
UNIVERSITETI I EVROPËS JUGLINDORE
УНИВЕРЗИТЕТ НА ЈУГОИСТОЧНА ЕВРОПА
SOUTH EAST EUROPEAN UNIVERSITY

**ВТОР ЦИКЛУС НА СТУДИИ (ПОСТДИПЛОМСКИ СТУДИИ)**

**МАГИСТЕРСКИ ТРУД**

**ТЕМА: „ЗАГРОЗУВАЊЕ НА СИГУРНОСТА ПО ПАТ НА ИНФОРМАТИЧКИ СИСТЕМИ“**

**Кандидат:**

**Иво Стојаноски**

**Ментор:**

**проф.д-р Исмаил Зејнели**

**Тетово, Февруари 2021**

**Содржина**

**Апстракт**

Во сегашното модерно време, постои сепозабележителна позитивна врска меѓу новата технологија и компјутерскиот криминал и начинот на кој овој криминал функционира е се потежок за откривање. Исто така во нашата држава има многу малку луѓе кои се запознаени со овие форми и облици на криминал и тоа ги прави граѓаните лесни мети врз кои овој криминал може да биде извршен.

Така, во овој магистерски труд се анализираат формите и облиците на компјутерскиот криминал што можат да ги загрозат информатичките системи и како всушност тие функционираат. Се објаснува начинот на функционирање на информатичките системи и се олеснува препознавањето и превенцијата од опасностите на компјутерскиот криминал. Понатаму, се објаснува развојот на компјутерскиот криминал, неговите карактеристики и дефинирањето, како и феноменологијата на овој вид криминал за олеснето запознавање со начините на извршување и препознавање. Исто така се задржуваме и на правната регулатива за овој компјутерски криминал, како во Македонија, така и во други земји, а и меѓународната регулатива.

**Клучни зборови:** компјутерски криминал, феноменологија на компјутерски криминал, правна регулатива.

**Вовед**

Во модерното време, со се понапредната компјутерска технологија и компјутерски системи, криминалот наоѓа пат да навлезе во напредокот и да почне да користи. Овие напредоци исто така носат и промени во начинот на живот и функционирање во општеството, што го прави човекот зависен од ваквите промени.

Како главно обележје во овој магистерски труд, ќе се задржиме на објаснување на функционирањето на компјутерскиот криминал, првично од неговото појавување, па се до правните регулативи и превентивните мерки.

Како прв дел од магистерскиот труд, ќе биде претставен компјутерскиот криминал, неговото дефинирање, историскиот развој како и најважните карактеристики кои го обележуваат.

Вториот и најважен дел на овој магистерски труд ќе ги спомне феноменолошките карактеристики на компјутерскиот криминал, како што се компјутерските кражби, компјутерските измами, компјутерската пропаганда, хакирањето, создавањето на вируси со цел нивно објаснување, кога првпат се појавиле, како функционираат и кои мерки можат да се превземат за превенција. Исто така ќе се задржиме и на начините на извршување на овој вид криминал и нивниот тек од нивниот влез во компјутерскиот систем, па се до пренесувањето од еден компјутерски систем на друг.

Во третата глава ќе се задржиме на правната регулатива, каде прво ќе биде објаснета меѓународната регулатива на компјутерскиот криминал, за потоа да дојдеме до правната регулатива во Република Северна Македонија и неколку други земји како што се Русија, Британија и Бугарија за споредба со нашиот систем.

Како четврта и последна глава во овој магистерски труд ќе се задржиме на превентивните мерки и начините за спречување на овој вид на криминал, со цел насочување и поголема сигурност.

