пред да се стартува;
- Треба да се скенира секој e-mail или фајл кој ќе стигне преку Skype или Msn пред да се отвори, без разлика дали е од пријател затоа што може и тој самиот да не знае дека неговиот компјутер е заразен;
- Не ги посетувајте сајтовите чии адреси ги добивате од непознати лица;
- Секогаш треба да се има најнов антивирус;
- Треба редовно да се update вашиот антивирус за да се снабди со информации за нови вируси и тројанци;
- Задолжително да се користи Firewall;
- Задолжително да се користи Directory catalog;
- Задолжително да се користи Processmate;
- Да не се дозволува на компјутерот никој друг да внесува било какви фајлови;
- Да се користат легитимни софтвери затоа што во внатрешноста на нелигитимните софтвери може да се наоѓа простор за упад во компјутер. Ова важи и за најактуелните верзии на софтвери.

Најчести облици во кои се праќа црвот (вирусот) се:

- во облик на добри програми exe, com, bat;
- во облик на скриптови SCR, PIF, VBA, VBC (visual basic script);
- во облик на makro doc.

Најновите црви користат Microsoft outlock express. Outlock express овозможува движење на кодовите од мејлот веднаш штом мејлот стигне во инбохот, така да сега за покренување на црв (вирусот) од заразен мејл повеќе не е потребно ни да отвори mail.

Неавторизираниот пристап на друг корисник значи присуство на некој на компјутерот, без тоа да го сакате.

Една од последиците од тоа е да ги:

- чита, пишува и брише фајлови (да речеме дека го сака вашиот usename/password за интернет);
- да го рестартува/исклучува компјутерот, како и да го
- искористи компјутерот за да нападне други нови компјутери.

Притоа „црв" е дел од софтверот кој оди низ само еден персонален компјутер или низ мрежа на компјутерски системи, манипулира, уништува податоци или програмски кодови каде и да добие пристап. Црвите претставуваат вируси кои се реплицираат од еден комјутер на друг преку мрежата.[62] Дури и да се примети неговото присуство, тој може да избегне фаќање. Многу вируси имаат вградени „црви" во самите нив.

Тројанци е програм кој кога ќе дојде во компјутерот и ќе се покрене, овозможува пристап на персоналниот компјутер на интернет. Значи некој кој знае дека компјутерот е инфициран со тројанец (а може истиот и сам да го пратил), може многу лесно да пристапи до податоците. Тројанецот не се шири како вирус, туку најчесто се праќа/инсталира на одреден компјутер. Тој таму чека и игра улога на сервер на заразениот компјутер и нуди услуги на клиентите.

За разлика од вирусите, тројанците се комплексна Client-server апликација за пристап на оддалечен компјутер на мрежа. Серверот е тројанец кој се инсталира на компјутерот на непретпазлив корисник и по воспоставената врска на интернет, отвара одредени порт за воспоставување на сесија со клијент апликација преку која таканаречениот хакер од својот компјутер стапува во контакт со тројанецот и на тој начин доаѓа до доверливи податоци. Список на портови кои ги користат тројанците може да ги погледнете на http://onctek.com/trojanports.htmlпрати корисничко име и лозинка (кој се наоѓа во pwl фајл на компјутерот) на одредена e-mail адреса, да го искористи e-mail на

[62] *Colin Combe, Introduction to e-business management and strategy, Butterworth-Heinemann, 2006 pp.170.*

клиентот и да испраќа на сите адреси од адресарот, да прати копија на skype и др., да превземе целосна контрола над компјутерот.

Универзално правило за заштита од тројанци е да не се отвара ниту еден фајл кој ќе пристигне на e-mail и isq, без потреба. Само фајловите кои претходно сте ги барале да ви пристигнат можете слободно да ги отворите, како и преку start up, directory catalog или програма "msconfig".

Меѓу другото, најдобро е да пред да се стартуваат сомнителните програми, да се запишат сите имиња на програми и фајлови од start up, а потоа да се изврши споредба на пред и после стартување на сомнителни програми. Ако се појави некое ново име во списокот од програми во start up, значи се појавил тројанец па затоа заради безбедност на системот потребно е да се исклучи.

Без оглед, најдобра заштита од тројанец е firewall. Firewall или огнениот ѕид е систем кој се обидува да заштити приватна мрежа од хакери, софтвер вируси, извршување на корупција со податоци или неовластен пристап.[63]

Правата улога на firewall е да врши надгледување на влез и излез на програми во компјутерот, односно firewall е заштитен програм кој бележи се што влегува и излегува низ модемот или некаков надворешен линк со што спречува навлегување на сомнителни програми или хакерско воспоставување на конекција со компјутерот. Firewall е заштита од оние кои се обидуваат да извршат рушење на системот и заштита од back door тројанци.

Покрај, firewall, преку atguard има можност да се види листата на програми на зафатени и слободни порти кои ги користат како и комплетната историја на конекција. Atguard ги игнорира постојаните web-реклами и дава целосна статистика на се што имало влез и излез од компјутерот. За сега е тешко да се изврши заобиколување на Firewall, така што не постои програм кој би се поврзал на интернет без наше знаење. Firewall е непробоен ни за големите т.н. хакери па затоа се користи на сите системи на кои им е потребна безбедност од надворешни интернет влијанија.

Firewall програма има за задача да врши контрола и ограничување на пристап на сметачот за интернет и од секаков вид на мрежа. Типични задачи

[63] *Paul Beynon-Davies, E-business, Palgrave macmillan, New York, 2004 pp.221.*

на Firewall претставуваат: - Врз основа на адресата на испраќачот или примачот, се проверува контрола на пристап - Контрола на пристап врз основа на бараната услуга - Криење на внатрешната мрежа од надворешниот свет - Се проверуваат датотеките кои треба да поминат дали содржат вируси - Врз основа на изворот на сообраќајот, се проверува идентитетот - Најавување на активностите на интернет.[64]

Идејата на firewall е да на компјутерот му се овозможи надворешен пристап на она што самиот сопственик дозволил а останатиот пристап да биде оневозможен и блокиран.

Чуствуваме потреба да искажеме некој дополнителни информации кои се во контекст на сфаќањето на претходно изнесеното. Имено, секој систем што е поврзано со интернет или во мрежа има само една единствена IP адреса (тоа може да биде било кој компјутер кој преку провајдер добива привремена ip адреса и се поврзува на интернет, gateway сервер на некоја фирма која има пристап до интернет, рутер, интернет сервер кој понудува некои услуги како http, ftp,итн.). Секој пакет кој патува преку интернет мрежата има во себе рамки кои ја содржат адресата на потекнување и адресата на пристигање, така да се знае од кога и од каде е пратен податочниот пакет и каде и кога ќе пристигне информациониот пакет.

Со било кој компјутер поврзан на интернет се користат различни содржини како што се (http, ftp, isq, broadcast интернет радио). Податоците се пренесуваат преку tcp и udp пакети. Со цел да се разликуваат пакетите меѓу себе се креирани од различни програми, секоја програма си има свој „канал", односно своја порта по која се врши испраќање и прифаќање на пакети. Портите се стандардизирани така што ftp користи порта 20 и 21, telnet порта 23, http порта 80, isq порти 1508 и 1509. Притоа на овој принцип може да се изврши забрана преку firewall или дозвола за влез на програми во компјутерот, а со тоа и контрола на интернет сообракајот, во одредени насоки и на одредени програми. Така на пример за IP адреса 123.103.10.12 дозволува сообраќај по порта 23, тоа значи да некој со таа адреса дозволува да се поврзе преку telnet на компјутерот. Колку што се слободни број на порти и помал опсег на адреси кои имаат дозволен пристап, веројатноста на хакерите да влезат во

---

[64] *Дитер Голман, Компјутерска сигурност, АД Вербум, Скопје 2010 стр.238*

сметачот е многу мала. Ако имаме сервер на интернет потребно е да се разгледа секоја услуга која може да се понуди, дали е неопходно потребна таа услуга или не е, односно секоја понудена услуга е и истовремено потенцијална закана за пробив во компјутерски систем.[65]

Секое злосторство има различен ефект на општетството и на околината во кое е извршено, но компјутерските вируси преставуваат едно од најголемото зло на денешницата. Заканите од компјутерските вируси донесоа нова димензија во однос на ризиците кои произлегуваат од нив.

Компјутерските вируси може да оштетат критични информациони инфрастуктури, може да влијаат на работата на системот на радарска инсталација, електрична мрежа, комуникациски системи, нуклеарни централи и сл., а со тоа може да го отвори патот на непријателски сили како на пример прелет на авиони и фрлање на ракети.

Со помош на компјутерските вируси криминалците можат да дојдат до многу доверливи и осетливи информации од државен карактер, безбедносен карактер, финансиски податоци, лични податоци, од истражувачки и медицински карактер и сл.

Вообичаено е доколку се дојде до вакви информации, криминалците да ги продаваат за да се стекнат со материјална корист, несвесни дека овие информации во рацете на погрешни луѓе можат да предизвикаат сериозни загрозувања по безбедноста. Доколку информации од државен и безбедносен карактер на една држава ги поседува друга држава што значи истата има пристап до важни бази на податоци, безбедносни, воени тајни, полициски досиеја, истражувања и сл., и со објавување на истите или користење во злонамерни цели, со тоа директно ја загрозува национална безбедност.

---

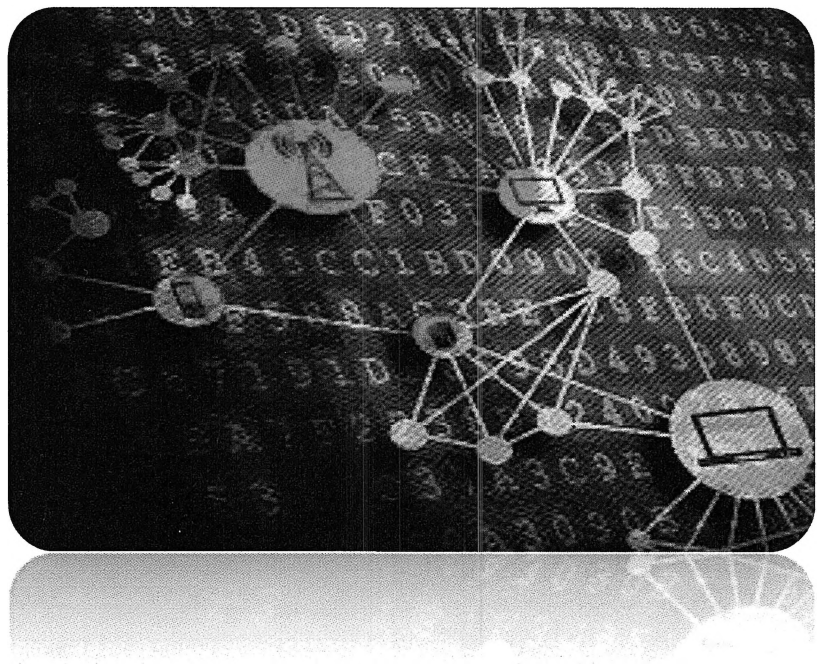
[65] *Магистерски труд под наслов „Видови и облици на злоупотреба на Информатичката технологија" одбранет на 21.10.2009 година на Филозофскиот Факултет Св.„Кирил и Методиј" Скопје – Институт за одбранбени и мировни студии.*

❖

Заштитата од компјутерски вируси на компјутерските системи на државата односно државните институции, како и на компјутерскиот систем на поединецот е важна колку и заштитата од воен напад врз државата, или заштитата на поединецот од кражба, напад врз него и сл. Би сакала да направам една компарација, кога купуваме стан или кола истите веднаш ги осигураме од кражби, поплави, пожари и сл., со цел да се заштитиме од несакани последици, но кога купуваме компјутер и на самиот компјутер внесуваме огромен број на лични податоци (лични податоци, банкарски сметки, броеви, финански сметки, пасворди, фотографии), а особено на службени компјутери каде што имаме службени материјали кои се класифицирани како доверливи, ние немаме инсталирано антивирус, или пак имаме но не го обновуваме навремено.

Недоволното вложување во заштитата на компјутерската безбедност преставува ризик од несакано инсталирање на вируси, кои нанесуваат штети во огромни размери, затоа во иднина се повеќе треба да се вложува во истата.

1.1.8 КОМПЈУТЕРСКА САБОТАЖА И ШПИУНАЖА



Неавторизирана модификација, прикривање или бришење на компјутерски податоци или функции често се нарекува и компјутерска саботажа. Може да се искористи за придобивање на економска предност над конкурентот, за промовирање на нелегални активности на терористи или за крадење на податоци или програми. Компјутерска саботажа имаме во случај кога некој ќе уништи, избрише, промени, прикрие или на друг начин ќе онеспособи податок, програм или ќе го оштети компјутерот кој е од значење за државен орган, институција, јавна служба.[66]

Основно обележје на Компјутерската шпионажа е оддавање тајна, додека основен облик е овозможување достапност на доверливи информации. Шпионажата може да биде мотивирана од политички или економски причини, поради што многу земји преку ангажирање на своите тајни служби доаѓаат до откривање на политички, воени, економски тајни на другите земји. Криминалот и шпионажата мигрираат кон дигиталниот свет. Шпионажата не е воопшто нов

[66] http://www.computerweekly.com/feature/The-law-and-cyber-sabotage (06.03.2016).

феномен, но во последните денеции светот се пресели во едно ново царство на шпионирање „компјутерска шпионажа", која го смени обликот на модерното војување.

Покрај хакерите и групите кои тие ги организираат за неовластено навлегување во заштитени системи, во денешно време постојат и специјалализирани тајни владини служби кои преку навлегување во компјутерскиот систем на другите држави прибираат податоци од разузнавачка природа. Поимот **компјутерска шпионажа** може да се дефинира како еден од најмодерните облици на разузнавање. Но исто така постои и индустриска шпионажа која е само од комерцијална природа.

Во компјутеризираниот свет постојат во основа два типа на саботажа и тоа: физичка саботажа и логичката саботажа.[67]

Трговските тајни се исто така еден вид информации кои не се за широка употреба а на некој начин се во функција на здобивање предност во однос на конкуренцијата. Под поимот трговска тајна се подразбира хемиска формула, компјутерска апликација, процес, метод, уред, техника, информации за цени, листи на потрошувачи или некоја друга информација која не е наменета за јавноста. Општо гледано ако економската вредност на информацијата наложува таа да не биде јавно дистрибуирана, може да се дефинира како трговска тајна.

Неавторизиран пристап до информациите (трговските тајни), било да се електронски или пишани, од вработени или поранешни работници во компанијата или од надворешни лица, се дефинира како компјутерска шпионажа.

Како што е познато развојот на економијата на било која држава се базира на развојот на нејзините компании, а нивниот развој зависи директно од поседувањето на вистинските информации во вистинско време. Денес, силата на една држава не се мери само по вооружувањето кое таа го поседува, туку од нејзината економска моќ. Еден од аспектите на "модерната војна" се состои

---

[67] *Петровиќ С. „Полицијска информатика", Криминалистичко – полицијска академија, Београд, 2007. стр. 104.*

од превземање на информации кои пак резултираат со намалени профити и во некои случаи пропаѓање на компании.

Информациите стекнати на овој начин се најчесто оние кои доаѓаат од секторите за истражување и развој, од финансиски извештаи, листи на клиенти, податоци за набавки, планови за маркетинг, информации за вработени лица во компанијата, одлуки на бордот на директори и други витални информации, а заинтересирани за нив се конкурентските компании од истата или од некоја странска држава. Сите овие информации можат да бидат употребени во водењето на бизнис политиката на една компанија и имаат потенцијал да ја постават истата во економска предност пред другите компании.

Најчесто, компјутерската шпионажа се врши од компаниите. Но во некои случаи, овие активности произлегуваат и од владите на некои земји. Од друга страна, жртви на компјутерската шпионажа, покрај компаниите, се и владите на земјите.

Постојат повеќе причини за вршење компјутерска шпионажа. Меѓутоа, мора да се забележи дека не секогаш оваа активност води кон негативни последици. Постојат компании кои јавно го признаваат вработувањето на луѓе за надгледување на активностите на конкурентните компании. Ова не претставува никаква опасност бидејќи не се работи за крадење на трговски тајни кои подоцна ќе се употребат против компанијата од која биле украдени, туку едноставно претставува подготовка за борбата која треба да се води на пазарот.

Од друга страна, одредени компании и влади на земји, крадат трговски тајни за да се стекнат со определана предност. Имено, развојот на нова технологија е долг и скап процес, па прашањето е зошто да вложиме една милијарда долари и десет години развој на технологија која веќе постои, или е во тест фаза, кога таа технологија можеме да ја имаме за еден милион долари (или помалку) и за неколку месеци.

Значи, главна причина е можноста за зголемување на профитот и воедно ослабување на конкуренцијата без скоро никакви инвестиции.

Кражбата на информации може да биде извршена од лица кои работат или работеле во компанијата или од надворешни лица. Најчесто информациите се чуваат на локалните хард-дискови, дискети, компакт дискови и други медиуми во електронска форма. Поради тоа, кражбата може да биде извршена со копирање на податоците на нов медиум или превземање на истиот.

Компјутерската шпионажа е акт или начин на добивање на тајни без одобрување на носителот на информации (лични, чуствителни, комерцијални или од доверлива природа), од поединци, конкуренти, ривали, групи, влади и непријатели, за лична, економска, политичка или воена предност, со користење на нелегални методи на интернет, мрежни или поединечни компјутери. Компјутерската шпионажа е метод кој се користи преку интернет. За изведување на компјутерска шпионажа воглавно се користат малициозни софтвери, вклучувајќи тројански коњи (специјални тројанци направени да го шпионираат корисникот), вируси, шпионски програми (RAT, Keyloger). Шпионажата може во целост да се изврши на интернет од страна на професионалци, од бази во некои далечни земји и сл.

Доколку украдени податоци од национелаен интерес се користат поната му од страна на некој непријател без разлика дали е внатрешен или надворешен, тоа преставува закана за националната безбедност на државата.

Во последните децении со самиот напредок на технологијата, алатките на компјутерската шпионажа станаа неопходни за современи воени операции.

Модерните комуникации отвараат уште едно поле на делување на шпионите. Пред се, интернет, како глобална комуникациска алатка, овозможува брз, ефикасен и економичен пренос на податоци на огромни растојанија. Но недостатокот од механизми за контрола на комуникациите овозможува лесен пристап до одредени информации. До овие информации може да се дојде или при нивниот транспорт, или со директно пробивање на локален компјутер кој е постојано приклучен на мрежа. Механизми за наоѓање на сторителот постојат преку ip адресите, но не се секогаш ефикасни.

Компјутерската шпионажа е еден од најважните и интригантни меѓународни проблеми и закани во светот денес. Да се разбере оваа тема е важно поради разбирањето на начинот како технологијата влијае на односите помеѓу државите. Компјутерската шпионажа е се повеќе напредна, ефикасна и професионална. Таа станува прифатена и се преферира како начин на војување.

Сеуште неможе да се каже дека компјутерската шпионажа ќе го замени традиционаниот начин на војување, но веќе влијае на природата на конфликт помеѓу државите. Сето тоа укажува дека оваа промена започнала со Студената Војна помеѓу САД и Русија, кои своите напори ги фокусирале на што е можно повеќе собирање на тајни операции за војување.[68]

Телефонските прислушкувања се исто така голема опасност за сигурноста на трговските тајни. Европската унија, како најголема опасност од овој вид го истакнува *echelon* системот за кој членките сметаат дека може да биде употребен против нивните компании. Познато е дека echelon системот служи за глобално прислушкување на електронските и аналогните комуникации. Според САД, овој систем е наменет за заштита од терористички напади и откривање на други криминални активности, но самиот факт дека овој систем присклушкува, претставува опасност по компаниите кои не работат во САД.

Иако последиците ги сноси компанијата, нејзиното оштетување значи оштетување на целата држава. Пред се, штетата која е нанесена на компанијата повлекува намалени профити или пак целосни загуби. Ако една компанија работи со загуба, таа отпушта одреден број вработени за да ги намали загубите. Од друга страна, секоја загуба на една компанија значи загуба и за државата во која компанијата се наоѓа одразена преку намалување на профитот од даноците кои компанијата ги плаќа.

Компјутерскиот простор дава исклучителна средина за шпионажа, дозволува анонимност и го олеснува трансферот на огромно количество на информации. Некои држави ова го дефинираат како упад или неовластен

[68] *Види пошироко:Dana Rubenstein, Nation State Cyber Espionage and its Impacts, pdf.*

пристап до податоци, или напад на информациски систем, а некои го сметаат за кражба на интелектуална сопственост, сопствени информации, податоци со значителна економска вредност. Во сите држави компјутерската шпионажа е кривично дело и истата е казнива.

Компјутерската шпионажа преставува голем ризик кој со текот на времето ја поткопува националната економија на една држава. Многу земји користат компјутерска шпионажа за потикнување на економскиот раст врз основа на напредни технологии насочени кон науката и технологијата. [69]

Постоењето на многу начини информациите да бидат украдени ги поттикнува компаниите да инвестираат во нивна заштита, а на ова се надоврзуваат и државите кои како превентивни мерки воведуваат закони кои се однесуваат конкретно на овој тип на криминал.

Главните начини на заштита се :

- енкриптирање на важните податоци – иако секоја енкрипција може да биде пробиена, за тоа треба подолго време. Енкрипцијата не е наменета податоците никогаш да не бидат прочитани, туку да не бидат прочитани во периодот кога тие се најважни. Кога информацијата ќе застари, не е важно дали некој ја поседува или не;
- секој документ кој содржи доверливи информации мора да се уништи пред да се фрли во ѓубре;
- разговори за тајните на компанијата не смеат да се одржуваат во несигурна околина – разговорите кои поттикнуваат излагање на витални информации треба да се избегнуваат како на јавни места, така и во просториите на компанијата, доколку има присуство на непознати лица;
- не смее потполно да се верува на консултанти и привремено вработени лица;
- користење на услуги на компании кои се занимаваат со обезбедување;

---

[69] *Alexander Klimburg, National Cyber Security, pp. 16, 2012 by NATO Cooperative Cyber Defence Centre of Excellence. (https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf).*

- постојат компании чија дејност е спречување на компјутерската шпионажа. Овие компании вработуваат луѓе кои се инфилтрираат во компанијата која треба да ја заштитат и ги испитуваат потенцијалните кражби на тајни податоци т.е. ги превземаат сите мерки за да не дојде до ваков инцидент;
- чување на информациите на сигурно место – секоја тајна мора да биде складирана на сигурно место каде ограничен број на луѓе имаат пристап;
- поединците кои имаат пристап до информациите би требало да потпишат договор кој забранува откривање на информациите кои тие ги поседуваат;
- секој документ кој содржи тајни податоци мора да биде означен на пр. „строго дов", „службена тајна", „државна тајна" и сл..

Иако многу земји низ светот сториле компјутерска шпионажа, САД, Русија и Кина се сметаат за најнапредни земји во светот во однос на компјутерската шпионажа, и дека поседуваат најплодни компјутерски шпиони.

Голем играч во компјутерската шпионажа е Кина. Во последните години Кина го зголемува посветеното време, ги зголемува ресурсите, работната сила потрошени на компјутерската шпионажа. Ослободителната војска на Кина или PLA, вклучува посебно Биро во Одделението за Разузнавање, специјално наменето за Компјутерска шпионажа. И покрај тоа што е тешко да се потврди изворот на било кој компјутерски напад, според Извештајот на Конгресот на САД во Октомври 2011 година, е потврдено дека токму Кина е одговорна за напад на мрежите на САД и крадење на доверливи информации во неколку случаеви. Меѓутоа не е предизвикана голема штета, се чини дека целта на Кина била кражба на економски, финансиски тајни за да ја подобри својата економија.

Исто така, голем играч во компјутерската шпионажа е Русија. Се располага со информации дека Русија поседува понапредно компјутерско оружје од Кина. Како и Кина, така и Русија има посебни единици посветени на компјутерската шпионажа, каде што директно од колеџ се регрутираат лица со добри компјутерски вештини „хакери". За разлика од Кина, својата компјутерска

моќ Русија ја користи да ја дополни проагресивната форма на војување, наместо едноставно крадење на економски тајни.[70]

Како алатки кои се користат за компјутерска шпионажа кои ги споемнавме погоре во текстот се малициозни софтвери, вклучувајќи тројански коњи (специјални тројанци направени да го шпионираат корисникот), вируси, шпионски програми (RAT, Keyloger).

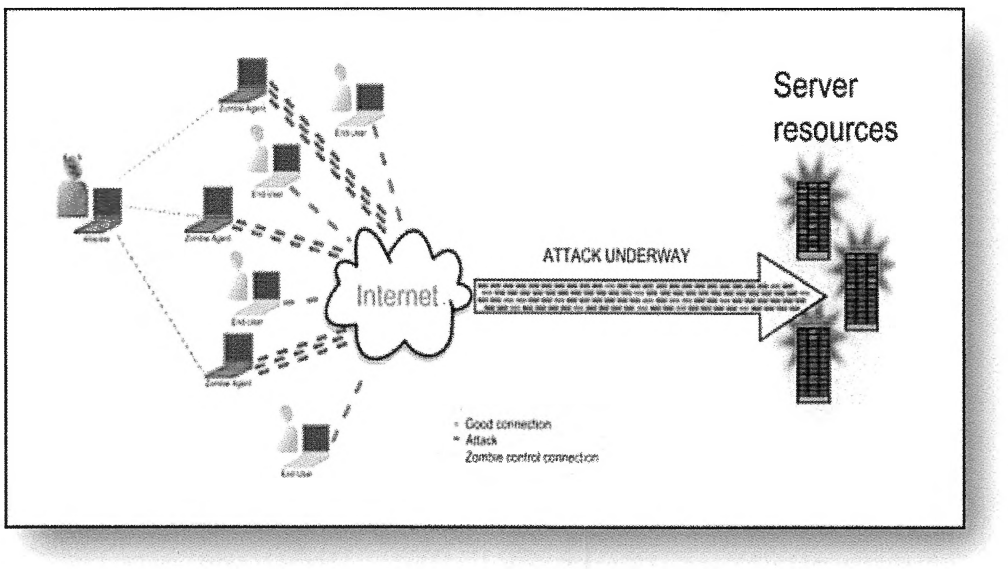
Последиците од компјутерска шпионажа се предизвикување на значителна штета за држава, државен орган, установа или правно лице во кое сторителот работи или за друг државен орган, установа или правно лице. Сторителот може да биде и лице кое го врши делото во рамките на својата службена должност и овластување.[71]

[70] *Види пошироко:Dana Rubenstein, Nation State Cyber Espionage and its Impacts, pdf.*
[71] *Владо Камбовски . „Казнено право, посебен дел", Просветно дело АД Скопје, 2003 оп. цит. стр. 460 - 461.*

1.1.8-а DOS (Denial of Service) нападите се едни од најискористените хакерски напади

DoS (Одбивање на Услуга) нападите се едни од најголемите закани на безжичните мрежи. DoS нападот се случува кога противник предизвикува мрежата да стане недостапна за легитимните корисници, или услугите да бидат прекинати или одложени. [72]

За разлика од вирусите, тројанците, црвите овие напади не извршуваат трајна штета (бришење на податоци од хард дискот, крадење лозинка) туку предизвикуваат оневозможување на работата на некој ресурс (сервер). [73]



Слика 1

DOS нападите се извршуваат со користење на DOS алатки кои праќаат голем број на пакети преку интернет. Секој компјутер или било кој уред кој е споен на интернет и кој има мрежни услуги кои се темелат на TCP (Transmission Control Protocol), преставуваат потенцијални жртви. DOS напад со рефлексија се прави во специјални случаеви на напади од повеќе извори.

---

[72] *Елена Конеска, Јасминка Сукаровска Костадиновска, Митко Богданоски, Сашо Гелев, DoS напади кај безжичните мрежи и методи за намалување на ефектите од овие напади, Европски Универзитет – Скопје, Р. Македонија, УДК: 004.7.056.*

[73] *Слика 1, DOS напад, (https://www.google.com/search?q=dos+attack&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjQmLiXspHLAhUTS5oKHZ2XC-gQ_AUICigE&biw=1366&bih=609#imgrc=Xwh5slFJ4YyXfM%3A),*

Тие се користат за прикривање на идентитетот на вистинскиот напаѓач. Било кој компјутер може да да се користи како рефлектор со додавање на IP адреса на компјутерот-жртва во изворното поле на побарувањето. Со додавање на тие информации компјутерот – рефлектор ќе испрати одговор на жртвата наместо напаѓачот. Ако постојат многу компјутери – рефлектори резултатот на тоа ќе биде DOS напад. Разликата помеѓу zombie компјутер и компјутер – рефлектор е тоа што рефлекторите преставуваат легални корисници на интернет услугите. Заради тоа нападот со помош на рефлексија е многу тешко да се уништи.

DDOS (Distributed Deniel of Service) нападот е понапреден облик на DOS напад,при кој тројанец – напаѓач се инсталира на повеќе компјутери и така врши напади од повеќе локации во исто време. Тој преставува еден од најмоќните софтверски напади што досега воопшто е откриен. Истиот важи за најнепредвидлив и затоа е многу тешко да се сопре ваков напад, бидејчи хакерите користат неколку стотини или многу повеќе претходно инфектирани компјутери кои ги имаат под своја контрола т.н. (zombie) и ја користат нивната моќ, односно нивната интернет конекција напаѓајќи некој веб сервер или др. Тоа го прават така што ја пингираат (ping) жртвата од сите компјутери кои ги имаат под своја контрола во исто време, а тоа го правата со посебен софтвер кој ги контролира сите компјутењри кои они ги имаат под контрола.

Како заштитна мерка која ја користат компаниите од ваков тип на напад е инсталација на специјализиран софтвер што го контролира протокот на податоци. Тоа значи, доколку една IP адреса побарува многу повеќе податоци од лимитот кој е зададен, софтверот автоматски го прекинува протокот на податоци кон таа IP адреса се додека побарувањето на податоци од таа IP адреса не падне под нормалата.[74]

Како еден од најголемите примери за DDOS напад, е Естонскиот пример. Во 2007 година беше извршен DDOS напад на целата интернет инфрастуктура на Естонија. Нападот бил многу добро испланиран и

---

[74] *Види пошироко:Susan W. Brenner, CybercrimeCriminal Threats from Cyberspace, 2010, pdf, стр.49, стр.64.*

координиран, и истиот предизвикал хаос и застој во функционирањето на државата, и бизнис процесите.

Главни цели на напад биле:

- Претседателството и Собранието на Естонија;
- Владините Министерства;
- Политички партии;
- Познати весници;
- Банки;
- Комуникациски инфрастуктури.

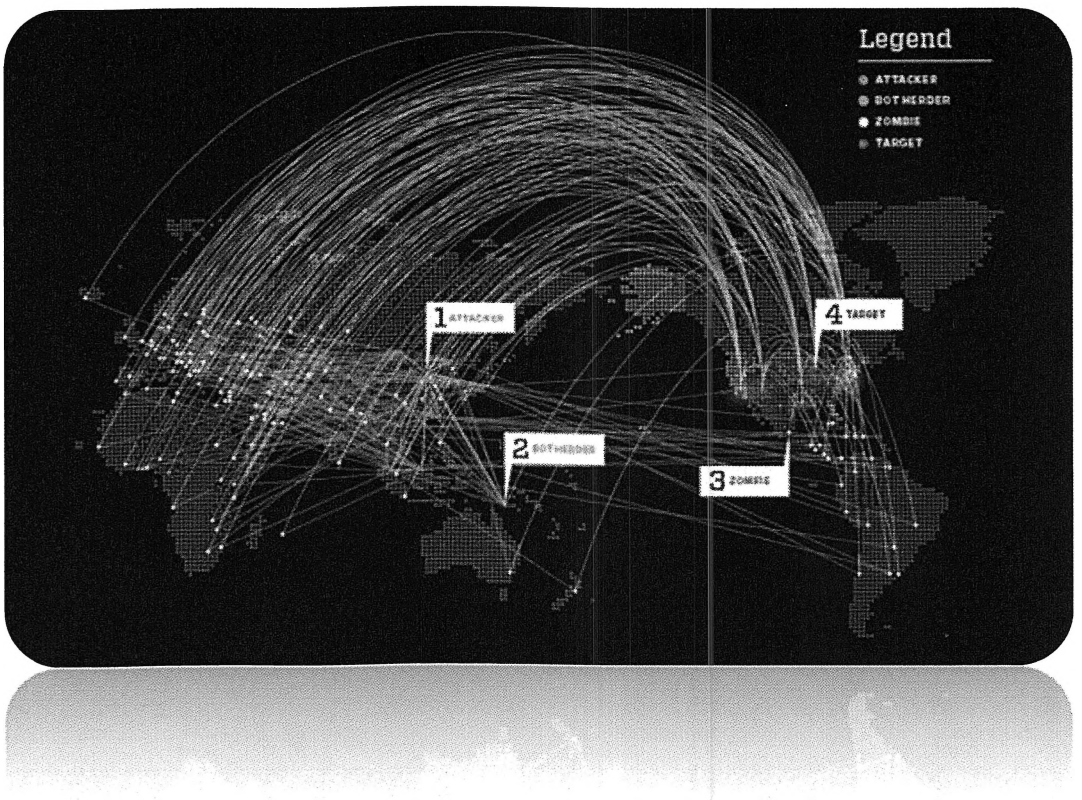
Нападите биле толку силни што Естонија морала да блокира било каков странски пристап до сајтови.

Од страна на Владата на Естонија за овој напад била обвинета Русија, но до денес нема цврсти докази дека навистина нападот е дојден од страна на Русија.[75]

Слика2[76]

[75] *Muhammad Saleem, Jawad Hassan, "Cyber warfare", the truth in a real case, pdf, cmp.2.*
[76] *Слика 2, DDOS напад,(https://www.google.com/search?q=ddos+attack&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjCp4ics5*

Слика3,[77]



Малициозни софтвери, како што се вируси, црви, тројански коњи се исто така популарни алатки за попречување на нормални компјутерски операции, тајно собирање на податоци, или пак целосно уништување на компјутерот. Други видови на напади се „логички бомби", кои всушност се малициозен софтвер дизјниран да лежи заспан до одредено време, или додека не се активира од страна на одреден настан, како и IP измама каде што напаѓачот успева да се маскира со цел да добие пристап до заштитените мрежи или приватниот компјутер. Овие напади може да бидат погубни кога се во поголем обем. Откако напаѓачот ќе добие пристап до посакуваната мрежа на својата жртва, тогаш тој манипулира, со тоа што жртвата не е свесна за тоа, а со тоа се загрозува сигурноста на некоја нација.

HLAhVkLZoKHZNQBQkQ_AUICSgD&biw=1366&bih=609#imgdii=UM1VxqGgDjGrmM%3A%3BUM1VxqGgDjGrmM%3A%3B1dFvHvLAXNYV2M%3A&imgrc=UM1VxqGgDjGrmM%3A)

[77] *Слика 3, DDOS напад, (https://www.google.com/search?q=ddos+attack&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjCp4ics5HLAhVkLZoKHZNQBQkQ_AUICSgD&biw=1366&bih=609#imgdii=UM1VxqGgDjGrmM%3A%3BUM1VxqGgDjGrmM%3A%3B1dFvHvLAXNYV2M%3A&imgrc=UM1VxqGgDjGrmM%3A)*

Компјутерскиот вирус неможе директно да оштети физички дел од компјутерот, туку само датотека (File). Тие може да уништат документи, поголем број од вирусите ја успоруваат работата на компјутерот. Како што кажавме некои вируси имаат одложено време на активирање и тие се нарекуваат „логички бомби“. Овој вид на вирус може да се активира на претходно одреден датум, кога корисникот (домаќинот) извршува некоја работа на компјутерот.

Терминот „вирус“ се употребува за да се заокружат сите групи на инфективни програми, а тие може да се поделат во три групи:

1. Црв (Worm);
2. Тројанец (Trojan Horse);
3. Програма за шпионирање (Spyware);

1.1.8-б ЦРВИ (WORM)

Црвите претставуваат вируси кои се реплицираат од еден комјутер на друг преку мрежата.[78] Се работи за независна програма или сет од програми, кои се во можност да ги множат своите оперативни делови на други компјутери користејќи веќе постоечка мрежа „Интернет“, или пак веќе вмрежени компјутери. Ги користат безбедносните пропусти на компјутерот за да дојдат до него. Како независни програми се подразбира дека на оваа група на вирус не е потребен програм односно домаќин на кој ќе се закачи. Според начинот на размножување постојат два типа на овој вирус:

- Црв со еден домаќин и
- Мрежен црв

Првиот тип е препознатлив по тоа што кога се размножува на друг компјутер го брише оригиналот, а со тоа останува само една копија кај вмрежените компјутери. Популарно овој вирус се нарекува „зајак“ (Rabbit).

Мрежниот црв се состои од повеќе сегменти односни делови, така што секој дел функционира на посебен компјутер во мрежата и извршува различни функции. Како најбитна функција е размножување на други компјутери. Оној мрежен црв кој ги контролира другите се нарекува „октопод“. Како решение на овој тип на вирус се препорачува преинсталација на системот.

Исто така црвите се користат да заразениот компјутер го создадат како „зомби“ компјутер кој ќе биде под контрола на авторот на црвот, односно на вирусот. Мрежа од такви заразени машини (компјутери) се нарекува „Botnets“, и многу често се користи од страна на испраќачите на несакана електронска пошта „Spam“пораки. Така наречените спамери се сметаат за извор на средства за создавање на вируси односно црви, и истите нудат продажба на IP адреси на заразени компјутери, додека други се обидуваат да уценат компании со закани од DOS напади.

---

[78] *Colin Combe, Introduction to e-business management and strategy, Butterworth-Heinemann, 2006 pp.170.*

Листа на црви кои избегнуваат детекција:

Оклопен црв „Armored worms“– овој црв не дозволува да биде пронајден од аналитичарот и не дозволува да биде анализиран неговиот код. Овој црв се користи да направи следење, демонтирање и враќање назад;

Црв празнина „Cavity worms“ – овој црв се крие во нерасределениот простор на дискот, пребришува дел од податоците без тоа да го примети домаќинот на компјутерот;

Стелт црв „Stealth worms“ – како што сугерира самото име овој вид на црв се обидува да го прикрие своето присуство од анти вирусни алатки, дури и во целост неможе да биде откриен. Истиот ги превзема податоците од комјутерот и ги пренасочува на друга датотека;

Автоматска енкрипција „Self-encrypting worms“ – овој вид на црв се обидува да се сокрие од анти вирусните алатки, има алгоритам декрипција на почетокот на кодот кој се менува со секоја нова инфекција и на тој начин се обидува да го збуни анти вирусот;

Полиморфен црв „Polymorphic worms“ – овој вид на црв мутира, создава различни копии од себе за да избегне детекција од анти вирус, а со тоа истиот вирус може да изгледа различно на различни системи, па дури и во рамките на различни датотеки.[79]

[79] *Види пошироко: Eric Goetz, Guofei Jiang, William Stearns, Viruses and Worms, 2002, pdf.*

1.1.8-в ТРОЈАНЕЦ (Trojan Horse)

Тројански коњ претставува програма која навидум изгледа легитимна, но всушност содржи друга програма или блок на несакани злонамерни кодови, скриени во блок на пожелен код[80]. Слично како и неговиот историски имењак, Тројанскиот коњ или таканаречениот тројанец е малициозна компјутреска програма, која се појавува на компјутерот и го намамува корисникот односно жртвата, да го инсталира. Откако ќе се инсталира намерно врши дејствија кои корисникот не ги очекува. Тоа често вклучува обезбедување на пристап до ослетливи информации, и му овозможува на напаѓачот да украде податоци, да инсталирара додатни малициозни софтвери, а со тоа да ги следи сите активности на корисникот на компјутерот.

Овој тип на вирус има за цел да се вовлече во компјутерот и да отвори некоја некоја врата, во компјутерската терминологија „порта" низ која напаѓачот ќе може да пристапи до саканите податоци од компјутерот. Овие вируси уште се нарекуваат и „Back Door"(Задна врата) вируси. Тројанецот како вирус е многу тешко да се регистрира од страна на самиот корисник на заразениот компјутер. Единствено како показател може да се каже дека е побавнато работење на компјутерот односно на процесорот.

Некои тројанци ги користат безбедносните мани на постарите верзии на Google Hrome и Internet Explorer, за користење на компјутерот како анонимно proxy за да може успешно да се сокрие на интернет, а со тоа на контролот на вирусот му овозможува користење на интернетот за нелегални цели, а со тоа сите докази и инкриминирани активности насочуваат на IP адресата на заразениот компјутер.[81]

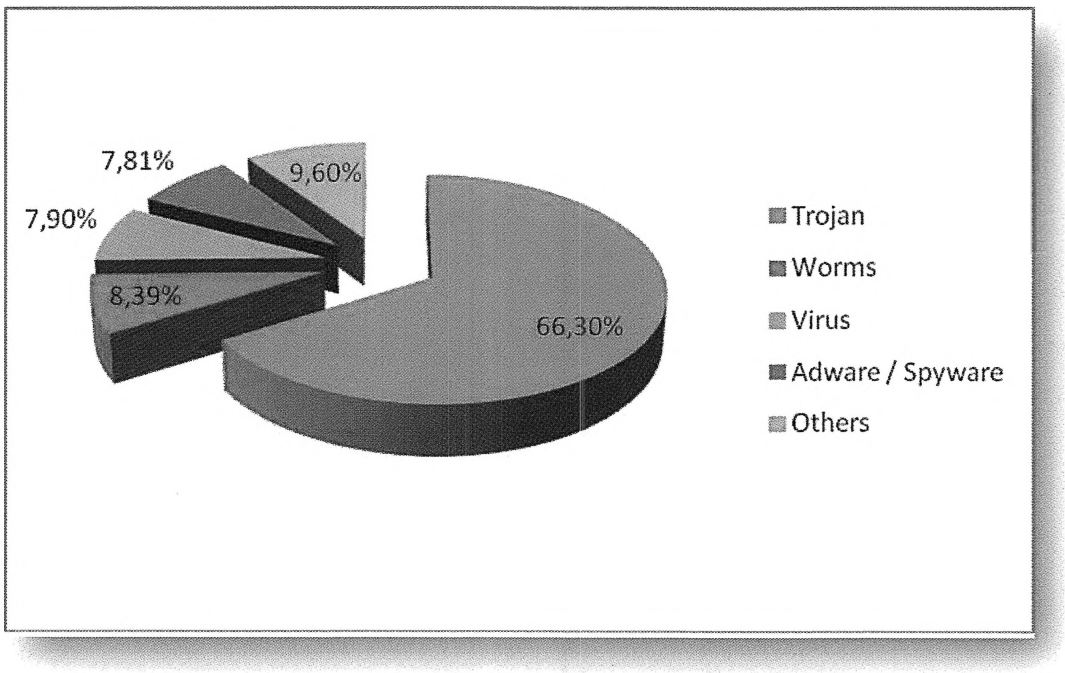
Во земјите од Герамнско говорно подрачје (Германија, Швајцарија), шпионскиот софтвер е направен и се користи од страна на Владата, истиот се нарекува „Govware", кој преставува тројански коњ односно софтвер кој се

---

[80] *Gojko Grubor, Milan Milosavljevic, Osnove zastite informacija: metodolosko-tehnoloske osnove, Univerzitet Singidunum, Beograd 2010 str.112.*
[81] *An introduction to malware, CERT-UK, pdf.*

користи за да пресретне комуникции на целните компјутери. Овие земји имаат и законска рамка за регулирање на користење на таков вид на софтвер.

Приказ на малвер трендови, слика [82]



Најголемиот проблем е што моментално не постои целосна и ефикасна заштита од овие напади, така да, сите интернет корисници можат да бидат жртви на овие напади. Банкарските тројанци најчесто се изработуваат од страна на професионални компјутерски крадци кои што имаат големо искуство и компјутерско и програмерско познавање. Една од најпозните групи на напаѓачи е руската група RBN (Russian Business Network).[83]

Пример за овие напади е познатиот тројанец Haxdoor.ki кој, во 2006 година, нападнал голем број на шведски и германски банки во тие земји, при што биле собрани голем број на банкарски податоци[84].

---

[82] https://www.google.com/search?q=cyber+worm&espv=2&biw=1366&bih=609&source=lnms&tbm=isch&sa=X&ved=0ahUKEwi3_KOyuuvMAhUCsBQKHRIQAYAQ_AUIBigB#tbm=isch&tbs=rimg%3ACcehRy4zkXlqIjiiLkFHC9Dce3Lxe198WUs2NsBdRFfgezJIS6xnvjgHGwcZE4oGea9vm-wqF8RhcYXTrcTutZdkvyoSCaluQUcL0Nx7EeeMpxXqwIMBKhIJcvF7X3xZSzYRI5kr928cnY8qEqk2wF1EV-B7MhEqSLnNqxAauSoSCUhLrGe-OAcbETQ0I_1htfqsXKhIJBxkTigZ5r28RWBvhdIRJ3BYqEqmb7CAXxGFxhRFq_1QJJcPflkyoSCdOtxO61I2S_1EWsnGqxWysp-&q=cyber%20worm&imgrc=Olw_FSRCUoJyiM%3A (21.05.2016).

[83] "Russian Business Network (RBN): RBN - Georgia CyberWarfare." Russian Business Network (RBN). 5 Nov. 2008 http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare.html

[84] Swedish bank hit by 'biggest ever' online heist (2007) ZdNet, httpp://news.zdnet.co.uk/security/0,1000000189,39285547,00.htm

1.1.8-г ПРОГРАМИ ЗА ШПИОНИРАЊЕ (Spyware)

Spyware е софтвер кој врши инвазија на приватноста на корисниците со собирање чуствителни информации, лични податоци, следење на интернет посети и сл. Овие информации потоа може да се пренесат на трети лица.

Шпионскиот софтвер прикриено сам се инсталира на компјутерот, за потоа да може да ги надлегува локациите на интернет-мрежата на кои корисникот се конектира и за да можат да прифаќаат конекција на реклами[85]

Spyware е било која технологија која помага во собирање на информации за некое лице или компанија, организација без нивно знаење. Шпионскиот програм се става на компјутерот тајно, најчесто со инсталирање на некоја нова програма, со цел да ги собере саканите информации. Исто така може да влезе во компјутерот преку посетување на компромитирана интернет страна или со отварање на малициозен прилог во e-mail.[86]

Често вклучува собирање на доверливи информации како на пример лозинки, броеви од кредитни картички, следење на клучни зборови, следење на навики на прелистување, собирање на e-mail адреси и сл. Ваквите активности влијаат на ефикасноста на мрежата, го забавуваат системот а со тоа влијаат на целиот бизнис процес. Се класифицираат во четири главни категории: тројанци „Trojans“, софтвер „Adware“, Следење на колачиња „Tracking cookies“ и систем монитори „Sistem Monitors“.

- „Trojans“ – Тројански шпионски софтвер кој ги инфицира компјутерите во форма на тројански малвер;
- Adware“ – рекламен вирус, преставува еден вид на „досадни вируси“. Единствена работа на овие вируси е рекламирање на фирми и отварање на прозорци со реклами, и сето тоа без одобрение на корисникот. Тие работат на тој начин кога се поврзува корисникот на Интернет собираат адреси на фирми кои

[85] *Кенет К.Лаудон, Џејн П.Лаудон, Менаџмент информациски системи : Управување со дигитална компанија, Скопје:Арс Ламина, 2010 стр. 302.*
[86] *Mike McGuire, Samantha Dowling, Cyber crime: A review of the evidence, 2013, стр.5. pdf.*

најчесто даваат пари за ваков вид н огласување. Овие вируси ја менуваат и почетната страница на Интернет пребарувачот. Оваа група на вируси не е деструктивна, туку само смета на нормалната работа на корисникот;

- „Tracking cookies“ – следење на фајлови на хард дискот кои ги прати корисникот на интернет, ги снима вашите записи и поднесува извештај на креаторот;
- „Sistem Monitors“ – со цел да се следи секоја активност на компјутерот, да се фатат чуствителни податоци како што се посета на сајтови, пораки и многу повеќе.[87]

Постојат повеќе видови на софтвери за заштита на од овој тип на вируси, и тоа: Microsoft AntiSpyware, Spyware Doctor и сл.

Секоја голема компанија мора да ги превземе соодветните мерки за спречување на компјутерска шпионажа. Доколку постои "дупка" во начинот на обезбедување на податоците и истите бидат превземени, тогаш државата, со нејзините механизми превзема одредени мерки овие информации да бидат вратени онаму каде што припаѓаат, а сторителите да бидат казнети за делото.

❖

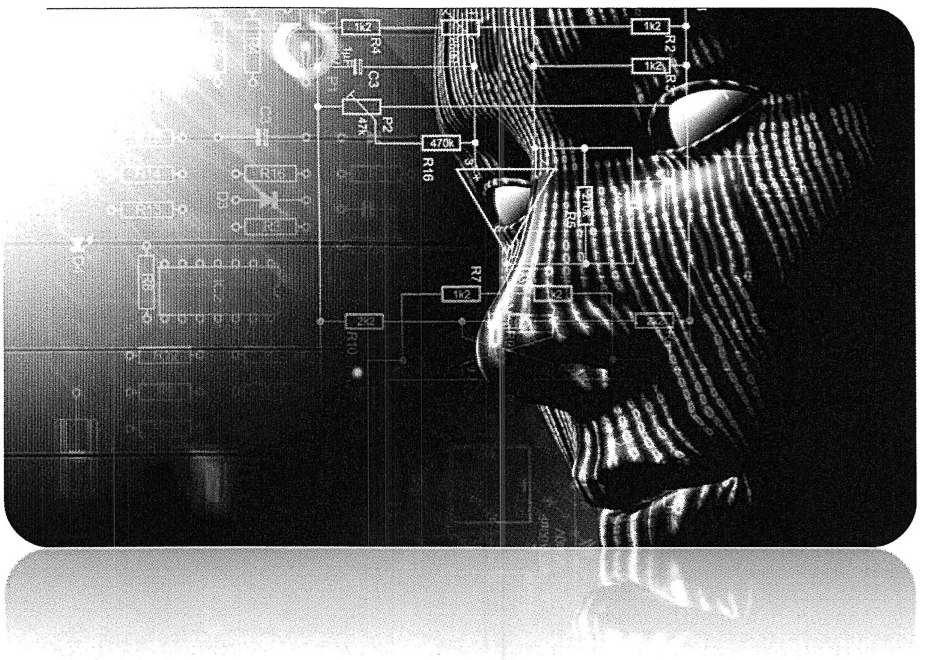
Компјутерската саботажа и компјутерската шпионажа директно ја напаѓаат глобалната економска положба на секоја држава. Така, секоја влада мора да изработи соодветни механизми за заштита на своите компании. Но, ниту една компанија не смее да се потпре само на механизмите обезбедени од државата, туку мора да вложи напори да ги заштити своите информации.

Мора да се сфати дека инвестицијата во безбедноста на информациите не е оптеретување за буџетот, туку овозможување на понатамошната работа, која ќе придонесе позитивни добитки од економски аспект, а со тоа и добро заштитени инфрастуктури кои се од витално значење за националната безбедност на современите држави. Поради тоа треба компјутерската

[87] http://usa.kaspersky.com/internet-security-center/threats/spyware#.Vs7Pp_krLDc (25.02.2016),

безбедност во сите институции а особено оние кои имаат бази, податоци, информации кои се од национален интерес да биде на највисоко ниво, да се вложуваат средства за обезбедување на инфрастуктурата, се со цел да се заштити од напади и да не се дозволи неовластено навлегување во компјутерските системи кое би предизвикало последици од големи размери.

1.9 ХАКЕРСТВО



Компјутерските криминалци или популарно наречени хакери се по правило лица со посебни стручни и практични знаења и вештини од доменот на високата информатичка технологија кои своите знаења ги користат за нанесување на штети на одредени заштитени системи. Хакерството како модерен феномен произлегува од техничкиот предизвик да се пробие заштитата на одреден информатички систем и да се навлезе во него. Колку е заштитата посилна толку е предизвикот поголем. Овие кривични дела се вршат прикриено без просторна поврзаност помеѓу сторителот и жртвата и по правило тешко се докажуваат т.е остануваат во темната бројка на криминалитетот. Честопати дури ни администраторите на мрежните системи не можат да приметат неовластено навлегување во системот од страна на хакер се додека системот не претрпи некоја штета

Во времето кога информатичката технологија беше во полн ек и милионските мрежи беа засегнати од информациите што ги содржеа, хакерите беа сметани за деца кои се желни да ја запознаат и истражат најновата технологија. Меѓутоа, денес тоа е веќе минато. Во време кога корпоративните системи изобилуваат со чувствителни и доверливи информации, банкарски податоци, хакерите се опишуваат како вистински махери желни за профит, а

нивните вештини се достапни на црниот пазар за оној што најмногу може да понуди, а дури се зборува дека зад најпрофитабилните и најисклучителните хакери стои руската мафија. Но каде се крие вистината? Кога хакерите престанаа да бидат оние добронамерни истражувачи што сакаат да научат нешто повеќе за системите и преминаа во криминалци? Дали хакерите воопшто некогаш имале невини намери? Можеби одговорот на ова прашање лежи во спознавањето на вистинската природа и психа на хакерот. А, тоа најдобро можат да го посведочат експертите, луѓето директно вклучени во тој бизнис и, се разбира самите хакери.

"Генетските" корени на се она што денес се нарекува хакерство може да се лоцираат во 60-тите 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 за да заштедат некој денар при телефонските повици, млади деца ги пробиваа телефонските системи. Ова хоби стана популарно и дури доби свое име: phone-phreaking. Набргу овие млади луѓе почнаа да „копаат" малку подлабоко во мрежите што ги поддржуваа телефонските системи. Тие беа заведени под називот „crackers" (кракери), затоа што научија како најдобро да го разберат системот разбивајќи го целосно и разгорувајќи ги неговите пропусти. Употребување 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.

Хакерстовото во основа објаснува како технички способни тинејџери можат да го доизменат или пробијат програмскиот код за да ги зајакнат неговите можности. Негативната конотација на овој поим датира од 80-тите години на 20 век кога медиумите го искористија овој термин да опишат некои компјутерски ентузијасти. Терминот се задржа и денес се користи како општ поим за нелегалните активности на сајбер-криминалците. Од надворешна страна, хакерите и нивните намери се карактеризираат како криминални. Компјутерската субкултура во која живеат прави суштинска разлика меѓу „лошите" хакери, кои имаат за цел да им наштетат на системите во кои навлегуваат, и „добрите" хакери (познати под името „етички хакери" – ethical hackers), кои можат да влезат во некој систем без намера да направат штета. Но терминот „хакер" се злоупотребува како дефиниција за некој кој нелегално провалува во компјутерски систем, независно од неговите чесни намери.

На почетокот суштината на хакерството беше во опседнатоста со техниката, а дефинитивно не во парите. Денес, ситуацијата е комплетно поразлична. Сеуште постојат опсесии, но исто така постојат закоравени криминалци и терористи кои се свесни колку навистина е значаен компјутерскиот систем на една компанија. Паричната придобивка сега е централна движечка сила која се крие зад многу од најактивните хакери на денешницата. Денес повеќето од хакерските операции имаат зли намери. Мноштвото вируси, црви и тројанци се направени од финансиска мотивација, а обидите се да се украдат информации, пари и ресурси од заразените компјутери.

Креаторот на вируси е многу поразличен вид од хакерот. Многу хакери го прават она што го прават за да докажат нешто, и тоа или самите на себе или на своите жртви. Но не се сите со пакосни намери. Но ова не важи за оние што создаваат вируси.

Вирусите можеби стануваат пософистицирани секоја година, но и полициската способност да се детектираат нивните креатори не заостанува зад нив. Сепак, се уште постојат креатори на вируси кои се недостапни за законот. Едно од тие лица е таканаречениот мрачен осветник (dark avenger), авторот на еден од првите полиморфни вируси. Овие зарази се менуваат со секое ново копирање и на тој начин многу тешко може да се детектираат. Мрачниот осветник никогаш досега не бил осуден.

Повеќето успешни хакери имаат манипуалтивни способности што ги користат да ја извлечат привилегираната информација што им е потребна. Во светот на хакерот, друштвеното уредување претставува збир од вештини што ги поседуваат сите докажани стручњаци. Се избегнува директен контакт со целта за сметка на комуникацијапреку телефон. Хакерот може да ја манипулира личноста на која и се јавува убедувајќи ја да ги открие влезните кодови и лозинки од својот компјутер.

Професионалците за обезбедување на системите често тврдат дека најслабите елементи во секоја мрежа не се хардверските компоненти, туку луѓето кои ги користат компјутерите.Не постојат печатени статистички податоци за напади со social engineering, но се додека луѓето не можат целосно да бидат отстранети од мрежата, хакерите ќе ги користат своите моќи

на убедување кон истите, за да ја разоткријат само информацијата која им е потребна за успешно да изведат еден хакерски напад.

Ако ја погледнеме историјата на хакерството, јасно можеме да видиме дека штом се развие некоја нова технологија таа станува привлечна за хакерската заедница. Професионалците за обезбедување на системи малку беа изненадени кога се појави првиот вирус за мобилни телефони во 2004 година. Црвот познат како cabir, ги зарази сите уреди што го користеа оперативниот систем Symbianos, кој прераснал во основа за многу мобилни телефони, особено на оние од Nokia. Значи, дали воопшто може да се навлезе во психата на хакерите и културата што тие ја создаваат? На индивидуално рамниште тие имаат многу разновидно потекло, но заедно делат слични способности. Исто така, затоа што компјутерите денес им се познати на луѓето, информациите за некој хакер не предизвикуваат страв како пред 15 години па затоа постојат се помалку јавни дискусии за културните аспекти на хакерството. Повеќето деца имаат свој личен компјутер, па дете со компјутер веќе не претставува аномалија. Истовремено, некои филмови го промовираат хакерскиот стил на живот како нешто привлечно кон кое треба да се тежнее и ги прикажуваат луѓето што можат да ги контролираат компјутерите како „кул-личности, затоа децата можат да добијат навистина конфузна претстава за хакерите". Оваа конфузна и комбинирана претстава може само да придонесе за овековечување на културата на хакерите и креаторите на вируси.

❖

Повеќето хакерски дејства што денес се изведуваат, не се претерано пакосни, но на секој хакер, кој пробива една мрежа само од забава, постојат уште други со малку алтруистички мотиви.

Подемот на организираните хакерски банди и он-лајн мафијата, која ги поддржува нивните активности е загрижувачки тренд. Кога вештините на хакерите се користат за негативни дејства, односно за злонамерни напади на системи на инфрастуктури од национален интерес, може директно да се влијае на националната безбедност на државата.

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. Се додека не сфатиме подобро зошто луѓето стануваат хакери и креатори на вируси, тие засекога ќе останат меѓу нас.[88]

[88] *Магистерски труд под наслов „Видови и облици на злоупотреба на Информатичката технологија" одбранет на 21.10.2009 година на Филозофскиот Факултет Св.Кирил и Методиј Скопје – Институт за одбранбени, безбедносни и мировни студии.*

1.9.1 БОТНЕТ МРЕЖИ

Примарната мотивација за навлегување во компјутерските системи (*Computer hacking)* се базира од чист вандализам и желба за идентификување внатре во т.н. „хакерски заедници", па се до стекнување на финансиска корист. Денес, голем број од нападите преку интернет е насочен кон искористување на поединци и разни организации поради финансиска заработка, што често резултира со големи финансиски губитоци и уништување на бизниси низ целиот свет.[89]

Истражувањата кои во 2006 година се спроведени од страна на FBI (*Federal bureau of investigation)* покажуваат дека Соединетите Американски Држави годишно трошат 67.2 милијарди долари во борбата против вируси, т.н.[90]

Spyware програми, компјутерски кражби и останати кривични дела поврзани со искористување на персоналните компјутери. Една од најголемите закани на интернет е постоење на огромен број на компромитирани компјутери. Мрежите од такви компјутери се нарекуваат *botnet* мрежи или „зомби армии", а компјутерите кои се нивен дел се присутни во домовите, училиштата, работните простори и владини објекти ширум светот. Главно, тие се наоѓаат под контрола на еден или неколку хакери т.н. *Botmaster* , а се употребуваат при извршување на разни видови на напади – од дистрибуирани напади за оневозможување на услуги (*Distributed denial-of-service,* Ddos), испраќање на непожелни пораки по електронска пошта, користење на алатки за снимање на притиснатите типки од тастатурата (анг. *Keylogger)* до ширење на вируси, *malware* програми и сл.

За разлика од другите типови на напади преку интернет, нападите од *Botnet* мрежите, кои воглавно се состојат од неколку илјади компјутери, потенцијално претставуваат голема компјутерска сила која потоа може да се искористи за различни напади на широко подрачје. Од тие причини, хакерите се посебно заинтересирани за искористување на *botnet* мрежите, а се со цел

---

[89] *Хрватска Академска и Истражувачка Мрежа – CARNet (Croatian Academic and Research network)http://www.cert.hr/* .

[90] http://www.cis.hr/dokumenti/botnetmreze.html

зголемување на нелегалната материјална корист. Истовремено,штетата која што може да се предизвика со употреба на такви мрежи, е неспоредливо поголема од штетата направена со традиционални, дискретни напади.

Интересно е дека, дури од неодамна почна да се чуствуваат заканите предизвикани со појавувањето на *botnet* мрежите. Односно, целокупната интернет заедница, законодавните тела, индивидуалните корисници како и големите компании, наголемо водат расправи за можноста за спротивставување на овој проблем, кој како што може да се заклучи денес е една од најголемите (ако не и најголема) безбедносна закана на интернет заедницата.

Инаку, ботнет мрежата се состои од низа на поврзани компјутери, кои меѓусебно соработуваат и со кои управува еден хакер или помала група. Бот претставува крајниот компјутер (или сервер), кој што претставува член на ботнет мрежата. Исто така, овој термин се употребува и за злонамерно обликувани извршни датотеки, кои служат за стекнување на контрола над компјутерот и негово приклучување кон ботнет мрежата.

Прва појава на ботнет мрежа е забележана во 1999 година, а истата била поврзана со употреба на црвот *prettypark.* Оваа мрежа овозможувала спојување на оддалечени irc (*Internet relay chat)* сервери, со цел стекнување на основни податоци за системот, кориснички лозинки, mail адреси, надимци и сл. Меѓутоа, ограничените можности со кои располагал *prettypark* црвот не бил толку штетен за интернет заедницата како неговите следбеници.

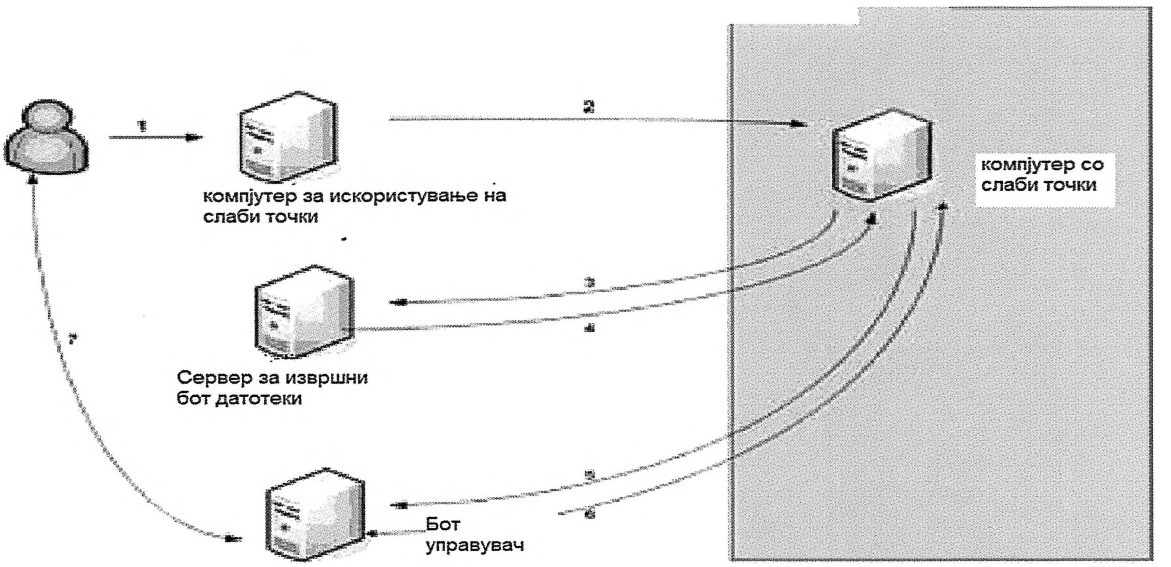
Едни од најпознатите ботови се *agobot* и *sdbot.* Со нивната појава, се зголемуваат можностите кои што ги нудеа нивните претходници. Моменталната генерација на ботнет мрежи, интегрира комплексни состави за управување и контрола (анг. *Command and control, c&c)* со многу моќни алатки. Тие се пренесуваат како црви, се кријат како вируси и можат да извршат големи и координирани напади. Меѓусебно комуницираат со користење на irc, http (Hypertext transfer protocol), p2p (*Peer-to-peer)* како и други канали.

Притоа, може да се констатира дека не постои голема разлика помеѓу црвите, вирусите и ботнет мрежите. Главната разлика помеѓу нив е таа што ботовите имаат посебно вградени механизми кои на нивните сопственици им

овозможуваат контрола над цела низа на оддалечени компјутери и координација помеѓу нив. Од тука се заклучува дека ботовите всушност се само напредни видови на црви и вируси.

Следниот приказ претставува вообичаен тек на ботнет напад кој се состои од седум чекори, и тоа:

- Прв чекор: хакерот кој што го контролира компјутерот во ботнет мрежата (анг. *Bot herder)* го вчитува кодот за напад на компјутерот кој се употребува за напад;
- Втор чекор: компјутерот кој се употребува за напад ги бара слабите точки и го извршува нападот. Компјутерито кои што немаат соодветна заштита од одредени безбедности проблеми, претставуваат жртви на нападот;
- Трет и четврт чекор: на компјутерот жртва му се праќа наредба за превземање на извршни датотеки од одреден сервер (најчесто од компромитиран ftp (*File transfer protocol)* сервер);
- Петти чекор: превземените извршни датотеки се активираат на компјутерот жртва претварајќи го на тој начин во бот. По ова, новорегрутираниот бот се поврзува со одреден централен компјутер и „се пријавува на должност";
- Шести чекор: централниот компјутер (кој што ги надгледува ботовите) му дава упатства на нападнатиот компјутер на пр.упатство за превземање на нови единици, кражба на личните податоци на корисникот на компјутерот, инсталација на *spyware* програми, напад на други компјутери и сл;
- Седми чекор: *bot herder*-от ги контролира сите бот компјутери со издавање на наредби преку централниот компјутер (бот управувач).



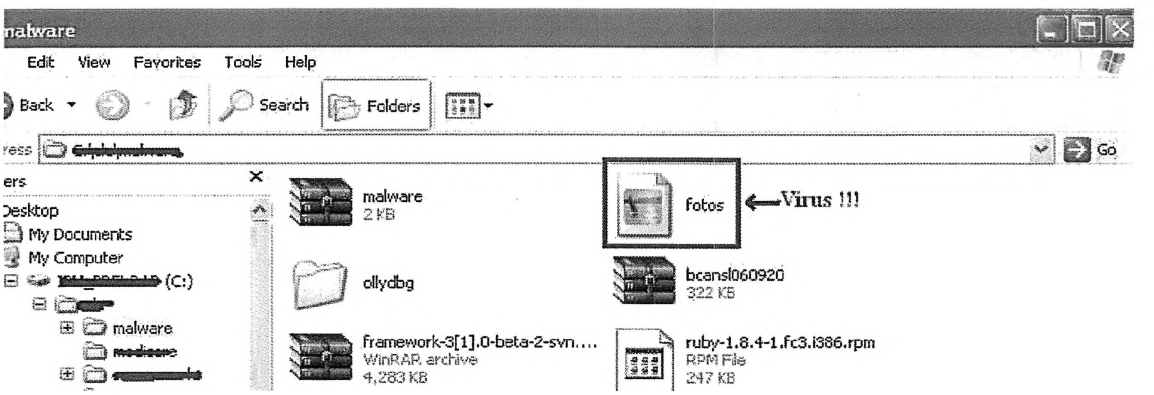
Шема:Вообичаен тек на ботнет напад

Зависно од целта на нападот и употребените алатки, може да се идентификуваат различни однесувања на ботнет мрежата. Исто така, ако се вложи повеќе труд во разбирањето на нивното офанзивно (напаѓачко) однесување, од добиените информации може да се изведат важни заклучоци за природата на мрежата, целта која што нивните корисници се обидуваат да ја остварат, па дури и податоци за потеклото на хакерот. Офанзивното однесување на ботнет мрежите се манифестира во четири различни видови, и тоа:

- Ширење зараза врз други компјутери;
- Кражба на осетливи информации;
- Испраќање на несакана електронска пошта; и
- Дистрибуирани напади за оневозможување на услуги.

Ширење зараза врз други компјутери. Ботнет мрежите често шират зараза врз други компјутери на ист начин како што го прават другите *malware* програми (црви и вируси). За таа цел, често се користат принципите на социјалниот инжинеринг и испраќање на злонамерно формулирани пораки по пат на електронска пошта. Со овие методи се наведува корисникот да ги активира испратените датотеки, што доведува до компромитација на компјутерот. Пораката испратена по пат на електронска пошта, формулирана е

на тој начин што ќе има привлечен наслов на пр.„интересна фотографија“, „мораш да ја погледнеш оваа фотографија“ и сл, а истовремено содржи одреден скриен софтвер кој што изгледа како jpg (фотографија) датотека, кој што *windows explorer*-от ја прикажува како датотека без .exe екстензија. Корисникот, кој што не се сомнева во содржината на датотеката, лесно ја отвора активирајќи ја на тој начин скриената содржина, што има за последица ширење на зараза на неговиот компјутер.



Пример за злонамерно формулирани пораки

Друг, често користен начина на ширење на зараза е искористување на слабите точки од далечина. Бот програмите ја пребаруваат мрежата и пронаоѓаат компјутери со слаби точки притоа активно искористувајќи ги нивните слабости. За да го постигне ова, секој бот ја пребарува сопствената подмрежа, пронаоѓајќи вклучени компјутери кои што ги тестира на нивните слаби точки. Ако се пронајде таков компјутер, се лансира напад и доаѓа до компромитирање на ранливиот компјутер.

Кражба на осетливи информации.

Поновите ботнет мрежи користат софистицирани алатки за кражба на осетливи податоци од заразените компјутери. Најчесто користени алатки за оваа цел се *keylogger* алатките и т.н. прислушкувачи на мрежниот сообраќај (анг. *Network traffic sniffers).* ***Keylogger*** алатките го модифицираат составот на заразениот компјутер, така што тој ги следи сите активности на корисникот и ги забележува сите притискања на типките од тастатурата, додека **прислушкувачите на мрежниот сообраќај** го следат целиот сообраќај испратен преку подмрежата на заразениот компјутер. Ваквите алатки ги бележат и систематизираат сите добиени осетливи информации, кои потоа ги испраќаат кон своите сопственици, односно *botmaster*-и користејќи разни комуникациски канали.

Испраќање на несакана електронска пошта

Ботнет мрежите често се употребуваат за испраќање на несакани пораки по пат на електронска пошта, од различни причини. Главните предности при користење на бот мрежите за оваа цел се тие што корисниците не можат да го откријат изворот од кој се испраќаат пораките, како и фактот што ботнет мрежите можат да испратат поголема количина на електронска пошта. Како што веќе споменавме, одредени пораки се користат за дистрибуција на скриени софтвери, други за наведување на корисниците да посетат злонамерно обликувани *web* страни при што доаѓа до инсталирање на разни *malware* програми на нивните компјутери. Таквите *web* страни се користат за различни цели, (на пример за рекламирање на нелегална трговија и сл). Други пак се употребуваат за вршење на напад за кражба на идентитет и личните податоци на корисникот итн.

Дистрибуирани напади за оневозможување на услуги

Дистрибуираните напади на оневозможување на услуги *(ddos)* е еден од најстарите механизми кои ги користат ботнет мрежите. Во почетната фаза од

развојот, хакерите ги користеа ботнет мрежите за лансирање на напади на одреден број на големи организации, со цел исцрпување на сите достапни процесни ресурси и завземање на комуникацискиот канал, што има за последица успорување или потполно оневозможување на нивните услуги. Често пати, овие напади се користат и за уцена на давателот на услугите, кој што за одредена надокнада на сопствениците на ботнет мрежите се ослободуваат од овие напади.

Евидентно е подобрувањето и развојот на ботнет мрежите. Новите мрежи не само што успеваат да ги измамат антивирусните av алатки и ids (Intrusion detection systems) системи, туку успешно ги заобиколуваат и системите за следење на аномалии во податоците. Постојат различни техники кои ботнет мрежите ги користат за заобиколување на av и ids системите базирани на потписи. Ваквите техники го зголемуваат животниот век на ботнет мрежите и овозможуваат поголем успех при компромитација на нови компјутери.

Ако на компјутерот е извршен напад за оневозможување на услуги, постојат малку начини за ефикасна заштита. Бидејќи компјутерите вклучени во ботнет мрежата се географски оддалечени и распрскани, тешко е да се открие точниот идентитет на напаѓачот. Еден од начините на заштита е т.н.пасивна детекција на оперативниот систем (анг.*Passive os fingerprinting)* при што администраторите може да ги конфигурираат *firewall*-ите на мрежата така што тие превземаат нови акции при ботнет нападот и тоа акции базирани врз информациите за оперативниот систем на компјутерите од кои што се врши нападот. Исто така, структурата на централно управуваните ботнет сервери има вродени недостатоци и проблеми. Односно ако дојде до откривање на еден сервер на ботнет каналот, често доаѓа и до откривање на останатите сервери. Неповрзаноста на едниот сервер може да предизвика паѓање на целата ботнет мрежа.

Некои сигурносни компании (*symantec, trend micro, fireeye, simplicita* i *damballa)* објавиа разни решенија за спречување и запирање на ботнет мрежите, при шти тие се разликуваат кај малите корисници и големите

корпорации. Малите корисници, како мерки на превенција можа да го превземат следното:

- Користење на надградени антивирусни и *anti-spyware* програми;
- Користење на надградени оперативни системи и нивни најнови update;
- Користење на локален firewall, со следење на неговите аларми;
- Пријавување на невообичаено однесување;
- Избегнување на посета на сомнителни web страни;
- Избегнување на отворање на сомнителни содржини на електронска пошта;
- Избегнување на инсталација на програми и алатки превземени од несигурни извори;

За разлика од нив, големите корпорации можат и треба да го сторат следното:

- Изработка/набавка на соодветни заштитни механизми со соодветно поставување на делокругот на нивното дејство;
- Блокирање на воспоставените излезни врски преку приклучокот 6667, доколку не им е потребна irc комуникацијата; и
- Редовно следење на ids и ips системите, со цел откривање на аномалии во остварениот сообраќај.[91]

❖

Од гореизнесеното, очигледно е дека ботнет мрежите претставуваат се поголема опасност за компјутерската сигурност, а со самото тоа и употребата на компјутерите. Иако нивното присуство не е нова појава, секојдневно тие се надградуваат со нови програмски алатки и нови идеи што ги прават поопасни,

[91] http://www.cert.hr/ Botnet Mreze.pdf (CCERT-PUBDOC-2007-12-213) .

за што е потребно вложување на дополнителни напори за сочинување на противмерки и осмислување на начин за нивна детекција и одстранување. Од расположливите информации, јасно се гледа целта за користење на ботнет мрежите, а тоа е се поголемата финансиска добивка. Со оглед на ова, на корисниците на компјутери, посебно на стручните лица во големите корпорации, од примарен интерес би требало да им биде откривањето на нови техники на заштита. Ваквиот пристап, секако на нив им носи поголеми заработки и помали финансиски загуби.[92]

Исто така со безбеден компјутерски ситем, самите Влади, корпорации, и големи бизнис заедници, стекнуваат позитивен имиџ во јавноста, а со тоа и поголем финансиски бенифит како и имиџ на сигурна безбедносна средина. Ботнетот, како и другите видови и облици на високотехнолошкиот криминал, е сериозна закана на националната безбедност на соврмените држави, поради тоа што со нивна употреба може да се дојде до многу информации и податоци од државен, безбедносен, воен карактер, кој доколку се употребат директно се наштетува на самата држава.

[92] *Магистерски труд под наслов „Видови и облици на злоупотреба на Информатичката технологија" одбранет на 21.10.2009 година на Филозофскиот Факултет Св.Кирил и Методиј Скопје – Институт за одбранбени, безбедносни и мировни студии.*

2. НЕАВТОРИЗИРАНА РЕПРОДУКЦИЈА НА КОМПЈУТЕРСКИ ПРОГРАМИ (СОФТВЕРСКА ПИРАТЕРИЈА)

Софтверот е една од највредните технологии во информатичкото време, која покренува се, од компјутер до интернет. За жал затоа што софтверот е толку вреден и затоа што е многу лесно за кратко време на компјутерот да направиш точна копија на оригиналот, софтверската пиратерија е широко распростанета. Терминот „софтверска пиратерија" покрива различни активности: нелегално копирање програми, фалсификување и дистрибуција на софтвер, како и размена на програми.

Загрижува големиот процент на пиратеријата при што, според податоците односот пиратеријата и оригиналот изнесува околу 20:1.

Пиратеријата ја вршат поединци и организации, па и многу држави не успеваат да одолеат на предизвикот за бесплатно користење на програми посебно на ,,полн хард диск,, софтвер и програми.[93]

Од индивидуални корисници на компјутери до професионалци кои се занимаваат со големопродажба на украдени софтвери, пиратеријата постои и во домовите, работните околини и сл. Софтверските пирати не само што крадат од компаниите кои произведуваат софтвер, туку и нанесуваат штета на корисниците, го намалуваат фондот за истражување и развој на нови софтвери. Со почитување на законските прописи, не само што се намали софтверската пиратерија, туку би се спречила појавата на поголеми економски проблеми. Тоа што на дискот стои „microsoft" лого или пишува дека софтверот е оригинално инсталиран на компјутерот, не значи дека тој е легален.

Едноставно кажано, софтверското пиратство претставува нелегално производство и користење на софтверски производи со прекршување на авторските копирачки права.

Покрај програмскиот софтвер, кој што ги опфаќа компјутерските програми и софтвертските производи, цел на софтверското пиратство вклучува и други дела издадени во електронска форма, како што се на пример:

---

[93] *Саша Здравковиќ, Патентна заштита за софтвер у Србији, Завод за заштиту интелектуалне својине, Београд, 2010, стр 72.*

- ДВД
- Видео игри
- Компјутерски фонтови
- Музички цд-а и др.

Постојат повеќе видови на софтверско пиратство.

Најкарактеристични се:

➢ **интернет пиратство.** Овој вид на софтверско пиратство претставува електронски трансфер на софтверски производи со заштитени авторски права. BSA (Buisness Software Alliance) , асоцијација за софтверска индустрија, оценила дека постојат околу 80 000 интернет страници кои продаваат нелегален софтвер а 90% од софтверот продаван преку интернет е фалсификат. Потрошувачите не можат да си ги повратат парите откако ќе откријат дека купениот софтвер е фалсификат, а голем дел од нив воопшто не ги добиваат порачаните производи.

➢ **фалсификување.** Фалсификувањето претставува производство и продажба на софтверски производи кои личат на оригиналите. Бидејќи вложувањата во производство на ваков вид на софтвер се мали, се продава по ниски цени.

➢ **случајно пиратство.** Случајното пиратство претставува намерно или ненамерно делење на софтвер меѓу корисниците. Според проценките со овој вид на пиратство се остваруваат околу 50% од економските загуби. **Рентање.** Рентањето претставува привремено изнајмување на софтверски производ без дозвола на авторот. (на пример изнајмување на двд-а).

Во една од студиите направена од BSA (Buisness software alliance) од 2000 година, која се однесува за застапеноста на пиратството во светски размери, утврдено е дека во Азија и Источноевропските земји пиратството е застапено со најголем процент. Процентот на застапеност на пиратството е најмал во економски поразвиените земји, од причина што можат повеќе да инвестираат во борбата против продавачите на пиратски софтвер. Проценето е дека дневно се продаваат околу 40 000 софтверски производи кои не се оригинали. Во Европа и Азија можат да се најдат огромни маркети во кои се

продава исклучиво пиратски софтвер. Во Велика Британија пиратството се поистоветува со организиран криминал, бидејќи во многу случаи парите заработени со продавањето на пиратски софтвер се користат за трговија со дрога, проституција и други незаконски активности.

Софтверот е заштитен со Закон уште од самиот момент на негово создавање. Со законот им се дава ексклузивни права само на произведувачите на софтверот да ги размножуваат своите софтверски производи и да го дистрибуираат размножениот материјал. На корисниците на софтверот им е дозволено да го копираат купениот софтвер само на еден компјутер и да направат само една копија за архивски цели. Не им е дозволено ниту на студентите да копираат софтвер наменет за едукативни цели и да го делат на своите колеги, без дозвола на издавачот. Забрането е делење и на текстуални или други податоци симнати од web sajt, ако на него е означено дека е заштитен. Во САД производството на 10 или повеќе копии од некој софтверски продукт во рок од шест месеци со вредност од 2500$, се казнува со затворска казна од 6 месеци, или парична казна од 250 000$.

Софтверското пиратство има штетно влијание како на производителите на софтверот, така и на неговите корисници во однос на производителите тоа се однесува на следново:

- нивната сопственост и "животно дело" се користи без нивна дозвола и без никаква компензација за тоа;
- неможност за утврдување на точниот број на продадени примероци, што често доведува до погрешна проценка за квалитетот на софтверот, обесхрабрувајќи ги притоа за производство на подобар софтвер;
- малата заработувачка ги истиснува помалите компанија надвор од бизнис но и потешко опстанување на нови производители. Можен начин производителот да се заштити од пиратството е кога купувачот го купува цд-ром-от да добие код за пристап до програмот. Флопи дисковите можат да се заштитат со постоење на можност за копирање само од оригиналите, а не и од копија на копија. Резултатот е потешко производство на пиратски софтвер.

Штетите во однос на корисниците се:

- можност за пренесување на компјутерски вируси кои можат да предизвикат делумна или целосна загуба на податоците;
- немање на адекватна документација за комплетните можности на софтверскиот пакет;
- немање на техничка подршка од производителот на софтверот;
- немање на можност за надоградување на софтверскиот продукт, што обично е поефтино од купување на негова нова верзија.

За да се заштити секој корисник од купување на пиратски софтвер, корисно е да ги знае следниве совети:

- „изворот" на софтверот да биде познат;
- да купува софтвер исклучиво од авторизирани дистрибутери, или пак од продавач на софтвер со добра репутација. Ако не е сигурен за статусот на дистрибутерот директно нека контактира со издавачот на софтверот;
- ако некој му понуди софтвер со цена многу пониска од цената по која продаваат авторизираните продавачи, логично е да се запраша за неговата оригиналност.

Да се биде авторизиран продавач на софтвер има многу предности.

На нив им е овозможен пристап до креаторите и сопствениците на софтверот, имаат право да го рекламираат софтверот што го продаваат, и да им ги гарантираат на своите потрошувачи сервис.[94]

❖

Последиците од користењето на софтверската приратерија се различни, спречуваат корисниците да добијат високо квалитетна техничка подршка и производ со надградби, се намалува можноста за работа, се намалува

[94] *Магистерски труд под наслов „Видови и облици на злоупотреба на Информатичката технологија" одбранет на 21.10.2009 година на Филозофскиот Факултет Св.Кирил и Методиј Скопје – Институт за одбранбени, безбедносни и мировни студии.*

финансирање на тековните напори за разој, а како една од најголемите последици е со самото користење на нелегални копии на софтвер истите може да содржат грешки или вируси, и истите да бидат користени во различни области, односно со нивна помош да се дојде до класифицирани информации, доверливи информации, а со тоа да се влијае на националната безбедност на секоја држава.

3. ИСТОРИСКИ ОСВРТ НА ВИСОКОТЕХНОЛОШКИОТ КРИМИНАЛ

Се е почнато така неодамна во 1969 година кога за првпат повеќе компјутери биле поврзани во единствена компјутерска мрежа. Интернетот, тогаш познат како ARPAnet, зачнат е со иницијална конекција со четири главни компјутери со Универзитетите од југозапад САД (University of California, UCLA – Los Angeles, Stanford Research Institute, SRI, University of California, UCSB – Santa Barbara, University of Utah – Salt Lake City). Предисторијата на овој настан го опфаќа пронаоѓањето на адекватен одговор од заканата за потенцијален нуклеарен напад.

Според тоа, ARPAnet бил дизајниран да овозможи комуникација и во услови на нуклеарен напад и ако една или повеќе мрежни локации бидат уништени. Понатаму, развојот на Интернетот е започнат како проект на Американското Министерство за одбрана за креирање на националната компјутерска мрежа која би продолжила да функционира во можно пост-апокалиптично време, дури и ако нејзиниот поголем дел биде уништен во нуклеарна војна или природна катастрофа.[95]

Сеуште неможе да се најде единствен став за точноста на почетоците на високотехнолошкиот криминал. Најчесто се поврзува со самата појава на компјутерот и неговото користење. Поголемиот дел на мислења се дека датира од раните шеесети на минатиот век, и во текот на наредните години со се поголемта примена на компјутерот во секојдневниот живот, државите увиделе колку е голема опасноста од новиот вид на криминал.

Професорот Susan W. Brenner потеклото на високотехнолошкиот криминал го дели во две фази, и тоа првата до 1990-тите кога компјутерите постануваат се пософистицирани, и втората фаза е од 1990-тите до денес.

Полесно би можеле да го поделиме пред појавата на интернетот, и после појавата на интернетот. Кога компјутерот не е поврзан на мрежа, злоупотребата на истиот е невозможна, и штетите се 0%.

---

[95] *Slobodan R. Petrović „ Kompjuterski criminal" Vojnoizdavački zavod, Beograd 2004, III izdanje, str. 66–73.pdf*

Денес има над два билиони корисници на интернет. Во Северна Америка 78,6%, во Австралија 67,6%, во Европа 63,2%, во Средниот Исток 40,2%, во Азија 27,5%, во Африка 15,6%.[96]

Со се поголемото користење на интернет се зголемуваат и злоупотребите на високотехнолошкиот криминал, користењето на високата технологија за извршување на криминални активности при што се нанесува огромна штета на населението. Интернетот по својот дизајн е ранлива мрежа. Но неговата предност е брза и интерактивна комуникација, која претходно недостасувала, и не ја нудел ниеден друг медиум.

Почетоците на кривични дела поврзани со високотехнолошки криминал се забележани од 1960 година, со физички оштетувања на компјутерски системи и цубверзија на телефонски мрежи. Исто така во 1960 година за прв пат се сретнува зборот „hack" кој бил употребен во група за правење на модели за возови на МИТ, во врска со начинот на манипулирање со моделите на возови.

Во 1970 година се појавуваат „phreaks" телефонски криминалци, кои провалиле во телефонски централи и украле бесплатни телефонски повици. Најпознат криминалец од оваа област е John Draper, кој што е и креатор на „blue box" – електронска направа која произведува звуци со бранова должина и со кои се остваруваат бесплатни телефонски повици.

Во 1983 година е снимен филмот „War Games" кој всушност преставува инспирација за голем број на луѓе да станат хакери.

До средината на 1990-тите измамите со платежни картички е брзо растечки проблем за полицијата. Извештајот на ФБИ во 1970 година бил дека загубите од платежни картички низ целиот свет се 110 милиони Американски долари, а во 1980 година 1,63 милијарди Американски долари. Полицијата

[96] *http://www.thecultureist.com/2013/05/09/how-many-people-use-the-internet-more-than-2-billion-infographic/ (03.04.2016).*

постојано се соочува со нови методологии на злоупотреба на платежни картички.