## ГЛАВА ПРВА

## ПОИМ, КАРАКТЕРИСТИКИ И РАЗВОЈ НА КОМПЈУТЕРСКИОТ КРИМИНАЛ

### 1. Поим за компјутерски криминал

Давањето на една дефиниција за формите на криминал кои се нови се појавува како еден голем проблем на криминологијата. Исто како и кај другите, и кај компјутерскиот криминал не постои една дефиниција за која би се рекло дека е прифатена, затоа што е многу тешко поради големината на феноменолошката разлика да се опфатат сите кривични дела кои би можеле да се класифицираат под компјутерски криминал во една дефиниција. Така компјутерскиот криминал можеме да го претставиме како една целина од кривични активности кои се извршуваат преку компјутерски системи за сопствена придобивка или предизвикување штета.[1]

Литературата на криминологијата има сфаќање дека компјутерскиот криминал спаѓа во кривични дела од област на заштита на имот и тие дела се карактерно најблиски до кривичните дела од областа на заштита на имот. Најраспространета дефиниција во криминологијата го дефинира компјутерскиот криминал, како збир на сите видови деликвентно однесување со кое уредите за обработка на податоци се користат како средство за извршување на казниви дела или како директна цел за казниви дела.[2]

Првата дефиниција за компјутерски криминал е дадена во Прирачникот за правда на Министерството за правда на САД каде го претставува компјутерскиот криминал како противзаконско дело каде треба детално и добро познавање на компјутерска технологија за успешно справување со него.

Најопштата дефиниција дадена за компјутерскиот криминал е од страна на Комисијата на Европската унија преку Соопштение кое е дадено во 2001 година со кое компјутерскиот

[1] Parker B.D., Fighting computer crime, New York( USA), 1983, стр.70.
[2] Konstantinović-Vilić S., Nikolić-Ristanović V., Kriminologija, Niš, 2003, стр.178-179

криминал е секое кривично дело кое на било кој начин вклучува користење на информатички технологии.[3]

Една дефинизија која може да се оддвои од просторот на поранешна Југославија е таа на д-р Ѓорче Игнатовиќ, каде компјутерскиот криминал го претставува како посебен вид на однесување каде компјутерскиот систем е средство или предмет за извршување на кривично дело, кое на друг начин или кон друг објект воопшто не би било можно да се изврши или би имало некои поинакви карактеристики.[4]

Друга широко употребувана дефиниција го претставува компјутерскиот криминал како друштвено опасна појава, која за нејзино постигнување извршителот користи компјутерско познавање, преку компјутерскиот систем како средство или објект за извршување на кривичното дело.[5]

Од овие дефиниции може да се заклучи дека спектарот на компјутерскиот криминал е многу широк како и дека под компјутерски криминал спаѓа секоја кривична активност која се извршува со помош на компјутер со мрежи и програми. Создавањето на компјутерските вируси и нивното распространување, како и објавувањето на лични податоци и заштитени податоци претставува друг дел покрај делата кои се насочени за добивање на имотна корист.[6]

И покрај наведувањето на сите овие дефиниции за компјутерскиот криминал, децидна дефиниција сеуште нема и веројатно не постои дефиниција која може да ја опфати целосната сложеност и проблематика на компјутерскиот криминал, па мора да се задоволиме и да ги користиме дефинициите кои ни се дадени во овој момент.

## 2. Историски развој на компјутерскиот криминал

Компјутерскиот криминал првично почнува да се појавува кон крајот на шеесетите години на минатиот век за осумдесетите и деведесетите да земе поголем замав и да ги

[3] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2001:0051:FIN
[4] Ignjatović Đ., Pojmovno određenje kompjuterskog kriminala, Beograd, 1991, стр. 142–143.
[5] B.Simonović,*Kriminalistika*, Pravni fakultet u Kragujevcu, Kragujevac, 2004, стр. 665
[6] T.Aleksić i M.Škulić, *Kriminalistika*, Beograd, 2007, стр. 46-63.

натера светските сили да ја забележат опасноста која може да ја предизвика тој вид на криминал и да почнат со воведување на мерки за справување со тој криминал.

- На почетокот компјутерскиот криминал во голема мера бил извршуван од вработени во некоја фирма кои биле незадоволни или пак сакале да и наштетат на таа фирма.
- За време на тие почетоци на компјутерскиот криминал софтверските напади не биле толку чести колку што биле физичките напади и уништувањето и штетата врз хардверот на компјутерските системи.
- Со ширењето на телекомуникациските ситеми низ ИТ светот, луѓето што биле насочени кон криминал почнале да учат да ги напаѓаат системите и мрежите и да крадат многу важни податоци.
- Првите појавувања на опасен софтвер се во 1980тите, со што тој софтвер бил наменет за напади на пресонални компјутери.
- Со растењето на интернетот и неговото проширување низ светот и светските системи, криминалците почнале со напаѓање на недоволно заштитени системи за различни намени, како вандализам, политички дејствија или финансиска корист.
- За време на 1990тите години компјутерскиот криминал постојано расте се додека не се појавуваат нови оперативни системи кои се позаштитени и се приморани за создавање на нови начини на извршување на кривичните дела, а тоа се скем е-маиловите.