Крајот на 1990-тите и почетокот на 2000 година, измамите со платежни картички преоѓаат во кражби на идентитет, односно најчесто организирани групи крадат податоци од платежни акртички, финансиски сметки, при што иницираат банкарски заеми односно кредити, купуваат автомобили со податоци и парични средства од други луѓе, при што се предизвикува хаос во финансискиот систем, а оштетени се невини жртви.

Во Февруари 1998 година од страна на Судот во Њујорк, Владимир Левин е осуден на три години затвор. Тој бил водач на Руска хакерска група која успеала да изврши компјутерска кражба вредна 10 милиони долари. Левин во 1994 година организирал заговор и илегално пренел 12 милиони Американски долари од „CitiBank" и ги префрлил на голем број меѓународни банкарски сметки. Откако Банката приметила дека и недостасуваат пари, ги контактирала ФБИ кои координирано со Интерпол, успеале да го уапсаат организаторот на оваа криминална група.

Кевин Митник е еден од најдобрите хакери на сите времиња. Тој е уапсен во 1995 година, и добива осум години затвор, поради кражба на 20.000 податоци од платежни картички, упад и неовластено користење на компјутерски системи во САД. По излежување на затворската казна, тој почнува да се занимава со компјутерска безбедност, и станал основач на фирмата која се занимава токму со компјутерска безбедност „Defensive Thinking"во Лос Анџелес.

До средината на 2000-тите тројанците беа познати алатки за индустриска шпионажа. Според експертите, најголема безбедносна ранливост со која се соочуваат компјутерските корисници, мрежи, е-мејлови е скриениот вирус „Тројански Коњ", кој се маскира како бенигна апликација, и обезбедува пат до внатрешната мрежа преку која напаѓачите можат да ја уништат, да украдат информации и сл.

Во текот на 2007 година „спам“ пораките (несакани пораки) се зголемија експлозивно. Според тогашните проценки околу 88% од сите добиени е-мејлови во интернет сообраќајот биле спам пораки. Во овој момент спам пораките се едни од најголемите измами кои предизвикуваат лажно изнудување парични средства на жртвите, како и „phishing“.

Во текот на 2000-тите се случуваа блокирања на DNS адреси, DOS напади на најпопуларните интернет страни како што се Amazon, E-Bay, хакирања на многу корисници на е-мејлот Yahoo и сл.[97]

Компјутерскиот простор е нова средина за кривични дела. Денес тој е еден од најголемите правни граници. Од 2000 до 2008 година интернетот се прошири со просечна стапка од 305% на глобално ниво, а во моментов 1,46 милијарди луѓе се на интернет.

❖

Во одреден момент во историјата, одредени работи стануваат актуелни. Денес може да се каже дека организираниот криминал стана составен дел на високотехнолошкиот криминал и обратно. Најголемите криминални организации го користат високотехнолошкиот криминал за извршување на криминалните активности (меѓународната трговија со дрога, оружје, органи). Исто така напредокот во технологијата стана вистински проблем во војувањето. **Терористичките групи најмногу се потпираат на високата технологија во планирање и извршување на терористичките акти.**

Како што се шири интернетот, глобалната комуникациска мрежа, така треба Владите, Приватниот Сектор, поединците да ја зголемат соработката и

[97] *A Brief History of Computer Crime:An Introduction for Students, M. E. Kabay, PhD, CISSP-ISSMP.pdf*

спремноста за да се спротиставата на армијата од компјутерски криминалци од секој вид. Како што се развива технологијата, така се развива и техниката за заштита од напади, но со уште поголема брзина се развиваат нови техники и методи за напади и злоупотреба на информации.

4. ВИСОКОТЕХНОЛОШКИОТ КРИМИНАЛ ВО ОДНОС НА КЛАСИЧНИТЕ ВИДОВИ НА КРИМИНАЛ

Високотехнолошкиот криминал е брзо растечки вид на криминал,кој ги опфаќа кривичните дела извршени преку интернет или преку други форми на компјутерска технологија. Лицата кои се занимаваат со вршење на овие кривични дела се повеќе и повеќе ја искористуваат брзината, практичноста, достапноста и анонимноста на интернетот и компјутерската технологија за вршење на различни видови на кривични дела од областа на високотехнолошкиот криминал. Карактеристично за оваа криминална област е тоа што високотехнолошкиот криминал не познава граници, било физичка или виртуелна, предизвикуваат сериозни повреди и претставуваат многу реални закани во целиот свет.

Во поново време неможе веќе да се замисли дејствување на организирана криминална група која не ги користи услугите на компјутерските криминалци било да е при сторување на кривичните дела, остварувањето на меѓусебна комуникација користејќи сретства за глобална комуникација (социјални мрежи, разговори преку интернет каналите и сл.) за полесно прикривање на нивните активности и отежнување на истражните органи при обезбедување на докази за кривична постапка.

Бројот на компјутерски напади во светот на годишно ниво се проценува на околу 1,5 милиони напади, што значи дека на секоја минута на глобално ниво се случуваат приближно по три компјутерски напади.[98]

Загубите од високотехнолошкиот криминал на глобално ниво на светската економија се проценува на околу 445 милијарди долари годишно, а додека штетата на поединци предизвикана од хакерски напади изнесува околу 160 милијарди долари годишно.[99]

---

[98] http://www.cbs.com/shows/csi-cyber/news/1003888/these-cybercrime-statistics-will-make-you-think-twice-about-your-password-where-s-the-csi-cyber-team-when-you-need-them-/ (17.04.2016).

[99] http://www.mcafee.com/jp/resources/reports/rp-economic-impact-cybercrime2.pdf (17.04.2016).

Високотехнолошкиот криминал се повеќе се претвора во индустрија со „добавувачи, пазари, даватели на услуги („високотехнолошкиот криминал како услуга"), финансирање, системи на трговија и пролиферација на бизнис модели. Развојот на оваа „индустрија" се повеќе ја подржува употребата на крипто валутите како **Биткоин** и заштитата што ја имаат лицата кои што ги вршат овие кривични дела од технологиите за прикривање на активностите на интернет (во прв ред Тор).

БИТКОИНОТ се појавил во 2009 година како програм со отворен код. Тој е дигитална валута која уште се нарекува и виртуелна валута или пак електронски пари и криптовалута пред се поради криптографијата која се користи при создавање и трансферот. Тој е првото децентрализирано плаќање P2P (peer to peer). Биткоинот не е контролиран од ниту еден ентитет, како Централна Банка и поради тоа се нарекува децентрализирана валута. Биткоинот се користи за он лајн плаќања, корисниците испраќаат и примаат биткоини преку софтверска апликација наречена „паричник" која може да се користи на компјутер, мобилен уред или како веб-апликација. Тие може да се стекнат во замена за продукти, сервиси или други валути.

Користењето на Биткоинот за плаќање на сервиси и услуги е во постојан пораст, како и неговата цена која во моментов изнесува 427.06 Американски долари, и истата постојано се менува а интересно е што секогаш е во нагорна линија.

Голема предност е и неговата анонимност, односно корисниците не се идентификуваат по име. Трансакциите се прават само преку приватен клуч и лозинка. Нема граници, нема ограничувања, а трошоците се ниски.

Покрај тоа постојат услуги да им помогнат на трговците во обработка на трансакциите, конвертирање на Биткоинот во легална валута, и депонирање на средствата директно на банкарски сметки. Предност е што сите овие услуги се поефтини од трансакции со платежни картички и сл.[100]

---

[100] *Ronald A. Glantz, Pantera, 2014, стр.2. pdf.*

Од 2014 година економистите не се сложуваат до кој степен Биткоин преставува пари, но тоа не спречува тој да се користи како пари. Од крајот на 2013 година бројот на продавници кои примаат биткоини како средство за плаќање драстично се зголемува, постојат над 35000 онлајн продавници и над 1000 продавници. Биткоин е се популарен во земји со проблематични национални валути, бидејќи може да ја намали инфлацијата, како и контролите на капиталот и санкциите.

Меѓутоа биткоин се користи за да се исперат нелегално стекнатите пари во легални пари, односно повеќето криминалци особено кои извршуваат кривични дела од областа на високотехнолошкиот криминал (хакирање на веб сајтови, навлегување во банкарски сметки, злоупотреба на платежни картички) се стекнуваат со поголема сума на пари и за да ги подигнат тие пари а да не бидат откриени од страна на надлежните институции, истите тие криминалци со овие парични средства купуваат биткоини, кои подоцна ги менуваат во легални валути и ги подигаат и ги пуштаат во легален промет, со што се стекнуваат со противправна имотна корист.

Исто така со биткоин тргуваат на „црни страни" каде може да купат најразлични производи, да добијат најразлични услуги, се користи за купување на нелегално оружје, дрога, податоци од банкарски сметки, платежни картички, лекови кои неможат да се добијат без лекарски рецепт во слободна продажба, и други производи кои или се нелегални и забранети, или се украдени.

❖

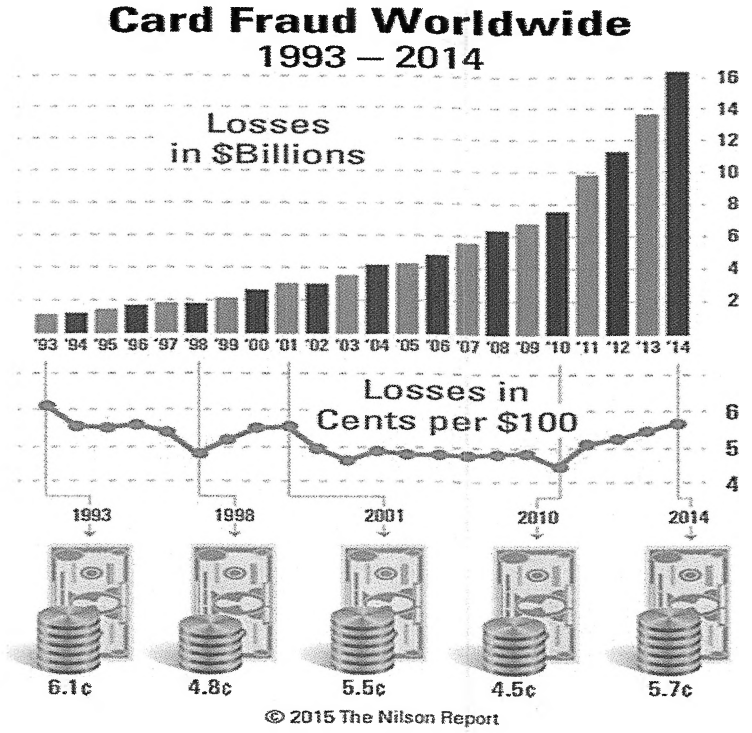
Ова говори и укажува дека трговијата со биткоин има повеќе негативни страни отколку позитивни. А ризикот е се поголем затоа што се зголемува бројот на земји кои оваа виртуелна валута со закон ја легализираат, а со тоа е се потешко да се следи патот на црниот бизнис со биткоин и се потешко ќе им биде на истражителите да дојдат до крајниот корисник, односно до криминалецот.

Притоа онлајн форумите претставуваат место каде што може да се најде се поврзано со компјутерски напади, од видеа со учење како да се направи напад, како да се направи бомба, алатки кои може да се користат при напади до податоци за потенцијални жртви, пробивање на банкарски сметки, злоупотреба на платежни картички и сл.

Развојот на технологијата, достапноста на интернетот и се поголемата употреба на плаќањата преку интернет влијае на криминалците да го насочат своето дејствување на интернет. Лесниот начин на видео стриминг (гледање во живо преку интернет) им овозможува на криминалците од растојание, директно (во живо) продукција на материјали со злоупотреба на деца преку видео камерите. Пристапот и се поголемата експанзија на користењето на социјалните мрежи претставува лесен начин за пронаоѓање на потенцијални жртви.

Употребата на платежните картички како едно од основните средства за плаќање е во постојан пораст, а со тоа и злоупотребите на платежните картички на глобално ниво се во пораст. Загубите предизвикани од трансакции со лажни платежни картички на светско ниво во 2014 година достигна 16,31 билиони долари. Забележан е постојан пораст на загубите од ваквите трансакции.[101]

[101] *https://www.nilsonreport.com/publication_chart_and_graphs_archive.php (17.04.2016).*



Во Европа во 2013 година загубите од трансакции со фалсификувани платежни картички на ниво на Единствена Европска Евро Област (SEPA)[102] изнесуваа 1.44 билиони евра, што е зголемување од 8 % во однос на 2012 година.

Во 2013 година во СЕПА 66 % од вкупната вредност на плаќања со фалсификувани платежни картички отпаѓаат на плаќања преку интернет или телефон, 20 % на плаќања на ПОС терминали на продажни места и 14 % на трансакции на банкомати.[103]

Во Р.Македонија криминалот со злоупотреба на платежни картички е во континуиран пораст, особено во последните години најчести се злоупотребите на интернет трговија „e-commerce", односно онлајн плаќања. Настапува ерата

[102] *СЕПА е европска иницијатива за хармонизација на плаќањата во евра, цел со која сака да се постигне безбедност и брзина на финансиските трансфери.*
[103] *https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf (17.04.2016).*

на интернет трговијата која овозможува размена на производи било кога, било каде со брзина на светлоста. До последните четири до пет години немаше понуда на домашни сајтови и луѓето практично немаа што да купуваат. Потоа полека почна да се појавува понуда на туристички аранжмани, авио карти, техничка роба и др. Карактеристично за Македонскиот пазар е тоа што голем број на интернет трговци не даваат конкретни попусти, што е тренд во светот, и тоа е една од главните причини што луѓето купуваат на странски интернет страни.

На глобално ниво најголемиот дел од плаќањата со фалсификувани платежни картички отпаѓа токму на овој начин на вршење на кривичните дела. Во Република Македонија 15.4% од лицата кои користат интернет, нарачале/купиле стоки или услуги. Мнозинството од нив, речиси 70 % купиле облека или спортска опрема.[104]

[104] *Државен завод за статистика, http://www.stat.gov.mk/PrikaziSoopstenie.aspx?rbrtxt=77 (17.04.2016).*

СЕКСУАЛНАТА ЕКСПЛОАТАЦИЈА НА ДЕЦА ПРЕКУ ИНТЕРНЕТ

Сексуалната експлоатација и на девојчиња и на момчиња се случува глобално, и алармантен е фактот дека поголемиот дел од ваквите случувања останува обвиткан со молк.

„Детската сексуална злоупотреба претставува вклучување на детето во сексуална активност која детето не ја разбира, не е во можност да даде согласност за таквата активност врз основа на претходна информираност, или активност за која детето не е соодветно подготвено од аспект на својот развој и не може да даде согласност, и со која се прекршуваат законите и социјалните табуа во општеството. Сексуалната злоупотреба на децата се докажува преку ваквата активност помеѓу дете и возрасен и друго дете кое според возраста или развојот има воспоставено однос на одговорност, доверба или моќ, а активноста се врши со намера да се исполнат или задоволат потребите на другото лице. Тука може да биде вклучено, но не е ограничено на: подведување или присилување на детето да се вклучи во незаконска сексуална активност; користење на детето за експлоатација во проституција или други незаконски сексуални практики; експлоатација на децата за порнографски изведби и материјали“[105]

Сексуалната експлоатација на деца преку интернет како негативна појава е присутна во криминалните дејствија уште многу одамна. Со појавата на високата технологија и глобалната мрежа за комуникација се олесни начинот на нејзино производство и дистрибуција и стана лесно достапна до поголема група на луѓе, со што се претвори во една цела индустрија што во крајна мера ги гази основните морални норми како и правата на децата кои станаа инструмент за заработка во рацете на меѓународната криминална мрежа.

---

[105] *УНИЦЕФ, Запоставени и жигосани- Анализа на состојбата:сексуална злоупотребана деца, канцеларија на УНИЦЕФ, Скопје, декември, 2010, стр.24.*

Сексуалната експлоатација на деца преку интернет на глобално ниво е во пораст. Злоупотребата на деца е кривично дело кое што е нетолерантно од најголемиот број од луѓето. Но и покрај тоа бројот на овие кривични дела не е толку ретко. Според проценките само во 2005 година повеќе од еден милион фотографии и видео материјали со злоупотреба на деца се наоѓале на интернет. Според проценките бројот на овие материјали се зголемува за околу 50.000 нови фотографии секоја година. Околу 70 % од фотографиите кои се наоѓаат на интернет се однесуваат на деца помлади од 10 години. Загрижува податокот дека овие фотографии најчесто остануваат на интернет засекогаш.[106]

Во Р.Македонија поединци пристапуваат на веб страни (најчесто на социјалните мрежи) на кои се поставени содржини со злоупотреба на деца, вршат преглед на содржините. Информациите за овој вид на криминал најчесто се добиваат при меѓународна размена на информации.

Во врска со **Сексуалната експлоатација на деца преку интернет** забележана е злоупотреба (прикажување и објавување на порнографски материјал) преку Социјалната мрежа Facebook, видео стриминг (гледање во живо на интернет) преку Сервисот Skype и сл. Причина за овој тренд е лесната достапност на интернет на деца и недоволната контрола на родителите во однос на лицата со кои комуницираат нивните деца преку Социјални друштвени мрежи.

Во Македонското Кривично Законодавство прегледувањето содржини на Сексуалната експлоатација на деца преку интернет не претставува кривично дело, казниво е само производството, дистрибуцијата и чување на содржини од овој вид.

[106] *http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/index_en.htm (17.04.2016).*

ИНТЕРНЕТ ИЗМАМИТЕ

Претставуваат сериозен проблем за правните лица кои своите бизниси ги договараат по електронски пат. Измамниците најчесто ја пресретнуваат електронската комуникација при што ги доведуваат во заблуда претставниците на правните лица и плаќањата ги насочуваат кон други сметки. На вршењето на овие кривични дела најчесто им претходи вршење на т.н. phishing каде што се врши кражба на лозинката на добавувачот на стоката. Исто така се испраќаат пораки со лажна содржина за добивање на наследство, или пак откако ќе биде пробиен односно компримитиран мејлот на жртвата се испраќаат пораки до сите лица кои ги има во контакт листата, дека лицето доживеала некаква несреќа во странство и потребно е веднаш да му се пратат парични средства.

Класичните измами кои порано се вршеа преку телефон или при личен контакт со жртвата, сега се повеќе се заменува со измами преку интернет или електронска пошта.

Најчест тренд на онлајн измамите претставуваат превземањата на интернет кориснички сметки (најчесто бизнис профили). При тоа се врши манипулација или наведување на лицата на тој начин што се врши промена на содржина на мејл пораките или се креира лажна, се со цел остварување на материјална добивка.

Имено, при овој вид на измами, најчесто со помош на фишинг (phishing) на e-mail поштата се презема контрола на сметката и истиот се набљудува од страна на измамниците, се до моментот додека не се пресретне бизнис комуникација каде се вршат насоки за исплата и достава на фактури и слично. Во дадениот момент од страна на измамниците се врши промена на содржината на конкретната мејл порака при што се менуваат банкарските податоци и броеви на сметките каде треба да се изврши договорената исплата.

При тоа најчесто жртви се правните лица кои имаат деловна соработка со странски фирми и вршат онлајн трансакции, додека кај физичките лица најранливи се оние кои на нивните компјутери немаат доволна заштита и не се информирани за типовите на измами кои се актуелни при он-лајн измамите. При злоупотребата на платежните картички најчесто жртви се лица кои вршат он-лајн трансакции на небезбедни сајтови.

Најчеста мета на криминалците се податоците за Е-маил адреси, броеви од платежни картички, кориснички имиња од профили на социјални мрежи, кориснички имиња од сметки на е-банкинг и др.

Нов тренд на онлајн измамите појава на интернет измами со нелегално преземање и измамничко посредување во деловната комуникација преку електронска пошта (e-mail) помеѓу македонски компании и нивните бизнис партнери од странски земји. Имено, добро организирани меѓународни криминални групи со примена на т.н. spam пораки, методи на phishing и social engineering, успеваат да ја „украдат" лозинката за пристап до e-mail-от на еден од бизнис партнерите при што добиваат непречен пристап до историјата на целокупната комуникација. Овие групи креираат нови e-mail адреси кои минимално се разликуваат од оригиналните и тешко се приметуваат во комуникацијата. Оригиналната порака ја преземаат, ја модифицираат и ја праќаат на еден од лажно креираните e-mail адреси. Потоа праќаат порака до партнерот дека ја имаат променето банкарската сметка за уплата на средства и бараат авансните средства да бидат уплатени на нова сметка која ја доставуваат во прилог.[107]

❖

Високотехнолошкиот криминал во однос на класичните висови на криминал драстично се разликува, односно дека самите кримианлци кои во минатото извршувале калсични висови на криминал, сега ги користат

[107] http://mvr.gov.mk/vest/874 (17.04.2016).

позитивните аспекти на високата технологија за да ги извршат криминалните активности. Интернетот, како современ начин на комуникација стана неминовност во животите на современиот човек. Република Македонија, како современа и модерна држава не заостанува зад овој тренд.

Меѓутоа, покрај благодетите што ги носи користењето на интернетот, паралелно се појавуваат и негативните страни од неговата употреба, што особено се огледа во фактот што постојано се појавуваат нови начини на извршување на кривични дела, кои влијаат на националната безбедност на државите.

5. ДЕТЕКТИРАЊЕ НА ВИСОКОТЕХНОЛОШКИОТ КРИМИНАЛ КАКО СОВРЕМЕНА И СЕРИОЗНА ЗАКАНА ПО НАЦИОНАЛНАТА БЕЗБЕДНОСТ

Високотехнолошкиот криминал преставува една од најголемите закани во модерните конфликти, затоа што релативно мали снаги и така наречени непознати напаѓачи може да нанесат огромни загуби на помоќните, особено во доменот на употребата на информатичката технологија. Затоа повеќето развиени земји во светот даваат големо внимание на заштитата, одбраната од компјутерските напади и закани. Поради тоа Европската Унија предлага и настојува одбраната од компјутерските закани да се регулира во нормативно – правна и страгетиска сфера. Затоа посебно е значајна стратегијата на Европската Унија, која има и важност за Р.Македонија.

Современите безбедносни закани кои се појавуваат во областа на политиката, економијата, културата, религијата, енергетика, информатика, екологија и други области, наметнува потреба од вклучување поголем број на државни и друштвени организации во работата во која се осигурува националната безбедност. Покрај зголемениот број на организации кои се занимаваат со прашањата за националната безбедност, постои потреба на безбедносните закани и предизвици да им се одговори на единствен начин.

Република Македонија во својата национална стратегија ги истакнува вредностите како што се заштита на безбедноста на граѓаните, заштита на суверенитетот и интегритетот на државата. Ваквиот пристап се соочува со нови предизвици кои се јавуваат со забрзаниот развој на информатичката технологија. Во согласност со тоа неопходно е во таа сфера Р.Македонија да ги усклади своите безбедносни ставови со Европските, со што во иднина би предупредила и одговорила на новите предизвици, и би имала решение за истите.

Светот и понатаму се соочува со традиционалните, но и со нови предизвици и закани по безбедноста. На зголемувањето на бројот на ризици

влијае културната и економската разлика. Националните, верски и политички екстремизам, ескалација на организираниот криминал, корупцијата, создаваат опасност за целиот регион, како и аспирација за изградба на заеднички механизам за превенција од ризиците и заканите. **Поради тоа безбедноста денес се гледа глобално, додека националната безбедност се поврзува со состојбата во непосредното опкружување.**

Како едни од најголемите закани на денешницата се идентификуваат и злоупотребата на новите технологии и научни достигнувања во областа на информатиката, генетските истражувања, медицината и други научни области. Република Македонија во голема мера се залага за унапредување на односите со државите како од регионот така и од светот. Отворена е за соработка со земјите кои се уклучени во процесот на Европските интеграции, но особено се грижи за заштита на своите национални интереси.

Свеста за неопходноста од информатичката технологија и нејзината вклученост во секојдневниот живот на поединецот, самата држава и нејзините институции е подигната на високо ниво во развиените делови на светот. Инциденти со злоупотреба на информатичката технологија секојдневно се случуваат, од бројни ситни измами до големи завери кои може да ги загрозат и државните субјекти. Напредокот, растот и зачувување на сите сегменти сега во голема мера зависи и од компјутерската безбедност, затоа што напредокот на информатичката технологија колку го олеснува секојдневното функционирање, толку носи и нови тешкотии, опасности и закани. *Се поголемата софистицираност и функционалност на информационите системи бара големо и високостручно внимание, затоа што се зголемуваат случаевите на злоупотреби и напади на критичните инфрастуктури на државата, кои прифатиле во поголем дел од нивната работа да се заснова на новата технологија, а со самото тоа и зависи од неа, а со тоа директно се влијае на националната безбедност.*

Како едни од најголемите детектирани високотехнолошки закани врз националната безбедност се следниве закани, за кои подетално и поопширно се зборува во оваа докторска дисертација, а тоа се: Компјутерскиот тероризам,

Компјутерската војна, Компјутерскиот простор, Компјутерската шпионажа и саботажа, Компјутерски вируси, Компјутерска измама, Крадење на идентитет, Компјутерски вандализам, Финансиски кражби и злоупотреби, Фалсификување на податоци и документи, Хакерство, Неавторизирана репродукција на легално заштитени компјутерски програми, кои се опфатени во Конвенцијата за Компјутерски криминал.

КОНВЕНЦИЈА ЗА КОМПЈУТЕРСКИ КРИМИНАЛ ПРЕДВИДУВА ЧЕТИРИ ГРУПИ[108]**:** дела против доверливост, интегритет и достапност на компјутерските податоци и системи – тоа го прави незаконскиот пристап, пресретнување, користење на компјутерот, некој програм и пасворд, дела поврзани за компјутер, како што се фалсификување, кражби, дела поврзани за содржината како што се детска порнографија која е најчеста во оваа група, опфаќа поседување, дистрибуција, чување или овозможување и достапност на овие материјали, дела поврзани со кршење на авторските и сродни права, кои опфаќаат репродуцирање и дистрибуција на неавторизирани примероци.

Принципи и одговорности за одбрана од компјутерски закани – Компјутерската безбедност е важна за целокупната средина, а може да се види низ сите негови сфери (меѓународни, меѓуинституционални, приватни, јавни). Основни принципи кои компјутерската безбедност ја прават возможна и на основа на која се постигнува успешни резултати во борбата против компјутерските закани се:

1. **Поврзување и јакнење на соработката помеѓу сите Сектори**. Сите институции без разлика дали се цивилни, полициски или војни, економски или академски, кои веќе достигнале некое одредено ниво на компјутерска безбедност, би требало да ги соединат во заеднички цели подобрувањата и унапредувањата. Истовремено, заедничката доверба и размената на информации се клучен услов за успешна соработка на приватниот и јавниот сектор.

---

[108] *Konvencija o Visokotehnološkom Kriminalu, Budimpešta, 23.novembar 2001.*

2. **Индивидуална одговорност** – За безбедност на информационо комуникацистите системи кои ги користи секој граѓанин, организација или институција, поединци или група, мора да сносат одговорност и да се грижат за системите на најдобар можен начин.

3. **Одговорност на бизнис секторот** – Бизнис секторот покрај останатото треба во интерес на државата секојдневно да ги почитува минимум пропишаните стандарди за компјутерска безбедност.

4. **Меѓуинституционална Соработка** – Соработката помеѓу државните институции, телата и организациите треба да доведат до заедничка грижа за компјутерската безбедност во Јавниот Сектор, но и во останатите сектори важни за нормалното функционирање на државата.

5. **Меѓународна Соработка** – Како еден е од приоритетите за безбеден компјутерски простор е соработката со други држави, меѓународни организации во полето на компјутерска безбедност, ангажираноста и донесувањето на стандардите и меѓународната безбедносна политика во оваа област, како и примена на тие стандарди и механизми во сопствената безбедносна политика во оваа област.

6. **Адекватноста на мерките** – Мерките превземени во полето на компјутерската безбедност, законскиот оквир и политиката која ќе се води на тоа поле мора да бидат во склад со основните човекови права и слободи, мора да се почитува слободниот пристап на информации и останатите демократски принципи. Потребно е да се направи рамнотежа помеѓу потребата за загарантирана безбедност и почитување на основните слободи и права. Јакнењето на компјутерската безбедност во јавната администрација и критичната инфрастуктура на информационо комуникациските системи, е обврска на секоја држава. И не само тоа, одгворност на секоја држава е да стално го унапредува нивото на компјутерска безбедност. Економијата на секоја развиена држава се потпира на информационите системи и меѓусебната умреженост, со што на тој начин би се обезбедил просперитет на државата, при што безбедноста на компјутерскиот простор постанува подеднакво

значајна како и безбеднсота на средината од присуство на криминални активности.

Компјутерската безбедност е телото на технологии, односно одбрана на компјутери, сервери, употреба на процеси и практики со цел да се заштитат компјутерите, мрежите, електронските системи, податоците, програмите, информациите од напади, закани, оштетување или неовластен пристап.

Компјутерски напади и закани напредуваат многу побрзо отколку што може да се одреди чекор со нив, и постојано се развива карактерот на безбедносните ризици. За да се справиме со истите не е доволен традиционалниот пристап, туку потребно е да се фокусираат повеќето ресурси на најважните компоненти на безбедносниот систем со што би се заштиитиле од компјутерските напади и закани.

Доколку високотехнолошкиот криминал стане широко распространета појава, тогаш граѓаните може да ја изгубат вербата во државните органи, во правилното и безбедно функционирање на системот, што ќе допринесе да се чуствуваат небезбедни, како и дека средината во која живеат е незбездна.

Со оглед на зголемувањето на свеста за проблемот и вистинското зголемување на високотехнолошкиот криминал, граѓаните со право бараат државата да превземе мерки за да обезбеди компјутерска безбедност на национално ниво. Државата е таа која е одговорна за спроведување на законот, за редот и мирот, како и за безбедноста на своите граѓани.

Влијанието на високотехнолошкиот криминал врз националната безбедност може да се фокусираат преку две главни начела.

Прво нацијата односно државата е таа која е одговорна за личната и колективна безбеднот како и сигурноста на граѓаните. Како што споменавме

погоре во текстот високотехнолошкиот криминал предизвикува различни видови на штети на граѓаните и организациите. Со навлегувањето на компјутерскиот простор во секој аспект од животот на граѓаните, државата треба да обезбеди лична и национална безбедност во компјутерскиот простор, и ито така потребно е државата да ја прошири својата инволвираност.

Второто начело е тоа дека комерцијализација на техничките и оперативни способности значи намалување на влез во компјутерска воена средина. Фактот дека компјутерски криминални организации нудат ресури, инфрастуктура па дури и на клиентите им нудат услуги за разумни трошоци, значи извршување на директен напад на националната безбедност.

6. ВИСОКОТЕХНОЛОШКИОТ КРИМИНАЛ И ОРГАНИЗИРАНИОТ КРИМИНАЛ

6.1 ПОИМ И ДЕФИНИЦИЈА НА ОРГАНИЗИРАН КРИМИНАЛ

„Организираниот криминал" е многу значаен термин кој стана дел од речникот на многу политичари, а исто така и на пошироката јавност. Тој често се применува без јасна референтна точка и всушност е многу неодреден и нејасен.[109] Во светската литература можат да се најдат стотици дефиниции за организираниот криминал од автори од различни провиненции и различни подрачја. Меѓутоа, појавата на организираниот криминал не датира од толку скоро. Организирани криминални групи постоеле уште во средниот век (во 17-ти век бандите ги напаѓале големите градови). Криминални организации со широка акциона распространетост, нивното преминување од локални во национални, па и меѓународни размери, се врзуваат за монополизам и финансиска аристрократија.[110]

Организираниот криминал преставува една добро организирана криминална организација, со строга хиерархија, дисциплина, одговорност, лојалност и поделба на задачите, чија цел е остварување на што поголем профит и легализација на незаконско стекнатиот имот, благодарение на постигнатиот степен на друштвен углед, било да е тоа на основ на влез во структурите на власта или воспоставување на врски со органите на власта, државни органи, и влијание во политичките партии. За остварување на своите цели, на организираниот криминал посебно му одговара состојба во која поптолно не функционира правната држава и каде што е изразена „сивата економија", затоа што полесно може да стапи во однос со поедини државни и други органи, пред се поради обезбедување на заштитата која им е потребна.

Од наведената дефиниција може да се заклучи дека организираниот криминал по својата содржина, значи длабоки односи со државата и нејзините

---

[109] *Michael Woodiwiss and Dick Hobbs, 'Organized evil and the Atlantic Alliance: moral panics and the rhetoric of organized crime policing in America and Britain' , во British Journal of Criminology, Vol. 49, 2009, pp. 106–128.*
[110] *Милан Милутиновиќ „Криминологија,, Београд., 1967, стр.89.*

органи на различни нивоа во структурите на власта, без оглед на тоа дали овие органи активно соработувале, или прекутно дозволиле таква криминална делатност. Постоењето на вакви врски секако преставува еден од условите за создавање и постоење на организираниот криминал, поради тоа што му овозможува елиминација и неутрализирање на активностите на државните и другите органи за нормално функционирање на државата.

Организираниот криминал настојува со различни методи (подмитување и други видови на коруптивност, уцени, притисоци, изнуди и сл.) да стигне до највисоките органи на власта, со што би си обезбедиле поголема концесија и пристап и што поголем друштвен статус за шефовите на криминалните организации. Со своето делување организираниот криминал всушност овозможува создавање на современи успешни криминалци кои на основа на стекнатата слава и моќ, постигнуваат одреден друштвен углед кој делува повратно како влијание на органите на власта, полицијата, судството и други субјекти. На таков начин незаконски се стигнува до огромен имот кој потоа се легализира, и се овозможува незаконското богатење да се оправда.

Една од карактеристиките на организираниот криминал која е тесно врзана со постигнатото друштвено влијание и углед, е оневозможување да се забележи незаконското работење во одредени работни односи, така што не е ретка појавата тешко да се разликува легална организација од поединечен облик на организиран криминал.[111]

❖

Посебно влијание треба да се насочи кон понатамошното подобрување во борбата против организираниот криминал, пред се поради растот на организираниот криминал. Најголем авторитет и надлежност во борбата против организираниот криминал имаат Министерствата за внатрешни работи на современите држави. Улогата на полицијата во водењето на истраги за

[111] *Мичо Бошковиќ, Организиран криминал, Прв дел – Полициска Академија, Београд 1998, стр.9.*

организиран криминал е првенствена и клучна, пред се поради тоа што на организираните криминални групи им се потребни легитимни државни структури за да ги одржат и прошират нивните криминални активности.

6.2 ЕТИМОЛОГИЈА НА ОРГАНИЗИРАНИОТ КРИМИНАЛ

Колку чудно и да звучи со оглед на тоа дека е во прашање феномен на кој се поклонува огромно внимание, како во бројни научни трудови така и во популарна белатристика а посебно во филмови, поголемиот број на автори кои на научна основа од гледна точка на феноменологија и етимологија во однос на овој облик на криминалитет, така и во светол нормативен аспект, кои работат на проблематиката на организиран криминал, го искажуваат нивниот став дека дефинирањето на организираниот криминал е многу тежок проблем. Проблемот во дефинирањето на организираниот криминал не произлегува од основниот збор „злодело" туку проблемот е во зборот „организиран".

Во поглед на големиот проблем за дефинирање на организираниот криминал во Американскиот Закон за организиран криминал (The Organized Crime act of 1970), воопшто не постои посебна дефиниција за организиран криминал, што преставува посебна реткост, со оглед на тоа дека е доста невообичаено поимот кој е клучен за одреден законски акт дури и се наоѓа во насловот, во самиот тој акт воопшто да не е дефиниран.

Недостатокот од адекватно дефинирање на организираниот криминал од страна на поедини Американски Држави во седумдесетите години во САД, се истакнал како голем проблем. Дефиницијата во Американската Држава Мисисипи е многу едноставна „Две или повеќе лица кои се договараат заедно да извршат кривично дело заради остварување на профит на континуирана основа". Ваковата едноставност во дефинирањето, истовремено овозможува голема ширина во тумачењето, што создава и голема можност за претерана арбитрерност. Овој тип на дефинирање се применува во поедини правни системи, чии креатори сакаат со така широки појмовни одредувања да опфатат што е можно поголем број криминални активности.

Во Калифорнија е применет значително широк пристап, со елементи на таксативно набројување на конкретни криминални активности, па во таа држава поимот Организиран криминал е дефиниран како „Организиран

кривичен настан се состои од здружување на две или повеќе лица, кои во континуитет учествуваат во една или повеќе активности: транспорт на нелегална стока, проституција, лихварство, напади, кражби" итн.[112]

Етиологија на криминалот преставува истражување на примерок на криминално прашање, но тоа незначи дека таа цел мора да се достигне затоа што еден единствен примерок неможе со целост да делува на целиот комплекс примери, и дефинитивно да се одреди како пример за криминалитетот, а додека за криминалното однесување како значајни факти се статистичките корелации, квантитативно и квалитативно проценување на факторите кои допринеле до тоа однесување, што насочува на правилен пат и правец на криминалошко истражување.[113]

Етиолошкото разгледување во однос на организираниот криминал претежно се излагања од страна на Американски автори, што преставува логична последица со оглед на фактот дека Организираниот криминал своите најразвиени современи форми ги доживеал во САД. Поголемиот дел на разгледувања кои се однесуваат на етиолошкиот фактор на создавање на криминални организации, во основ се однесува пред се на малолетничките банди, на кои првенствено во Американската историја им се посветувало големо внимание.

Разгледувајќи ги механизмите на нивното настанување, може да се види дека е во тесна врска со организираниот криминал, и неспорно е дека од редовите на малолетничките банди се регрутира членство за озбилни криминални организации, исто како што и многу малолетнички банди преставуваат почеток на опасните видови криминални организации, кои јасно може да се дефинираат како организиран криминал.[114]

Транснационалниот организиран криминал како општествена штетна, негативна и деструктивна појава има тенденција на високо ниво на

---

[112]*Милан Шкулиќ, Организиран Криминал, Београд 2003, стр.28,29,30.*
[113]*Милан Шкулиќ, Организиран Криминал, Београд 2003, стр.92.*
[114]*Милан Шкулиќ, Организиран Криминал, Београд 2003, стр.93.*

адаптибилност, жилавост и истрајност во остварувањето на своите цели. Под транснационален организиран криминал се подразбираат криминални групи кои имаат организатор (или организатори) во една држава, но поради обемот на криминалните активности делуваат во други држави.[115]

Од етиолошко стојалиште, можеме да констатираме дека транснационалниот организиран криминал неминовно ги содржи причините и оптималните услови што лежат во основата на појавувањето на организираниот криминал.

Како најзначајни основни причини за настанување на криминалитетот можеме да ги потенцираме противречностите на општествените односи кои продуцираат несоодветен материјален развој, нерамноправност антагонизам во економската, социјалната, политичката и културната сфера и слабоста, неподготвеноста, нерешителноста и корумпираноста успешно да се справат со овие внатрешни безбедносни закани. Исто така причините за појавата на организираниот криминал може да се бараат и во правни, географски, геополитички и геостратегиски констелации на конкретното општество. Значаен сегмент преставуваат и соодветните законски мерки преземени во функција на ефикасното попречување на транснационалниот организиран криминал.

Успешната борба против овие облици на криминалитет не може во целост да се води без согледување, анализирање и сфаќање на нивната етиолошка сложеност.

Појавата на организираниот криминал е најчеста во земјите кои сеуште се во транзиција. Овие држави преставуваат идеална почва за брз и успешен развој на многу форми типични за дејствувањето на организираниот криминал. Во последно време организираниот криминал успешно се вгнездува во легалните бизниси, неговата инфилтрација во поголем број на современи држави го детерминира и меѓународниот карактер на организираниот криминал.

---

[115] *Марјан Габеров, „Транснационален организиран криминалитет- трендови и случувања", Септември, 2014 г стр.4.*

Организираниот криминал, а со него и корупцијата во основа имаат три причински димензии:

Општествена, на државната управа (администрацијата) и индивидуална.

За целосно елаборирање на причините за појавата на организираниот криминал ќе ги потенцираме следните основни предуслови:

- Современиот процес на глобализација кои ги зафати скоро сите држави во современиот свет;
- Евидентните потешкотии и проблеми во непреченото функционирање на политичкиот и економскиот систем како и останати општествени подсистеми на транзиционите општества;
- Несинхронизираност на кривично – правните решенија;
- Либерализација на економскиот пазар на глобален план;
- Економската меѓузависност, економските реформи, економската несигурност;
- Исклучителноста мобилност и можностите за трансфер на парите и капиталот;
- Неспособноста за снаоѓање на државите во услови на поизразена економска криза;
- Големата економска и финансиска криза.[116]

[116]*Види пошироко: Митко Котовчевски, Национална Безбедност, Скопје 2013 стр.348.*

6.3 УЛОГАТА НА ВИСОКОТЕХНОЛОШКИОТ КРИМИНАЛ ВРЗ ОРГАНИЗИРАНИОТ КРИМИНАЛ, ОЧЕКУВАЊА И ПРЕДИЗВИЦИ

Високотехнолошкиот криминал го загрозува еден од највиталните аспекти на животот и работата во современото општество, а тоа е непреченото одвивање на протокот на информации. Според неговата природа тој спаѓа во прекугранични криминал и во себе содржи елементи на мултидимензионалност и организираност.

Интернетот како глобална меѓукомпјутерска врска овозможува полесна приватна и работна коресподенција, но интернетот воедно може да користи и за криминални цели. Интернетот даде нов облик на класичниот криминалитет, и воедно допринесе за создавање нови облици на криминалитет, како што се, ширење на детска порнографија, разни облици на загрозување на лична сигурност, ширење на разни облици на организиран криминал.[117]

Притоа треба посебно да се има во предвид дека високотехнолошкиот криминал некогаш е поврзан со делување и активности на поединец, додека криминалот поврзан со компјутерски мрежи во поголемиот број случаи резултира со делување на организирана група, и тоа строго специјализирани. Тие групи од една страна се „традиционални" конвенционални групи кои се занимаваат со организиран криминал и кои се усовршиле и ја осовременила примената на високата информациона технологија и се спремиле за излез на „компјутерската сцена".

Пак од друга страна се јавуваат и посебни организирани криминални групи кои се нарекуваат „компјутерска мафија" и кои имаат сопствени правила, друг начин на однесување и многубројни специфичности (виртуелно опкружување, информационо „оружје", специјализирано знаење и друго). [118]

Секоја нова технологија која беше создадена е адаптарирана од страна на криминалците. Организираните криминални групи покажаа неверојатна

[117] *Брансилав Симоновиќ, op. cit., страна 673-674. пдф*

[118] *Милан Милошевиќ, Допринос Стручних лица сузбијању организованог високотехнолошког криминалитета, Организовани криминалитет, Зборник, Стање и мере заштите, пдф. стр.311.*

способност да се адаптираат на новите технологии и да ги користат, и истите им одиграа суштинска улога во трендот на глобализацијата. Меѓународните организирани криминални групи и се придружија на револуцијата на информационата технологија со регрутирање на компјутерски експерти.

Високотехнолошкиот криминал е меѓународен феномен кој е тесно поврзан со развојот на економското ниво во различни земји и региони. Овој вид на криминал може да ја загрози безбедноста на сите граѓани во државата, а пред се финансиската состојба на една држава. Организиран криминал кој се однесува на било кој криминален облик извршен со помош на висока технологија или пак е насочен против истата спаѓа во делот на организиран криминал поврзан со висока технологија.

Како што се зголемува светската зависност од технологијата така и високотехнолошкиот криминал станува извор на приходи за организираните криминални групи. Високотехнолошкиот криминал им нуди можност на организираните криминални групи да вршат криминални активности во безбедни компјутерски мрежи, а со самото тоа да бидат невидливи за безбедносните служби.

Меѓународните организирани криминални групи се повеќе стануваат компјутерски писмени, и ги користат новитетите кои ги нуди високата технологија за нелегални активности и незаконско богатење. Со слободниот пристап на интернет содржините лесно добиваат информации за ранливоста на безбедносните системи, а со тоа и методологијата за извршување на компјутерски напади.

Во минатото криминалниците за извршување на одредено кривично дело користиле некое орудие, оружје и сл., но денес модерните криминалци ја користат високата технлогија и компјутерските мрежи за извршување на кривичните дела и криминалните активности, и со оглед на тоа, денес, компјутерот преставува единствен доказ и може да послужи како доказен материјал.

Се повеќе компјутерот постанува единствено средство за извршување на криминални активности во сите области на кривични дела, а особено во областа на високотехнолошкиот криминал (неовластено навлегување во компјутерски систем, компјутерски измами, детска порнографија, интелектуална сопственост, интернет измами, изработка и злоупотреба на платежни картички, злоупотреба на лични податоци, пиратерија, перење пари преку интернет и сл.).

Во виртуелниот свет не постојат граници, карактеристика која го прави многу атрактивен за криминални активности. Кога властите се обидуваат да го контролираат овој виртуелен свет, истрагата е бавна и мачна, и невозможна во некои случеви, сепак националните правни системи се големи.[119]

Меѓународните организирани криминални групи ја користат информационата технологија како подршка за нивните криминални активности. Таа им овозможува непречено и побезбедно да ги извршуваат кривичните дела, без оглед на државните граници. Анонимноста на високотехнолошкиот криминал го прави идеален канал и инструмент за многу активности на организираниот криминал. Тајноста е клучен дел од стратегијата на организираниот криминал а високата технологија нуди одлични можности за негово одржување.

На пример:

ЕЛЕКТРОНСКОТО ПЕРЕЊЕ ПАРИ: ширењето на електронското банкарство и електронското плаќање е благослов за перење пари. Дигиталната технологија има направено услови за перење пари, толку многу колку што има постигнато во законската економија со online продажба на мало. Повеќето истражувачи тврдат дека организираните криминални групи се во првите редови на усвојување и развој на новите технологии за да на нив им се олесни перењето на пари.

---

[119] *Phil Williams, Organized Crime and Cybercrime: Synergies, Trends, and Responses,pdf.*

Милијарди долари се трансферираат секој ден, преку берзи, брокерски куќи, платежни картички, поединци и влади.[120]

Онлајн аукции нудат слични можности да се движат пари низ навидум легитимни купувања, но се плаќа многу повеќе од вистинската вредност на производот.

Коцкањето преку интернет исто така дозволува движење на пари особено оф-шор финансиски центри на Карибите.[121]

Користењето на технологијата однсоно електронскиот трансфер на пари им помага на криминалците во прикривање на приносите од криминалните активности. Финансиските институции веќе нема да бидат единствени кои ќе нудат трансфер на парични средства кои транзитираат со брзина на светлината.

Развојот на неформални банкарски институции и паралелни банкарски системи, може да дозволат да се заобиколи надзорот на Централната Банка, и исто така може да се дозволи затајување на готовинските уплати кои ги имаат организираните криминални групи.

Со појавата и ширењето на различни технологии на електронската трговија, може лесно да се предвиди како традиционалните контра мерки против перењето пари, наскоро ќе стане ограничено. Криминалците имаат можност да продаваат одредена количина на дрога, во замена за трансфер на парични средства на одредена сметка, кои потоа анонимно ги префрла на друга сметка во друга финансиска институција во странство која ги штити податоците на своите клиенти, за подоцна легално да ги подигне.

---

[120] *Mitchel P. Roth, PhD, Global Organized Crime, pp 63. pdf*
[121] *Phil Williams, Organized Crime and Cybercrime: Synergies, Trends, and Responses, pdf.*

Исто така, организираните криминални групи го користат интернетот како комуникација (обично шифрирана), а со тоа се зголемува пазарот на дигитално шифрирани технологии. Од овој вид на технологија имаат потреба сите, а особено банките кои сакаат да ја осигураат приватноста и доверливоста на клиентите и нивните финансиски трансакции. Криптографијата им преставува силна алатка на криминалните групи како и на терористите, за прикривање на нивните активности, а за властите дополнителна тешкотија за водење на истраги и собирање на докази.

Интернетот како широко поле и напредната висока технологија преставува големо олеснување во извршување на ***ДЕТСКАТА ПОРНОГРАФИЈА*** низ целиот свет. Користејќи ги глобалните дистрибутивни мрежи и интернетот овој вид на криминалци делуваат во повеќе држави, и треба да се напомене дека тоа се добро организирани криминални групи, на кои е многу тешко да се влезе во траг. Содржината со детска порнографија ја сместуваат виртуелно на одредени сервери кои ги имаат закупено во сосем трети држави, со лажни податоци на лица и фирми кои претежно не постојат, користат proxy сервер за да го скријат трагот од каде што пристапуваат на интернет, и сите овие методи им ги овозможува високо развиената технологија односно високотехнолошкиот криминал.[122]

СКРИЕНИ ИНТЕРНЕТ СТРАНИ ИЛИ ДЛАБОКИ ИНТЕРНЕТ СТРАНИ

Тоа се страни кои преставуваат магацин на податоци на интернет. Овие податоци се за 500 пати поголеми од нормалните податоци на интернет. Истите скоро и да е невозможно да бидат откриени од страна на владините служби. На овие страни се нуди нелегална продажба на оружје, односно шверц на оружје, оружје за масовно уништување, нелегална трговија на дрога и други забранети производи, украдена стока и сл. Голем број на организирани криминални групи ги користат овие страни за вршење на криминални активности, а исто така ги нудат и своите услуги, односно продажба на нелегална стока.

---

[122] *Phil Williams, Dimitri Vlasis, „Combating Transnational Crime" – Crime in Cyberspace pp.197. pdf*

Во иднина овие скриени интернет страни ќе бидат се повеќе користени од страна на организираните криминални групи.

НИГЕРИСКИ ИЗМАМИ

Меѓу организираните криминални групи кои направија транзиција како и високотехнолошкиот криминал се Нигериските практичари на измамата 419, која се нарекува така поради Нигерискиот Кривичен Закон. Тие се вклучени во кривични дела со интелектуална сопственост, како што се пиратеријата, изнуда на пари, компјутерска измама. Секој кој користи компјутер веројатно слушнал за овој вид на измама, која е премногу добра за да биде вистинита, дека нуди голема сума на пари кои треба да бидат пренесени на Западни банкарски сметки, и се што е потребно е вашата банкарска сметка и други лични податоци, а за возврат примачот наводно ќе добие добар паричен надомест.

До 2006 година САД беа најмногу погодени од овој вид на измама, и загубите кои им беа нанесени на Американските државјани беа над 800 милиони Американски долари годишно. Тоа се всушност глобални организирани криминални групи кои делуваат и надвор од Нигерија, и тоа Англија, Холандија, Индија и во многу други држави низ светот.[123]
Во последно време се повеќе измами од овој вид се случуваат во Р.Македонија, каде што оштетени се Македонски државјани.

❖

Едноставно можеме да кажеме дека новите технологии одиграа голема улога кон глобализацијата. Организираните криминални групи кои го извршуваат својот криминал со помош на високата технологија се во голема предност пред останатите традиционални криминални групи. Нивниот метод е различен од традиционалниот, но тоа што ги поврзува е исто, однсоно желбата за моќ, финансиска добивка, освета, страст и сл. Глобалната природа на високотехнолошкиот криминал, како и лесното поминување на електронските

[123] *Mitchel P. Roth, PhD, Global Organized Crime, pp 86., pdf*

граници, придонесоа ФБИ и други Агенции за спроведуавње на законот да излезат надвор од САД, се со цел подобрување на соработката со другите агенции од целиот свет. ФБИ сега го рангираше високотехнолошкиот криминал како трет на листата на нивни приоритети, веднаш зад тероризмот и шпионажата. Повеќето власти инсистираат на тоа дека тероризмот и високотехнолошкиот криминал, не се само менување на обликот на организираниот криминал, туку и на начинот на кој поединците се организираат да вршат кривични дела исто така. [124]

Организираниот криминал регрутира тинејџери, кои прават повеќе инциденти на интернет отколку на улица. Во еден објавен извештај на McAfee безбедносна организација, се вели дека водечките компјутерски криминални групи доаѓаат од Европа, и сугерира дека криминалните тимови се фокусираат на најдобрите студенти од водечките академски институции, и им помагаат да се здобијат со потребните вештини за да извршат високо технолошки криминал во огромни размери.[125]

[124] *Mitchel P. Roth, PhD, Global Organized Crime, pp 100., pdf*
[125] *Mcafee Virtual, Criminology Report, Organised Crime And The Internet, pdf.*

7. МОДЕЛИ НА ЗАШТИТА ОД ВИСОКОТЕХНОЛОШКИОТ КРИМИНАЛ

7.1 УЛОГАТА НА ДРЖАВАТА ВО ЗАШТИТАТА ОД ВИСОКОТЕХНОЛОШКИОТ КРИМИНАЛ

Критична инфрастуктура често се идентификува како инфрастуктура која кога не функционира, макар и на ограничен период, може негативно да влијае на економијата, или да ги изложи луѓето и производите на безбедносен ризик.

Европската Комисија нагласува дека доколку дојде до повреда на критичната инфрастуктура на некоја земја членка, тоа може да има влијание и на друга држава, како резултат на меѓузависноста помеѓу инфрастуктурите. За Европската популација многу е битна проценката која се однесува на: потенцијални жртви, во смисла на број на смртни случаеви или повреди, потенцијални економски ефекти, во смисла на финансиски загуби, влошување на квалитетот на производите или услугата и заштита на животната средина, потенцијални ефекти на популацијата, во смисла на губење на доверба од јавноста, физички страдања и нарушување на секојдневниот живот, вклучувајќи го губењето на основната услуга.

Во поголем број на земји од Европската Унија нападите на безбедноста на компјутерите имале голем пораст во последните години. Се проценува дека 40% од нападите бара четири дена за проблемот да се реши. Во 90% од случаевите нападот е успешен поради неправилна конфигурација на системот на безбедност и недостаток на посебни вештини. Трошковите за заштита како на Владата така и на приватниот сектор се многу високи. Тоа покажува на потребата за нагласување на компјутерската безбедност на национално но и на Европско ниво.

Критична информациона инфрастуктура од национален интерес преставува информационен систем и компјутерски услуги кои подржуваат институционални функции:

- Органи на државната управа кои се занимаваат со работи поврзани со безбедноста, правда, одбрана, финансии, комуникации, сообраќај, енергетика, животна средина, здравје;
- Народна Банка и банкарски систем;
- Владини Институции како и Јавни претпријатија кои се занимаваат со области поврзани со комуникации, сообраќај, енергетика, здраство, извори на вода и нивно чување;
- Како и било кои други институции, административни канцеларии, јавни или приватни претпријатија чија дејност е поврзана со национален интерес.

Стратешки цели и мерки за ускладување со Европската стратегија за компјутерски криминал во Европската Унија по прашањето за Компјутерска Безбедност се искажани низ пет стратешки приоритети:

- Постигнување на еластичност во смисла системите автоматски да се враќаат во првобитна положба после инцидент;
- Смалување на Компјутерскиот криминал;
- Развој на политиката на компјутерска одбрана и капацитет во согласност со заедничката безбедносна и одбранбена политика;
- Развој на индрустиски и технолошки ресурси за Компјутерска безбедност;
- За воспоставување на поврзани меѓународни политики на Компјутерска безбедност за Европската Унија и промовирање на основните вредности на Европската Унија.

Стратегијата на Компјутерска безбедност на Европската Унија сугерира со правни акти:

- Да се одредат минимум заеднички барања за мрежна и информациона безбедност која ќе ги обврзе државите членки да воспостават национални компетентни органи мрежна и информациона безбедност, да воспостават функционален CERT и да усвојат национална стратегија за мрежна и информациона безбедност и национален кооперационен план за мрежна и информациона безбедност;
- Да воспостават механизми за координирана превенција, детекција, ублажување на ефектите и адекватни одговори, како и за размена на информации и взаемна подршка помеѓу националните компетентни органи за мрежна и информациона безбедност;
- Подобрување на подготовките за учество на приватниот сектор;
- Европскиот Парламент и Совет даваат директиви во однос на мерките за осигурување на високо ниво на мрежна и информациона безбедност низ Европската Унија.
- Од земјите членки како и од земјите кандидати за членство се бара да имаат Национална стратегија за мрежна и информациона безбедност (NIS), Кооперационен план за NIS, Национален компетентен орган за NIS, Тим надлежен за компјутерски инциденти (CERT).

Компетентен орган е една од најзначајните национални институции со обврска да ги прати примените на директивите на национално ниво, соработка со националните компетентни органи на други држави членки, со соодветни безбедносни служби и органи за заштита на податоци во својата земја, исто така прима и постапува по прием на информација за инцидент кај јавната администрација, јавни оператори за телекомуникациски и информациски услуги.

Покрај компетентните органи предвидено и секоја држава членка да ги формира следниве функции на национално ниво:

- Орган за информациона безбедност (IAA);
- Орган за ТЕМПЕСТ (TA);
- Орган за одобрување на криптографски решенија (CAA);
- Орган за дистрибуција на криптографски материјали (CDA).[126]

ENISA

Најзначајна институција во Европска Унија од областа на мрежната и информационата безбедност е Европската Агенција за мрежна и информациона безбедност (ENISA) формирана во 2004 година и Европски Тим за реакција на компјутерски инциденти (CERT) формиран 2012 година.

Европската Агенција за мрежна и информациона безбедност (ENISA) основана е со уредба на Европската Комисија.

Истата е оформена за подобрување на способноста на Европската Унија, земјите-членки на ЕУ и на бизнис заедницата за да спречи, адресира и одговори на проблемите во однос на безбедноста на информациите.

Со цел да се постигне оваа цел, ENISA веќе е центар на експертиза за безбедноста на информациите и поттикнување на соработката помеѓу јавниот и приватниот сектор.

[126] *http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf (26.04.2016).*

ЗАДАЧА НА ENISA СЕ:

- Да врши активности за воспоставување на високо ниво на безбедност на мрежата и податоците во Европската Унија;
- Собирање и анализа на податоци за безбедносните инциденти во Европа и новите ризици;
- Подигање на свеста и соработка меѓу различните актери во областа на безбедноста на информациите, особено преку развивање јавни-приватни партнерства со индустријата во оваа област.[127]

НАДЛЕЖНОСТИТЕ НА ENISA СЕ:

- Подршка и развој на политиката и прописите на Европската Унија во областа на безбедноста на мрежата и податоците;
- Соработка помеѓу надлежните тела и другите заинтересирани институции;
- Подршка на истражувања, развој и стандардизација;
- Соработка со органите во Европската Унија вклучувајќи ги оние кои се надлежни за заштита од високотехнолошки криминал, заштита на приватноста и податоците;
- Учество и соработка со трети земји и меѓународни организации поради промовирање меѓународна соработка во областа на безбедноста на мрежата и податоците.

Со уредба се утврдуваат органите на Агенцијата, нивниот делокруг, работните задачи, состав, избор и траење на мандатот. Органи на ENISA се Управен Одбор, Извршен Одбор, Извршен Директор и стално тело на заинтересираните страни. Агенцијата донесува годишни и повеќе годишни програми за работа чиј нацрт го прави Извршниот Директор а го усвојува Управниот Одбор. Европската Агенција за мрежна и информациона безбеднсот

[127] *Правилник за обезбедување на безбедност и интегритет на јавните електронски компјутерски мрежи и услуги и активности кои што операторите треба да ги преземат при нарушување на безбедноста на личните податоци, Закон за електронски комуникации, Службен весник на РМ. Бр.39/2014 и 188/2014.*

се финансира со средствата од буџетот на Европската Унија, со средства од трети земји кои учествуваат во работата на Агенцијата, како и донации на држави членки. Управниот Одбор го усвојува буџетот по спроведени процедури утврдени со уредба.[128]

Овој правен акт треба да го имаме во предвид, затоа што се воспоставува орган со кој Р.Македонија како земја кандитат за членство во Европската Унија треба да воспостави соработка, а кога ќе постане земја членка ќе биде полноправен член.

Република Македонија превзема одредени активности насочени кон областа на информационата безбедност, со следниве приоритети:

- Заштита на критичната инфрастуктура;
- Борба против високотехнолошкиот криминал;
- Научно истражувачка и развојна работа во областа на информационата безбедност.

Исто така, во тек е формирање на Институција надлежна за истражување и развој во областа на информационата безбедност, верификација на софтверски апликации, уреди и системи, како и Институција за превенција, координација и решавање на компјутерски инциденти, така наречен Национален **CERT**„Community Emergency Response Team“ или **CSIRT** „Computer Security Incident Response Team“, кој веќе функционира во рамките на АЕК (Агенција за Електронски Комуниакции) во Р.Македонија.

Со овие активности треба да се постигне:

- Да се стекне доверба корисникот за безбедно функционирање на информациониот систем;
- Подигање на свеста на граѓаните за заштита на личните податоци во информациониот систем;
- Заштита на податоците;

[128] *https://www.enisa.europa.eu/ (26.04.2016).*

- Заштита на информационите и телекомуникациски системи;
- Безбедност на електронските трансакции;
- Ефикасни механизми за заштита и остварување на правата во процесите на електронското тргување и електронката размена на податоци.

Дијапазонот на злоупотреби е широк и започнува од неовластен пристап до податоци, преку кражба на идентитет на корисници како и на институции. Ваквите активности влијаат на корисникот и на информациониот систем кој се мета на напади, и исто така придонесуваат да други корисници или институции ги одбиваат овие концепти, што во крајна линија доведува до успорување на технолошкиот развој. Од овие причини, а посебно поради тоа што постои реална опасност да нападите на информационите системи и нивните корисници во иднина ќе бидат се почести, неопходно е да се изготват и имплементираат мерки кои овој вид на закани ќе ги сузбијат, како и да обезбеди брзо откривање на нападот и на сторилетите.

Министерството за Внатрешни работи е посебно осетливо на безбедносните проблеми кои се однесуваат на информационите системи. Во ова Министерство покрај разни бази во кои се наоѓаат податоци добиени од оперативни активности на вработените, постои и база со податоци на сите граѓани на Р.Македонија. Овие податоци имаат клучно значење во утврдување на идентитетот на некое лице.

Што се однесува на користење на интернет, последните истражувања говорат дека поголемиот дел сметаат дека денес ризикот да постанеш жртва на компјутерски криминал е зголемен.

Луѓето на различен начин се штитат, дел од нив ги промениле онлајн шифрите, други пак не ги отвараат мејловите од непознати лица, а дел инсталирале антивирус. Мерките на заштита најчесто ги спроведуваат младите, отколку постарите лица, образуваните од помалку образуваните граѓани, како и оние кои редовно користат интернет. Како расте потребата на луѓето од користење на интернет, информациите кои ги добиваат од

интернетот, алатки кои им помагаат во работата, така се зголемува и нивната изложеност на опасност во таа област. Се повеќе деца се приклучуваат на друштвените мрежи каде злоупотребите се се почести. Интернет комуникацијата и начинот на функционирање на друштвените мрежи е таков што никогаш неможеш да бидеш сигурен кој е од другата страна. Секојдневно сме сведоци на злоупотреби на интернет, било да е тоа на Социјалната мрежа Facebook, Twitter, Instagram и др.

Но социјалните мрежи не се единственото место каде што корисникот може да постане жртва на компјутерска закана. Секој корисник на интернет со самото приклучување на интернет постанува потенцијална жртва, и досегашната пракса покажува дека скоро и да не постои лице кое не постанало жртва на некој вид на закана на интернет. Сето тоа говори дека е потребна едукација на граѓаните, за да секој пристап на интернет биде се побезбеден.

Во Р.Македонија децата сеуште немаат прилика да изучуваат во редовна настава програма за безбедно користење на интернет, друштвени мрежи и слично, но загрижувачки е фактот дека голем дел од родителите немаат ни основно информатичко познавање, и поради тоа неможат на своите деца да им пренесат знаење. Но неможеме да кажеме дека само децата се оние на кои им е потребна едукација во врска со користењето на интернетот, тука се сите корисници. Важно е сите да се вклучат во подигање на свеста од опасностите кои се јавуваат на интернет, како и превенција и обезбедување на сигурно и безбедно опкружување во онлајн светот. Тоа може да се постигне со организирање на семинари, работилници, курсеви во кои ќе учествуваат стручни лица. Во однос на ова најважно е да се овозможи лесен пристап на материјали и литература од оваа тематика, со што голем број на корисници ќе се информираат за компјутерскиот простор.

Според примерот на ENISA наша обврска е да се покрене кампања во која ќе се зголеми свеста на населението за компјутерската безбедност. Целта е да се промовира компјутерската безбедност помеѓу граѓаните за да го променат својот став према компјутерските закани, и да им се пренесат најновите информации низ едукација и примери. За да се пристапи одговорно

спрема обезбедување на компјутерскиот простор, неопходна е соработка помеѓу приватниот и државниот сектор како и академската фела. Многу е значајно сите овие споменати три сектори своите активности да ги извршуваат со меѓусебна кооперација, а поголемиот дел од сето тоа се одвива во компјутерскиот простор. Поради тоа без заеднички активности на полето на обезбедување на овие активности, нивната сигурност сериозно би била доведена во прашање.

Денес критичната инфрастуктура која го контролира воздушниот сообраќај, испорачува вода, подржува финансиски системи, произведува струја, во целост зависат од поврзаноста на информациониот систем. Соработката помеѓу државните институции, приватниот сектор, невладини организации, истакнати поединци, организации кои во целост својата работа ја базираат на современата технологија и пратат иновации секој во својата област, оваа соработка е неопходна за општото добро. Секојдневно граѓаните на Р.Македонија ја користат информационо комуникациската технологија за најразлични потреби. Но тие сеуште не се доволни свесни од заканите кои може да ги донесе оваа технологија.

За да се подигне свеста на граѓаните потребно е да се превземат конкретни мерки во однос на едукацијата, особено за компјутерскиот простор со сите негови користи и закани. Како еден од приоритетите во образовниот систем е спроведување на едукација за новите технологии, како на пример вклучување во редовен образовен програм, програми за подигање на свеста, образовни интернет сајтови. Реална е потребата да се применува обука на сите државни службеници за безбедно користење на информационо комуникациската технологија. Исто така потребно е да се воспостави меѓународна соработка како основа за воспоставување на стандарди на полето на компјутерската и информационата безбеднсот, што во иднина би значело сигурна, отворена информационо комуникациска структура која подржува меѓународна соработка, ја зајакнува меѓународната безбедност и ја подржува слободата на иновации.

Подеднакво важно за самата држава, народ и поединец е јакнење на соработката на полето на компјутерската безбедност, затоа што компјутерскиот простор стана глобална територија која ги избриша сите граници помеѓу луѓето.

За сигурна иднина во светот во кој незапирливо напредува информатичката сфера потребно е размена на искуства на оваа тема помеѓу земјите, примери од нивната пракса, соработка на правно и полициско ниво, на глобално ниво донесување и примена на закон за истрага и процесуирање на криминалците од оваа област.

Скоро сите развиени земји имаат донесено своја Стратегија за Компјутерски Криминал, а Р.Македонија е на добар пат за донесување на својата стратегија, како и насочување на своите цели и мерки према глобалните. Во контекст на ова е потребата да се следи патот према Европската Унија, кој мора да биде усогласен со Европските трендови.

8. СТРАТЕГИИ ВО БОРБАТА ПРОТИВ ВИСОКОТЕХНОЛОШКИОТ КРИМИНАЛ

Стратегијата за компјутерска безбедност на Европската Унија е усвоена во 2013 година, и преставува сеопфатен акт кој Европската Унија го сочинила за оваа област. Во самиот документ во повеќе наврати се истакнува дека основната вредност на која се темели Европската Унија мора да се почитува и во компјутерскиот простор.

Тоа значи дека постоечките меѓународни правни акти во областа на човековите права се сосема применливи и во виртуелниот свет, како што се Меѓународната Конвенција за човекови и политички права, Европската Конвенција за човекови прави и Повелбата на Европската Унија за основни права. Иако компјутерскиот простор е „виртуелен" во него не смее да постои помала толеранција на кршење на човековите права.

Се чини дека ова начело понекогаш се заборава, со оглед на тоа дека интернетот се почесто се доживува како простор каде што кршењето на човековите права, нанесувањето на материјална и нематеријална штета и сторувањето на кривични дела имаат помала тежина во однос на стварниот свет.

8.1 ПРИОРИТЕТИ И АКТИВНОСТИ

За да се исполни овој приоритет неопходно е учество на бројни друштвени фактори, како во јавниот така и во приватниот сектор. Потребно е да се усвои регулатива која ќе одговара, во рамките на земјата членка да се одреди орган кој ќе биде надлежен за информатичката безбедност и ќе воспостави национални тимови за превенција и реагирање на компјутерски инциденти – CERT (Computer Emergency Response Team). [129]

Треба приватниот сектор да се охрабри да биде припремен на предизвиците кои ги носи технолошкиот развој, како и да го зголеми вложувањето во информатичката безбедност. Поголемиот дел од приватниот информациски сектор, го смета за терет инвестирањето во безбедноста, и поради тоа потребно е да се промени таквиот став за општо добро.

Со цел ефикасна превенција и заштита, е од голема важност да надлежните државни тела да разменуваат информации за опасности и инциденти во информациониот систем, како и да одржуваат посебни вежби – симулација на компјутерски инцидент, во кој заеднички би учествувале со преставници од приватниот сектор.

Со оглед на тоа дека јавните институции, приватниот сектор и граѓаните не се доволни свесни за ризикот и опасностите во компјутерскиот простор, потребно е да се споделуваат информации за компјутерските закани и со тоа навремено ќе се превземат мерките за заштита.

Европската агенција за безбедност на мрежата и податоците (ENISA) е таа која треба да изготвува извештај за компјутерските инциденти, да организира работилници и да го подобрува јавно-приватното партнерство. Европол, Eurojust се надлежни за заштита на податоци и исто така имаат значајна улога во подигање на свеста и информираност за компјутерските

[129] http://whatis.techtarget.com/definition/CERT-Computer-Emergency-Readiness-Team .

ризици и инциденти. За оваа цел Европол пред неколку години го формира Европскиот Центар за Компјутерски криминал.

Компјутерскиот криминал е облик на криминал кој е во најголем пораст. Компјутерскиот криминал стана дел од нашето секојдневно живеење, иако често не сме ни свесни дека со него се сретнуваме, или дури и во него учествуваме. Милиони луѓе дневно се жртви на кривични дела во компјутерскиот простор. Посебно е тешко тоа што компјутерскиот криминал нема граници, односно на сторителите на овие кривични дела им е големо олеснување глобалната поврзаност и масовноста на новата технологија.

Имајќи го во предвид растот на компјутерскиот криминал, кривичните прописи треба да содржат норми со кои ќе биде овозможено строго и ефикасно да се казнуваат сторителите на овие кривични дела. Конвенцијата на Советот на Европа за високотехнолошки криминал и Директивата на Европската Унија за нападите на информационите системи, преставува добар оквир за дефинирање на кривични дела во компјутерскиот простор и санкционирање на сторителите. Исто така соработката на државите членки со Европскиот Центар за борба против компјутерски криминал (EC3) во рамките на Европол, Eurojust и други релевантни институции е од големо значење за адекватна и координирана акција за сузбивање на кривични дела.

Компјутерската одбрана треба да се сконцентрира на откривање, реагирање и обновување од софистицирани компјутерски напади. За да се избегне дуплирање во вршење на овие активности, ќе се настојува Европската Унија и НАТО да бидат координирани во вршење на активностите со цел да се зголеми отпорноста на критичните инфрастуктури на државните институции, одбранбените системи и други информациони системи од кои државите членки зависат.

Хардверските и софтверските компоненти на Европската Унија и трети земји, мораат да бидат сигурни, безбедни и да гарантираат заштита на приватните податоци. За остварување на оваа цел Стратегијата констатира

дека од големо значење е промовирање на единствен пазар за безбедносни информациони производи.

Повеќето фирми кои учествуваат на пазарот за нови технологии, вложувањето во безбедноста на своите производи го смета за товар, и поради тоа многу производи не ги исполнуваат безбедносните услови. Јавните и приватните субјекти се повикани да воспостават добра безбедносна пракса и да створат потикнување на пазарните услови за развој и усвојување на безбедносни информациони решенија. Истите треба да се насочат на добро управување со ризици, како и на усвојување на безбедносни стандарди и воспоставување на процедури за сертфификација.

Европската Комисија побарала од ENISA да развие технички правци и препораки за усвојување на стандарди и добри безбедносни пракси во информациските системи. Во правец на ова, Комисијата го подржала развојот на безбедносните стандарди во областа клауд „cloud" виртуелна платформа за чување податоци, посебно потребата за заштита и чување на податоците.

8.2 ЕВРОПСКА СТРАТЕГИЈА ЗА КОМПЈУТЕРСКА БЕЗБЕДНОСТ

Европската Стратегија за Компјутерска Безбедност преставува прв сеопфатен акт кој Европската Унија го направила за оваа област. Во повеќе наврати низ стратегијата се потенцира дека основните принципи и вредности на кои постои Европската Унија мора да се почитуваат и во компјутерскиот простор. Во оваа стратегија е констатирано дека на ниво на Европската Унија се настојува да се промовира отвореност и слобода на изразување на интернет, и дека ќе се вложат напори за примена на постоечките меѓународни правни акти во компјутерскиот простор. Преставниците на Европската Унија сметаат дека во компјутерскиот простор може да се применуваат постоечките правни акти со кои се регулираат човековите права.

Иако компјутерскиот простор е виртуелен, во него не смее да постои кршење на човекови права, но ова правило се заборава со оглед на фактот дека интернетот се доживува како простор каде кршењето на човековите права, нанесувањето материјална и нематеријална штета не се сметаат за кривични дела, како што е во реалниот свет.

За да се достигне потребното ниво на заштита на информационите системи, имајќи го во предвид брзото ширење на технологијата, односно нејзината употреба во различни области, неопходна е соработка помеѓу сите актери на ниво на Европската Унија и на национално ниво, кои би превзеле одговорност и би ги прифатиле идните предизвици.[130]

❖

Европската Стратегија за Компјутерска Безбедност преставува збир на принципи и активности кои се базирани на заштита и промовирање на правата на граѓаните, и исто така утврдено е дека Европската Унија треба да има најбезбедно интернет опкружување.

---

[130] *http://pravoikt.org/strategija-saiber-bezbednosti-eu-otvoren-bezbedan-i-zasticen-saiber-prostor/ (09.03.2016).*

Денешниот свет е преполн со опасности, но истовремено овозможува и нови привилегии. Европската Унија е таа која може сериозно да се спротистави на новите предизвици и закани. На глобално ниво сериозно и одговорно влијание, единствено би имала само Европската Унија. Само на тој начин Европската Унија би допринела за еден мултилатерален, делотворен систем кој би водел кон сигурен, праведен и обединет свет.

8.3 КОНВЕНЦИЈА ЗА КОМПЈУТЕРСКИ КРИМИНАЛ

Конвенцијата за Високотехнолошки криминал е усвоена на 08.11.2001 година, а потпишана истата година во Будимпешта на 23.11.2001 година, а Р.Македонија донесе Закон за ратификација на Конвенцијата за Компјутерски Криминал кој стапи на сила 02.07.2004 година.[131] Преставува резултат на четиригодишно работење на експертска група од Советот на Европа помогната од експерти од САД, Канада, Кина и други држави кои не се членови на Советот на Европа. Конвенцијата е потпишана од 38 држави (помеѓу нив се и држави кои не се членки на Советот На Европа а тоа се: Канада, Јапонија, Јужна Африка и САД), а ја ратификуваа 11 држави: Албанија, Бугарија, Кипар, Данска, Естонија, Хрватска, Луксембург, Унгарија, Македонија, Романија и Словенија.[132]

Видливо е дека помеѓу државите кои ја ратификувале Конвенцијата нема големи технолошки развиени држави, а всушност од нив ќе зависи успехот на конвенцијата на глобално ниво. Непобитен факт е дека поголемиот дел од државите кои ја ратификуваа Конвенцијата се нови членки на Европската Унија или земји кандидати за влез во Европската Унија.

Оваа Конвенција спаѓа во кругот на така наречени Рамковни Конвенции, нејзините одредби не се директно применливи, така што секоја држава треба да ги имплементира во своето законодаство.

Една од причините за нејзиното донесување е уверувањето дека ефикасната борба против компјутерскиот криминал бара зголемена, брза, функционална соработка од кривичен аспект, и тоа мора да го имаат во предвид земјите од нашиот регион доколку сакаат да имаат резултат и успех во борбата против компјутерскиот криминал.

---

[131] *Закон за ратификација на Конвенцијата за Компјутерски Криминал, бр. 07-2623/1, 16 јуни 2004 година Република Македонија, Скопје.*

[132] *Светлана Николовска ,,Методика на истражување на компјутерски криминалитет" Ван Гог, Скопје, 2014, стр.43.*

Верувајќи во потребата да се изгради како прашање на приоритет заедничка криминална политика насочена кон заштита на општеството од компјутерски криминал, меѓу другото, преку усвојување на соодветно законодаство и негување на меѓународната соработка, свесни за темелните промени што настануваат со дигитализацијата, конвергенцијата и континуираната глобализација на компјутерските мрежи, убедени сме дека оваа Конвенција е неопходна за одвраќање од актите насочени против тајноста, интегритетот и достапноста на компјутерските системи и мрежи, и компјутерските податоци, како и против злоупотребата на таквите системи, мрежи и податоци преку криминализација на дејствијата опишани во оваа Конвенција и преку воведувања овластувања потребни за ефикасна борба против таквите кривични дела, преку овозможување на нивно откривање, спроведување истрага и подигнување на обвинение на национално и меѓународно ниво и преку обезбедување аранжмани за брза и сигурна меѓународна соработка.

Целите на Конвенцијата се хармонизација на домашните материјално-правни одредби кои се поврзани со компјутерскиот криминал, обезбедување на домашното процесно право средства кои се неопходни за спроведување на истрага и покренување на постапка против сторителите на кривични дела од областа на компјутерскиот криминал, и кривични дела извршени со употреба на компјутерската технологија.

Членот 35 од Конвенцијата за Компјутерски Криминал е контакт точката **24/7**, во кој се бара секоја страна потписничка да определи место за контакт кое ќе биде ставено на располагање 24 часа во текот на сите седум дена од неделата, со цел спроведување истражни и други процесни дејствија во однос на кривичните дела поврзани со компјутерски системи и податоци, или заради прибирање докази во електронска форма за одредено кривично дело. Во Р.Македонија од 2008 година функционира дежурниот центар **24/7.**

8.3.1 ДОПОЛНИТЕЛЕН ПРОТОКОЛ НА КОНВЕНЦИЈАТА ЗА КОМПЈУТЕРСКИ КРИМИНАЛ ЗА ИНКРИМИНАЦИЈА НА ДЕЛА ОД РАСИСТИЧКИ И КСЕНОФОБИСТИЧКИ ВИД ПО ПАТ НА ИНФОРМАТИЧКИ СИСТЕМ

Дополнителниот протокол на Конвенцијата за Компјутерски Криминал за инкриминација на дела од расистички и ксенофобистички вид по пат на информатички систем, е донесен од страна на Советот на Европа на 28.01.2003 година.[133]

Република Македонија донесе посебен Закон за ратификација на Дополнителниот протокол на Конвенцијата за Компјутерски Криминал за инкриминација на дела од расистички и ксенофобистички вид по пат на информатички систем кој стапи на сила 13.07.2005 година.

Имајќи предвид дека целта на Советот на Европа е постигнување поголемо единство помеѓу неговите членки, потсетувајќи дека сите човекови суштества се раѓаат слободни и еднакви во достоинството и правата, убедени дека делата од расиситички и ксенофобистички вид преставуваат повреда на човековите права, како и закана за Правната држава и демократската стабилност, сметајќи дека националното и меѓународното право треба да предвидат соодветен правен одговор на пропагандата од расистички и ксенофобистички вид што се распростанува по пат на информатички систем, свесни дека информатичките системи нудат форма без преседан за олеснување на слободата на изразување и комуникација во целиот свет, и поради тоа е донесен и ратификуван овој дополнителен протокол.

Целта на овој протокол е да се комплетираат страните на протоколот, одредбите на Конвенцијата за Компјутерски криминал во поглед на инкриминацијата на делата од расистички и ксенофобистички вид по пат на информатички системи.

---

[133] *Законот за ратификација на Дополнителниот протокол на Конвенцијата за компјутерски криминал за инкриминација на дела од расистички и ксенофобистички вид по пат на информатички системи, Бр. 07-2621/1 5 јули 2005 година Скопје.*

„Расистички и ксенофобистички материјал" означува било каков материјал во писмена форма, било каква слика, или друго преставување на идеи, или на теории што препорачуваат или охрабруваат омраза, дискриминација, или насилство, против некое лице или група на лица, засновани на раса, боја, потекло или национална и етничка припадност, или вера, доколку ова последносто служи под изговор за еден или друг од овие елементи, или кои поттикнуваат на такви дела.[134]

Од посебно значење за областа на високотехнолошкиот криминал е **Конвенцијата на Обединетите Нации против транснационалниот Организиран криминал со дополнителни Протоколи, Палермо 2000 Година.**[135]

Палермо Конвенцијата преставува значаен напредок во глобалното одредување, дефинирање на трансационалниот организиран криминал и утврдување на промените кои државите треба да ги спроведат во нивните кривични законодаства, за да биде ефикасно спротиставувањето на организираниот криминал.

Врската на транснационалниот организиран криминал и високотехнолошкиот криминал е користењето на модерната технологија која секој ден е посовремена, во извршување на кривични дела, односно ангажирање на лица способни за работа со компјутери, особено за перењето пари, односно користењето на високата технологија за да се прикријат трагите, и парите од нелегалните бизниси (дрога, шверц на оружје и сл.) да се преточат во легални бизниси и да се искористат за истите.

Оваа Конвенција бара од државите потписнички да оформат национални тела кои ќе извршуваат надзор на финансиските институции кои се подложни

---

[134] http://www.pravo.org.mk/documentDetail.php?id=5616 *(03.04.2016 година).*

[135] *Потојниот текст од Конвенцијата е завршната верзија од работата на АД ХОК комитетот при ООН во Виена од Јули 200 година. Во Ноември 2000 година текстот од Конвенцијата е одобрен од Генералното Собрание на ООН во Њујорк, а од 12-15.12.2000 година во Палермо – Италија, конвенцијата беше отворена за потпишување и на истата пристапија повеќе од 130 земји.*

на перење, и да се обезбеди на органите кои се занимаваат со борба против перење пари можност да соработуваат во размена на информации како на национално така и на меѓународно ниво.[136]

[136] *http://www.osce.org/me/montenegro/117630?download=true (03.04.2016).*

8.3.2 – а Г8 – ПОДГРУПА ЗА ВИСОКОТЕХНОЛОШКИ КРИМИНАЛ

Г8 државите – подгрупата за високотехнолошки криминал е основана во 1997 година во Вашингтон, каде што се предвидени истраги кои вклучуваат електронски докази. Во истрагите поврзани со компјутерски мрежи важно е земјите да ги зачуваат електронските податоци или да побараат од интернет провајдерот да ги зачува податоците. За да се подобри традиционалниот метод за добивање на помош Г8 создал мрежа за да се забрзаат контактите помеѓу земјите членки или други држави, тоа е мрежата 24/7.

Мрежата се обврзува да ги направи сите напори за обезбедување на бараните податоци што е можно побрзо, да ги контактира интернет провајдерите, а тоа го бара и од сите земји членки или други дражви.[137] Целта е да се изгради глобален капацитет за спречување на криминални и терористички злоупотреби на високата технологија, како и на интернетот. За таа цел тие донеле заклучоци дека треба да се донесат сет мерки за спречување на сериозни кривични дела, вклучително и во сферата на телекомуниакциите. Тоа вклучува кражба на податоци и информации, продажба на истите, примена на вируси и други штетни програми. Самитот на Г8 кој се одржал во 2006 година во Санкт Петербург бил посветен за борбата против терористичките закани, при што е потврдена посветеноста на соработката со меѓународните партнери, вклучувајќи ефикасно справување при секој обид за злоупотреба на компјутерскиот простор за терористички цели, потикнување на терористички акти, користење за комуницирање помеѓу терористите, планирање на терористички акти, како и регрутирање и обука на терористи.

Во 2011 година групата имала состанок во Довил – Франција, при што во донесената декларација е вклучен и делот за интернетот.[138]

---

[137] *http://www.oas.org/juridico/english/cyb_pry_G8_network.pdf (03.04.2016)*
[138] *http://www.cybercrimelaw.net/G8.html (03.04.2016).*

9. ЗАКОНСКА РАМКА НА ВИСОКОТЕХНОЛОШКИОТ КРИМИНАЛ

9.1 НАЦИОНАЛНО ЗАКОНОДАСТВО НА Р.МАКЕДОНИЈА

Како што веќе споменавме, високотехнолошкиот криминал ги опфаќа сите оние облици и форми на криминални поведенија поврзани со злоупотреба на компјутерот и информатичките системи воопшто, па како такви, односно општествено опасни, противправни однесувања, со намера на сторителот за себе или за друг да прибави некаква корист (имотна или неимотна) или на друг да му предизвика штета, законодавецот соодветно ги инкриминира и пропишува како кривични дела со соодветни кривични санкции.

Така, во **Кривичниот законик на Р.Македонија,**[139]се дефинирани поимите „компјутерски систем“ и „компјутерски податоци“.

Имено, во чл.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“.

Во чл.122, т.23, е наведено дека: „под компјутерски податоци се подразбира презентирање на факти, информации или концепти во облик погоден за обработување преку компјутерски систем, вклучувајќи и програма подобна компјутерскиот систем да го стави во функција“.

[139] *Службен весник на Република Македонија бр.19 од 30.03.2004 година – пречистен текст.*

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

Прикажување на порнографски материјал на малолетник [160]

Член 193 [161]

(1) Тој што на малолетник кој не наполнил 14 години ќе му продаде, 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.

(2) Ако делото е сторено преку средства за јавно информирање, сторителот ќе се казни со затвор од три до пет години.

(3) Со казната од став (2) ќе се казни тој што ќе злоупотреби малолетно лице за изработување на аудиовизуелни слики или други предмети со порнографска содржина или за порнографска претстава, како и тој што учествува во претставата.

(4) Тој што ќе присили малолетно лице на изработување и снимање слики или други предмети со порнографска содржина или за порнографска претстава, ќе се казни со затвор од најмалку осум години.

(5) Ако делото од ставот 4 на овој член е сторено врз малолетник кој не наполнил 14 години, сторителот ќе се казни со затвор најмалку четири години.

(6) Ако делото од овој член го стори правно лице, ќе се казни со парична казна.

(7) Предметите од ставовите (1), (2), (3) и (4) на овој член ќе се одземат.

Производство и дистрибуција на детска порнографија

Член 193-а [162]

(1) Тој што произведува детска порнографија со цел за нејзина дистрибуција или ја пренесува или ја нуди или на друг начин ја прави достапна детската порнографија, ќе се казни со затвор од најмалку пет години.

(2) Тој што набавува детска порнографија за себе или за друг или поседува детска порнографија, ќе се казни со затвор од пет до осум години.

(3) Ако делото од ставовите (1) и (2) на овој член е сторено преку компјутерски систем или друго средство за масовна комуникација, сторителот ќе се казни со затвор од најмалку осум години.

(4) Ако делото од овој член го стори правно лице, ќе се казни со парична казна.

Правење и внесување на компјутерски вируси 211

Член 251-а 212

(1) Тој што ќе направи или ќе преземе од друг компјутерски вирус со намера за внесување во туѓ компјутер или компјутерска мрежа, ќе се казни со парична казна или со затвор до една година.

(2) 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.

(3) 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 затвор од една до пет години.

(4) Обидот за делото од став (2) е казнив.

(5) Ако делото од овој член го стори правно лице, ќе се казни со парична казна.