Неколку од попознатите компјутерски криминалци во 1980тите и 1990тите години се Роберт Морис од САД, Владимир Левин од Русија за извлекување на над 10 милиони долари од системот на Ситибанк и Кевин Митник кој во 1995 година успеал да фалсификува над 20.000 броеви на кредитни картички за што бил осуден.

Извршените компјутерски напади кои се се почести за нивна цел ги земаат и државните, но и приватните фирми и успеваат да им направат големи штети поради недоволната заштита или касната реакција на фирмите.

Неколку примери за штетата и опасноста од компјутерските напади се:

- Велика Британија во 2003 година има загуби од 120 милиони фунти, предизвикани од директен компјутерски криминал и околу 28 милиони од таканаречените „вируси“.[7]
- 2003 година Австралија има загуби од 5.5 милиони долари од криминални напади и „вируси“ заедно.[8]

Поврзаноста на приватниот сектор заедно со државниот во овие напади и овој криминал, создаваат потреба за заштита и поврзаност на компјутерските мрежи со глобалната мрежа, каде поради зголемувањето на компјутерскиот криминал и опасноста од него напредувањето и зголемувањето на безбедноста на компјутерските системи и интернетот станува многу важен развојот и напредокот на таа безбедност и заштита.[9]

### 3. Карактеристики на компјутерскиот криминал

Кога ги гледаме горенаведените дефиниции и ги истражиме подетално ќе забележиме дека компјутерскиот криминал има повеќе карактеристики кои се различни во споредба со другите форми на криминалитет, иако конкретна дефиниција која го објаснува овој криминалитет сеуште немаме. Ако ги анализираме овие кривични дела ќе забележиме дека тие се многу често добро скриени поради оддалеченоста помеѓу сторителот и жртвата, како и неговата лесна размена и прилагодливост кон различни жртви, земји или пак самиот изглед на овој криминалитет. Така, преку овие податоци можеме да заклучиме дека компјутерскиот криминал е многу тежок, прво да се открие, а потоа и да се докаже за да може да се казни сторителот се додека не се пронајде очигледна штета врз оштетениот што исклучиво може да се забележи во компјутерскиот систем.[10]

Поради тоа што компјутерската технологија се повеќе расте, а со тоа и можностите за компјутерски криминал се зголемуваат, се појавуваат многу посложени дела кои не и биле предходно познати на судската пракса и тоа заедно со огромното распространување на компјутерскиот криминал паралелно со најновите технологии можеме да заклучиме

[7] Hi-Teh crime: The Impect to UK Business, www.nhtcu.org
[8] Australian Institute of Criminology, www.aic.gov.au
[9] Robinson J., Internet as the Scene of Crime, International Computer Crime Conference, Oslo,2000., www.ccips.org
[10] Zivkovski Z. I., Otkrivanje i razjašnjavanje kompjuterskog kriminaliteta, 2012, стр.162-165.

дека една од побитните карактеристики на компјутерскиот криминал е динамиката на развој и неговата различниост во споредба со другите видови на криминалитет.[11]

Со започнувањето на користењето на интернетот, и неговото ширење посебно во последните дваесет години компјутерскиот криминал драстично се проширува во рамките на целиот свет, и со тоа се прави уште посложен начинот на пронаоѓање на сторителот кој со добар интернет и брз компјутер може од каде било во светот да ја нападне жртвата и да изврши компјутерски криминал. Со ова што е кажано погоре можеме да заклучиме дека како друга многу битна карактеристика на компјутерскиот криминал се забележува и неговата распротранетост, без разлика на граници или територија.