Компјутерска измама

Член 251-б 213

(1) Тој што со намера за себе или за друг да прибави противправна имотна корист со внесување во компјутер или информатички систем невистинити податоци, со невнесување на вистинити податоци, со менување, бришење или прикривање на компјутерски податоци, со фалсификување на електронски потпис или на друг начин ќе предизвика невистинит резултат при електронската обработка и преносот на податоците, ќе се казни со парична казна : или со затвор до три години.

(2) Ако сторителот прибавил поголема имотна корист, ќе се казни со затвор од три месеци до пет години.

(3) Ако сторителот прибавил значителна имотна корист, ќе се казни со затвор од една до десет години.

(4) Тој што делото од став (1) ќе го стори само со намера да оштети друг; ќе се казни со парична казна или со затвор до една година.

(5) Ако со делото од став (4) е предизвикана поголема штета, сторителот ќе се казни со затвор од три месеци до три години.

(6) Тој што неовластено изработува, набавува, продава, држи или прави достапни на друг посебни направи, средства, компјутерски програми или компјутерски податоци наменети за извршување на делото од став (1),ќе се казни со парична казна или со затвор до една година.

(7) Обидот за делото од ставовите (1) и (4) е казнив.

(8) Ако делото од овој член го стори правно лице, ќе се казни со парична казна.

(9) Посебните направи, средства, компјутерски програми или податоци наменети за извршување на делото ќе се одземат.

(10) За делото од став (4) гонењето се презема по приватна тужба.

Правење, набавување или отуѓување средства за фалсификување

Член 271[230]

(1) Тој што прави, набавува, продава или дава на употреба средства за правење лажни знаци за вредност ќе се казни со парична казна или со затвор до една година.

(2) Тој што неовластено изработува, набавува, држи, продава или дава на употреба инструменти, предмети, компјутерски програми и други сигурносни заштити или компоненти кои служат за заштита против фалсификување, како и средства за неовластено прибавување на банкарски податоци, заради правење лажни пари или преправање на вистински пари или, други инструменти за плаќање, хартии од вредност или лажни платежни картички ќе се казни со затвор од три до десет години.

(3) Со казната од ставот (2) на овој член ќе се казни тој што средствата за изработување на лажни платежни картички неовластено ќе ги монтира на банкарските уреди или ќе ги употреби на друг начин со намера за прибавување

на банкарски податоци од вистински платежни картички и податоци за носителите на таквите картички.

(4) Средствата од ставовите (1) и (2) ќе се одземат.

Издавање чек без покритие и злоупотреба на платежна картичка [233]

Член 274 [234]

(1) Тој што со намера за себе или за друг да прибави противправна имотна корист ќе издаде или ќе пушти во промет чек за кој знае дека нема покритие во износ кој е изрично забранет со договорот за употреба на чекот, па со тоа ќе прибави поголема противправна имотна корист, ќе се казни со парична казна или со затвор до три години.

(2) Со казната од став (1) ќе се казни и тој што со намера за прибавување противправна имотна корист ќе употреби банковна платежна или банкомат картичка за подигање пари или плаќање на стоки и услуги, за кои знае дека нема покритне во износ кој изречно е забранет со договорот за употреба на картичката, па со тоа прибави поголема имотна корист.

(3) Ако со делото од ставовите (1) и (2) е прибавена значителна имотна корист, сторителот ќе се казни со затвор од една до пет години.

(4) Ако сторителот на делото од ставовите (1) и (2) обезбеди покритие пред да дознае дека е откриен, може да се ослободи од казна.

(5) Ако делото од овој член го стори правно лице, ќе се казни со парична казна.

Изработка и употреба на лажна платежна картичка

Член 274-б [237]

(1) Тој што ќе направи лажна платежна картичка со намера да ја употреби како вистинска, или прибавува лажна картичка со таква намера, или ќе му ја даде на друг на употреба или тој што лажната картичка ќе ја употреби како вистинска, ќе се казни со затвор од шест месеца до пет години и со парична казна.

(2) Со казната од ставот (1) на овој член ќе се казни и тој што прибавува банкарски податоци од вистински платежни картички и податоци за носители

на тие платежни картички со намера да ги искористи за изработка и употреба на лажна платежна картичка или вака прибавените податоци ги дава на друг со таква намера.

(3) Ако сторителот од ставот (1) на овој член стекне поголема имотна корист, ќе се казни со затвор од една до осум години.

(4) Ако делото од ставовите (1), (2) и (3) на овој член е сторено од член на група, банда или друго злосторничко здружение, сторителот ќе се казни со затвор најмалку четири години.

(5) Ако делото од овој член го стори правно лице ќе се казни со парична казна.

Компјутерски фалсификат 310

Член 379-а

(1) Тој што со намера да ги употреби како вистински неовластено ќе изработи, внесе, измени, избрише или направи неупотребливи компјутерски податоци или програми што се одредени или подобни да служат како доказ за факти што имаат вредност за правните односи или тој што таквите податоци или програми ќе ги употреби како вистински, ќе се казни со парична казна или со затвор до три години.

(2) Ако делото од став (1) е сторено во однос на компјутерски податоци или програми што се користат во работењето на државни 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 затвор од една до пет години.

(3) 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 затвор до три години.

(4) Обидот за делото од ставовите (1) и (3) е казнив.

Злоупотреба на лични податоци

Член 149 114

(1) Тој што спротивно на условите утврдени со закон без согласност на граѓанинот прибира, обработува или користи негови лични податоци, ќе се казни со парична казна или со затвор до една година.

(2) Со казна од став (1) се казнува тој што ќе навлезе во компјутерски иинформатички систем на лични податоци со намера користејќи ги за себе или за друг да осгвари некаква корист или на друг да му нанесе некаква штета.

(3) Ако делото од ставовите (1) и (2) го стори службено лице во вршење на службата, ќе се казни со затвор од три месеци до три годиии.

(4) Обидот е казнив.

(5) Ако делото од овој член го стори правно лице, ќе се казни со парична казна.[140]

Оштетување и неовластено навлегување во компјутерски систем

Член251

(1) Тој што неовластено ќе избрише, измени, оштети, прикрие или на другначин ќе направи неупотреблив компјутерски податок или програма илиуред за одржување на информатичкиот систем или ќе го оневозможи илиотежне користењето на компјутерски систем, податокот или програмataили на компјутерска комуникација,ќе се казни со парична казна или со затвор до три години.

(2)Со казната од став 1 ќе се казни и тој што неовластено ќе навлезе вотуѓ компјутер или систем со намера за искористување на неговитеподатоци или програми заради прибавување противправна имотна илидруга корист за себе или за друг или предизвикуваше имотна или другаштета или заради

[140] *Кривичен законик – Сл. весник на РМ бр. 37/96) , (Измени и дополнувања – „Службен весник на Република Македонија" бр. 80/99, 4/02, 43/03, 19/04, 81/05, 60/06, 73/06, 7/08, 139/08, 114/09 и 51/11) , (Одлуки на Уставен суд на Република Македонија – „Службен весник на Република Македонија" бр. 48/01, 16/02, 40/04, 50/06*

пренесување на компјутерските податоци што не му сенаменети и до кои неовластено дошол на неповикано лице.

(3)Тој што делата од ставовите 1 и 2 ќе ги стори спрема компјутерскисистем, податоци или програми што се заштитени со посебни мерки назаштита или се користат во работењето на државни органи, јавнипретпријатија или јавни установи или во меѓународни комуникации, иликако член на група создадена за вршење такви дела,ќе се казни со затвор од една до пет години.

(4)Ако со делото од ставовите 1 и 2 е прибавена поголема имотна користили е предизвикана поголема штета,сторителот ќе се казни со затвор од шест месеци до пет години.

(5) Ако соделото од став 3 е прибавена поголема имотна корист или е предизвиканапоголема штета, сторителот ќе се казни со затвор од една до десет години.

(6)Тој што неовластено изработува, набавува, продава, држи или правидостапни на друг посебни направи, средства, компјутерски програми иликомпјутерски податоци наменети или погодни за извршување на делата одставовите 1 и 2,ќе се казни со парична казна или со затвор до една година.

(7)Обидот за делото од ставовите 1 и 2 е казнив.

(8)Посебните направи, средства, компјутерски програми или податоцинаменети за извршување на делото ќе се одземат.

ЗАКОН ЗА КРИВИЧНА ПОСТАПКА НА РЕПУБЛИКА МАКЕДОНИЈА

Во 2004 година во Р.Македонија донесени се измени на Законот за Кривична Постапка во делот на примена на посебни истражни мерки (пим) со цел примена на софистицирани техники за прибирање на докази и нивна употреба пред суд. Па така во член 146 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 злосторничко здружение, може да се нареди преземање на посебни истражни мерки:

1) следење на комуникации и влез во дом и други простории или во превозни средства заради создавање на услови за следење на комуникации, под услови и постапка 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 (симулиран) откуп на предмети, како и привидно (симулирано) давање поткуп и привидно (симулирано) 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 (симулирана) банкарска сметка, на која може да се вложуваат средства што потекнуваат од сторено кривично дело и
8) регистрирање на привидни (симулирани) правни лица или користење на постојни правни лица заради собирање на податоци.[141]

[141] *Службен весник на РМ, бр. 67 од 29.05.2009 година.*

ЗАКОН ЗА ПОДАТОЦИ ВО ЕЛЕКТРОНСКИ ОБЛИК И ЕЛЕКТРОНСКИ ПОТПИС

Со овој закон и подзаконски акти се овозможува:

- давање на правна сила на податокот во електронски облик, односно неможноста да се одбие или да не се прифати истиот како доказ само затоа што е во електронски облик;
- изедначување на правната важност на електронскиот документ со документот во писмена форма;
- изедначување на важноста и давање на сила на доказ на електронскиот потпис со квалификуван сертификат даден во врска со електронски податоци со своерачниот потпис даден во врска со хартиени документи;
- формирање и функционирање на правни лица кои ќе издаваат сертификати за електронски потпис. Со сертификатите за електронски потписи се овозможува сигурна комуникација, кореспонденција и вршење на трансакции по електронски пат помеѓу правни и физички лица. На тој начин се овозможува замена на писмената комуникација и се отстрануваат бариерите поврзани со растојанието помеѓу субјектите.[142]

[142] *Службен весник на Р. Македонија бр.98/08 од 04.08.2008 година.*

ЗАКОН ЗА ЗАШТИТА НА ЛИЧНИТЕ 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 обработката на личните податоци. Главни начела на кои се заснова законот и кои треба да се почитуваат во практиката 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 се воспоставува *Дирекцијата за заштита на лични податоци* како самостоен и независен државен орган со советодавни и контролни надлежности во областа.[143]

[143] *Сл. Весник на Р. Македонија, бр.43 од 04.03.2014 година.*

ЗАКОН ЗА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

Со овој Закон помеѓу другото се уредуваат мерките и активностите за информатичка безбедност, односно: сертификација на комуникациско-информатички системи (кис) и процеси; проценка на можно нарушување на безбедноста на 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 во кис; дистрибуција на криптоклучеви и друг криптоматеријал; криптографска заштита на кис; определување на зони и простории заштитени од компромитирачко електромагнетно зрачење и инсталирање на уреди за чување на класифицирани информации.

Целта на овој закон е обезбедување на законито 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, нејзиниот територијален суверенитет и интегритет, уставниот поредок, јавниот интерес, слободите и правата на човекот и граѓанинот.

За обезбедување на доверливост, интегритет и достапност на класифицираните информации во кои се спроведува процес на безбедносна акредитација, кој опфаќа: акредитација, сертификација и евалуација.

Со Законот се воспоставува *Дирекција за безбедност на класифицирани информации* како самостоен орган на државната управа со бројни надлежности во оваа област.[144]

---

[144] *Сл. весник на Р Македонија" бр. 9/04 од 27.02.2004 година.*

ЗАКОН ЗА СЛОБОДЕН ПРИСТАП ДО ИНФОРМАЦИИ ОД ЈАВЕН КАРАКТЕР

Овој Закон 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.

Целта на законот е да се обезбеди јавност и отвореност во работењето на имателите на информации, а на физичките и правни 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 во 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. [145]

[145] *Службен весник на Р. Македонија бр.86/08 од 14.07.2008 година.*

9.2 МЕЃУНАРОДНИ КОНВЕНЦИИ И ДОГОВОРИ

Правната регулатива за високотехнолошкиот криминал, на меѓународен план, датира уште од втората половина на осумдесетите години, кога Американскиот конгрес во 1986 година го изгласа „Законот за компјутерски измами и злоупотреби" и „Законот за приватноста на електронските комуникации". Од тогаш, до денес многу земји ги изменија своите кривични закони и донесоа низа од посебни законски во согласност со меѓународните прописи и правни акти, како и препораките на меѓународните организации, а се со цел сообразување на националните законодавства со модерните текови на општеството и ефикасна борба со компјутерскиот криминал.

Во духот на ова, се и претходно наведените измени и актуелни законски решенија во Кривичното Законодавство на Р.Македонија. На сличен начин, водејќи се од актуелната Конвенцијата на Советот на Европа за компјутерски криминал се сообразени законодавствата како на членките на ЕУ, така и на земјите кандидати.

Кривичните дела извршени со помош на компјутер се извршуваат во компјутерскиот простор „cyber space", и со тоа не запираат на државните граници. Во принцип, тие може да се извршат било каде и против било кој низ целиот свет.

Ефикасна акција за борба против високотехнолошкиот криминал е потребна како на Национално, така и на Меѓународно ниво.

Во повеќето земји фокусот за заштита од високотехнолошкиот криминал е насочен на национално ниво. Законската регулатива ширум светот забележува големи разлики особено во делот на високотехнолошкиот криминал. На национално и меѓународно ниво потребата за ефикасна борба против високотехнолошкиот криминал е широко позната.

9.3 СПОРЕДБЕНО ПРАВО

Високотехнолошки Крининал во Турција

Турција ја потпиша Конвенцијата за Компјутерски Криминал од Будимпешта на 10.11.2010 година, но сеуште ја нема ратификувано, и го нема потпишано дополнителниот протокол. На 07.12.2011 година Турција ја ратификуваше Конвенцијата за заштита на деца од сексуална експлоатација и сексуална злоупотреба.

Иако Турција ја нема потпишано Конвенцијата за Компјутерски Криминал и нејзиниот дополнителниот протокол, нејзиниот Кривичен Закон содржи одредби кои се применуваат во случаи на компјутерски криминал. Член 9 (дела поврзани со Детска порнографија) е дел од еден поширок концепт според Турскиот Закон.

Одредбите кои се однесуваат на член 16 до член 18 од Конвенцијата, Турција одржува систем за задржување и зачувување на податоци како што се дефинирани во согласност со Европската Директива.

Исто така Турција прави подготовки за создавање на нацрт закон за безбедност на информации во поглед на ратификација на Конвенцијата.

Турција е составена од 81 провинција и 921 област, и сите се под надлежност на Министерот за Внатрешни работи. Тој ја врши оваа должност преку жандармерски генерален командант на вооружените сили, Генерален директорат на Националната полиција и крајбрежна командна стража. Единици за Компјутерски криминал и технички тимови за подршка постојат во рамките на Турската жандрмерија ASOC во пет провинциски жандармерии. Во иднина се планира да има во сите 81 провинција компјутерски единици.

Дигитални докази за време на истрага се обезбедуваат со наредба на судијата во согласност со Турската Кривична постапка. Вработените во овие единици се обучени и опремени за извршување на овие функции.

Форензичките лаборатории изготвуваат експертски извештаи по завршување на истражувањето на дигиталните докази. Вработените во овие лаборатории имаат право да даваат експертски извешати, и исто така имаат соодветни обуки и се опремени за извршување на овие функции.

Според Турскиот кривичен Законик Јавните обвинители се одговорни за спроведување на овие истраги. Тие ги вршат овие истражувања преку судски единици за спроведување на законот како што е КОМ – Единицата за Компјутерски криминал која ги води вие истраги по добиени инструкции од обвинителот кој е задолжен за случајот. Јавните обвинители немаат посебни Единици за Компјутерски криминал, но тие го имаат UYAP (Национален правно информатички систем) кој се состои од Обвинители во големите градови во Турција.

Во прилог на Единиците за Компјутерски Криминал постои посебна единица наречена TUBITAK, која е одговорна за прашањата за компјутерска безбедност, дигитални докази и сл.

Поради структурата на интернетот, меѓународната соработка има многу важно место во истрагите за компјутерски криминал.

Во Јули 2011 година Владата на Турција формирала посебен Оддел за Компјутерски Криминал, во рамките на Турската Национална Полиција. Тие имаат овластување да ги водат сите дела поврзани со компјутерски криминал, како и детската порнографија. Тие исто така се неформална контакт точка 24/7 за спроведување на законот. Во прилог на оваа централа единица има 81 провинциски единици како и 17 регионални форензички лаборатории. Испитуваења и анализи се вршат во лабораториите од страна на добро обучен кадар. Вкупно има 700 вработени во регионите, од кои 150 во Истанбул.

Исто така во Турција има Национален Совет за Компјутерска Безбедност во кој се преставници од Министерството за Транспорт и Врски, Министерството за Надворешни работи, Министерството за Одбрана, Министерството за Телекомуникации, Поморски, Единицата за Финансиско Разузнување.

Оваа група е задолжена за креирање на националната политика за Компјутерски криминал, компјутерските закани, одбрана на клучни стратешки средства како и подигнување на јавната свест.

Во однос на меѓународната соработка Турција за да добие податоци од странски земји, потребна и е меѓународна правна помош. Генералниот Директорат за меѓународно право и надворешни односи во рамките на Министерството за правда е централен орган за извршување на сите барања за меѓународна правна помош во кривичната материја.

Турција ги зачувува податоците, како што е пропишано во чл.31 од Конвенцијата за Компкутерски Криминал од Будимпешта.

Соработка со странски полициски органи Турција врши согласно со билетарални договори, или преку меѓународни организации како што се Интерпол, Селек и Европол. Полициската соработка е возможна за размена на информации, соработка во заеднички тимови и паралелни истраги во рамките на соодветните договори.

Министерството за Правда на Турција е централен орган надлежен за сите барања за меѓународна правна помош. Тоа исто така е контакт точка на точката 24/7. Исто така и Полцијата има контакт точка на точката 24/7.

За добивање податоци од Интернет Провајдери во Турција, потребно е официјално барање од Обвинителство. За време на истрага доколку се потребни податоци од Интернет провајдери, полициските службеници се обраќаат официјално до Обвинителот, а потоа Обвинителот разгледува дали

ќе даде Наредба до Интернет Провајдерот. Во однос на ова ист е случајот и во Р.Македонија.

Во Турција Интернет сервис провајдерите податоците ги чуваат минимум шест месеци до две години. Ретроактивно може да се добијат податоци за период од три месеци.

Соработката со Интернет провајдерите е од витално значење, како за Турција, така и за сите земји вклучувајчи и ја Македонија.

Високотехнолошки Криминал во Хрватска

Хрватска ја ратификувала Конвенцијата за Компјутерски Криминал од Будимпешта на 17.10.2002 година, и дополнителниот протокол за ксенофобија и расизам на 04.07.2008 година. Исто така Хрватска на 21.09.2011 година ја ратификувала Конвенцијата за заштита на деца од сексуална експлоатација и сексуална злоупотреба.

Хрватска во рамките на подготовка на Ратификација на Конвенцијата за компјутерски Криминал од Будимпешта, направила измени во Кривичниот Закон во однос на кривичните дела поврзани со Детска Порнографија, Достапност на Компјутерски податоци, компјутерски фалсификат, компјутерска измама и сл.

Законодаството на Хрватдска е усогласено со Конвенциите од Будимпешта и Ланзароте. Во Кривичниот Закон на Хрватска од Јануар 2013 година[146] влезена е во сила посебна глава за кривични дела за компјутерски криминал. Исто така Хрватскиот закон е усогласен во однос на правилата за собирање и обработка на податоци во областа на електронските комуникации.

Законот за собирање на податоци бара од Интернет провајдерите да ги чуваат податоците 12 месеци. Покрај тоа може да изречат мерка забрана на осудени лица да имаат пристап на интернет, како и забрана на интернет провајдерите да дозволуваат интернет сообраќај на овие лица.

Одделот за високотехнолошки криминал е основана преку Правилникот за внатрешна организација на Министерството за внатрешни работи, кој беше усвоен од страна на Владата на 20 јуни 2012 година. Тој се наоѓа во рамките на службата за економски криминал и корупција, која е дел на Националната полиција на Канцеларијата за сузбивање на корупцијата и организираниот криминал.

Одделот за високотехнолошки криминал систематски, следи и проучува феноменолошкиот и етиолошките аспекти на компјутерскиот криминал и

[146] *Кривичниот законик е донесен во октомври 2011 година, а стапи на сила од јануари 2013 година.*

предлага решенија во однос на подигање на нивото на ефикасност во борбата против компјутерскиот криминал, директно спроведува сложени кривични истраги во областа на кривичните дела против и со употреба на компјутерски системи и мрежи, врши форензички анализи и следење на интернет, обезбедува специјализирана поддршка на другите организациони единици на полицијата, соработува со другите организациони единици на Министерството, Владата, органи и правни лица, полицијата на други држави и меѓународни институции во нивна надлежност, учествува во планирањето и развојот на програми за обука на полициските службеници за прашањата на компјутерскиот криминал, учествува во изготвување на нормативни документи, извештаи и мислења на експерти во областа на компјутерскиот криминал и врши други работи од својот делокруг.

Има пет полициски службеници, вклучувајќи го и раководителот. Во рамките на секоја од 20 полициски области има помеѓу еден и четири одговорни лица за економски криминал, вклучувајќи компјутерски криминал. Ова го прават уште 35 лица кои се способни за спроведување на основниот компјутерски криминал, напади и испитувања. Форензичкиотцентар кој е дел од Министерството за внатрешни работи, врши посложена анализа на дигитални докази.

Постојат дополнителни осум полицајци распоредени во регионалните центри кои се способни за повеќе комплицирани процедури за испитување отколку што може да се врши од страна на локалните службеници. Овие регионални центри се сметаат како повеќе ефикасна алтернатива за репродукција на Централна единица за борба против компјутерски криминал за 20 полициски области. Регионалните канцеларии ќе биде во состојба да спроведат некои основни форензички анализи.

Во однос на меѓународната соработка, во Хрватска одговорни за барањата за меѓуанродна правна помош се судовите и државниот правобранител.

Главните пречки со кои се соочува Хрватска во областа на меѓународната соработка, е одбивањето на некои земји да обезбедат и

информации, како што се идентитетот на администраторите на веб-сајт или идентитетот на сопствениците на бесплатни е-мејл сметки, без доставување официјално барање за меѓународна правна помош.

Хрватската Академска истражувачка мрежа „CARNET“ е Национална истражувачка мрежа која е финансирана од Владата. Има канцеларии во сите поголеми градови, и нејзина цел е да промовира образовни програми и да ги охрабри претпријатијата преку иновативна технологија за доброто на општеството.

Соработката со Интернет Провајдерите е иста како и во Турција, односно се бара налог од Надлежниот Обвинител. Давателите на интернет услуги се должни да ги чуваат податоци во период од една година.

Хрватска има Центар за оперативна технологија за телекомуникациски надзор „OTC“ кој е орган кој делува како посредник помеѓу Агенцијата за спроведување на законот LEA и Интернет провајдерите ISP. Постапката за испраќање барања до Интернет провајдерите во Хрватска е централизиран.

Високотехнолошкиот Криминал во Србија

Во Република Србија има посебна глава во Кривичниот законик каде што се систематизирани посебно кривични дела со елементи на компјутерски криминал насочени против имотот и се насловени како ,,Казнени дела против безбедноста на компјутерските податоци ".[147]

Од 2006 година формирано е Специјализирано Одделение за борба против компјутерскиот криминал во рамките на округот на Јавното Обвинителство во Белград со назив Специјално Обвинителство за Високотехнолошки криминал, проследено со формирање на посебно одделение за борба против високотехнолошкиот криминал во рамките на посебна служба за борба против Организираниот криминал на Министерството за Внатрешни работи и специјалниот истражен и Судскиот Совет за Високотехнолошки Криминал на Вишиот суд во Белград со широка национална надлежност. Оттогаш широк спектар на криминална активност се занимаваа со безбедноста на компјутерски криминал. Најчесто се случуваат неовластен пристап до компјутерски системи, компјутерска измама, фалсификување и злоупотреба на кредитни картички и повреда на авторско право и сродни права со новиот тренд на зголемување на случаи на детска порнографија.

Србија ја ратификуваше Конвенцијата за Компјутерски Криминал од Будимпешта на 14 април 2009 година и Дополнителниот протокол на ксенофобија и расизам на 14 април 2009 година, Конвенцијата за заштита на деца од сексуална експлоатација и сексуална злоупотреба е ратификувана од страна на Србија на 29-ти јули 2010 година.

Министерството за внатрешни работи има одговорност за истраги за кривични дела кои вклучуваат дистрибуција на нелегални содржини на интернет и злосторства кои се однесуваат на повреда на правата од интелектуална сопственост. Единицата за високотехнолошки криминал е

---

[147] *Чл. 186 – а,б,в,г,д,ђ,е, Закон о изменама и допунама Кривичног закона Република Србије, ЈП Службени гласник бр. 39/2003, Београд и Кривични законик Републике Србије, ЈП Службени гласник бр. 85/05.*

овластена да врши истраги за злосторства против компјутерски системи, како и сите кривични дела кои вклучуваат технологија.

Меѓународната соработка ја остваруваат преку разни меѓународни полициски организации како што се Европол, Селек, Интерпол и Мрежата 24/7.

Постојат два посебни дела во Одделот за високотехнолошки криминал: за интелектуална сопственост и Високотехнолошки криминал. Единицата за високотехнолошки криминал е составен од 20 луѓе и обезбедува функции на точката за контакт 24/7 како и спроведување на законот. Таа е наменета за подобрување на способноста за истражување на компјутерски криминал. Одделот за компјутерски криминал е во состојба да демонстрираат напредни способности во оваа област. Тие се технички добро опремени, како и со високо компетентен и искусен персонал.

Во прилог на спроведувањето на овие напредни технички истражувања, Одделот за борба против високотехнолошки криминал нуди совети и помош на други единици, пребарување и заплена на уреди и опрема, ракување со процедурите и изворите на електронски докази. Таа исто така има способност за следење во живо на интернет комуникации (за сериозни кривични дела). Тие се во можност да вршат на интернет следење на сите компјутери базирани на кривични дела, а не само за сериозен и организиран криминал.

Во однос на вештачењата има посебен Оддел кој врши вештачења на компјутерска опрема на подрачјето на цела Србија.

Обвинителство е точка на контакт за сите правни барања 24/7. Одделот за високотехнолошки криминал служи како контакт точка 24/7 за сите барања за спроведување на законот додека се осигура дека формалните постапки правилно се почитуваат.

Извршување на барањата за меѓународна правна помош се во надлежност на домашните судови и јавни обвинители со одредени процесни дејствија спроведени од страна на Министерството за Правда, Министерството

за Внатрешни работи и Министерството за Надворешни работи. Барањата се доставуваат до странски орган, преку Министерството за Правда. Испорака исто така може да се направи директно на странски судски орган, или во итни случаи преку Интерпол.

Соработката со Интернет Провајдерите е иста како и во Турција и Хрватска, односно се бара налог од Надлежниот обвинител, кој потоа се доставува до Интернет Провајдерот. Идентификуван е проблем со недоволната регулација на Интернет Провајдерите во смисла на нивната обврска за задржување на податоците.

Високотехнолошкиот Криминал во Албанија

Албанија ја ратификуваше Конвенцијата за Компјутерски Криминал од Будимпешта на 20 Јуни 2002 година и Дополнителниот Протокол на ксенофобија и расизам на 26 Ноември 2004 година, Конвенцијата за заштита на деца од сексуална експлоатација и сексуална злоупотреба е ратификувана на 14 Април 2009 година.

Секторот против компјутерскиот криминал во Тирана е во рамките на Управата против Финансискиот криминал, Одделот за Криминалистички истраги. Овој Сектор е одговорен за спроведување на процедурални мерки за превенција, следење, документирање и борба против компјутерскиот криминал. Компјутерска лабораторија одговорна за испитување на компјутерски уреди и документирање на кривични дела поврзани со компјутер.

Полициски службеници од овој Сектор ги имаат сите напредни обуки за водење на компјутерскиот истраги.

Овој Сектор служи како точка контакт 24/7.

Форензичка лабораторија има доволно опрема и софтвери за да вршат вештачење на компјутерска опрема како и мобилни телефони.

Меѓународната соработка Албанија ја извршува преку Министерство за Правда. Барања од окружните судови и офицери од Обвинителство се испратени до централната власт и од таму до странските органи.

Албанија е вклучена во непосредна размена на информации за случаи на компјутерски криминал со земјите во регионот во форма на заеднички средби и заедничко водење на истраги.

Секторот против Компјутерскиот Криминал служи како 24/7 точка на контакт во согласност со Конвенцијата за Компјутерски Криминал од

Будимпешта Член 35. Сепак, бројот на барања останува мал и овој канал досега главно се користи за Европските земји.

Во однос на соработката со Интернет Сервис Провајдерите и добивање податоци во Албанија може да се добијат само преку Обвинител и само ако има кривична истрага иницирана заеднички од страна на полицијата и соодветното обвинителство. Во случаи на полициска истрага, информации од интернет провајдерите се добива преку Секторот за следење на телекомуникациите и односите со разузнавачките служби во Генералното обвинителство.

Интернет провајдерите имаат обврска да ги обезбеди потребните податоци.

Задржувањето на податоци е задолжително во согласност со член 101 од Законот за електронските комуникации во Албанија.

Законски времето на зачувување на податоци во Албанија е две години.

10. ИНСТИТУЦИОНАЛИЗИРАЊЕ НА БОРБАТА ПРОТИВ ВИСОКОТЕХНОЛОШКИОТ КРИМИНАЛ

10.1 МИНИСТЕРСТВО ЗА ВНАТРЕШНИ РАБОТИ

Министерството за Внатрешни Работи на Р.Македонија, во рамките на своите надлежности и законски 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. При тоа Министерството мерките и активностите ги превзема врз основа на Кривичниот Законик на Р.Македонија и Законот за Кривична Постапка.

Исто така, една од позначајните улоги на Министерството 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 спроведување на кривичното дело и пред воопшто да настане кривичното дело (на пример анимирање на јавноста преку јавни гласила, преку различни флаери со пораки, директна соработка на полицијата со граѓаните итн).

За таа цел, најпрво во Јануари 2005 година формиран е Одделот за Организиран Криминал при МВР на РМ во чии рамки постоеше посебно Одделение за Компјутерски криминал и фалсификати во склоп на Секторот за Финансиски Криминал, потоа во 2008 година прерасна во Единица за борба против компјутерскиот криминал исто во склоп на Одделот за Организиран Криминал. Во 2014 година оваа Единица се одвои од Одделот за Сузбивање на Организиран и Сериозен Криминал и прерасна во **Сектор за Компјутерски Криминал и Дигитална Форензика** при Централните Полициски Служби во Министерството за Внатрешни Работи. Во склоп на Секторот се две Одделенија и тоа Одделение за истраги за Компјутерски Криминал и Одделение за Дигитална Форензика.

Секторот за Компјутерски Криминал и Дигитална Форензика има надлежност на територијата на цела држава, како и водење на меѓународни истраги со други земји.

Надлежностите на **Одделението за истраги за Компјутерски криминал** е работа на случаеви поврзани со компјутерскиот криминал, компјутерски инциденти, неовластено навлегување во компјутерски системи, измами на интернет, електронско плаќање (фалсификување и злоупотреба на платежни картички), детска порнографија, злоупотреба на лични податоци, злоупотреби на социјалните мрежи, злоупотреба на лични податоци и др. Како една од најзначајните мерки и активности што ги превзема одделението е борба со организираниот криминал преку употреба на посебни истражни техники и водење на проактивни истраги (водење на истраги пред да е сторено кривичното дело).

Надлежностите на **Одделението за Дигитална Форензика** се анализа и вештачење на компјутерска опрема и компјутерски системи, анализа на мобилни телефони, анализа на опремата со цел на обезбедување на квалитетни електронски докази потребни за докажување на делото и водење на кривичната постапка.[148]

[148] *http://moi.gov.mk/ (26.04.2016).*

10.2 ОСНОВНО ЈАВНО ОБВИНИТЕЛСТВО

Јавното обвинителство е единствен и самостоен државен орган кој ги гони сторителите на кривични дела и на други со Закон утврдени казниви дела.

Во функција на зајакнување на позицијата на Јавниот Обвинител за да поуспешно одговори и постапи на предизвиците кои ги носи времето, во остварувањето на поефикасна борба против организираниот криминал, корупцијата и другите сериозни казниви дела, во месец декември 2007 година е донесен и Законот 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 организиран 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 гонење на организиран криминал и корупција.

Со новите измени Одделението за гонење на сторители од областа на организираниот криминал и корупција основано според поранешниот Закон во рамките на Јавно обвинителство на Република Македонија, прераснува во посебно Обвинителство и тоа како **Основно Јавно Обвинителство за гонење на организиран криминал и корупција**, основано за целата територија на Р.Македонија, со седиште во Скопје.

Во рамките на ова посебно Обвинителство е гонење на сторители на кривични дела од областа на организираниот криминал. При тоа, битна е улогата при спроведувањето на Посебните истражни мерки како еден од начините за водење на предистражна постапка.[149]

[149] *http://iorm.gov.mk/?p=690 (26.04.2016).*

10.3 МЕЃУНАРОДНА СОРАБОТКА (ИНТЕРПОЛ, ЕВРОПОЛ, СЕЛЕК)

10.3.1 И Н Т Е Р П О Л

INTERPOL

Интерпол е најголемата меѓународна полициска организација во светот, со 190 земји членки. Нејзината улога е да овозможи на полицијата низ целиот свет да работи заедно за да го направи светот побезбедно место "Поврзување на полицијата за побезбеден свет".

Високо-технолошката инфраструктура на техничка и оперативна поддршка помага да се задоволат растечките предизвици на борбата против криминалот и во 21 век. Официјалното име на организацијата е "ICPO-Интерпол". Официјалниот кратенката „ICPO" се залага за "Меѓународна криминалистичка организација. На француски јазик, е „OIPC", "Организација на Интернационален полициски криминал".

Зборот „Интерпол" е контракција на „меѓународна полиција", а бил избран во 1946 година.

До 1956 година Организацијата бил позната како Меѓународна Полициска Комисија.

Генералниот секретаријат се наоѓа во Лион - Франција, и работи 24 часа на ден, 365 дена во годината. Интерпол, исто така, има седум регионални

канцеларии низ светот и претставништво во седиштето на Обединетите нации во Њујорк и на Европската унија во Брисел. Секој од 190-те земји членки одржува Национално централно биро располага со сопствен високо обученкадар за спроведување на законот.

Интерпол ја има универзалната улога во меѓународната полициска соработка.

Интерпол обезбедува на полицијата низ целиот свет да имаат пристап до алатки и услуги потребни за да ја извршуваат својата работа ефикасно. Исто така обезбедува насочена обука, стручна поддршка, релевантни податоци и безбедни канали за комуникација. Оваа комбинирана рамка помага на полицијата на терен да ги следи најновите трендови на криминал, анализира информации и изведува операции.

Интерпол има за цел да ја олесни меѓународната полициска соработка, дури и кога не постојат дипломатските односи меѓу одредени земји. Се преземаат мерки во рамките на постоечките закони во различни земји и во духот на Универзалната декларација за човекови права.

Визијата на Интерпол е да во еден свет секој професионалец кој спроведува закон да биде во можност преку Интерпол безбедно да комуницира, да споделува информации и да има пристап на витални информации на полицијата, како и обезбедување на безбедноста на граѓаните во светот. Интерпол постојано се стреми да обезбеди и промовира иновативни и врвни решенија за глобалните предизвици во работата на полицијата и безбедноста.

Интерпол ја олеснува меѓусебната помош меѓу сите органите на прогонот. Овозможуваат полициските служби да комуницираат безбедно едни со други во целиот свет, исто така овозможуваат глобален пристап до полициските податоци и информации. Обезбедуваат оперативна поддршка на одредени подрачја. Негуваат континуирано подобрување на капацитетот на полицијата за спречување и борба против криминалот и развој на знаење и

вештини потребни за ефикасност на меѓународната полиција. Се стремат за иновации во областа на полицијата и безбедносните прашања.

Структура и управување

1.Вовед;
2.Генерално Собрание;
3.Извршен Комитет;
4.Генерален Секретаријат;
5.Национални Централни Бироа;
6.Комисија за контрола на датотеки на Интерпол.

Вовед

Активностите на Интерпол се водени од земјите-членки, од една јасна рамка на управните тела и статутарни состаноци.

Стратегија

Генералното собрание и Извршниот Комитет формираат раководење на организацијата.

Генералното собрание

Управното тело на Интерпол - Генералното собрание го сочинуваат делегати назначени од секоја земја-членка. Тоа се состанува еднаш годишно да ги преземе сите важни одлуки поврзани со политиката, ресурси, методи на работа, финансиите, активности и програми.

Извршен Комитет

Избрани од страна на Генералното собрание, Извршниот одбор на чело со Претседателот на Организацијата. Таа обезбедува насоки и насока на организацијата и го надгледува спроведувањето на одлуките донесени на Годишното собрание.

Имплементација

Ден-за-ден имплементација на стратешките одлуки на Организацијата се врши од страна на Генералниот Секретаријат и Националните Централни Бироа.

Генерален Секретаријат

Се наоѓа во Лион, Франција, Генералниот секретаријат работи 24 часа на ден, 365 дена во годината и е воден од страна на Генералниот Секретар. Секретаријатот има седум регионални канцеларии низ светот, заедно со специјални претставници во седиштето на Обединетите Нации во Њујорк и на Европската Унија во Брисел.

Национални Централни Бироа (NCBs)

Секоја земја-членка на Интерпол одржува Национално Централно Биро поврзано со Националната Полиција со нашата глобална мрежа. Составени од високо обучени национални службеници за спроведување на законот, Националните Централни Бироа се движечката сила на Интерпол, придонесуваат за нашите казнени бази на податоци и соработуваат заедно за прекугранични истражувања, операции и апсења.

Надзор

Советници - тие се експерти во чисто советодавна функција, кои можат да бидат назначени од страна на Извршниот Комитет и потврдено од страна на Генералното Собрание.

Комисија за контрола на датотеки на Интерпол (CCF)

CCFгарантира дека обработката на личните податоци - како што се имиња и отпечатоци од прсти - е во согласност со правилата на Интерпол, со цел да се заштитат основните права на поединците и соработката меѓу Полицијата на меѓународно ниво.

ПРИОРИТЕТИ

Стратегиската рамка на Интерпол ги поставува приоритетите и целите на организацијата за даден период од три години. Тоа обезбедува фокусирана и ефикасна структура за водење на ИНТЕРПОЛ програми и активности во текот на овој период, како и пријавување на напредок и успеси.

Во Октомври 2013 година, за време на својата 82 седница на Генералното Собрание на Интерпол усвои Стратегиски Рамковен Договор 2014-2016 година.

Рамковниот договор содржи четири стратешки приоритети и две корпоративни приоритети. Овие приоритети се во согласност со визијата и мисијата на организацијата и се одразуваат на динамична средина и предизвиците на меѓународната полициска работа во 21 век.

Стратешки Приоритети

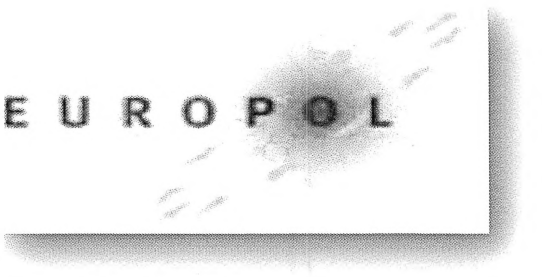
1. Сигурен глобален полициски информациски систем;
2. 24/7 поддршка на полицијата и спроведување на законот;
3. Иновации, јакнење на капацитетите и истражување;
4. Помагање во идентификацијата на злосторства и криминалци.

Корпоративни Приоритети

1. Обезбедува организациска одржливост;
2. Консолидирање на институционална рамка.[150]

[150] *http://www.interpol.int/en (25.11.2015г.).*

10.3.2 ЕВРОПОЛ



Европол е агенција на Европската унија за спроведување на законот, чија главна цел е да се помогне во остварувањето на побезбедна Европа, за доброто на сите граѓани на ЕУ. Тоа го прават преку помагање на земјите-членки на Европската Унија во борбата против сериозниот меѓународен криминал и тероризмот.[151]

Големи криминални и терористички мрежи претставуваат сериозна закана за внатрешната безбедност на ЕУ и на безбедноста и животот на својот народ. Најголемите закани за безбедноста доаѓаат од тероризам, меѓународната трговија со дрога и перење пари, организирани измами, фалсификување на еврото, трговија со луѓе. Нова опасност е компјутерскиот криминал и други закани на денешницата. Тоа се неколку милијарди евра бизнис, кој брзо се прилагодува на новите можности и традиционалните мерки за спроведување на законот.

На 29 октомври 1993 година, Европскиот Совет одлучи дека Европол треба да биде формирана во Хаг - Холандија. Градот има долга традиција за вмешаност во меѓународен закон и ред, и е дом на Меѓународниот Суд на правдата и Меѓународниот кривичен трибунал за поранешна Југославија. Денес, Европол е еден широк спектар на меѓународното право и организации за правда, вклучувајќи го Eurojust, Агенцијата на ЕУ кои се занимаваат со судската соработка, како и на Меѓународниот Кривичен Суд.

---

[151] *Светлана Николоска, Современи методи во сузбивањето на транснационалниот економско финансиски криминал, Скопје, 2015г.*

На Конвенцијата за основање на Европол според член К3 од Договорот од Мастрихт било договорено во 1995 година и по ратификацијата од страна на земјите-членки, стапил во сила на 01.10.1998 година. Конвенцијата навела она што треба да биде Европол, она што треба да се направи, и како тоа да се направи. Во согласност со Конвенцијата од секоја земја-членка се бара да назначи национална единица преку која ќе се поврзуваат нејзините надлежни органи и Европол. Националните единици треба да назначат минимум еден офицер за врски во седиштето на Европол кој ќе ги застапува интересите на нивните национални власти и да се олесни протокот на информации во двете насоки.

Во втората половина на 1990-тите години, Европската унија беше подложена на серија на промени, кои исто така влијае на Европол. Во 1995 година бројот на земјите-членки на ЕУ се зголеми од 12 на 15 со пристапот на Австрија, Финска и Шведска.

Во 1997 година, беше потпишан Договорот од Амстердам, за изменување на Договорот од Мастрихт од 1992 година на Европската Унија. Во новиот договор "третиот столб" на ЕУ, правда и внатрешни работи, беше сведено да се фокусираат на полициската и судската соработка во кривичната материја. Целокупната нејзината цел била да се креира област на слобода, безбедност и правда.

Договорот од Амстердам приклучи на Шенген Договори во правото на ЕУ.

Услуги кои ги врши Европол

- Центар за поддршка на полициските операции;
- Центар за информации и криминални организации;
- Центар за експерти за за спроведување на законот;
- Еден од најголемите концентрации на аналитички способност во ЕУ;
- Произведува редовни проценки и извештаи;

- Висока безбедност, 24/7 оперативен центар;
- Централна платформа за експерти за спроведување на законот од земјите на Европската Унија.

Европол е центар за поддршка на полициските операции, центар за информации, и центар за експерти за за спроведување на законот. Анализата е во срѓта на активностите. Европол се вработени околу 100 аналитичари, кои се меѓу најдобрите обучени во Европа. Ова му дава на Европол да е еден од најголемите концентрации на аналитички способности во ЕУ.

За да им се даде на партнерите на Европол подлабок увид во кривичните проблеми со кои се занимаваат, Европол произведува редовни проценки кои нудат сеопфатен и прогресивни анализи за криминал и тероризам во Европската Унија. Европската Закана за организиран криминал за оценување (ОКТА) идентификува и ги оценува новите закани. ОКТА ја опишува структурата на организирани криминални групи и начинот на кој тие функционираат, како и главните видови на криминал кои влијаат на Европската Унија. Ситуација на ЕУ против тероризмот и Тренд Извештај (ТЕ-САТ), на годишна основа, дава детален извештај за состојбата на тероризмот во Европската Унија.