На почетокот на појавувањето на информатичките технологии, знаењето да се ракува со компјутери и разбирањето на начинот на функционирање на компјутерите било голем приоритет ако сакаш да се занимаваш со тоа нешто, посебно ако се знае дека за време на тие почетоци немало големи услови за учење на информатички технологии, а со тоа и пропорционално откривањето на компјутерски криминал станува многу тешко. За разлика од тогаш, во овој момент со напредокот на компјутерските технологии и многу големата достапност на компјутери и интернет до сите луѓе, разбирањето и нивното учење е многу олеснато, што дава можност и криминалот многу побрзо да се зголемува поради толку големата достапност. Затоа компјутерскиот криминал во последните години е толку пораснат во споредба со почетоците на информатичките системи, бидејќи лицата кои биле стручни и ја познавале компјутерската технологија на почетокот биле далеку помалку отколку сега.

Многу значајна карактеристика во овој вид на криминал е дека лицата кои ги извршуваат делата се во најголем дел непознати поради сите тие заштити и прикривања кои новата технологија ни ги нуди, а воедно и се убрзува и олеснува брзината на извршување, а ризикот се намалува со оглед на тоа дека нема никаков физички контакт меѓу сторителот и жртвата.

[11] Gillespie A. A., Cybercrime: Key Issues and Debates Florence, Kentucky (USA), 2015, стр.17.

Во компјутерскиот криминал постои и темна бројка на кривични дела и последици кои се предизвикани од тие дела. Според некои податоци таа темна бројка е многу голема и се движи околу 90% до 99%, што значи дека бројката на неоткриени случаи е огромна во споредба со откриените и расчистените случаи. Многу голем проблем е тоа што полицијата добива многу мал број на пријави, што понатаму и се многу помал број на решени случаи.

Во врска со таа темна бројка можеме да одделиме неколку крактеристики кои се позначајни, а тоа се:

- Дека многу е мал ризикот на откривање;
- Најчесто сигурносните програми кои се користат се или лоши или застарени;

## ГЛАВА ВТОРА

## ФЕНОМЕНОЛОШКИ КАРАКТЕРИСТИКИ НА КОМПЈУТЕРСКИОТ КРИМИНАЛ

### 1. Обем

Со растењето на можностите за злоупотреба на компјутерската технологија, растат и различните можности да се извршат противправните дела, со што класификациите на тие дела се неизбежни. Новите компјутерски технологии можат да се употребат за извршување на веќе познатите форми на криминал, а и за сосема нови кои се поврзуваат со злоупотребата на компјутерите, компјутерските системи и мрежите.

Познатите (постари) форми на криминал ги завземаат:

- Проневерата;
- Измамата;
- Фалсификувањето;

Додека новите фориме можеме да ги претставиме како кривични дела кои се извршуваат исклучиво преку користење на компјутер, и тоа:

- Хакирање;
- Пишување и заразување со вируси;

Самите можности кои ни ги даваат новите компјутерски технологии, иако се многу корисни и практични, со нив носат и големи закани кои можат да создадат големи проблеми преку прислушкување, следење и набљудување, кражби преку компјутери како и повреда на приватноста и терористичките напади кои во последно време се многу застапени.[12]

[12] Jovašević D., Hašimbegović, T., Krivičnopravna zaštita računarskih podataka,2008.godina; стр.3.

При анализа на предходна работа и изтражување на криминолози и адвокати поврзана со компјутерскиот криминал, В. Водинелиќ во обид да ги вклучи модерните форми на кривични дела, ја прави следната поделба:[13]

- Неовластено користење на компјутери;
- Компјутерска шпиунажа;
- Манипулирање со компјутери;
- Саботажа на компјутери;[14]

Со оваа поделба се покрива најголем дел од криминалните активности кои ги опфаќа компјутерскиот криминал.

## 2. Видови на компјутерски криминал

### 2.1. Компјутерски кражби

Два основни начини на извршување на овие дела се:

- Влезот преку информатички систем и крадење на податоци и важни информации;
- Физичкиот напад преку кој се крадат деловите на хардверот или опремата која се користи;

Ние ќе се задржиме на влезот преку информатичкиот систем, како облик на незаконско присвојување на податоци. Неколку различни форми се важни во овој начин на извршување на кривичното дело, и се именуваат според нештото што е присвоено за време на ова кривично дело, како на пример кражба на податоци, кражба на услуги или пак лозинки или кодови.