Европол е високо-безбедносен оперативен центар. Се справува со повеќе од 18.000 случаи годишно, претворајќи квалитетна анализа на оперативните успеси. Овој сервисен центар работи нон-стоп: 24 часа на ден, 7 дена во неделата.

Европол служи како центар на ЕУ за експертиза, обезбедување на централната платформа за експерти за спроведување на законот од земјите на Европската Унија.

EUROPEAN CYBERCRIME CENTRE

Европскиот центар за компјутерски криминал (EC3) започна со своите активности во Јануари 2013 година. Истиот е за зајакнување на одговор за спроведување на законот за компјутерски криминал во Европската Унија (ЕУ) и да помогне да се заштитат европските граѓани, претпријатија и влади. Неговото основање било приоритет во Стратегијата за внатрешна безбедност на ЕУ. Новиот Европски центар за компјутерски криминал (EC3) ќе ги штити европските граѓани и компании од компјутерскиот криминал.

Заканата од компјутерски криминал е во пораст и во ЕУ е клучна цел и главно се должи на:

- нејзината напредна интернет инфраструктура;
- своите интернет-ориентирани стопанства и системи за плаќање.

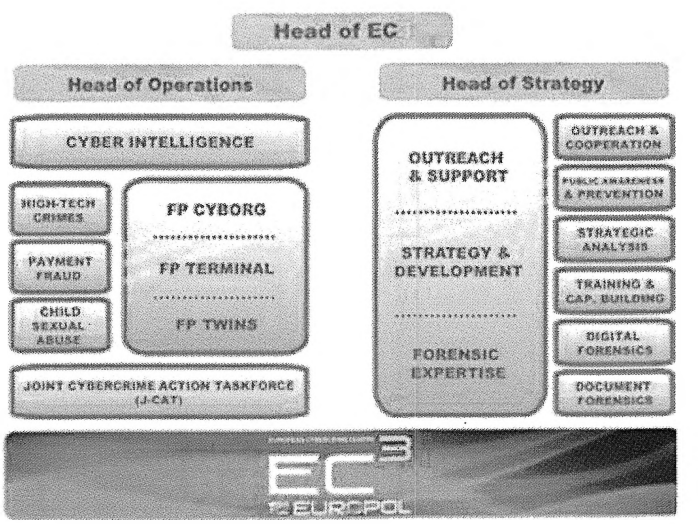
Со поставување на EC3 рамките Европол Центарот се подготви не само на постоечките капацитети за спроведување на законот на Европол, но исто така значително се проширува и на други можности, особено на оперативно и аналитичка поддршка на истрагите на земјите-членки.

EC3 доби задача да се фокусираат на следниве три области:

- Компјутерскиот криминал извршен од организирани групи, особено оние кои генерираат големи криминални профити како што се онлајн измами;
- Компјутерскиот криминал кој предизвика сериозни повреди на жртвата, како што се онлајн сексуална експлоатација на деца;
- Компјутерскиот криминал (вклучувајќи и компјутерски-напади) кои влијаат на критичната инфраструктура и информациски системи во Европската Унија.

Во однос на овие три области, EC3 Европол:

- Служи како центар за криминални и разузнавачки информации;
- Поддржува операции и истраги на земјите-членки, со помош на оперативна анализа, координација и експертиза;
- Обезбедува спектар на стратешки производи, анализа, овозможување информирани одлуки на тактичко и стратешко ниво во однос на борбата против и спречување на компјутерски криминал;
- Утврдува сеопфатна теренска функција поврзување на компјутерскиот криминал поврзан со органите на прогонот со приватниот сектор, академските институции и други партнери кои не се за спроведување на законот;
- Работилница за обука и градење на капацитети, особено во однос на надлежните органи во земјите-членки;
- Обезбедува високо специјализирани технички способности и дигитални форензичари и поддршка за истраги и операции;
- Претставува начин за спроведување на законот на ЕУ во областите од заеднички интерес (барања за истражување и развој, управување со интернет, и развој на политики).[152]



[152] https://www.europol.europa.eu/ec3, (18.11.2015г.)

10.3.3 SOUTHEAST EUROPEAN LAW ENFORCEMENT CENTER (SELEC)

СЕЛЕК

СЕЛЕК Центарот претходно СЕКИ се наоѓа во Букурешт – Романија, истиот е формиран на 7 Октомври 2011 година СЕКИ Центарот стана СЕЛЕК, додека оперативните и стратешките способности беа зачувани и пренесени на новиот SELEC.

СЕЛЕК го наследи успехот на СЕКИ Центарот - 12 години од оперативни активности, заеднички истраги, состаноци, работилници и стратешка анализа за покривање на најчувствителните трансгранични кривични области во регионот на Југоисточна Европа. Во текот на овој период, интензивна размена на информации преку офицерите за врска и комуникациски канали Центарот успешно ги поддржа напорите за спроведување на законот во земјите-членки.
СЕЛЕК има 12 земји-членки: Република Албанија, Босна и Херцеговина, Република Бугарија, Република Хрватска, Република Македонија, Република Грција, Унгарија, Молдавија, Црна Гора, Романија, Република Србија и Република Турција.

Од оперативна перспектива, новиот СЕЛЕК одржува флексибилност и оперативната ефикасност, додека зголемување на капацитетот за анализа со поширок информацискиот систем и на соодветно ниво на заштита на личните податоци во согласност со стандардите на ЕУ. Новата Конвенција предвидува меѓународно правно лице во Центарот и исто така ја дефинира и одржува соработка со други големи меѓународни организации за спроведување на законот.

ГЛАВНА ЦЕЛ НА СЕЛЕК

Целта на СЕЛЕК во рамките на соработката меѓу надлежните органи, е да се обезбеди поддршка за земјите-членки, како и подобрување на координацијата во спречувањето и борбата против криминалот, вклучувајќи сериозен и организиран криминал, каде таквиот криминал вклучува или се чини дека вклучува елемент на прекугранична активност.

ЗАДАЧИ НА СЕЛЕК

Новата конвенција предвидува:

- Координација на регионалните операции и истраги, поддршка, превенција на криминалните активностите на земјите-членки во прекуграничните случаи;
- Да им обезбеди на земјите-членки можност да разменат информации и криминалистичко разузнавање, како и оперативна помош на брз и навремен начин;
- Собира, средува, анализира, обработува и дистрибуира информации и криминалистичко разузнавање;
- Произведува стратешка анализа и проценки на закани во врска со нивната цел;
- Воспоставување, функционирање и одржување на компјутерски информатички систем, што подразбира исто така да се обезбеди заштита на личните податоци.

Корисните добивки за државите-членки, како и партнери на СЕЛЕК, се гледа во способноста да се справи со мултинационални истраги и операции во регионот на Југоисточна Европа, со минимална инвестиција. СЕЛЕК се стреми да продолжи да бидат депозитар на добрите практики во спроведувањето на законот и обезбедување на свеста преку мултинационални состаноци и конференции, да ги здружува претставниците на земјите-членки, како и на своите партнери.

Организациска Структура

СЕЛЕК е предводена од Генералниот Директор кој дејствува како Главен Извршен Директор и законски застапник. Генералниот Директор има асистенција од двајца директори, односно Директорот за Операции и Директор за правни и за внатрешни работи.

Советот е највисоко тело на СЕЛЕК при донесување на одлуки и се состои од претставници на високо ниво од секоја земја-членка. Секоја земја има право на еден глас во процесот на донесување одлуки.

Советот ги има како свој Претседател и Заменик-Претседател високите функционери од надлежните органи на земјите-членки, доделени за период од една година по азбучна ротација меѓу земјите-членки.

Оперативни Партнери

Соработката со СЕЛЕК е достапна за било која држава или меѓународна организација или тело, која има посебен интерес за соработка за спроведување на законот во Југоисточна Европа и регионот:

- Ја изразува својата подготвеност да соработува со СЕЛЕК;
- Се согласува да се обезбеди поддршка на СЕЛЕК, вклучувајќи и финансиски придонес и
- Изразува подготвеност да потпише договор за соработка со СЕЛЕК.

Држави, меѓународни организации и тела кои сакаат да станат оперативни партнери со СЕЛЕК треба да:

- Аплицираат за таков статус и
- Исполнуваат критериуми за подобност.

Овој договор за соработка се уредува, меѓу другото е соодветен со прописите за заштита на личните податоци, мерки на безбедност, финансиски односи и решавањето на споровите помеѓу СЕЛЕК и оперативниот партнер.

Откако нацрт-текстот на договорот за соработка е одобрен од страна на Советот на СЕЛЕК, треба да биде потпишан од страна на Генералниот Директор во име на СЕЛЕК.

Барањата од државите за добивање на статус на оперативниот партнер со СЕЛЕК се испраќаат преку дипломатски канали.

Оперативните Партнери имаат право да учествуваат во оперативните активности и размена на лични податоци или информации.

Оперативната Партнери ќе ја уживаат привилегијата да присуствуваат на состаноците на Работната група и сите други состаноци, тренинзи и семинари организирани од страна на СЕЛЕК. Тие можат да бидат вклучени во размена на информации и други активности.

Советот избира Менаџмент на СЕЛЕК, во согласност со одредбите и условите утврдени во Конвенцијата на СЕЛЕК.[153]

❖

Од клучна и посебна важност во водењето на сложени меѓународни истраги е користењето на Интерпол, Европол или Селек. Неопходна е кооординацијата која ја даваат овие три многу важни организации, затоа што без нивна помош е невозможно да се разменат корисни информаци за истрагата која заеднички ја водат повеќе земји кои се членки на некоја од овие организации.

Со помошта на овие организации се реализираат многу важни сложени меѓународни истраги, се утврдуваат сторители кои делуваат на подрачјето на целиот свет. Исто така со користењето на нивните бази се доаѓа до многу

[153] http://www.selec.org/m105/Home *(25.11.2015г.)*

корисни информации, како и со известувања за најнови трендови на злоупотреби особено од областа на високотехнолошкиот криминал сите полиции од целиот свет се во постојан чекор.

11.ВЛИЈАНИЕ НА ВИСОКОТЕХНОЛОШКИОТ КРИМИНАЛ ВРЗ ПОЛИТИЧКИТЕ, ЕКОНОМСКИТЕ И СОЦИЈАЛНИ АСПЕКТИ НА СОВРЕМЕНОТО ОПШЕТСТВО

11.1 ЕКОНОМСКО ВЛИЈАНИЕ

Економското влиајние на високотехнолошкипот криминал е двојно, првенствено се должи на напади од страна на компјутерски криминалци, со што се нарушува угледот на самите фирми како во јавниот така и во приватниот сектор, или на поединци. На пример кога ќе се пробијат одредени информации и податоци на некоја финансиска компанија, во тој случај невозможно е компанијата да ја врати довербата кај клиентот, со што се нарушува меѓусебниот однос, и се става во прашање понатамошната соработка.

Економско – финансиски компјутерски деликти се поврзани со искористување на одредени стручни знаења во делот на финансиите, но и искористување на одредена позиција и овластувања на сторителите за извршување на конкретни криминални поведенија, а бидејќи нивната работа е компјутеризирана, неминовно е користење на компјутерските системи со внесување на лажни податоци и на тој начин извлекување финансиски средства од туѓи сметки. Најпознати се компјутерските проневери, но и компјутерските измами поврзани со изработка и употреба на лажни платежни картички и секако перењето пари како второстепен криминал со кој се легализираат криминално стекнатите пари од компјутерски кривични дела и нивно електронско трансферирање во т.н. безбедни зони или ,,рајски острови" каде што има слаба контрола на финансиските трансакции.[154]

Јавна тајна е дека многу од приватните компании, а посебно банките не ги пријавуваат во полиција компјутерските инциденти, интернет измами и сл. Како

[154] *Светлана С. Николовска, „Методика на истражување компјутерски криминалитет", Скопје, 2013, стр.31.*

една од главните причини за тоа е негативната реклама за самата компанија, потенцијалната штета на нивната репутација. Соочувањето со високотехнолошкиот криминал им преставува тешкотија за развојот на бизнисот, и истиот влијае на намалување на работни места.

Вториот многу важен момент за влијанието на високотехнолошкиот криминал врз економскиот аспект на општеството е неговото место во комерцијалниот сектор, што укажува на тоа дека повеќето прекршувања треба да се третираат од страна на жртвата, а не да се прикриваат. Тие не сакаат да ги изложуваат во јавност безбедносните проблеми со кои се соочуваат, поради комерцијалните конкуренти кои ги имаат.

Додека се решат овие прашања, тие преставуваат голема пречка во регулирање и контрола на високотехнолошкиот криминал, кој преставува скапа технологија и потребни се човечки ресурси и стручен кадар. Решението исто така треба да се гледа и во стратегија на превенција за криминалот. Зголемената употреба на напади со алатки од високотехнолошки криминал, актуелни методологии кои се користат за следење на интернет нападите, слабостите и критичната инфрастуктура би можеле да привлечат компјутерски напади, да изнудат пари, штета на економијата а најмногу да влијаат на националната безбедност.

11.2 ПОЛИТИЧКО ВЛИЈАНИЕ

Политичко мотивираниот високотехнолошки криминал се зголемува постојано. Компјутерските мрежи на Владини институции постојано се цел на напад. Хакирање на сајтови на владини и невладини организации, како и на сајтови на политички партии стана секојдневна работа во светот, а сето тоа негативно влијае на политичкото сценарио на секоја земја. Исто така, тоа влијае на инвестирањето на средства на странски компании и меѓународни организации во помалите земји.

Политички – штетите се однесуваат на нанесување на повреди на националните и верските чувства, но како политички штети се мислат и штетите настанати од извршени кривични дела со елементи на компјутерски тероризам, шпионажа и саботажа каде што сторителите криминално делуваат со политички мотиви.

А тоа пак доведува до криминални активности, односно финансирање на воени лидери кои се насочени против Владата, како и финансирање на други политички струи на кои им е целта рушење на постоечката Влада.

Влијанието на високотехнолошкиот криминал постои и ќе постои во иднина, се чуствува од страна на сите влади кои се поврзани на интернет. Самите Влади, бизнис заедницата, поединците, сите можат да бидат погодени од нападите на високотехнолошкиот криминал.

Заканата не е ограничена само на државни или воени тајни, но може да се провлекува и на комерцијални интереси.

Како и со секој вид на високотехнолошки криминал решение за спречување е многу тешко и сложено, така и за политичко мотивирано влијание. Но основните безбедносни мерки на претпазливост и свест можат да го ублажат политичкото влијание.

11.3 СОЦИЈАЛНО ВЛИЈАНИЕ

Високотехнолошкиот криминал имплицира социјално влијание особено во сиромашните земји, и во земјите во развој. Истрагите за високотехнолошки криминал не се воопшто евтини, и за истите потребно е да се има буџет и социјални проекти од оваа област во корист на општеството.

Распределбата на националните средства за превенција од високотехнолошкиот криминал преставува национален проблем, и има социјално влијание. Друго социјално влијание е избегнување на собири, а тоа влијае на социјалното вмрежување на луѓето, а со тоа избегнуваат користење на технологијата за да бидат безбедни од кривични дела.

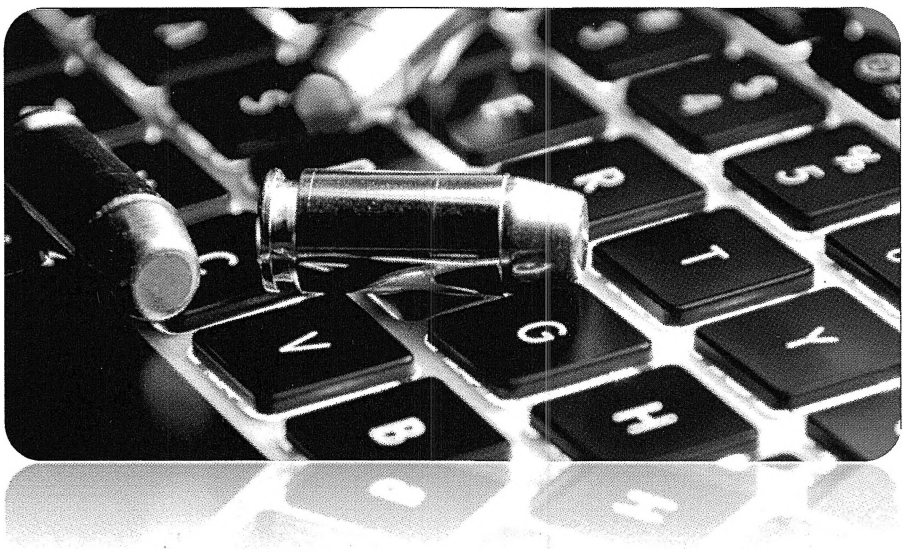
Поголемиот дел од младината не го сфаќаат високотехнолошкиот криминал сериозно, и го гледаат како единствена егзистенција за нив и нивните семејства, и не ги сфаќаат последиците од овие дела. На овој начин високотехнолошкиот криминал влијае врз младите, и најважно од се е дека овој вид на криминал бара интелектуални, софистицирани лица со високо ниво на интелегенција.[155]

[155] http://www.hanyang.ac.kr/home_news/H5EAFA/0002/101/2012/29-3.pdf (08.04.2016)

IV ГЛАВА

1.ВИСОКОТЕХНОЛОШКИОТ КРИМИНАЛ КАКО МЕХАНИЗАМ НА СОВРЕМЕНО ВОЈУВАЊЕ

1.1 КОМПЈУТЕРСКИ „CYBER“ ВОЈНИ



Светот во кој живееме се менува, на новиот милениум големо влијание има развојот на информатичкото општество, растот на електронскиот бизнис и развивање на нови глобални пазари. Информатичкото општество е изградено на една кревка рамка „интернет“. Интернетот е во постојана опасност од напади, досега од страна на хакери, но сега се соочуваме со развојот на интернет терористички организации. Овие организации го користат компјутерскиот простор за војување. Една од многубројните закани на високотехнолошкиот криминал која преставуваат реална, сериозна, брзо растечка закана за националната безбедност на современите држави се компјутерските војни.

Компјутерската војна (војување во компјутерскиот простор) е интернет конфликт, вклучувајќи политички мотивирани напади на информации и информациските системи. Компјутерската војна е нов облик на водење воен

собир чија примена во меѓународната заедница брзо расте. Меѓутоа неговата природа е специфична и се разликува од досега познатите облици на војна.[156]

Таа е релативно ново поле на истражување и студии. Компјутерската војна е реална, и истата се води. Компјутерската војна се спроведува со напади со кои може да се исклучат официјални веб-сајтови и мрежи, да се нарушат или оневозможат основните услуги, да се украдат или да се изменат класифицирани податоци, и да се оневозможи финансискиот систем - меѓу многу други можности.

Компјутерската војна означува употреба на компјутер, интернет и други средства за чување или ширење на информации за спроведување на напад на непријателски информатички центри помеѓу средствата за информатичка технологија.

Било која земја може да води компјутерска војна на која било друга земја, без оглед на ресурсите, бидејќи повеќето воени сили се во мрежа-оддалечени и се поврзани на интернет, кој не е безбеден. Од истата причина, невладините групи и поединци, исто така може да започнат компјутерска војна.

Воено поле на компјутерската војна се на пример комуникациски и информациски содржини. Напаѓачите можат да унишат инфрастуктури на непријателските држави доколку во голема мера истите се темелат на компјутерски содржини.

Компјутерската војна се однесува на спроведување и подготвени да ги спроведат, воени операции во согласност со принципите на поврзани информации. Тоа значи попречување ако не и уништување на информации и комуникациски системи, широко дефинирани да се вклучи дури и воена култура, на кој противник се потпира со цел да се „знае" кој е, од каде е, она што може да се направи и кога, зошто е таа борба, која закана е на прво место, итн., тоа значи дека се обидува да ги знае сите за противници. Тоа значи

---

[156] *Mladenović D. Dragan u dp. Tehnološki, vojni i društveni preduslovi primene sajber ratovanja, vojnotehni čki glasnik/military technical courier, 2012., vol. Lx, no. 1.*

вртење на „рамнотежа на информации и знаење" во полза на себеси. Тоа значи користење на знаење, така што помалку капитал и труд може да се прошири.[157]

Ефикасна заштита од компјутерска војна е обезбедување на информации и мрежи. Безбедносните надградби треба да се применуваат на сите системи - вклучувајќи ги и оние кои не се сметаат за критични, бидејќи било кој чувствителен систем може да се одлучи да се користи за извршување на напади.

Последиците од компјутерската војна се слабеење или прекинување на основната физичка инфрастуктура. Критичната инфрастуктура се системите, и ако тие се уништени ќе има влијание врз економската безбедност, банкарството, јавното здравје, физичката безбедност, комуникацијата, јавниот превоз, електронското тргување и сл. и ќе се предизвикаат импликации врз националната безбедност.

Некои тврдат дека нова тактика на компјутерската војна е да се предизвика штета на критичната инфрастуктура во компјутерскиот простор, и да се одржува таа штета.

Компјутерскиот простор се однесува на меѓусебно поврзани компјутери, сервери, рутери, кабли и сл. Тоа значи прекин на интернет конекција, паѓање на некој сервер, паѓање на рутерите и др. Сепак се чини дека тоа е помалку веројатно, односно дека интернет терористите или други воени планери би можеле да предизвикаат значајно оштетување на критичната инфрастуктура преку интернет воена тактика. Но иако се игнорираат овие напади, тие може да станат корисно оружје, особено поради глобализацијата на општеството овозможена од современите начини на комуникација преку INTERNET, фактот на растечка популација на млади, образовани, но невработени луѓе, кои ќе бидат достапни во иднина за компјутерска војна.

---

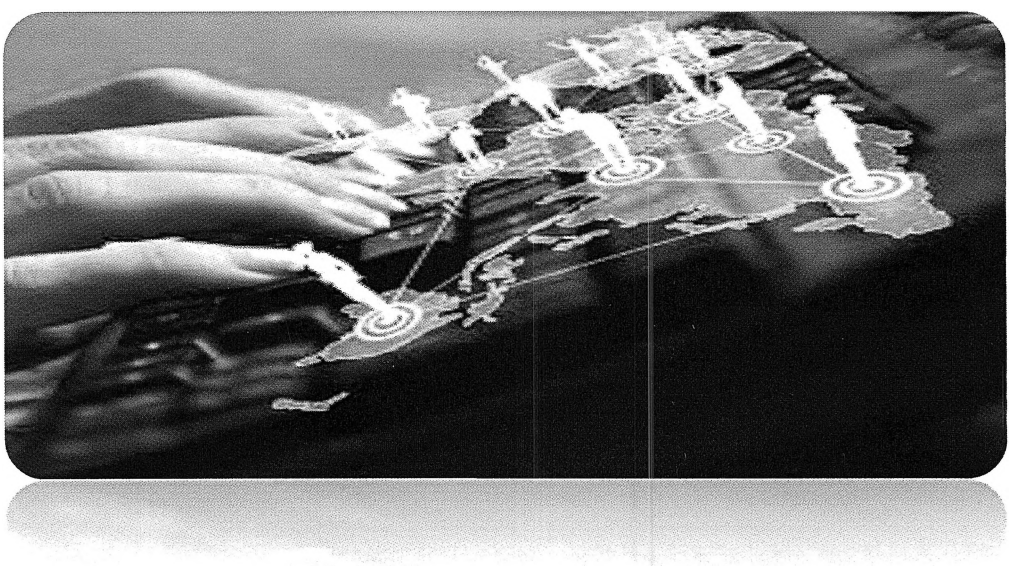
[157] *John Arquilla and David Ronfeldt, CYBERWAR IS COMING,Chapter Two, pp 8. pdf,*

ЦЕЛИ И МЕТОДИ НА НАПАД

Со компјутерската војна напаѓачот може да има разни стратешки цели:

- Дистрибуција на пропаганда или предизвикување на паника помеѓу цивилите;
- Трајно оштетување на клучни елементи на технолошката инфрастуктура (електрани, комуникациски центри и др.);
- Собирање на тајни информации;
- Напади со вируси (тројански коњи и сл.)

Во зависност од намената може да се користат алатки како на пример: „зомби компјутери“ кои се користат за DDOS напади кои пак овозможуваат добивање на контрола над центрите.



Категории:

- Интернет и
- Воена теорија

Примери на Компјутерско војување:

- Во 1998 година САД проби во системот на воздушната одбрана на Србија, како и на контролата на воздушниот сообраќај, со цел да го олесни бомбардирањето на Српските цели;
- Во 2007 година во Естонија „ботнет" од над еден милион компјутери го оневозможи работењето на Владата, бизнис заедницата, медиумите во земјата. За овој напад Естонската влада се сомнева дека доаѓа од Русија, мотивиран од политички тензии кои ги имаат овие две земји, но досега нема признание за тоа од страна на Русија;
- Исто така во 2007 година непознати лица успеале да пробијат во високата технологија и во воените агенции на САД и да превземат голем број на доверливи информации;
- Во 2009 година компјутерска шпионска мрежа наречена „GhostNet" пристапиле до доверливи податоци кои припаѓале на Владини како и на приватни организации во повеќе од 100 земји низ целиот свет.
  „GhostNet" бил пријавен дека е со потекло од Кина, иако таа земја ја негирала одговорноста.[158]

Компјутерската војна не е само нов сет на оперативни техники. Таа се појавува, според нашето мислење, како нов начин на војување што ќе бара нови пристапи за планови и стратегии, и нови форми на учење и организација.

Новите технологии се стремат да произведат потоп на информации кои мора да се земат во предвид, да се филтрираат и интегрираат во реално време. Компјутерската војна може да бара големи иновации во организациски дизајн, особено промена од хиерархии за мрежи.

---

[158] *Види пошироко: Paulo Shakarian Jana Shakarian Andrew Ruef, Introduction to Cyber-Warfare, стр.2-3. pdf.*

Информатичката револуција веќе го покрена прашањето за интер и интра-сервис врски, во случај на воена коалиција и во воените врски. Компјутерската воена доктрина може да побара врски. Тоа може да се значи особено тесна комуникација, консултации и координација меѓу службениците одговорни за стратегија, планови и операции во оваа област.[159]

Зошто треба да се очекува нешто различно за компјутерската војна. Нови информации апликации за технологијата почнаа да се трансформираат во светот на бизнисот. Светот во најголем дел, се движи полека во усвојувањето на револуцијата на информатичката технологија. Всушност, делови од војската на САД, покажуваат голем интерес за примена на информатичката револуција. [160]

Војската на САД има превземено голем број на чекори за да се соочи со заканата од компјутерска војна. Тие вклучуваат организациски, оперативни, кадровски промени од страна на сите вооружени служби, како и заеднички команди кои вршат оперативни војувања. Клучна стратешка цел на военото раководство на САД е да се постигне информациона супериорност во однос на сегашните и потенцијалните противници. Лесната достапност до информациите на интернет и дава нови димензии на шпиунажата, правејќи го моќна алатка во рацете на современите контраразузнавачки агенции.

Во текот на последната деценија САД во воената доктрина ја вклучија компјутерската војна. Подготовките за прв пат започнале во 2002 година, по директива на Претседателот, при што е наведено во нивната стратегија, со процедури и протоколи за компјутерска војна. Истото било објавено во 2003 година од страна на Министерството за Одбрана на САД, и кога како дел од нормалните воените операции се вклучени обуки на воениот персонал за компјутерска одбрана. Во 2009 година војската на САД воспоставува Компјутерска Команда во Fort Meade, Maryland. САД исто така почнуваат да вложуваат повеќе средства за обезбедување на инфрастуктурата која може да

[159] *John Arquilla and David Ronfeldt, CYBERWAR IS COMING,Chapter Two, pp 23. pdf,*
[160] *John Arquilla and David Ronfeldt, CYBERWAR IS COMING,Chapter Two, ,pp 19. pdf*

е ранлива на компјутерски напад, како што се електричната енергија, водата, нафтата, системите за гас и сл.[161]

Денес светското население е поголемо и интегрирано од кога било досега. Денес во светот имаме многу религиозни групи, организации, меѓународни трговски партнери, меѓународни тела како што се Обединетите Нации, Меѓународниот Суд, мултинационални корпорации и сл., многу географски различни, во една или друга форма, но во голем степен еволуирале преку технологијата, технолошките откритија, поморскиот транспорт, воздушниот сообраќај, комуникациската технологија и други достигнувања.

Додека делата кои потекнуваат од високотехнолошкиот криминал е тешко да се перципираат, истражуваат и процесуираат, се создава атмосфера граѓаните да се чуствуваат незаштитени, несигурни во моќта на државата да ги заштити.

За националната безбедност до неодамна се сметало дека најважна е воената компонента, денес научно-техничката револуција доведе до формирање на информациско општество во кое информацијата е главен фактор во управување со светот.

Зголемувањето на светската интеграција, особено на дигиталанта интеграција станува очигледна со бројот на интернет корисниците.

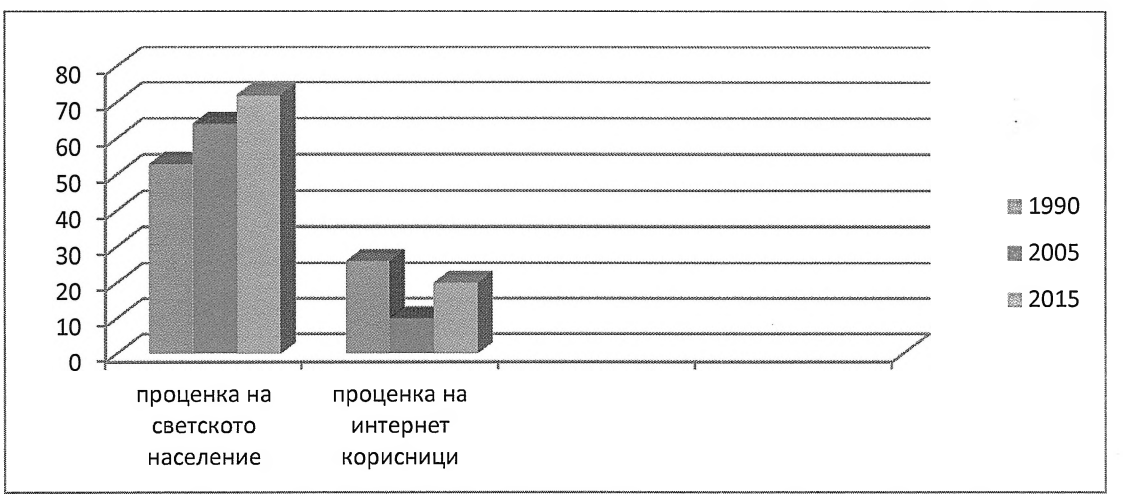
(Види во Табела 1).

[161] *Види пошироко: Dana Rubenstein, Nation State Cyber Espionage and its Impacts, pdf.*

Табела бр. 1 Број на интернет корисници,[162]

	ГОДИНА		
	1990	2005	2015
Проценка на светското население	5.3 билиони	6.4 билиони	7.2 билиони
Проценка на интернет корисници	2.6 милиони	1.0 билион	2.0 билиони
Процент на корисници на светското население	< 1%	15.6 %	27.8 %

Графикон бр. 1 Број на интернет корисници

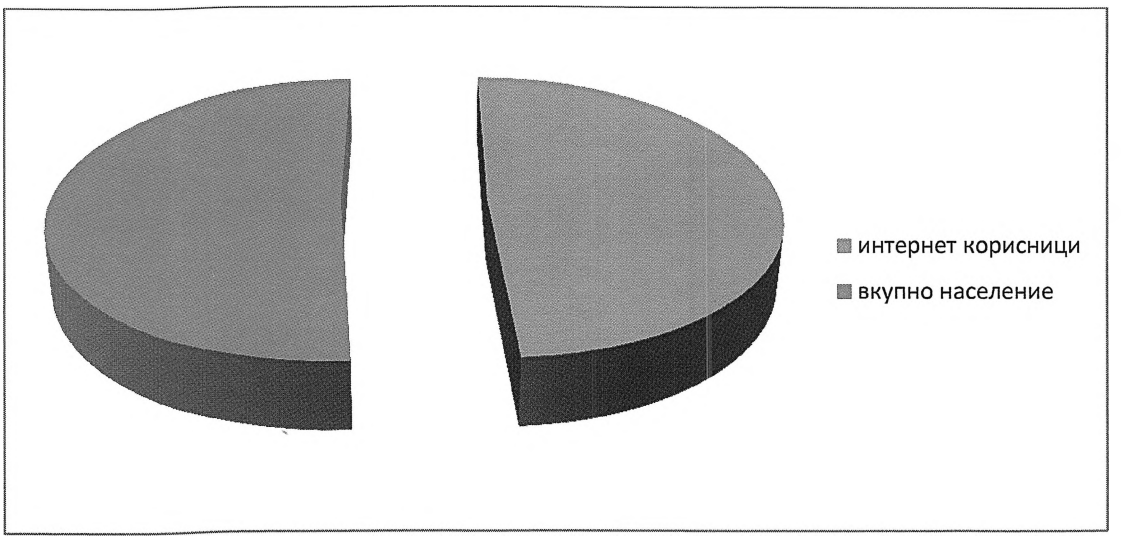


Од табелата и графиконот бр. 1 можеме да согледаме дека бројот на интернет корисници во периодот 1990-2015 рапидно се зголемува. Ваквата тенденција на зголемување на бројот на интернет корисници се очекува да продолжи и во наредните години и тоа со се поголем интензитет.

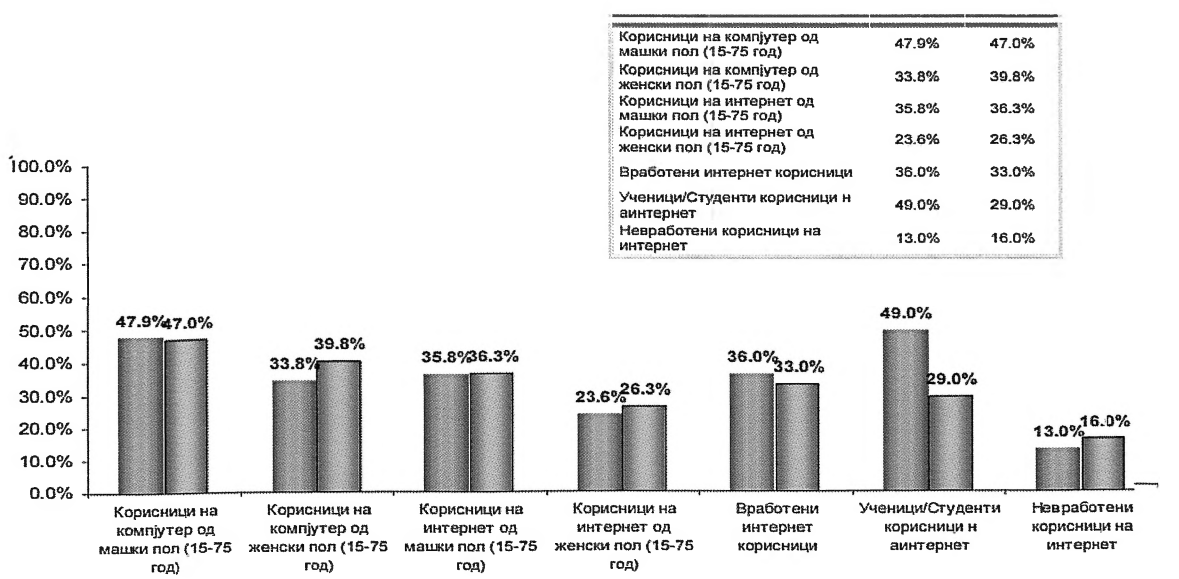
Во Македонија интернет користат околу 1.100.000 луѓе или 51 проценти од населението, а 878.300 се приклучени на социјалната мрежа "Facebook", покажуваат податоците на специјализираниот статистички веб сајт „Интернет ворлд стат".

[162] *Lech J. Janczewski, Andrew M. Colarik, Cyber Warfare andCyber Terrorism, ,pp 61. pdf*

Графикон бр. 2. Број на интернет корисници во Република Македонија



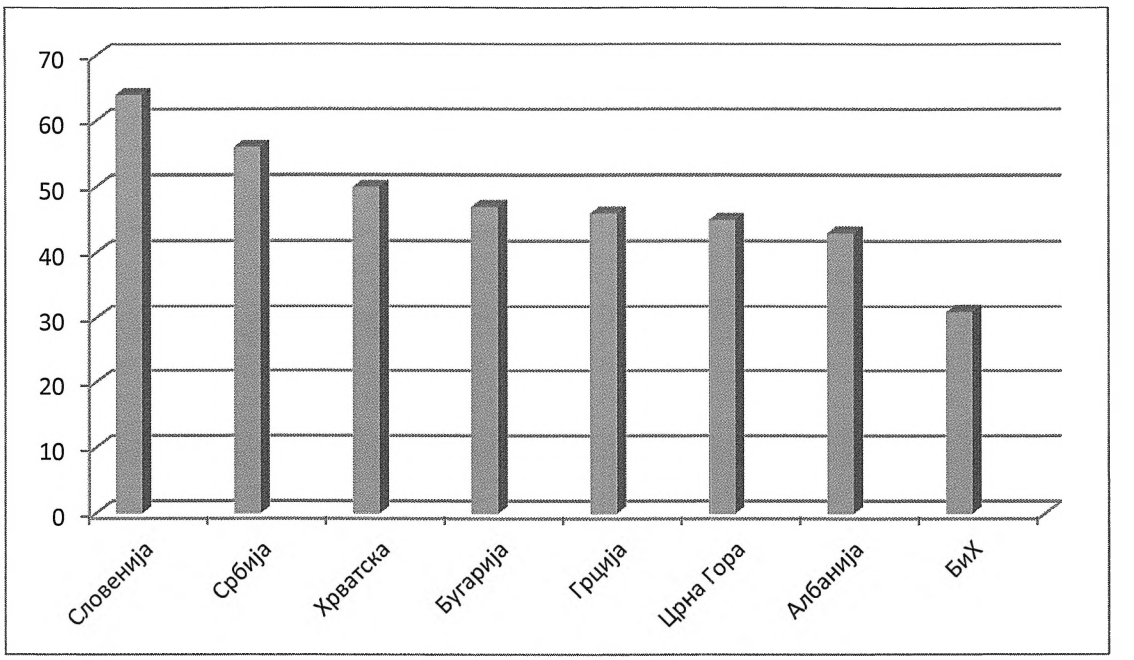
Графикон бр. 3. Профил на корисниците во Република Македонија



Извор: Државен завод за статистика

Од земјите во регионот повеќе од Македонците интернет користат Словенците (64,9%) и Србите (56,2%), а помалку граѓаните на Хрватска (50,1%), Бугарија (47,9%), Грција (46,2%), Црна Гора (45,9%), Албанија (43,4%), БиХ (31,2%) и Косово (20,7%).

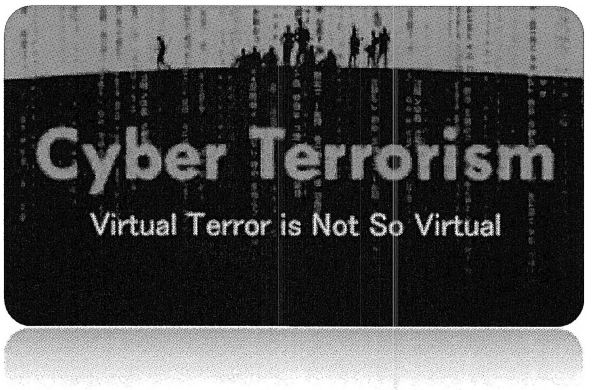
Графикон бр. 3. Број на корисници на интернет во земјите од регионот



Во Европа интернет користат 476 милиони луѓе, а „Facebook“ 209 милиони. Глобалната онлајн мрежа најмногу ја користат жителите на Исланд, Монако и Норвешка, околу 97 %.

Според Интернет ворлд стат, во светот има 2,1 милијарди интернет корисници или 30,2 проценти од вкупната светска популација.

1.2 КОМПЈУТЕРСКИ ТЕРОРИЗАМ



Со самиот развој на технологијата, општеството и граѓаните во него се движат во чекор со збиднувањата кои ги зафати технологијата. Масовната комерцијализација на интернетот овозможи брз проток на информации кои се шират за секунда на секој дел од земјата во т.н. „cyber простор" (компјутрески простор). Намерната злоупотреба на информации во компјутерскиот простор мора да биде дел од терористички напад.

Во денешно време колку по технолошки е напредна една држава, толку е поранлива на компјутерски напади. Сепак ваквото проширување на информатичката технологија во светот има и своја негативна страна.

Мрежните поврзувања и напредната технологија донесоа нови и пософистицирани можности за прекршување на законите, извршување на напади и остварување на традиционалните начини на тероризам на нови нетрадиционални начини. Како што интернетот е се позастапен во секојдневниот живот, истовремено се проширува и зголемува неговата употреба, а како резултат на тоа се одвиваат посложени операции, се врши проток на доверливи информации поврзани со националната безбедност на една држава.

Можеме слободно да кажеме дека со ваква распростанета употреба на технологијата, не дели многу краток период од започнување на современо војување каде што главната причина на битките ќе биде за што поголемо прибирање на доверливи информации за противникот. Од тука се отвара простор за компјутерски или интернет тероризам, кој се повеќе ќе започне да се глобализира.

Бројот на терористички напади започна да ескалира во почетокот на 1990-те години, и од тогаш не поминува ден без терористички напад. Зборот тероризам потсетува на група на мажи со бради кои фрлаат кеса со експлозив, но во контекст на информацискатa безбедност, терористите може да доаѓаат во многу форми.

Во последниве години евидентна е појавата на нов облик на организиран високотехнолошки криминал, наречен ***„компјутерски или интернет тероризам“*** (cyber terrorizm). Во светот не постои унифицирана, единствена дефиниција за тоа како да се дефинира терминот тероризам. Иако зборот е комплексен по своето значење, одредени дефиниции се фокусираат на актерите на тероризмот, додека останатите се фокусираат на терористичките тактики и цели, како и методите кои се применуваат. Со цел да се гонат овие видови на терористички акти или да се направи од вооружените и други форми на насилство и криминал, националните и меѓународните институции, како и останатите структури, од пред извесно време бараа да се дефинира поимот тероризам.

Една од најчесто користените дефиниции произлегува од правните акти од САД. Според законот во САД, тероризмот е вграден условно во Годишниот извештај кој треба да биде поднесен од страна на државниот секретар до Конгресот секоја година. Тероризмот е дефиниран на следниот начин: „претходно планирано, политички мотивирано насилство извршено против невоени цели од страна на суб – национални групи или тајни агенти“.

Кога се зборува за поимот „cyber“ компјутерски тероризам, според Федералното Истражно Биро – ФБИ овој феномен се дефинира како:

„предумислени, политички мотивирани напади против информации, компјутерските системи, компјутерските програми и податоци што резултираат со насилство против цели кои не се воени од страна на суб – националните групи или тајни агенти".[163]

Трета голема закана после хемиско-биолошко и нуклеарно оружје е компјутерскиот тероризам. Се работи за посебен облик на напад врз компјутерските мрежи и врз базите на податоци со намера за примена на сила или закана кон Владата на една држава за нејзино подредување на определена политика или донесување определени одлуки, користењето на интернет просторот како поле за заработување на нелегално стекнати пари како и користење на интернетот за прикривање на потеклото на нелегално стекнати пари (перење на пари), со цел употреба на истите при финансирање на терористички организации или современо наречено „компјутерски тероризам".

Предмет на напад може да бидат важни инфрастуктури (водовод, гасовод, електродистрибутивни објекти и др.), со упад во компјутерскиот систем на контролата за летање ќе се предизвикаат авионски несреќи, активирање на нуклеарни бомби, ќе се предизвика страв, паника кај населението, големи човечки жртви. Терористите имаат голем арсенал на оружје вклучувајќи го и хемиското и биолошкото оружје, со што можат да предизвикаат еколошки катастрофи и хемиски загадувања, можности за страотни труења на системите за вода. Терористите го користат интернетот за пропагирање на нивните цели, што се состојат најчесто во ширење омраза, насилство, расизам.