Поради растењето на свеста на луѓето за тоа колку вредноста на информациите заедно со компјутерите и компјутерските системи драстично се зголемува, така и кривичните дела поврзани со тоа се зголемуваат. Така побарувачката за подобро заштитени

[13] Šarkić N., Prlja D., DamnjanovićK., Marić V., Ţivković V., Vodinelić V., Mrvić-Petrović N.: Pravo informacionih tehnologija, Beograd, 2011, стр.3.
[14] Jovičić D., Bošković M., Kriminalistika metodika, Banja Luka, 2002, стр. 446–449

компјутери дополнително расте, а воедно и интересот на криминалците за подобри напади и крадење на податоци кои би им донеселе уште поголема финансиска добивка.

Во поновото време, кражбата на податоци е многу голем проблем, а со тоа и потребата од подобра заштита станува многу голема. Со таа заштита се штитат информации кои потенцијално би можеле да бидат разлика меѓу голема работа на фирмата или нејзино затварање, поради тоа што интернетот нуди многу големо олеснување во тргувањето со вакви податоци, иако кражбата на тие податоци не е нова таа станува се поголем проблем кој константо расте, и му овозможува на сторителот преку интернетот и анонимноста која ја нуди лесно да се ослободува од информациите кои се стекнати и да добие некаков финансиски бенефит.

Специфичен случај за кражба на податоци е и повлекувањето од функција на Кетрин Аркулета од местото претседател на Федералната служба за управување со персоналот на САД, кога било откриено дека се украдени податоци од луѓе кои во периодот од 2000 година до денес конкурирале за вработување во федералната администрација, а бројот на луѓе чии податоци биле укредени се верува дека е околку 21.5 милиони.

Како една од најчестите кривични дела кои се извршуваат во целиот свет се кражбите на компјутерски услуги и неовластеното користење на тие услуги. Преку компјутерските услуги сторителот за цел има неовлестено користење на туѓи ресурси за негова корист, и како последици се оптоварувањето на мрежата или забавувањето во извршување на зададените задачи. Кај овие кривични дела најчести сторители се поранешни вработени кои имале пристап до компјутерскиот систем на фирмата и по нивното заминување продолжуваат да го користат за нивни цели кои најчесто се врзани со финансиската заработка. Исто така ова кривично дело многу често го извршуваат за користење на телефонски или интернет ресурси, на тој начин што се прикриваат трагите на самиот сторител преку извршувањето на некое кривично дело преку системот на таа телефонска или интернет компанија.

Компјутерските лозинки, кодови и индентификациони броеви како мерка за заштита од кражба или кривични дела се многу значајни за сите луѓе и доколку тие податоци се

изврши кражба на тие податоци може сериозно да се намали нивната безбедност и сигурноста на нивните лични податоци. Во Германија во 2014 година се украдени податоци од Федералната канцеларија за безбедност, со што бил загрозен пристапот до електронската пошта на околку 16 милиони луѓе и нивната приватност.[15]

Се проценува дека во иднина компјутерските кражби дополнително ќе се зголемуваат преку крадење на персонални информации, како примерот со германската Федерална канцеларија и со тие податоци сторителите ќе можат слободно да отвораат банкарски сметки, да купуваат или пак да поднесуваат пријави за добивање на некакви документи на име не оштетениот. Така со добивање на лажни идентитети да прават дополнителни кривични дела кои понатаму би му наштетиле на лицето чиј идентитет е украден. Многу често се случува лицето чиј идентитет е украден да не биде свесно за тоа се додека не пристигне некое побарување на негово име, а тој воопшто да не го направил тоа. Тоа укажува дека доколку идентитетот ти е украден, има голема шанса за користење на твоите информации за кривични дела кои во иднина би можеле да ти наштетат и да се плати многу висока цена, иако можеби оштетениот воопшто не направил ништо лошо, туку неговите податоци несвесно биле украдени или тој ги запишал во некоја страна која ги искористила за нелегални дела.

### 2.2. Компјутерски измами

Компјутерските измами како најраспространет облик на компјутерски криминал може да се најдат скоро секаде каде има размена на пари и стоки. Во литературата овие измами се третираат како економски криминал, што објаснува колку компјутерскиот криминал е сличен и близок во обликот со економскиот криминал.

Најзастапени области каде можат да се забележат компјутерските измами се:

- Осигурителните системи;
- Страни за менаџирање на финансиките средства;
- Даночните процедури;

[15] http://www.rtv.rs/sr_lat/evropa/milionska-kradja-lozinki-u-nemacko_454999.html

- Перењето на пари[16];

Карактеристиката по која овој тип на криминал се препознава е доведувањето на одредено лице во лажна сигурност, каде таа сигурност се употребува против тоа лице, за добивање на одредени финансиски бенефиции. Начини на кои може да се изврши компјутерската измама, исто како и нејзините облици се бескрајни, и можат да се издвојат од непрофесионални аматерски измами, па се до професионални измами во кој се има вложено многу труд и време да се постигнат, а поради тоа и е многу потешко да се откријат и спречат.

Како еден од најмногу застапените видови на компјутерски криминал, компјутерската измама неретко предизвикува огромни штети кои многу тешко и долго се поправаат. Како измама која првична цел и е добивање на некаква корист од лицето кое е измамено, компјутерската измама ги намамува потенцијалните оштетени лица преку лажни ветувања, каде треба да се пополнат податоци на одредена страна или документ и преку пополнување на тие податоци лицето да биде оштетено или ограбено. Оваа измама исто така не е потребно многу време за да го намами лицето поради тоа што се се извршува преку интернет и компјутер. Така лицата после внесувањето на нивните податоци и потпаѓањето под измамата губат секаква информација за страната или програмата каде што ја внесле информацијата и тука завршува измамата.

Многу познат случај на компјутерска измама е вирусот Мелиса кој на 26 Март 1999 се појвавува на илјадници емаил системи, и секаде е претставен како важна порака од колега или некој пријател. Неговата првична цел била да прати инфицирани меилови на првите 50 контакти на секоја листа така што секој инфициран компјутер би инфицирал 50 други компјутери. Многу големи компании како на пример Мајкрософт, Интел морале целосно да ги затворат своите емаил системи за да го прекинат ширењето на вирусот со што самиот Мелиса вирус предизвикал огромни финансиски штети, пресметани на околу 400 милиони долари.

[16] Matijašević J., Krivičnopravna regulativa računarskog kriminaliteta; Pravni fakultet za privredu i pravosude, Novi Sad ,2013стр. 166.

По деталната истрага која била спроведена, вирусот Мелиса е поврзан со 32 годишен програмер од Њу Џерси, Давид Смит кој бил обвинет за компјутерска измама и му биле досудени 20 месеци во федерален затвор во САД. Давид Смит е еден од првите луѓе кои биле обвинети за кривично дело, пишување на вирус.

### 2.3. Компјутерска проневера

Како компјутерска проневера се дефинира лажното прикажување или не прикажување податоци за да се добие одредена материјална корист. Како предмети на компјутерската проневера се сите податоци кои претставуваат вид на стока на одреден пазар.

Тие може да бидат:

- Пари;
- Заложни права;
- Кредитни рејтинзи;
- Лозинки;
- Кодови;
- Броеви кои се користат за идентификација;
- Биланси за проверка на состојбата;

Главна особина на компјутерската проневера се прикажува како наоѓање начин за придобивање на одредени информации од страна на лицето на кое се дадени да ги управува, така што ќе му донесат одреден финансиски бенефит на лицето кое ја извршува проневерата. На почетоците на компјутерската проневера, најголем дел од делата биле извршувани во банките каде има голем број вработени и простор да се прави проневерата.