На овој начин комјутерскиот тероризам директно влијае на националната безбеднот на државата.

Во времето кое што доаѓа терористите се повеќе ќе употребуваат висока технологија за остварување на нивните цели, како за обезбедување на

---

[163] *Според Федералното биро за истрага – ФБИ (http://searchsecurity.techtarget.com/sDefinition/0.,sid14_gci771061,00.html)*

средства за финансирање така и за вршење на шпиунажи, саботажи и терористички напади на објекти. Потенцијалот на терористичките организации и екстремните поединци во иднина постепено ќе се зголемува поради промените во технологијата, која ќе им обезбеди на следните генерации многу повеќе можности од оние кои ги имаат сегашните најобучени терористи.
Нова генерација терористи наоружена со информации, ќе може да се вклучат во драматични и деструктурни дејства. Виртуелниот простор е новото место на настаните во кое делуваат нови опасни играчи према нови правила и ново оружје. Затоа интелегентните и криминалистички служби, постануваат беспомошни против новиот тип противник кој не напаѓа со камион полн со експлозив туку само со броеви, на најосетливите места на националната инфрастуктура. [164]

Комбинација на класичен физички тероризам со компјутерски тероризам се смета дека е најефективен начин на тероризам.

Поради тоа што не е целосно јасно што е компјутерски тероризам, често се доаѓа до недоразбирање во толкувањето. Според концептот на компјутерски тероризмот често погрешно се разбрани случаевите на компјутерски или интернет злоупотреби, како што се активности на некој хакер, ширење на вируси и цела низа на компјутерски online инциденти кои носат само оштетувања и тешкотии.

Високотехнолошкиот криминал е посебен по цела серија свои обележја и како транснационален организиран криминал кој непрестано се развива, создава нови предизвици врз националната безбедност на современите држави.

Тоа треба да се класифицира како обид на компјутерските криминалци да ги тестираат своите вештини и да се покажат себеси во средината дека може да влијаат на нешто. Интернет тероризмот неможе да се поистоветува со хакерски активности кои вклучуваат неовластено навлегување во компјутерски

[164] *Види пошироко: Lech J. Janczewski, Andrew M. Colarik, Cyber Warfare and Cyber Terrorism, pdf.*

мрежи со цел попречување на нивната работа, без намера да се предизвика голема штета. Самите терорости може да користат хакерски техники за да го отргнат вниманието на нивното функционирање, но тоа не преставува интернет тероризам или терористички напад. Тоа е само уште еден индикатор кој укажува дека целата напредна технологија може да се користи за незаконски цели.

Незаконските напади и закани за напад врз компјутери, информациски мрежи и информации складирани во нив се главни орудија кои се користат од страна на терористите со цел да се заплаши јавноста, да се присили владата, обично се прикриени во компјурскиот тероризам.

Компјутерскиот тероризам исто така треба да се разликува од „Компјутерска Војна" манипулација на компјутери и компјутерски мрежи во контекст на меѓудржавни конфликти. Компјутерската војна врши офанзивни и дефанзивни активности на државните структиру во меѓународни конфликти. Комјутерскиот тероризам и Компјутерската војна може да се поклопат во користењето на одредени методи како на пр. Уништување на компјутерски мрежи, но тоа не значи дека се работи за иста активност.

Компјутерскиот тероризам не е нелегално заобиколување на правилата за користење на компјутерска опрема и интернет воопшто, од страна на тероиристите. **Во една реченица може да се дефинира како идеолошки мотивирани напади врз компјутерски системи, бази на податоци и мрежи, апликации, што се врши со помош на информатичка технологија и има ефект на предизвикување на страв, насилство и значителна материјална штета на не-борбени цели со цел да се влијае врз јавноста и политички процеси. Компјутерскиот тероризам се поистоветува со употребата на високото ниво на технолошките средства против високо технолошки цели.**[165]

---

[165] *Види пошироко: Serge Krasavin, Computer Crime Research Center, What is Cyber-terrorism.pdf*

Споредувањето на реална закана од Компјутерскиот тероризам со закана од секојдневниот тероризам кој исто така ги користи напредните информатички технологии, треба да се имаат во предвид два одделни аспекти кои заслужуваат особено внимание и анализа. Одлуката дали се потребни посебни противтерористички мерки не зависи само од фактот за вистинска закана на компјутерскиот тероризам туку и од тоа дали постои потенцијална подршка за информатичката технологија во реализација на терористички акт.

Компјутерскиот тероризам се извршува во компјутерскиот простор. „Cyber Space" или компјутерски простор е термин кој прв го употребил Wiliam Gibson во 1984 година во неговиот научно фантастичен роман „Neuromancer" како поим за домен кој го опфаќа мрежната комуникација поставена на компјутерите, за што најистакнат пример е Интернетот.

КОМПЈУТЕРСКИОТ ИЛИ ИНТЕРНЕТ ПРОСТОРОТ подразбира глобално информатичко опкружување, кое се состои од мешани цивилни и воени информациони мрежи и технологија, со електронски патеки кои ги поврзуваат групи, поединци, организации и народи од целиот свет, со кои се разменува голема количина најразлични податоци и информации, и се формира еден виртуелен свет – компјутерски простор. **Тој огромен простор во кој класичните термини, државна граница, гранични премини и царина, губи секаков смисол, и се повеќе станува арена за нови видови најразлични конфротации.**

Ова е особено затоа што денес повеќето земји веќе имаат значителни ресурси врз основа на информатичката технологија, вклучувајќи ги и одбранбените системи, системите за администрација, сложени системи за контрола и други информационо зависни области. Оние кои сеуште немаат ништо да направат на овој план, прават се за да остварат одредени резултати. Во овој контекст мора да се сфати дека идните непријатели, било да се држави, групи или поединци, може да се обидат да ги загрозат овие инфрастуктури со користење на традиционални алатки но и со нетрадиционални компјутерски методи.

Компјутерскиот простор во кој националните граници не се заштитени со географска баријера нити натоварени воени сили, е поле кое овозможува нови можности за војување. Како што се повеќе земји се „поврзани“ во глобалната мрежа и како индивидуални врски во рамките на овие земји стануваат се почести закани во компјутерскиот простор. Тоа е место каде се користат компјутери наместо тенкови, дигитални броеви наместо куршуми, заштитни бариери (*firewalls)* наместо бодликава жица и минско поле.

Компјутерскиот простор се состои од стотици илјади меѓусебно поврзани компјутери, сервери, рутери, свичеви и фибер оптички кабли, кои овозможуваат на нивната инфрастуктура да функционира и дека правилното функционирање на компјутерскиот простор е основа за економијата и националната безбедност.

Обезбедувањето на компјутерскиот простор е особено тешка стратешка задача која бара координација и фокусираност на целото општество, владата, државните и локални системи на владата и приватниот сектор.

Стратешки цели за обезбедување на компјутерскиот простор се:

- Спречување на компјутерски напад на критична инфрастуктура;
- Да се намали националната ранливост на компјутерскиот напад и
- Да се минимизира штетата и времето потребно за закрепнување доколку дојде до напад.

Со други зборови компјутерскиот простор е виртуелна средина на информации и интеракции помеѓу луѓето.

Напади на витални информациони структури на општеството е многу привлечно за терористите, од неколку причини. Како цели може да бидат централи, воени инсталации, банкарската индустрија, контрола на воздушниот сообраќај, инсталации на водовод и други големи центри кои влијаат на нормалниот тек на животот на луѓето. Најпрво со самото

поседување на компјутер се овозможува имплементација на напади на долги растојанија, со високо ниво на анонимноста со малку финансиски трошоци.

Интернетот и современата технологија донесоа многу погодности за современиот човеек но нажалост и за терористите.[166]

Компјутерските терористи може да работат насекаде во светот и може да ги сокријат своите идентитети далеку поефикасно, одколку терористите кои делуваат на традиционален начин. Со тоа се избегнува употреба и ракување со експлозив и спроведување на самоубиствени мисии. Но до некои атрактивни цели на терористите не е можно да се извршат со класични методи и нивното уништување не е можно на далечина и без свои терористички жртви.

Некои цели како што се комуникациски системи, енергетски системи, сообраќајните врски, неможе со еден класичен терористички напад да се нанесе таква голема штета и да се предизвика таков голем страв како што може со Компјутерскиот тероризам. Целта на нападот на компјутерските терористи може да се случи на илјадници километри од нивното физичко дејствување односно од нивната оперативна база, со што се заштитени од откривање и приведување.

Компјутерските терористи најчесто соработуваат со слаби држави или држави кои имаат неефикасни или корумпирани безбедносни агенции, со цел поефикасно да дејствуваат.

Повеќето хакерски напади се чуваат во тајност и се прикриваат од јавноста пред се за да се избегне паника и да се спречи зголемување на недоверба према системот, но успешен компјутерски теростички напад неможе да се сокрие од јавноста.

---

[166] *Милован Б. Јовановиќ, „Интернет и тероризам“, Правни факултет за привреду и правосуѓе, Монографска студија Примљен: 29.08.2014 Нови Сад Одобрен: 18.09.2014 УДК 004.738.5:316.77 .*

Развиената информатичка технологија им овозможува на терористите пристап до цели до кои не може да дојдат поинаку, на пример како што се системите за национална безбедност и одбрана.

Тероростите во однос на користењето на информатичката инфрастуктура сепак имаат одредени ограничувања. Иако компјутерските системи се ранливи, сепак тие се сложени структури. Самото тоа значи дека следењето на спроведувањето на самиот напад може да биде комплицирано, како и желбата да се постигне посакуваната штета. Освен во случај да дојде до жртви, смрт на луѓе и сл., самиот напад на информатичката структура не предизвикува емоционална реакција и успехот на нападот не е целосен. Поради тоа терористите не се мотивирани за користење на нови методи и техники, освен кога традиционалниот начин на делување не се смета за соодветен.

Колку што нападите извршени од далечина предизвикуваат погодности кај терористите, истовремено предизвикуваат и чуство на несигурност и потешкотии во контролата на остварените резултати. Доколку терорстите не се сигурни дека ќе го постигнат саканиот резултат тие не се склони да експериментираат.

Терористичките групи се развиваат во средини каде што младите имаат ограничени можности за напредување во нивните општества. Феноменот на транснационалниот криминал, тероризмот и корупцијата често се гледаат како посебен феномен. Овие феномени се зголемија во тандем бидејќи економските и политичките услови кои доведуваат до овие појави се прилично слични. Терористите најчесто се наоѓаат во земјите кои се во развој. Во овие земји нелегалните бизниси се најголеми и најпрофитабилни.

Тие се толку големи што имаат влијание врз политичката и бизнис сцената. Огромните приходи од нелегалните бизниси им дозволува да ги ангажираат најдобрите експерти и специјалисти како во тие земји, така и на меѓународно ниво. Олеснување им е користењето на информатичката технологија за да ги промовираат своите активности тајно, да ги поминат

границите без откривање. Некои од овие експерти незнаат дека работат за терористички организации, а други би работеле и доброволно бидејќи се добро платени.

Но секако не смее да се потцени и човечкиот фактор. Виталните системи може да зависат од информатичката технологија, но се уште има доволно човечки надзор и контрола за да се спречат тешкотии во работата и да се справат со извонредни и неочекувани ситуации.

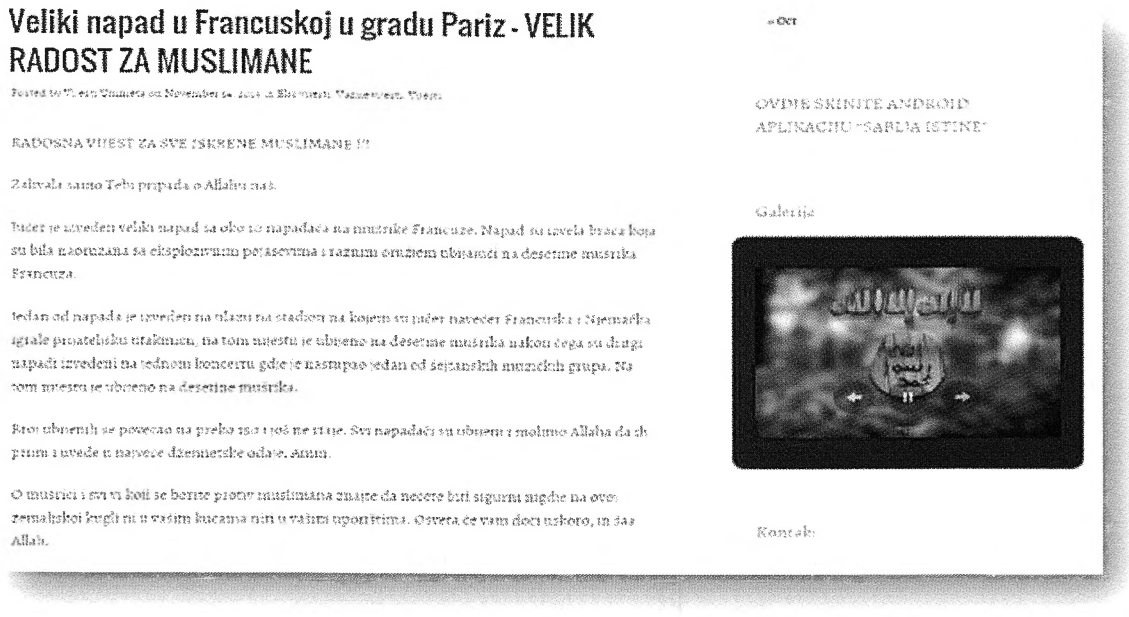
Терористите ја користат информатичката технологија како корисна алатка за подршка, како и благодетите на современиот технолошки напредок со цел да ги унапредат своите активности. Тие го користат компјутерот како средство за комуникација, за чување на податоци, ширење на пропаганда, регрутирање членови, собирање на податоци и др. Самите терористички групи се свесни дека информатичката технологија ја попречува нивната тајност, особено во делот на комуницирање, користењето на e-mail како едно од средставта за комуникација.[167]

Компјутрските терористички групи користат она што е познато како „hacktivism". Хактивисти се активисти вклучени во обезличување на местото на непријателот за политички или социјално мотивирани цели. Хактивизмот е предизвик на меѓународните односи не само затоа што ги надминува границите, туку и поради тоа што стана инструмент на националната моќ.[168].

---

[167] *Види пошироко: Alan Bryden, Philipp Fluri, Louise I. Shelley, Organized Crime, Terrorism and Cybercrime, pdf.*

[168] *Maura Conway, 'Hackers as Terrorists? Why it Doesn't Compute.' Computer Fraud and Security 2003, pdf., стр.5*



(Слика 2)[169].

Секоја индивидуа што има непријателски намери а воедно има компјутерско познавање може да нанесе интернет тероризам. Се разликуваат четири главни категории на интернет терористи:

- ***Хакерски групи спонзорирани од држава*** – компјутерски терористи спонзорирани од страна на државите се во се поголем подем и раст. Активностите на овие терористи се од онеспособување на државни компјутерски мрежи и системи до пробивање на витални државни информации кои подоцна се користат со цел да се разменат информации со друга држава;
- ***Криминални банди–*** повеќето од криминалните банди се вклучени во интернет просторот. Нивните активности се однесуваат на манипулирање на банкарски сметки, крадење на податоци од банките со цел да остварат финансиска придобивка;
- ***Незадоволни инсајдери–*** со намалување на бројот на вработени во организациите, се предизвикува незадоволство кај отпуштените. Се отпуштаат вработени од сите сектори, дури и лица кои располагаат со

[169]Слика, Интернет портал, (http://www.index.hr/vijesti/clanak/islamisticki-portal-na-bosnjackom-jeziku-pokolj-u-parizu-nazvao-radosnom-vijescu/855927.aspx, 2016г.),

осетливи и тајни информации. Желбата за одмазда и големото незадоволство кај овие отпуштени работници, преставува сериозна закана за компјутерската безбедност на организациите;

- ***Политички мотивирани хакери***– целта на оваа група на хакери е да ги оневозможат компјутерските системи и мрежи на големите организации со цел да пружат фер игра во компјутерскиот простор. Таа фер игра се однесува во остварување на подобри човекови права, подобри услови и стандарди за работа и сл.[170]

Првиот официјален регистриран компјутерски терористички напад е случен во во 1998 година од страна на Тамилските тигри кои на електронската пошта на Амбасадата на Шри Ланка испратиле повеќе e-mail бомби.

Овој напад не предизвикал било каква штета. Од тогаш се регистрирани серија на компјутерски напади поврзани со Израелско-Палестинскиот конфликт, конфликтот на Кина и Тајван, Индија и Пакистан и др. Иако овие напади се извршени од страна на мали групи, кои може да се окарактеризираат како терористички, повеќе наликува на една од формите на компјутерска војна (cyber war), отколку за терористички напад.

Најголемиот дел од општествените активности се одвиваат со помош на компјутерски системи и мрежи, како што се преносот на електричната енергија, воени операции, активности од воената сфера, бизнис нарачки, плаќање на производи за основни потреби, трансфер на пари и многу други операции, односно активности од кои зависи функционирањето на една држава. Сите овие инфрастуктури се одлично заштитени бидејќи се од витално значење за функционирањето на една држава. Имаат највисоко ниво на безбедност и најсовремени компјутерски системи во корист на својата заштита. Но никогаш не сме доволно заштитени и безбедни. Како што државите работат на својата компјутерска безбедност, така и компјутерските терористи работат на зголемување на својата моќ.

---

[170] https://www.vocabulary.com/dictionary/cyber-terrorist, https://www.ipredator.co/cyber-terrorism/ (25.02.2016).

Доколку би се извел компјутерски напад врз електричната инфрастуктура, тогаш би биле најсилни ефектите од компјутерскиот тероризам. Тоа би резултирало со прекин на доставување на електрична енергија, и во такви услови каде неможе да се вршат основни активности во едно општество, последиците би биле катастрофални. Државната, јавната и индивидуалната безбеднсот би биле загрозени а со тоа и државата ќе биде изложена на напад.

Во ваков случај тешко се одвиваат банкарските и финансиските функции, што доведува до големи финансиски загуби, а кај граѓаните појава на страв и паника за своите финансиски средства.

Голем ефект би се предизвикал и доколку се превземат системите за контрола како на воздушниот сообраќај така и на копнениот сообраќај. Во тој случај се манипулира со навигационите системи, се регулира брзината на возовите. Како потенцијална и една од најголемите цели на комјутерските терористи би било напад на здравствениот систем. Со оглед на тоа дека целиот здравствен систем е компјутеризиран, а сите ние имаме електронски здравствени картички, преставува примамлива цел на компјутерските терористи. Во електронските картони се внесени нашите лични податоци, здравствената историја, болести и сл. Со упад во овој систем терористите можат да менуваат здравствени картони на лицата, терапии на лекување и сл., а со тоа би се предизвикале катастрофални човечки загуби, без потрошено оружје.[171]

Компјутерскиот тероризам е 24/7, 365 дена во годината, гигант кој никогаш не спие. Треба да се инвестира во технологијата и експерти кои ќе ги следат системите 24 часа на ден, седум дена во неделата, 365 дена во годината.

Поголем дел од граѓаните никогаш не биле во контакт со било кој облик на терористичко насилство, туку стануваат свесни за овој облик единствено предку посредство на медиумите.

---

[171] *Barry C. Collin, The Future of Cyber Terrorism, pdf*

Некои истражувања покажуваат дека за 90% од инцидентите на интернет се обвинуваа Интернет аматерите, на 9,9% се припишува на "професионални" хакери и индустриските шпиони, и 0,1% се одговорни компјутерските-криминалци од светска класа. Други истражувања кои се занимаваат со закани за меѓународниот тероризам, покажуваат дека и покрај технолошкиот напредок, терористите нивните цели и тактики остануваат исти. Како заклучок може да се каже дека терористите ја прифатиле информатичката технологија како независна команда и контролна алатка, но дека се уште не се подготвени да нападнат важни информатички структури.

Очигледно е дека терористите ги корисат предностите на информатичката технологија, но не постои јасна слика дали и кога информатичките структури ќе постанат нивна цел на напад. Постои ризик од напад без разлика на заштитините мерки, иако актуелниот страв од напад може да биде поголем од вистинскат опасност.

Интернетот преставува широко поле на информации кои се слободно достапни, така на пример има на располагање инструкции и материјали потребни за да се создаде хемиско, биолошко оружје или пак бомба. Тоа значи дерка секој кој сака да направи бомба, да изврши атентат, да изврши киднапирање, ги има достапни online сите информации, тактики и техники за гореспоменатите активности.

Со развојот на информатичката технологија ние денес всушност живееме во интернет општество. Свесно го прилагодуваме општеството во чекор со најновите технологии, а со тоа самите свесно или несвесно предизвикуваме да бидеме изложени на нови видови загрозувања на нашата национална безбедност, јавна и приватна безбедност.

Информатичката технологија дава голем придонес во борбата против тероризмот, брза размена на информации, соработка на повеќе безбедносни агенции, спроведување на подобри анализи и др. Денес повеќе од било кога светот мора да се обедини преку технологијата.

Европската Комисија побарала од сите земји членки на Европската Унија да го класифицираат како терористички напад секој „напад преку навлегување во системот за информации", ако тоа доведува до сериозни промени или уништување на политички, економски или социјални структури. Франција ги проширила полициските овластување во делот на пребарување во приватен имот без судски налог кога станува збор за сомневање за терористички акт. Шпанија ги ограничува активностите на секоја организација која е поврзана директно или индиректно со ЕТА (Воена баскиска националистичка и сепаратистичка организација), Германската Влада ги намалила ограничувањата на телефонските прислушкувања, следење на e-mail комуникацијата, банкарските сметки и др.

Австралија вовела мерка за пресретнување на електронската пошта (дала овластување на сите домашни разузнувачки агенции, организации за безбедност) доколку дојдат до информации дека се подготвува терорстички напад, како и да биде замрзнат целиот имот на терористите. Индија овозможила осомничените за тероризам кои се уапсени, без судење да бидат обвинети и во некои случаеви вовела и смртни казни за овој вид на криминален акт, како и да се замрзне целиот имот и финансиските средства на терористите и истите да бидат на распоалгање на Владата.[172]

Терористите се секогаш еден чекор напред од анти-терористичките тимови и нивните активности, тие секогаш ја бараат најслабата точка на одбраната и се фокусираат на напад врз истата. Се разбира, тоа незначи дека треба однапред да се предадеме, и да се откажеме во борбата против тероризмот особено во информатичката сфера. Таа мора да биде избалансирана помеѓу реалното ниво на закана и нивото на кое не се ограничува употребата на информатичката технологија, и треба да се фокусира на превентивно дејствување и брза проценка и поправка на било каква штета. На пример фактот дека терористите ја користат информатичката технологија за шифрирана комуникација не значи дека треба да се укине

[172] *Lech J. Janczewski, Andrew M. Colarik, Cyber Warfare andCyber Terrorism, Kevin Curran, Kevin Concannon, Sean McKeever, Cyber Terrorism Attacks, pdf, pp 36.*

законската можност за шифрирана комуникација. Со други зборови, во развојот на мерки за безбедност треба повеќе да се фокусираат на ефикасна и квалитетна човечка контрола на витални информатички системи и ефикасна крипто-заштита, а помалку на ограничување на користењето на информатичко-технолошки достигнувања кои се генерално општествено корисни. Интернетот нуди многу можности, секако без посебна регулираност, нуди огромна публика, анонимност на комуникација и брз проток на информации.

Треба да располагаме со стратегија преку која ќе дејствуваме. Организациите и пошироката јавност треба да бидат проактивни во спроведувањето на прашањата поврзани со компјутерскиот тероризам. Тие секогаш треба да се во потрага за подобрување на нивната безбедносна инфрастуктура. Треба да се држи чекор со последните случувања во полето на компјутерскиот тероризамт, да се дознаат сите најнови закани и да се посветат на подобрување на сопствената електронска безбедност, поради тоа што безбедноста е континуран процес.

Треба да се воспостават работни односи или аранжамани со јавни или приватни институции кои би можеле да помогнат во однос на закани поврзани со компјутерскиот тероризам. Да се оформат работни групи, кои со активности и развој на насоки за повисоки стандарди за подобрување на организацискатa безбедноста, развивање на планови за излез од криза, следење на новите трендови на компјутерскиот тероризам, значително би помогнале со цел да се зголеми отпорноста на вакви напади.

Исто така со зголемување на свеста на населението за прашањата поврзани со компјутерскиот тероризам, со нивно образование, ќе ја сватат важноста на одбраната од такви напади и со тоа ќе помогнат во развојот на општеството да биде проактивно во справување со безбедноста на информациите.

Самите Влади може да донесат нови или да ги дополнат постоечките Закони поврзани за компјутерскиот тероризам, со тоа што ќе ги зголемат казните за сторителите.[173]

Компјутерскиот тероризам е закана за иднината. Обединувањето на технолошките и социо-политички трендови, укажува на тоа дека компјутерскиот тероризам е бран на иднината. Ако се спроведува војна во компјутерскиот простор, и ако борци на иднината се нерегуларни борци, тогаш компјутерскиот тероризам е логична парадигма на идни конфликти. [174]

Компјутерскиот тероризам во иднина ќе добива се поголема популарност. Станува збор за невидлива закана. Ниските трошоци и едноставноста во иницирањето на овие напади, зголемувањето на бројот на високо квалификувани професионалци во областа на компјутерите, компјутерските напади ќе бидат нормална појава во иднина. Доколку една држава има обврска да го брани својот компјутерски простор, најпрво што треба да направи е да обезбеди системи кои ќе спречат наевторизиран пристап. Со подигање на прагот на вештини и нивото на технологијата можат да одвратат напад на компјутерски терористи во компјутерскиот простор.

Генерално иднината на компјутерскиот тероризам и улогата која ја игра е нешто непознато. Но она што е познато е дека постои закана, и тоа е реално. Фактот е дека компјутерскиот тероризам е веќе тука и тука ќе остане. Иако некои безбедносни технологии, методи и стратегии кои се развиени и се имплементираат со цел спречување на компјутерскиот тероризам, самите организации стануваат поранливи со се поголемиот развој на технологијата.

Како резултат на тоа во иднина треба да се реализираат планови кои се од клучно значење за развојот на стратегија, отворени комуникациски канали со цел да се зголеми соработката помеѓу јавниот и приватниот сектор на сите земји во борбата против компјутерскиот тероризам.

---

[173] *Види Пошироко: Christopher Beggs, Developing New Strategies to Combat Cyber-Terrorism, pdf.*
[174] *Andrew Rathmell, Cyber Terrorism: The threat of the future, pdf.*

Предложениот план на „SPECTR FCC" има за цел размена на проблеми во постојните стратегии во борбата против компјутерскиот тероризам. Иако овој план не е дефинитивен, тој е наменет за решавање на основните проблеми со цел да се обезбеди рамка за целосна стратегија за борба против компјутерскиот тероризам. Соработка на земјите заедно ќе ја подигне свеста на сите прашања и градење на безбедна средина за сите.

Со разбирањето за постоењето на оваа закана, ние сме свесни за нејзините последици, и со превземање на стратешки планови, допринесуваме да имаме безбедна информатичка средина која ќе биде продуктивна.

Денес во проценките на заканата од компјутерскиот тероризам, важно да се погледне надвор од традиционалните терористички групи и погледот да се сврти кон добро обучените компјутерски експерти, кои веќе поседуваат значителни хакерски вештини. Следната генерација на терористите ќе расте во дигиталниот свет, кој ќе биде помоќен и полесен за користење на алатки за хакирање. Во нив се гледа поголем потенцијал за компјутерски тероризам отколку на денешните компјутерски терористи, и нивното ниво на знаење и вештина во врска со хакирање ќе биде поголем. Компјутерски тероризам, исто така, би можел да стане поатрактивен доколку реалниот и виртуелниот свет во иднина станат поблиски.

2. НОВИТЕ И ИДНИ ПРЕДИЗВИЦИ НА ВИСОКОТЕХНОЛОШКИОТ КРИМИНАЛ И НИВНОТО ВЛИЈАНИЕ ВРЗ НАЦИОНАЛНАТА БЕЗБЕДНОСТ

Компјутерската безбедност вклучува предизвици кои ги поминуваат националните граници. Постојат огромни празнини во разбирањето на овој проблем, како и во техничките способности кои се потребни за да се справиме со овие предизвици. Во изминатата деценија напредокот во комуникациските технологии и во технологијата општо, го доведе човештвото во сериозни проблеми. Очигледно е дека компјутерските закани се гледаат како едни од главните проблеми на националната безбедност, и преставува предизвикувачка политика на Владите. Посебна карактеристика на компјутерската безбедност е дека често е многу тешко да се идентификуваат точно сторителите на нападот, како и земјата од каде доаѓа нападот. Затоа поединци или групи многу лесно ја прикриваат својата ангажираност и трага, или се маскираат како друг корисник. Компјутерската безбедност преставува троен предизвик.

Постои двоен предизвик за промовирање како на јавната така и на приватната безбедност и обезбедување на информатичко технолошката мрежа и победа над криминалните групи кои ги користат за остварување на своите цели. Меѓутоа исто така, компјутерската безбедност преставува се поголем предизвик за демократскиот систем, јавниот и приватниот сектор кои ја обезбедуваат информатичко технолошката мрежа и следење на сообраќајот, мора да биде во рамнотежа со безбедноста на луѓето, особено на човековите права, приватноста и слободата на изразување. [175]

Компјутерскиот простор е новата линија на фронтот. Овој свет – компјутерскиот простор е еден свет од кој сите ние зависиме секој ден. Тој е нашиот хардвер, софтвер, нашите персонални компјутери, лап топи, мобилни телефони, кои станаа секојдневност во нашите животи. Тоа се широки

[175] *Benjamin S, Buckland, Fred Schrreier, Theodor H. Winkler „Demokratsko Upravljanje izazovi cajber bezbednosti", стр.12. пдф*

интернет мрежи под нас, безжични сигнали околу нас, на локалните мрежи во училиштата, болниците и бизниси.

Отворена нација неможе да ги затвори компјутерските системи поради страв од овие закани. Наместо тоа, таа мора да изгради национална еластичност потребна за да се задржи отворен и безбеден компјутерскиот простор. За да се ублажат ризиците од високотехнолошкиот криминал и да се донесуваат одлуки за компјутерската безбедност, од суштинско значење е да се има јасно разбирање за заканата и поглед кон иднината.

ВИСОКОТЕХНОЛОШКИ ЗАКАНИ

Во нашиот меѓусебно поврзан свет, закани за нашата национална и компјутерска безбедност, може да дојдат неочекувано од различни извори и правци. Ова е она што може да се означи како предизвик од 360 степени. Во последните години компјутерската експлоатација и малициозните (вируси) активности, стануваат се повеќе софистицирани и сериозни:

- Закани со краткорочно влијание;
- Закани со долгорочно влијание.

Закани со краткорочно влијание

- Влијание на секојдневните активности на индивидуалните крајни корисници, на пример да добијат информации за финансиска трансакција, способност да дојдат до друга информација и сл.;
- Влијание од ден за ден на активностите на бизнис заедницата и на Владите. Тоа може да резултира со значителни финансиски и други загуби, како на пример зголемување на трошоци поради измамнички активности и зголемување на трошоците за безбедност.

Закани со долгорочно влијание

- Национални нарушувања на безбедноста (протекување на доверливи информации, владини информации);
- Социјално незадоволство и безредија (губење на довербата на јавноста во владата);
- Губење на интелектуалната сопственост, кои можат да влијаат на долгорочната конкурентност на бизнисите и владите.

Постојаната употреба на технологијата и на интернетот во сите аспекти од секојдневниот живот, придонесува да се стане мета на криминалците. Како што општеството се потпира се повеќе на технологијата, опасноста од погоре

наведените закани со краткорочно и долгорочно влијание, овозможува да станат реални закани. Борбата против овие закани бара од државите да гледаат над нивните грубо пропишани линии и да имаат поотворен пристап и соработка со приватниот сектор.

ПРЕДИЗВИК – (украдени лични и финансиски податоци)

Украдените лични и финансиски податоци се користат за да се добие пристап до постоечки банкарски сметки и платежни картички, или лажно да се земе кредит.

Опсегот на криминални активности:

- Фишинг;
- Фарминг;
- Дистрибуција на малициозен софтвер;
- Хакирање на база на податоци, што е подржано од страна на малициозен код;
- Специјалисти или физички лица може да закупат мрежа со илјадници компромитирани компјутери и да извршат автоматски напад.

ПРЕДИЗВИК – (Малвери)

Постои значително зголемување на бројот на аматерски компјутерски криминалци кои обично ги прават своите пари од дистрибуција на спам пораки или пак од продажба на украдени информации. Ова резултира со поделба меѓу софистицирани и аматерски компјутерски криминалци. Софистицираните компјутерски криминалци повеќе се движат на скриени форуми.

Малвер (malware) - кратенка од малициозен софтвер, е општ термин со кој се означува широк спектар непријателски или инвазивен софтвер, т.е. софтвер кој се употребува со цел да се попречи функционирањето на компјутерот, да се добијат чувствителни информации, или да се оствари

пристап до приватни компјутерски системи. Може да биде во облик на код, скрипта, активна содржина и други видови софтвер. Во малвер се вбројуваат компјутерските вируси, црви, тројанци, руткитови, спајвер, адвер, и други малициозни програми. Поголемиот дел активни малвер закани се, обично, тројанци или црви, а помал дел се вируси. Некои малвер програми можат да бидат маскирани да изгледаат како легитимен софтвер и дури може да дојдат од официјалната веб страница на некоја компанија во форма на корисна или привлечна програма во која е всаден малверот заедно со софтвер за следење кој прибира статистички податоци за маркетиншки потреби.[176]

Малверот може да се категоризира во:

- Генерички малвер кој е насочен кон општа популација и
- Малвер кој се насочува кон специфични институции. На пример малвер кој е дизајниран да експлоатира одредени слабости ан компјутерите на крајните корисници, на владите и одредени бизниси.

ПРЕДИЗВИК – (Cloud „облак“ компјутери)

Cloud компјутерите може да бидат дефинирани како збир на виртуелни компјутерски ресурси, кои им овозможуваат на корисниците да добијат пристап до податоци, апликации. Слабостите во одредена cloud компјутерска околина може да се искористи од страна на компјутерските криминалци со помош на малвери. Cloud Computing - претставува вид на сервис кој се заснова на заеднички (споделени) компјутерски ресурси, а не на услугата на локален сервер или личен уред при користењето на апликациите. При cloud computing, зборчето “cloud“ се користи како метафора за “интернетот“, па оттука фразата “cloud computing“ значи “вид на комјутерско работење на интернет“ каде различни услуги (сервери, складирање на податоци и апликации) се

[176] *Марко Зврлевски и др., Прирачник за компјутерски криминал, Јануари 2014, стр. 35*

пренесуваат до компјутерите и уредите на организацијата или институцијата преку интернет.

Исто така компјутерските криминалци можат да ги злоупотребат cloud услугите за да работат на сервери и да извршуваат DDOS напади, кои се напади од повеќе извори.

Виртуелната инфрастуктура може да се користи како отскочна даска за нови напади.

ПРЕДИЗВИК – (Електронски докази)

Дигитална Форензика

Со користење на научни методи и алати форензичарот собира многу докази за набљудуваниот компјутер или медиум, така да моделите треба да бидат синхронизирани заради полесна истрага, и во текот на итрагата да се води сметка за чекорите на моделот и што поквалитетно документирање во текот на истрагата и да се избере модел кој одговара за истражување на дигиталниот криминал.

- Дигиталната Форензика е процес на откривање и толкување на податоци во елктронска форма, кои подоцна се користат во Суд;
- Традиционална форензика (анализа на компјутерски уреди во лабараторија);
- Форензика во живо, се употребува со цел да се обезбедат докази на лице место, за да не се загубат податоци;
- Анализа на мобилни теелфони

Електронски докази

- Добивање на податоци кои се чуваат од страна на трети страни, испитување на тие податоци кои се клучен елемент во високотехнолошкиот криминал, и им овозможува на извршителите и обвинителите да ги поврзат клучните точки кои ги користат криминалците за да ги извршат криминалните активности;
- Зајакнување на соработката помеѓу јавниот и приватниот сектор, односно независните носители на податоци и спроведувачите на законот.

Наведените предизвици треба да не насочат на подобра заштита од високотехнолошките закани, како и на начинот да се справиме со истите. Со постојано надградување на системите за заштита, со следење на новитети ќе го намалиме ризикот на заканите, а со самото тоа ќе го зголемиме процентот на успешност во справување со заканите кои доаѓаат од високотехнолошкиот криминал.

ПРЕДИЗВИК ВО СПРЕЧУВАЊЕ НА ВИСОКОТЕХНОЛОШКИ КРИМИНАЛ

Во последните години многу распростанети се компјутерски криминални активности кои се финансиски мотивирани, како што се: неовластен пристап, интернет изнуди, дистрибуирање на DDOS напади и сл.

Некои организации не биле свесни ни дека доживеале еден или повеќе компјутерски безбедносен инцидент, но истите избегнуваат да пријават дека им се случила таков инцидент пред се поради:

- Веруваат дека инцидентот не бил доволно сериозен за да го пријават на надлежните органи за спроведување на законот;
- Веруваат дека мали се шансите за успешна исрага;
- Се плашат од негативен публицитет, и мислат дека такво известување во јавноста ќе резултира со неповолна конкуренстка позиција.

Во контекст на високотехнолошкиот криминал, се претпоставува дека компјутерските криминалци се:

- Финансиски или кривично мотивирани;
- Ги користат можностите кои ги нуди компјутерскиот простор како што се: анонимноста, нема географски ограничувања, се здобиваат со потребните ресурси кои им се потребни за вршење на криминалните активности;
- Таргетираат слабо заштитени мрежи или системи, искористуваат ситуација кога за спроведување на законот надлежните органи се попречени од правниот и законодавниот систем, особено во меѓународни случаи.

Иако не постои апсолутна заштита за изложеноста на секој информационен систем на сериозни ризици, најдобар начин за борба со високотехнолошкиот криминалитет е неговата превенција. Превенцијата мора

да биде така организирана да ги одврати потенцијалните извршители на високотехнолошки криминал од извршување на кривични дела на тој начин што би се преземале адекватни мерки за избор на луѓе кој би се занимавале со работа на компјутер до мера на физичка и софтверска заштита.

ПОЛИЦИЈАТА И СТРАТЕГИИ ЗА ПРЕВЕНЦИЈА

Улогата на полицијата во сузбивање на високотехнолошкиот криминал како и превенција од истиот, е клучна и од голема важност. Полицијата континуирано работи на јакнење на своите капацитети и унапредување на квалитетот на работа во сите сегменти од делокругот на своите надлежности.

Секоја држава треба да донесе национална стратегија за високотехнолошки криминал, поради тоа што стратегијата преставува комплексна задача имајќи во предвид различни аспекти и актери кои треба да бидат вклучени во тој процес. Тука се мисли на политички, законодавен, економски, воен, полициски и сл. поглед при донесување на една стратегија, како и интеграција на приватниот и јавниот сектор. Секоја држава е должна да ја штити својата национална информатичка инфрастуктура, како и својот компјутерски простор кој покрива национален домен.

Со донесување на стратегија, државата има за цел изградба на ефикасен, функционален компјутерски простор, кој истовремено е усогласен со меѓународните стандарди и принципи. За да се одговори на заканите кои доаѓаат од високотехнолошкиот криминал, кои закани постојано се менуваат, државите мора да имаат флексибилна и динамична стратегија за високотехнолошки криминал. Стратегијата треба да има јасно дефинирани цели и приоритети, и да преставува визија на една земја во однос на високотехнолошкиот криминал.

Р. Македонија е во крајна фаза на изготвување на Националната стратегија за високотехнолошки криминал, која секако значително ќе биде од корист и ќе помогне во справувањето со високотехнолошкиот криминал и сите негативни појави и закани кои доаѓаат од него.

Соочени со традиционалните и нетрадиционалните безбедносни предизвици, државите делуваат хаотично. Потребно е да се стави акцент и да се зајакне соработката на владите со приватниот сектор, невладините и меѓународните организации, што овозможува користење на географски,

технолошки, научни ресурси кои сами не би можеле да ги обезбедат. За успешно спречување на високотехнолошкиот криминал потребна е одлична соработка помеѓу јавниот и приватниот сектор, односно помеѓу судството, полициските служби и интернет провајдерите, координарана активност и соработка на државите и нивните институции, посебно безбедносните, пред се поради обезбедување на клучните докази.

Спроведувањето на законот се работи во три нивоа, и тоа:

- Превенција на криминалот;
- Истрага и
- Гонење

Компјутерските напади често ги поминуваат националните граници, додека пак спроведувањето на истрагите од страна на надлежните органи може да бидат спречени од страна на корпоративната сопственост на давателите на услуга на информацискатa технологија.

Постои потреба од достава на модерна технологија на надлежните органи кои го спроведуваат законот, следење на најновите трендови на злоупотреба и новите видови на криминал и спроведување на обуки за истите, на полициските службеници кои ги водат истрагите за високотехнолошки криминал, со цел успешно да одговорат на потребите и барањата на општеството.

Како една од најбитните препораки е дека за случаи за високотехнолошки криминал, потребна е меѓународна соработка на самиот почеток на истрагата.

❖

Можеме да заклучиме дека справувањето со предизвиците на високотехнолошкиот криминал преставува широка област за работа.

Високотехнолошката безбедност во многу држави преставува нов проблем за актерите од полето на безбедноста. На пример во Велика Британија контролата на државната компјутерска безбедност е доверен на Меѓуодделенски Надзорни Комисии, Кабинетот на одборот за Национална безбедност, меѓународни односи и развој и неговиот подкомитет за проактивна безбеднсот и реагирање. Во САД контролата ја има Канцеларијата на Директорот за Национална Безбедност, но на ниво на Конгресот надлежноста ја делат четири одбора со толку пододбори и секој одбор може различно да го перцепира проблемот.

Како што овие закани и предизвици се интернационални, така се потребни и транснационални партнерства.

Исто така со право може да си ги поставиме следниве прашања:

- Како што доаѓа еволуцијата и идентификување на предизвиците на високотехнолошкиот криминал, како да се зачува анонимноста на мрежите;
- Дали несвесно присуствуваме на друг бран на револуција во конфликтите и војните, дали се менува изгледот на конфликтите од корен, и ако е така кои последици можеме да ги имаме по нашите вооружени сили и безбедносниот сектор, какви последици ќе има врз агенциите за контраразузнавање.[177]

[177] *Benjamin S, Buckland, Fred Schrreier, Theodor H. Winkler „Demokratsko Upravljanje izazovi cajber bezbednosti" cmp.30., pdf.*

2.1 ЕЛЕКТРОНСКИ ДОКАЗИ ВО ИСТРАГИТЕ

Сите законски постапки се потпираат на докази. Доказот е во физичка форма како што се документи, фотографии, докази кои се електронски уреди (компјутери, мобилни телефони, други уреди за складирање податоци, и сите преставуваат електронски докази. Според меѓународната дефиниција во областа на форензичките науки, дигитален доказ е секоја информација во дигитален облик која има доказна вредност и која е приспособена или пренесена во таков облик. Поимот дигитален доказ вклучува компјутерски складирани или генерирани доказни информации, дигитализирани аудио и видео доказни сигнали, сигнали од дигитален мобилен телефон, информации на дигитални факс машини и сигнали од други дигитални уреди.

Значи, дигитален доказ е било која информација генерирана, обработена, складирана или пренесена во дигитален облик која судот може да ја прифати како меродавна, односно секоја информација составена од дигитални 1 и 0, складирана или пренесена во дигитална форма, како и други можни копии на оригиналната дигитална информација кои имаат доказна вредност и на кои судот може да се потпре, во контекстот на форензичка аквизиција, анализа и презентација.[178]

Самата природа на податоците и информациите кои се чуваат во електронска форма, за разлика од традиционалните ги прави полесни за манипулирање. Тоа создава специфични прашања за правниот систем и бара ракување на тие податоци на начин на кој се обезбедуваат информациите.