Најчести облици на компјутерска проневера се фалсификувањата на:

- Патни налози;
- Книговодствени книги;

- Сметки;
- Фиктивни клиенти;
- Пописи;
- Лажно прикажување на загубите на одредена фирма;
- Лажно зголемување на некои резерви во фирмата;
- Кредитни извештаи;[17]

Овој вид на криминал е многу сличен со криминалот кој во англискиот речник има посебен израз и е наречен „White Collar" (бели јаки), поради извршувањето на криминалот преку компјутер и големите профити на криминалците преку проневерата.

Компјутерската проневера исто така се претставува и како случајно дело, кое ги претставува сторителите како лица на кои им се задала добра шанса за извршување на тоа дело и тие ја искористиле, а всушност немале претходна намера да го сторат тоа дело. Најдобар начин за намалување на ова кривично дело се чести проверки и финансиски контроли во фирмите, со што потенцијалните сторители ќе се исплашат и ќе размислат два пати дали да го сторат тоа кривично дело.

Во 2009 година во Индија се случила една од најголемите вакви проневери, каде Индиската федерална полиција го уапсила претседателот на одборот на Satyam корпорацијата со тринаесет други лица. Како водечка компанија за обезбедување на софтвер услуги во Индија, биле проневерени повеќе од 2.5 милијарди долари што довело до банкрот на компанијата и нејзино затворање. По тоа затворање на компанијата 20.000 луѓе ги изгубиле работните места, а акционерите изгубиле повеќе од 70 милијарди долари.[18]

---

[17] Petrović R. S., ; Kompjuterski kriminal; Ministarstvo unutrašnjih poslova Republike Srbije : Uredništvo ĉasopisa"Bezbednost" i lista "Policajac",Beograd 2000, стр. 131.

[18] Претседателот на управниот одбор со соработниците ги фалсификувал одлуките на управниот одбор и на тој начин од средствата на компанијата во повеќегодишен период проневерил преку 2,5 милијарди долари, при што проневерените пари ги уплаќал на фиктивни фирми и поединци. Надлежните органи во истрагата откриле дека во еден период корпорацијата им исплаќала плати на 13000 непостоечки работници. Проневерените средства потоа се користеле за купување на акции на берза и купување на преку 1000 недвижнини во Индија од странски фиктивни компании, при што потоа им биле отстапувани на членовите на семејствата кои учествувале во проневерата.

## 2.4. Компјутерско фалсификување

Главната карактеристика на компјутерското фалсификување можеме да ја забележиме како произведување на лажни или преработка на реални предмети со цел добивање на некаква финансиска добивка.

Под компјутерското фалсификување како најзастапени ствари кои се фалсификувани можеме да ги наброиме:

- Документите;
- Парите;
- Потписите;
- Хартиите од вредност;[19]

Исто така во помодерното време се јавува и нова ствар која може да биде фалсификувана и преку неа да се нанесе голема штета, а тоа е фалсификувањето на е-поштата која доколку е фалсификувана лицето кое ја прима поштата е излажано дека му ја праќа лицето чиј емаил стои како испаќач на таа е-пошта, а всушност некое друго лице ја испраќа таа е-пошта.

Компјутерското фалсификување во најголем процент се користи за фалсификување на парите и документите за патување (возачки дозволи, лични карти, пасоши). Статистиката вели дека со помош на компјутери во САД се фалсификувани околу 60% од сите банкноти и документи, и поради тоа во САД се посветува дополнително внимание на заштитата од фалсификување и се воведени посебни мерки за заштита како:

- Водени печати;
- Холограми;
- Микроштампи;

[19] Toren J. P., Intellectual Property and Computer Crimes (Intellectual Property usiness Crimes Series) , New York USA, 2003, стр. 6-41

Покрај ова, во Британија се јавува еден од попознатите случаи за фалсификување за карти за транспорт, каде Мејсон Марк од 2011 до 2013 година успеал да фалсификува повеќе од 100 прва класа билети за железнички транспорт, што по неговото откривање и судење била пресметана загуба на железниците од околу 17,000.00 фунти од избегнувањето на плаќање на тие билети.

Како една од најпопуларните и најшироко користените облици на компјутерски криминал, фалсификувањето во ова време каде информатичките технологии нагло напредуваат и се се фокусира на работа преку компјутери, добива големи бенефиции и можности за успех во вршењето на тие кривични дела.