Информациите добиени од електронски докази се пренесуваат и се чуваат на електронски уреди кои може да се користат на Суд.

Електронските докази имаат сличности со традиционалните докази, но имаат и некои карактеристики кои ги прават различни.

---

[178] *Whitcomb C M., „A Historical perspective of Digital Evidence: A Forensic Scientist s View, International Journal of Digital Evidence" vol.1, issuue 1, 2002., pdf.*

- Електронските докази се невидливи за необучено око. Електронскиот доказ често се наоѓа на места, каде што може да биде пронајден само од страна на специјалисти со посебни алатки. Овие специфични алатки се користат во дигиталната форензика, и служат за анализа на податоци пронајдени во компјутер;
- Електронските докази може да бидат копирани во повеќе наврати. Тие може да се копираат и секоја копија е иста на оригиналот. Оваа особина им овозможува на експертите да направат повеќе копии и да работат на истите односно да вршат анализа. Исто така со тоа се овозможува електронските докази да се изведат на суд и од страна на експертот да биде образложен. Слично како и други форензички докази така и електронските доакзи се многу чуствителни, и треба да се обрне повеќе внимание на истите, во насока на: Работа со електронски докази од страна на експертот. Секој електронски уред има свои карактеристики, така што одредени постапки мора да се следат за да се пристапи до меморијата. Еден од најголемите ризици е ненамерна промена на дел електронските докази.;
- Брзиот развој на извори на електронски докази – тоа подразбира дека новите технологии се развиваат толку многу брзо и има потреба за постојано ажурирање како на новите технологии, така и на процедурите и техниките кои треба да се применуваат со цел да се искористи нивната содржина.;
- Од голема важност е користењето на пронајдените електронски докази за подршка на случајот пред суд. Доказите потребно е да бидат обезбедени согласно законската процедура.

Интернетот и масовната употреба на дигиталните медиуми овозможија нови методи на извршување на кривични дела, традиционалните видови на измама и другите видови на криминал добија нови сигурни канали за комуникација. Организираните криминални групи со најновите технологии си го

олеснуваат прикривањето во извршувањето на кривичните дела, особено за дистрибуција на фотографии со злоупотреба на деца, фишинг, фарминг и др.

Со овие нови начини на извршување кривични дела и нови видови на кривични дела кои се извршуваат преку електронски уреди, единствен доказ во овие случаи се елктронските докази, и истите се релевантни.

Традиционалните докази мигрираат од хартија кон виртуелна средина и нивните процеси се менуваат во однос на традиционалните докази. Во изминатите години електронските докази покажаа дека имаат важна улога и се клучни докази во повеќето случаеви. Речиси секој вид на истрага може да има корист од електронските докази, нив ги има во секој електронски уред и во мобилните уреди кои сега всушност се паметни уреди идентчни на компјутерите.

Развојот на интернетот и неговите апликации нудат многу можности, социјални страни, интернет страни, меѓусебна комуникација, а неодамна и можност за чување на податоци во „облак" односно „cloud" (виртуелен простор) каде се складираат и чуваат податоци. Тоа е многу важно да се знае, за да при водење на случајот се бараат електронски докази и во вакви места за чување на податоци, особено кога тоа е важно за случајот.

Исто така, важно е да се знае дека некогаш мрежни ресурси на некоја компанија се управувани од страна на друга надворешна компанија и се хоостирани во оддалечени локации. Во вкави случаи се соочуваме со проблем затоа што истражителот неможе да оди во друга земја, и тогаш потребно е да се контактира администтароторот, и да се воспостави меѓународна соработка со таа земја. Администраторот на системот може да дозволи пристап на истражителот до ситемот каде што се наоѓаат податоците кои му се потребни како доказ.

Како извори на докази може да бидат сите електронски уреди кои може да функционираат самостојно, заедно или во функција на компјутерски систем. Со напредокот на технологијата се зголеми и бројот и видот на уреди кои може

да содржат електронски докази. Во последните многу популарни се таблет уредите, тоа се уреди малку поголеми од мобилните телефони, кои работат на принципот на допир на екранот. Тие доаѓаат во многу форми и големини и имаат способност за чување на податоци, иако најчесто во последно време како што кажавме погоре податоците се чуваат во „облакот", и истите може да бидат извор на корисни електронски докази.

Хард дискот е главното место каде се складираат и чуваат податоците. Тој може да биде поврзан на компјутер или да биде надворешен независен од компјутерот. Исто така податоци се чуваат и на ЦД (Компакт Диск), ДВД (Дигитален Видео Диск), БД (Blu Ray disk), мемориските картички се уреди за складирање на дигитални информации, тие често се користат во многу уреди како што се фото апарати, мобилни телефони, лап топ компјутер и др., при што тие може да задржат податоци без електрична енерфија, ги има во различни капацитети што значи може да соберат голема количиба на податоци, а е лесно да се сокрие.

USB мемориѕкиот уред (Universal Serual Bus) е стандарден уред за складирање и чување на податоци, кој може да се поврзува со компјутери. Го има во сите големини и видови, и истиот може да биде добар извор на електронски докази. Исто така мобилните телефони кои на почетокот на нивното појавување се користеа само за јавување, денес тие се користат за многу други работи како на пример испраќање е-мејлови, спроведување деловни активности, фотографирање, тие навистина се компјутери. Треба да се знае дека различни телефони имаат различни способности.

Компјутерскиот систем и неговите компоненти многу често се вредни докази за истрагата. На него има зачувано многу податоци како на пример фотографии, меѓусебна комуникација, пораки, финансиски податоци, интернет историја, бази на податоци, зачувани податоци за други уреди кои се поврзувале на компјутерот, и сето тоа преставува многу битен доказ.

Кога ќе се дојде до податок дека постои електронски доказ потребно е од самиот почеток да се направат консултации како помеѓу истражните служби,

Јавниот Обвинител, и Секторот за Компјутерски Криминал и Дигитална Форензика. Јавниот Обвинител треба да даде официјална Наредба за Вештачење на компјутерската опрема каде што има електронски докази. Како што кажавме вештачењето го вршат полициски службеници кои имаат лиценци за вештачење и се стручни во таа област.

Потребно е да се знае дека собирањето на електронски докази не се прави само во лабароторија. Тоа може да се стори и на терен, при извршување претрес на одредена локација, да се направи таканаречена „жива форензика" (Live Data Forensics), односно одземање на електронски докази од компјутерскиот уред на лице место, од страна на стручно лице вештак, со помош на одредени алатки и соодветна компјутерска опрема. Тоа се прави кога е потребно снимање на податоци пред да се исклучи уредот од струја или мрежа, и за утврдување на сомнението за кривичното дело. За тоа е потребна официјална Наредба од Надлежното Обвинителство или Суд.

Најбитно е да добро се обезбеди лице местото од каде што треба да се одземат електронски докази, затоа што многу е лесно истите да бидат променети или избришани. Потребно е да се обезбедат сите електронски уреди во просторијата. Обезбедувањето на лице местото се прави од страна полицискиот службеник кој го води претресот.

❖

Последните примери укажуваат дека во најголем број на истраги, клучните, или курцијални докази за истрагите се наоѓаат во електронска форма. Самото тоа зборува дека во иднина сите докази ќе бидат во електронска форма, а поради тоа треба да се стави акцент на осовремување на лабораториите во Министерствата за Внатрешни работи на современите држави, на снабдување на најсовремена опрема, како и најсовремени алатки за работа, и оспособување на кадарот.

2.2 ЕНКРИПЦИЈА

Криптографските техники претставуваат техники за заштита на безбедноста на интернет комуникациите каде спаѓа кодирањето кое уште е наречено енкрипција. Енкрипцијата е процес на трансформирање или енкриптирање на податоците на начин кој што е тежок, скап или одзема многу време за неавторизирано лице да го декриптира.

Една од главните методи за безбедност е енкрипцијата на податоците, така што само лице кој го има вистинскиот клуч или код, може да дешифрира и да даде смисол на податоците. Постојат многу форми на енкрипција, обично работи со превземање на оригинални информации и конвертирање на истите во нечитлива форма. За декриптирање на информациите се прави спротивното и се дешифрираат информациите во обичен текст. Енкрипцијата и дешифрирањето се врши на информации се прави со помош на алгоритам наречен број.

Енкрипцијата односно криптографијата датира уште од 1900-та година п.н.е., и нејзе ја користеле Египќаните, потоа и многу познати личности како Јулиј Цезар, Томас Џеферсон кој развил шифра тркало кое е направено во 1790-та година.

За собирањето на електронски докази многу е битно на уредот каде што се наоѓаат дали е заштитен со енкрипција. Во последно време енкрипцијата станува се популарна, особено ако некој сака да сокрие криминални активности, без разлика дали се работи за физичко лице или некоја компанија. Многу компании веќе бараат компјутерите на кои се работи да бидат енкриптирани, со користење на софтвери како што се „Microsoft BitLocker“, „TrueCrypt“, „Steganos“, и др.

Кога вештаците ќе наидат на криптиран „хард диск“ многу е тешко истиот да се декриптира, односно да се одклучи. Тоа преставува проблем за обезбедување на електронските докази.

Енкрипцијата преставува процес во криптографијата, кој означува на трансформирање на информации (plaintext со користење на алгоритми наречени шифра) да не биде читливо за кој било освен за оние кој имаат посебно знаење, обично назначено како клуч. Резултатот од процесот се енкриптирани информации (во криптографијата, назначено како шифра-текст).

Во многу контекси, зборот **енкрипција** исто така имплицивно укажува на обратен процес т.е. **декрипција** (пр. "софтвер за енкрипција" може исто така да декриптира), за да ја направи информацијата читлива повторно (т.е. да го направи не-енкриптирано). Постојат два одновни начини на енкрипција и тоа: енкрипција со таен клуч и енкрипција со јавен клуч.

Енкрипцијата е процес во криптографијата кој означува трансформирање на информации (plaintextco) користење на алгоритми наречени шифра, да не биде читливо за било кој освен за кои имаат посебно знаење, обично назначено како клуч. Резултатот од процесот се енкриптирани информации назначени како шифра-текст. Зборот енкрипција исто така укажува на обратен процес т.е дескрипција за да ја направи информацијата повторно читлива, односно да биде не-енкриптирана.

Енкрипцијата датира многу одамна, уште п.н.е., ја користеле и војниците за тајни комуникации. Денес енкрипцијата често се користи за заштита на информации. Таа се користи за заштита на датотеки како на пример заштита на фајлови на компјутер. Енкрипцијата исто така се корсти за дата во транзиција, односно податоци кои се пренесуваат преку локални мрежи, интернет мрежи, мобилни и друго. Енкрипцијата многу помага во безбедноста, бидејќи многу е тешко да се обезбедат сите мрежи. Еден од првите јавни клучеви за енкрипција бил наречен Pretty Good Privacy (PGP). Бил напишан во 1991 година од страна на Фил Зиммерма, а во 2010 година купен од страна на Symantec.[179]

---

[179] *Види пошироко: Lech J. Janczewski, Andrew M. Colarik, Cyber Warfare andCyber Terrorism, pdf.,стр.57-62.*

❖

Вмрежениот свет е големо поле за делување на криминалците. Секојдневно многу деца и возрасни се жртви на интернет, на невини луѓе им се украдени пари од сметки, а на криминалците им е од голема помош тоа што за високотехнолошкиот криминал нема граници. Прибавувањето на докази преку меѓународна правна помош потребно е да се стави на највисоко ниво, и да биде приоритет во иднина, зошто само така ќе може да се дојде до потребните електронски докази без разлика каде се наоѓаат. За овој вид на истраги од голема помош се ресурсите на институциите како што се Интерпол, Европол ЕС3, Европравда, Селек.

За водењето на истрагата исто така многу е важно обвинителот да има компјутерски познавања, да ги разбира извештаите на вештаците, да може да советува, да дава насоки на полицијата во текот на истрагата, да врши надзор на собирањето на електронските докази да бидат во согласност со законот. Обвинителот треба да работи рамо до рамо со истражителите, да им помага да ги избегнат правните стапици. Обвинителот треба да биде во можност да ја утврди најсоодветната надлежност за прогон посебно кога се работи за прекуграничен криминал, и добро да го презентира случајот во Судот.

Како што кажавме високотехнолошкиот криминал не познава географски граници, и поради тоа обвинителот има поголема улога во поттикнување на прекуграничните врски. Добивањето на електронските докази преку меѓународна правна помош ќе помогне многу во водењето на случајот.

3. ПОИМНИК НА МАКЕДОНСКИ ЗБОРОВИ ОД ИНФОРМАТИЧКАТА ТЕХНОЛОГИЈА

attachment; прилог, припратка

attention; внимание

back up; прави резерва, осигурува

bill; сметка

boot; подигање

browser modifier; модификатор на прегледувачот

browsing history; претходни прегледи

bug; грешка

cable modem; кабелски модем

cancel; откажи!

capital letter; голема буква

capitalization; претворање во големи букви

CAPS LOCK; само големи букви

CD burner; ЦД-режач

CD burner speed; брзина на ЦД-режачот

CD Player; ЦД-уред

CD-ROM; ЦД-РОМ

CD recorder; ЦД-снимач

close; затвори

command; наредба

command button; командно копче

command line; командна линија

computer language; компјутерски јазик

confirm; потврди!

conflict; конфликт

connect; поврзува

connect; поврзи!

connection; поврзување, врска

copy; копирај!, копија

data; податоци

data transfer; пренос на податоци

data type; тип податоци

data validation; проверка на податоците

database; база на податоци

database connection; врска со базата на податоци

datasheet; табеларни податоци

debug; отстранување грешки

decrypt; дешифрирај!

decryption; дешифрирање

default; стандардно, предодредено, по правило, подразбирливо

default button; стандардно копче, предодредено копче, подразбирливо копче

destination; одредиште, дестинација

destination file; дредишна, дестинациска датотека

detach; оддели

device; уред

device driver; двигател за уред

digital ID; дигитален идентитет

digital license; дигитална лиценца

digital photo; дигитална фотографија

digital signature; дигитален потпис

digital video; дигитално видео

digital video disk; дигитален видеодиск

dim; затемни!

disable; оневозможи!

disabled; оневозможен

disabled control; исклучена контрола, оневозможена контрола

desktop; работна површина

download; преземи!

domain; домен

e-mail; е-пошта

e-mail account; сметка на е-пошта

e-mail address; адреса на е-пошта

e-mail flooder; масовен испраќач на е-пораки

e-mail message; е-порака

e-mail server; сервер за е-пошта

edit; уреди!

error; грешка

file; датотека

folder; папка

hard disk; 1. цврст диск

2. тврд диск

3. диск

hardware; машински дел, хардвер

hidden; скриен

hidden text; скриен текст

hierarchical menu; хиерархиско мени

high-definition; висока дефиниција

high-definition DVD; ДВД со висока дефиниција

home page; почетна страница

homepage; почетна страница

host; домаќин

hosted; вдомен, поставен

hosting; вдомување, поставување

input focus; влезен фокус

input/output; влез/излез

insert; вметни

Internet; интернет

Internet address; интернет-адреса, и-адреса

internet forum; интернет-форум, и-форум

Internet information services; интернет-информативен сервис (ИИС)

Internet Protocol; интернет-протокол (ИП)

intranet; интранет

invalid; неважечко, погрешно

image; слика

junk e-mail; непотребна е-пошта

junk mail; непотребна пошта, шут-пошта

key; клуч, копче key sequence; комбинација на копчиња

keyboard; тастатура

link; врска

line spacing; проред

local area network; локална мрежа (ЛАН)

locate; лоцирај!

location; локација

locked; заклучен

lockup field; заклучено поле

log; дневник, записник

log file; датотека за евиденција

log off; одјавување

log on; пријавување

logging; евидентирање

password; лозинка

password authentication; проверка на лозинката

print device; уред за печатење

print preview; приказ пред печатење

printer; печатач

web; веб

web browser; веб-прелистувач, веб-прегледувач

web connection; веб-поврзување, веб-врска

web page; веб-страница

web page preview; преглед на веб-страницата[180]

---

[180] *ПОИМНИК на македонски зборови од областа на информатичката технологија, Министерство за Информатичко општество, Република Македонија, пдф.*

ЗАКЛУЧОК

Главен допринос на оваа доктроска дисертација е компаративната анализа на законската регулатива и правосудната пракса на високотехнолошкиот криминал, како во Р.Македонија така и во други современи држави. Ова анализа покажа дека во однос на тие држави, во Р.Македонија е потребно дополнително усогласување на законските регулативи. Во однос на тоа оваа докторска дисертација стави акцент на актите кои треба да се донесат а со тоа да се обогати нашиот правосуден систем, а со тоа и ќе ги исполни сите насоки кои се дадени со Конвенцијата за Компјутерски Криминал со цел усогласување на законската регулатива. Во многу елементи Р.Македонија е добро правно регулирана во борбата против високотехнолошкиот криминал од повеќето земји во регионот.

Високотехнолошкиот криминал не е иднина, туку сегашност. Високотехнолошкиот криминал има се поголем замав, применува иновации и бележи значаен пораст

Науката, индустријата, комуникацијата благодарение на развојот на информатичката технологија значително се развија. Но тоа има и негативна страна, односно се поголемо е антисоцијалното однесување, како и деструктивното и терористичкото однесување. Интернетот е сеуште нова работа, а поради тоа може да се појават нови и пострашни работи отколку што навистина се. Интернетот, како современ начин на комуникација стана неминовност во животите на современиот човек. Меѓутоа, покрај благодетите што ги носи користењето на интернетот, паралелно се појавуваат и негативните страни од неговата употреба, што особено се огледа во фактот што постојано се појавуваат нови начини на извршување на кривични дела.

Со се пософистицирана информатичка технологија видот на закани, начинот на извршување на напади, се повеќе се разликува од традиционалните видови и начини на закани и напади. Од една поширока

перспектива земјите денес се соочуваат со закани по нивната национална безбедност кои закани не се традиционални. Најважни импликации на овие промени се да се зголеми соработката на меѓународно ниво, да се нагалси оваа потреба за соработка помеѓу народите, се со цел успешно да се одговори на заканите кои доаѓаат од високотехнолошкиот криминал.[181]

Земјите во развој се борат против високотехнолошкиот криминал во согласност со нивните средства, но развиените земји мора да ја чувствуваат нивната одговорност дека се напредни во технологијата, и мора да го споделат товарот на земјите во развој и да им олеснат, колку што е можно, затоа што ако овие злосторства не се контролирани, тоа ќе влијае на целиот свет со само еден клик.

Високотехнолошкиот криминал е таков вид на криминал, кој што често пати ги поминува границите на една држава, на пример, делото е сторено во една држава, сторителот е од друга држава, а настанатата штета е во трета држава. Оттука, најдобра пракса при борбата со високотехнолошкиот криминал е интензивна соработка на меѓународно ниво со полициските служби од другите држави а посебно преку меѓународните институции како Интерпол, Европол и СЕЛЕК.

Државите треба да усвојат соодветни мерки за регулирање на истрагана овие кривични дела, да се соберат докази за кривичното дело што е можно повеќе.

Владите треба да усвојат мерки во рамките на своите ресурси. Тоа не значи дека одговорноста за преземање чекори кон намалување на високотехнолошкиот криминал е само на Владата на која било земја, тоа е обврска на меѓународната заедница, националните корпорации и поединци.

---

[181] *James A. Lewis, „Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats" pdf.*

Значи, за успешно справување со високотехнолошкиот криминал потребна е прекугранична соработка, еднакво законодавство и координиран истражен процес.[182]

Експертите предупредуваат дека во иднина бројот на компјутерски напади ќе биде се почест, а се потешко ќе биде да се утврди од каде доаѓа нападот, односно местото на извршување на кривичното дело не е како во минатото, односно го нема тоа значење, пред се затоа што компјутерските напади може да доаѓаат од трети земји а да биде нападната сосем друга земја. Лицата кои ги извршуваат овие кривични дела многу умешно и паметно го користат компјутерскиот простор, знаејќи дека во него нема да остават никакви докази за да во иднина бидат откриени, ги користат многуте алатки кои ги нуди напредната информациска технологија, а со кои алатки се прикрива трагата од каде доаѓа наапдот, односно се дава сосема лажен приказ. Сето ова ја отежнува работата на истражителите од институциите кои работат на сузбивање на високотехнолошкиот криминал.

Исто така, со брзиот развој на информацискатa технологија, сигурноста на податоците кои циркулираат низ комплексно дизајнираните инфомациски мрежи е загрозена. Голем е ризикот за напад и злоупотреба на информации и податоци. Потребно е да се креираат безбедни решенија кои ќе гарантираат и ќе обезбедат побрз пренос на податоците, и што е најважно побезбеден пренос во поглед на сигурноста.

Компаниите, организациите, институциите, потребно е да изградат соодветни системи за заштита на дигиталните податоци во компјутерските мрежи. Знаејќи дека не постои апсолутна заштита и дека секој информационен систем е подложен на ризици, потребно е навремено детектирање на заканата и ризикот од истата, со цел успешно справување, и штетите да се доведат до минимум.

---

[182] *Nadia Khadam, Insight to Cybercrime.pdf.*

Пред сите нас е долг, тежок и премногу сложен пат за борба со непознатото, однсоно со високотехнолошкиот криминал, пред се за да ја заштитиме националната безбедност на својата држава, безбедноста на граѓаните, да им овозможиме да имаат сигурен и безбеден информатички простор за работа, и да не бидат загрозени од новите предизвици и закани кои ги носи високотехнолошкиот криминал.

Но треба да бидеме и задоволни од самите себе затоа што сме доволно свесни за заканите кои ги носи информационата технологија и нејзиниот брз развој, и со усогласување на меѓународното законодаство, со носење на национални стратегии, стратешки планови за борба против високотехнолошкиот криминал, со образование и обука, секоја современа држава обезбедува безбедна и продуктивна информатичка средина.

Ние како преставници на овие институции и како корисници на интернет кој самиот по себе е „добар слуга а лош господар", сме одговорни да ја одржуваме нашата информатичка средина здрава и безбедна, за да биде посигурна во иднина.

КОРИСТЕНА ЛИТЕРАТУРА

1. Митко Котовчевски, Национална Безбедност, Скопје 2013.
2. Митко Котовчевски, Национална Безбедност, Скопје 2011.
3. Митко Котовчевски, Национална Безбедност на Република Македонија, Втор дел:Внатрешни извори на загрозување на националната безбедност, Скопје 2000.
4. Митко Котовчевски, Национална Безбедност на Република Македонија, Трет дел: Надворешни и глобални извори на загрозување на националната безбедност, Скопје 2000.
5. Ѓорѓе Игњатовиќ, Организовани Криминалитет, други део-Криминолошка анализа стања у свету, Београд 1998.
6. Emilio C. Viano, Jose Magallanes, Laurent Bridel, Transnational Organized Crime.
7. Тања Милошевска, Модели на поврзаност на тероризмот и на транснационалниот организиран криминал, Скопје 2014.
8. Phil Williams, Dimitri Vlasis, Combating Transnational Crime, Concept, Activities and Responses.
9. Милан Шкулиќ, Организовани Криминалитет, Појам и кривично Процесни аспекти, Београд 2003.
10. Организовани Криминалитет, Зборник – Стање и мере заштите.
11. Миќо Бошковиќ, Организовани криминалитет, први део – Криминолошки и криминалистички аспекти, Полицијска Академија, Београд 1998.
12. Оливер Бакрески – Координација на безбедносната заедница во Република Македонија, Скопје 2005.
13. Оливер Бакрески – Координација на Безбедносниот Сектор – *искуства и практики*- Скопје 2006.
14. Трајан Гоцевски – Основи на системот на Националната одбрана - *второ издание*.
15. Трајан Гоцевски – Основи на системот на Националната одбрана – *трето дополнети и изменето издание*.

16. Трајан Гоцевски – Основи на системот на Националната одбрана – *четврто дополнето и изменето издание*.
17. Наука –Безбедност- Полиција, Часопис криминалистичко-полицијске Академије Београд,2007;
18. Парламентарен надзор на Секторот за Безбедност (Начела, механизми и практики). Прирачник за Парламентарци, бр.5-2003.
19. Мирослав Хаџиќ, Драган Симиќ,Богољуб Милосављевиќ, „Национална и Глобална Безбедност", Београд 2005.
20. Владимир Урошевиќ, Сергеј Уљанов, Радоје Вуковиќ, Министерство унутрашних послова Република Србија, Полиција и Високотехнолошки криминал – Примери из праксе и проблем у раду, пдф.
21. Милан Милошевиќ, „Допринос Стручних лица сузбијању организованог високотехнолошког криминалитета, Организовани криминалитет" , Зборник, Стање и мере заштите, пдф.
22. Саша Мијалковиќ, „Национална Безбедност – од вестфалког концепта до постхладногратовском" пдф.
23. Марина Митревска, Антон Гризолд, Владо Бучковски, Ентони Ванис, превенција и менаџирање на конфликти, Скопје 2009.
24. Панде Лазаревски „ Стратешки истражувања" Одбрана, бр. 68, Скопје, 2001.
25. Хатиџа Бериша, Концепт Велике Албаније као претња националној безбедности Република Србија, Београд 2014, пдф.
26. Department Of Information Technology National Cyber Security Policy "For secure computing environment and adequate trust & confidence in electronic transactions ", Department of Information Technology Ministry of Communications and Information Technology Government of India Electronics Niketan, Lodhi Road New Delhi – 110003 pdf.
27. Phil Williams, Organized Crime and Cybercrime: Synergies, Trends, and Responses,pdf.
28. Mitchel P. Roth, PhD, Global Organized Crime, pdf.
29. Оливер Бакрески, Најсилно оружје досега, Современа Македонска Одбрана бр.9.пдф.

30. Информациона Безбедност: Стандарди или Правила, Данијела Д. Протиќ, Генералштаб Војске Србије, Управа за телекомуникације и информатику, пдф.;
31. Магистерски труд под наслов „Видови и облици на злоупотреба на Информатичката технологија" одбранет на 21.10.2009 година на Филозофскиот Факултет Св.„Кирил и Методиј" Скопје – Институт за одбранбени и мировни студии.
32. Alexander Klimburg, National Cyber Security, pp. 16, 2012 by NATO Cooperative Cyber Defence Centre of Excellence. (https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf).
33. A Brief History of Computer Crime:An Introduction for Students, M. E. Kabay, PhD, CISSP-ISSMP.pdf.
34. Introduction to Information Security, Linda Pesante, 2008 Carnegie Mellon University, пдф.
35. Susan W. Brenner, Cybercrime Criminal Threats from Cyberspace, 2010, pdf.
36. John Arquilla and David Ronfeldt, CYBERWAR IS COMING,Chapter Two, pdf.
37. Paulo Shakarian Jana Shakarian Andrew Ruef, Introduction to Cyber-Warfare, pdf.
38. Ronald A. Glantz, Pantera, 2014, pdf;
39. Muhammad Saleem, Jawad Hassan, "Cyber warfare", the truth in a real case, pdf.
40. Dana Rubenstein, Nation State Cyber Espionage and its Impacts, pdf;
41. An introduction to malware, CERT-UK, pdf.
42. Lech J. Janczewski, Andrew M. Colarik, Cyber Warfare andCyber Terrorism, pdf.
43. Mike McGuire, Samantha Dowling, Cyber crime: A review of the evidence, 2013, pdf.
44. Maura Conway, 'Hackers as Terrorists? Why it Doesn't Compute.' Computer Fraud and Security 2003, pdf.
45. Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication,Tallinn 2012.

46. Demokratsko Upravljanje izazovi cajber bezbednosti, Benjamin S, Buckland, Fred Schrreier, Theodor H. Winkler, пдф.
47. James A. Lewis, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, pdf.
48. Nadia Khadam , Insight to Cybercrime, pdf.
49. Eric Goetz, Guofei Jiang, William Stearns, VIRUSES AND WORMS, 2002, pdf.
50. Creating a Safer Information Society bylmproving the Security of Information Infrastructures and Combating Computer-related Crime. Europe 2002, pdf.
51. Clay Wilson Specialist in Technology and National Security Foreign Affairs, Defense, and Trade Division, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, pdf.
52. Mcafee Virtual, Criminology Report, Organised Crime and the Internet, pdf.
53. Christopher Beggs, Developing New Strategies to Combat Cyber-Terrorism, pdf.
54. Andrew Rathmell, Cyber Terrorism: The threat of the future, pdf.
55. Поимник на македонски зборови од областа на информатичката технологија, Министерство за Информатичко општество, Република Македонија, пдф.
56. Botnet Mreze (CCERT-PUBDOC-2007-12-213, (http://www.cert.hr/), pdf.
57. Александар Дончев, Современи безбедносни системи, Скопје, 2007.
58. Марина Митревска, Антон Гризолд, Владо Бучковски, Ентони Ванис, Превенција и менаџирање на конфликти – Случај Македонија (нова безбедносно парадигма) Скопје, 2009.
59. Ѓорѓи Тоновски., Меѓународни односи, авторизирани предавања, Факултет за општествени науки, Скопје, 2004.
60. Нацев Зоран, Теориски основи на доктрината и стратегијата на националната одбрана, НИП Ѓурѓа, Скопје 1999.
61. Нацев Зоран, Начевски Ратко „Војна, мир и безбедност, Македонска ризница, Куманово, 2000.
62. Јордан Спасески, Македонија столб на безбедноста и мирот на Балканот, Скопје, 2005.

63. Панде Лазаревски, Стратешки истражувања, Одбрана, бр. 68, Скопје, 2001.
64. Александар Дончев, Современи безбедносни системи, Скопје, 2007.
65. Марина Митревска, Антон Гризолд, Владо Бучковски, Ентони Ванис, Превенција и менаџирање на конфликти – Случај Македонија (нова безбедносно парадигма) Скопје, 2009.
66. Алекса Стаменковски, Основи за натамошна доградба на системот за безбедност во Република Македонија, Зборник на трудови од меѓународната научна и стручна конференција Реформите на Безбедносниот Сектор во Република Македонија и нивното влијание врз борбата против криминалитетот одржана на ден 15.09.2012 година, на Европскиот универзитет - Република Македонија, Скопје, 2012.
67. Влада на Р.Македонија., Национална концепција за безбедност и одбрана, Скопје.
68. IPU and DCAF, Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices, (IPU and DCAF: Geneva), 2003.
69. Peter Albrecht and Karen Barnes. "National Security Policy-Making and Gender." Gender and Security Sector Reform Toolkit. Eds. Megan Bastick and Kristin Valasek. Geneva: DCAF, OSCE/ODIHR, UN-INSTRAW, 2008.
70. Божидар Бановић, Вељко Турањанин, Високотехнолошки тероризам, Супротстављање Организованом Криминалу правни оквир, међународни стандарди и процедуре Тара, 2013.
71. Лидија Комлен Николић „Сузбијање високотехнолошког криминала", Удружење јавних тужилаца и заменика јавних тужилаца Србије, Београд.
72. Хатиџа Бериша, „Концепт Велике Албаније као претња националној безбедности Република Србија", Београд 2014, стр.24.
73. Југослав Ачкоски, „Сигурност на компјутерски системи, компјутерски криминал и компјутерски тероризам", Скопје, 2012.
74. Department Of Information Technology National Cyber Security Policy "For secure computing environment and adequate trust & confidence in electronic transactions", Department of Information Technology Ministry of

Communications and Information Technology Government of India Electronics Niketan, Lodhi Road New Delhi – 110003, pdf.

75. Department Of Information Technology National Cyber Security Policy "For secure computing environment and adequate trust & confidence in electronic transactions", Department of Information Technology Ministry of Communications and Information Technology Government of India Electronics Niketan, Lodhi Road New Delhi – 110003 pdf.
76. Никола Тупанчевски, Драгана Кипријановска „Основи на македонското информатичко казнено право", Скопје, 2008.
77. Chik B. Waren, "Challenges to Criminal Law Making in the New Global Information Society", 2011.
78. Creating a Safer Information Society byImproving the Security of Information Infrastructures and Combating Computer-related Crime, Europe 2002.
79. Светлана Николоска „Компјутерски кривични дела против слободите и правата на човекот и граѓаните во Република Македонија", Хоризонти бр. 6, Битола, 2010.
80. Don Parker, Computer abuse, Springfild, 1973, pdf.
81. August Bequai, Computer crime, Lexington, 1978, pdf.
82. Brvar Bogo, Pojavne oblike zlorabe računlnika, Revija za kriminalističko in kriminologijo br. 2/1982, Ljubljana
83. Зоран Сулејманов. ,Криминологија, Скопје, 2003.
84. Drakulic, Mirjana, Drakulic, Ratimir, "Cyber kriminal", Fakultet organizacionih nauka, Begorad, 2009.
85. Светлана Николовска „Методика на итражување компјутерски криминалитет", Скопје, 2013.
86. Wendy Parkes, Thomas Legault, "Identity Theft: Introduction and Background", CIPPIC Working Paper No.1 (ID Theft Series), March 2007, Ottawa: Canadian Internet Policy and Public Interest Clinic.
87. Aaron Emigh ,Radix Labs,„ Online Identity Theft:Phishing Technology, Chokepoints and Countermeasures"October 3, 2005.
88. Aaron Emigh ,Radix Labs,„ Online Identity Theft:Phishing Technology, Chokepoints and Countermeasures"October 3, 2005.

89. Кенет К.Лаудон, Џејн П.Лаудон, Менаџмент информациски системи : Управување со дигитална компанија, Скопје : Арс Ламина, 2010.
90. USAID, Анализа на состојбата со електронската трговија во Република Македонија, Скопје, ноември, 2010.
91. Кенет К.Лаудон, Карол Герсио Травер, Електронска трговија: бизнис, технологија, општество, Скопје:Арс Ламина, 2010.
92. Кенет К.Лаудон, Џејн П.Лаудон, Менаџмент информациски системи : Управување со дигитална компанија, Скопје : Арс Ламина, 2010.
93. Gojko Grubor, Milan Milosavljevic, Osnove zastite informacija: metodolosko-tehnoloske osnove, Univerzitet Singidunum, Beograd, 2010;
94. Кенет К. Лаудон, Карол Герсио Травер, Електронска трговија: бизнис, технологија, општество , Скопје:Арс Ламина, 2010.
95. Colin Combe, Introduction to e-business management and strategy, Butterworth-Heinemann, 2006.
96. Paul Beynon-Davies, E-business, Palgrave macmillan, New York, 2004.
97. Дитер Голман, „Компјутерска сигурност“ АД Вербум, Скопје 2010.
98. Владо Камбовски. „Казнено право, посебен дел“, Просветно дело АД Скопје, 2003.
99. Елена Конеска, Јасминка Сукаровска Костадиновска, Митко Богданоски, Сашо Гелев, DoS напади кај безжичните мрежи и методи за намалување на ефектите од овие напади, Европски Универзитет – Скопје, Р. Македонија, УДК: 004.7.056.
100. Colin Combe, Introduction to e-business management and strategy, Butterworth-Heinemann, 2006.
101. Russian Business Network (RBN): RBN - Georgia CyberWarfare." Russian Business Network (RBN). 5 Nov. 2008 http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare.html
102. Swedish bank hit by 'biggest ever' online heist (2007) ZdNet, httpp://news.zdnet.co.uk/security/0,1000000189,39285547,00.htm
103. Кенет К.Лаудон, Џејн П.Лаудон, Менаџмент информациски системи: „Управување со дигитална компанија“, Скопје: Арс Ламина, 2010.

104. Митко Богданоски, Александар Ристески, Марјан Богданоски, Индустриски сајбер напади – „Глобална Безбедносна Закана“ Зборник на трудови, Факултет за електротехника и информациски технологии – Скопје.

105. Мајкл Херман, Моќта на разузнавањето во Мир и во Војна, Академски печат Скопје, 2009;

106. Јордан Спасески „Македонија столб на безбедноста и мирот на Балканот“ Скопје, 2005.

107. Konvencija o Visokotehnološkom Kriminalu, Budimpešta, 23.novembar 2001.

108. Сашо Гелев, Јасминка Сукаровска Костадиновска, „Безбедност кај Компјутерските мрежи од аспект на контрола на пристап“, Електротехнички факултет, Универзитет Гоце Делчев, зборник на трудови, Штип. 2013.

109. Правилник за обезбедување на безбедност и интегритет на јавните електронски компјутерски мрежи и услуги и активности кои што операторите треба да ги преземат при нарушување на безбедноста на личните податоци, Закон за електронски комуникации, Службен весник на РМ. Бр.39/2014 и 188/2014.

110. Slobodan Nedeljković Ministarstvo unutrašnjih poslova Republike Srbije, Evropska Strategija bezbednosti i Sajber Pretnje – Značaj Za Srbiju, DOI: 10.5937/vojdelo 1503135N.

111. http://whatis.techtarget.com/definition/CERT-Computer-Emergency-Readiness-Team .

112. Vanesa Polić, „Komparativna Analiza Kompjuterskog Kriminala u Zakonodavstvima Republike Srbije i nekih stranih zemalja“, Univerzitet Singidunum.

113. Корелација Информационе и Националне Безбедности, Др Саша Мијалковиќ, Др Вера Арежина-Ќериќ, Др Горан Бошковиќ, пдф.

114. Закон за ратификација на Конвенцијата за Компјутерски Криминал, бр. 07-2623/1, 16 јуни 2004 година Република Македонија, Скопје.

115. Светлана Николовска ,,Методика на истражување на компјутерски криминалитет“ Ван Гог, Скопје, 2014.

116. Законот за ратификација на Дополнителниот протокол на Конвенцијата за компјутерски криминал за инкриминација на дела од расистички и ксенофобистички вид по пат на информатички системи, бр. 07-2621/1 5 јули 2005 година Скопје.

117. Закон о изменама и допунама Кривичног закона Република Србије, ЈП Службени гласник бр. 39/2003, Београд и Кривични законик Републике Србије, ЈП Службени гласник бр. 85/05.

118. Методија Ангелески „Вовед во Криминалистика" Скопје, 2007.

119. Eldan Mujanović, Samir Rizvo, „Uloga Interpola u Provođenju Postupaka Izručenja za teška kršenja Međunarodnog Humanitarnog Prava", Časopis za kriminalistiku, kriminologiju i sigurnosne studije, 2010.

120. Nadia Gerspacher (2005) "The Roles of International Police Cooperation Organizations European Journal of Crime, Criminal Law and Criminal Justice".

121. Светлана Николоска „Современи методи во сузбивањето на транснационалниот економско финансиски криминал", Скопје, 2015г.

122. Michael Woodiwiss, Dick Hobbs, „Organized evil and the Atlantic Alliance: moral panics and the rhetoric of organized crime policing in America and Britain" - British Journal of Criminology, 2009.

123. Камбовски Владо, 2005, „Организиран криминал", Штип.

124. Марјан Габеров „Транснационален организиран криминалитет - трендови и случувања", Септември, 2014 г.

125. Драган Младеновиќ и др. „Tehnološki, Vojni i Društveni Preduslovi Primene Sajber Ratovanja, Vojnotehniki Glasnik Military Technical Courier", 2012.

126. Марко Зврлевски и др., Прирачник за компјутерски криминал, Јануари 2014.

127. Whitcomb C M. „A Historical perspective of Digital Evidence: A Forensic Scientist s View, International Journal of Digital Evidence, 2002.

128. Colin Combe, „Introduction to e-business and strategy" 2006.

129. Закон за ратификација на конвенцијата за Компјутерски криминал Службен Весник на Република Македонија, бр.41 од 24.06.2004 година.

130. Службен весник на Република Македонија бр.19 од 30.03.2004 година – пречистен текст.
131. Кривичен законик – Сл. весник на РМ бр. 37/96) , (Измени и дополнувања – „Службен весник на Република Македонија“ бр. 80/99, 4/02, 43/03, 19/04, 81/05, 60/06, 73/06, 7/08, 139/08, 114/09 и 51/11) , (Одлуки на Уставен суд на Република Македонија – „Службен весник на Република Македонија“ бр. 48/01, 16/02, 40/04, 50/06.
132. Службен весник на РМ, бр. 67 од 29.05.2009 година.
133. Службен весник на Р. Македонија бр.98/08 од 04.08.2008 година.
134. Сл. Весник на Р. Македонија, бр.43 од 04.03.2014 година.
135. Сл. весник на Р Македонија” бр. 9/04 од 27.02.2004 година.
136. Службен весник на Р. Македонија бр.86/08 од 14.07.2008 година.
137. http://www.mcafee.com/jp/resources/reports/rp-economic-impact-cybercrime2.pdf .
138. Хрватска Академска и Истражувачка Мрежа – CARNet (Croatian Academic and Research network) http://www.cert.hr/.
139. http://www.coindesk.com/price/ .
140. https://www.nilsonreport.com/publication_chart_and_graphs_archive.php .
141. https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf
142. http://www.hanyang.ac.kr/home_news/H5EAFA/0002/101/2012/29-3.pdf
143. http://searchsecurity.techtarget.com/sDefinition/0.,sid14_gci771061,00.html
144. http://srbin.info/2014/02/19/ko-su-najpoznatije-teroristicke-grupe-hejzbolah-hamas-al/
145. http://www.stat.gov.mk/PrikaziSoopstenie.aspx?rbrtxt=77
146. http://mvr.gov.mk/vest/874
147. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/index_en.htm.
148. http://www.odbrana.mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/VD_3-2015/67-2015-3-11-Nedeljkovic.pdf .

149. http://it.mk/k-e-se-formira-natsionalno-telo-za-spravuvan-e-so-kompjuterski-intsidenti/.
150. https://www.techopedia.com/definition/2387/cybercrime.
151. https://www.europol.europa.eu/ec3.
152. http://www.selec.org/m105/Home.
153. http://www.interpol.int/en .
154. http://searchsecurity.techtarget.com/definition/cyberwarfare .
155. http://en.termwiki.cn/EN/cyber_terrorism.
156. http://www.crime-research.org/library/Cyber-terrorism.htm.
157. http://www.academia.edu/643030/Cyber-prostor_binarno_kodirani_urbani_pejza%C5%BEi.
158. https://articles.forensicfocus.com/2012/06/01/the-role-of-cyber-terrorism-in-the-future/.
159. http://searchsecurity.techtarget.com/definition/hacktivism.
160. https://www.vocabulary.com/dictionary/cyber-terrorist, https://www.ipredator.co/cyber-terrorism/ .
161. http://searchsecurity.techtarget.com/definition/spyware.
162. http://usa.kaspersky.com/internet-security-center/threats/spyware#.Vs7Pp_krLDc .
163. https://www.ncjrs.gov/App/publications/abstract.aspx?ID=171868.
164. https://www.csid.com/2014/03/combating-cyberterrorism-with-cyber-security/.
165. http://www.irma-international.org/viewtitle/32381/.
166. http://www.rand.org/pubs/reprints/RP1051.html.
167. http://fas.org/irp/threat/cyber/docs/npgs/ch5.htm.
168. http://www.irma-international.org/viewtitle/32381/.
169. http://us.norton.com/cybercrime-pharming .
170. http://www.computerweekly.com/feature/The-law-and-cyber-sabotage .
171. http://www.webopedia.com/TERM/S/software_piracy.html .
172. http://pravoikt.org/strategija-sajber-bezbednosti-eu-otvoren-bezbedan-i-zasticen-sajber-prostor/ .
173. http://www.weblens.org/invisible.html.
174. http://www.thecultureist.com/2013/05/09/how-many-people-use-the-internet-more-than-2-billion-infographic/ .

175. http://www.pravo.org.mk/documentDetail.php?id=5616 .
176. http://www.osce.org/me/montenegro/117630?download=true.
177. http://www.oas.org/juridico/english/cyb_pry_G8_network.pdf
178. http://www.cybercrimelaw.net/G8.html .
179. http://www.cbs.com/shows/csi-cyber/news/1003888/these-cybercrime-statistics-will-make-you-think-twice-about-your-password-where-s-the-csi-cyber-team-when-you-need-them-/ .
180. http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf .
181. https://www.enisa.europa.eu/ .
182. http://jorm.gov.mk/?p=690.