### 2.5. Компјутерска шпионажа

Шпионажа е кривично дело кое се извршува со цел злоупотреба на државна, деловна или воена тајна во цели против економскиот и безбедносниот воспоставен систем на државата, но и дело со кое се потпомага извршување на други насилни и безбедносно опасни криминални поведенија, со кое се загрозува безбедноста на државните органи, виталните стопански капацитети, но се загрозува и личната сигурност и безбедност на граѓаните, а сето тоа е предизвикано со оддавање или соопштување на тајни податоци кои потоа се користат за извршување на конкретен криминален напад. Во сферата на воено – политичкиот комплекс, како и во други особено важни општествени сфери, како што се економската и службената, секоја држава настојува одредени податоци да се зачуваат во тајност во однос на други држави.[20]

Шпионажата е криминално дејствие насочено спрема документи и податоци кои имаат степен на државна или воена тајна. Шпионажата како компјутерско кривично дело е актуелна, но во иднина сè повеќе шпионажата ќе развива со нови појавни облици и форми на компјутерски шпионажи. Вештите хакери продираат во компјутерските системи на безбедносните служби, доаѓаат до доста значајни податоци, а тоа го користат сè повеќе и разузнавачките служби, некои во своите редови вработуваат и вешти хакери сè со цел

[20]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година,стр. 264

на софистициран начин да ги обезбедат податоците кои им се потребни за интересни безбедносни органи, развој на воена технологија, поставеност на безбедносен систем и сл. Покрај безбедносната шпионажа, постои и економска шпионажа која е насочена кон обезбедување на компјутерски податоци кои се однесуваат на производсветн процес на успешна компанија, на водење на бизнис и сл. За вршење на шпионажа се користат широк спектар на најразлични методи и техники, тргнувајќи од традиоционалните до специфичните, високософистицирани компјутерски техники. Техничкиот пристап подразбира користење на прикриени комуникациски канали, тајно инсталирање на предаватели (трансмитер) на централните единици, периферискиапарати и комуникациски линии, тајно инсталирање на микрофони поради следење на вербалната комуникација на вработените, прислушкување (активна и пасивна инфилтрација) и електромагнетно прислушкување, а во поново време за упади во туѓи информациски системи поради користење на деловни тајни што се почесто го користат и хакерите. Сè повеќе се користи компјутерската шпионажа и се ангажираат вешти хакери – сторители бидејќи на тој начин се делува опасно, се обезбедуваат доста деловни, финансиски податоци, а сторителите кои криминално делуваат од друга држава, се надвор од дофатот на органите на законот. Сторителите остануваат безбедни внатре во националните граници, додека покренуваат над стотици агресивни акции спрема своите цели ширум светот. Поради тоа оправдано се верува дека во блиска иднина, а и веќе се случуваат, соработки со компјутерските хакери и Интернет шпионажата кои ќе бидат клучни за ефикасно постигнување на целта: стекнување на информациска доминантност над противникот.[21]

Основната карактеристика на ова дело е откривање на тајни, а основната форма се состои во соопштување, предавање или ставање на располагање на доверливи податоци со употреба на компјутери и информатичка технологија. Разузнавачките служби се ангажираат преку нивните членови за откривање на политички, воени, економски и службени тајни на други земји. Во Јапонија, сегашната филозофија е: „Зошто да потрошите

[21]Петровиќ С. *„Полицијска информатика“*, Криминалистичко – полицијска академија, Београд, 2007,стр.106 – 107.

10 милијарди на истражување, кога милион долари можат да поткупат инженер за конкуренција и многу брзо да го добијат истиот, ако не и подобар резултат.[22]

Базите на податоци во владата, војската, истражувањето и многу други институции се вистинска ризница на класифицирани информации, кои сега можат да бидат обелоденети на многу едноставен начин, со објавување на Интернет што го потврдува случајот Асанж и аферата Викиликс, како и случајот со американскиот офицер Сноуден кој ги предал воените тајни на Пентагон. Исто така, е-поштата е често мета на напади, бидејќи содржи комуникации меѓу државните службеници. Зад сцената на светската политика се одвива вистинска информатичка војна во која покрај вообичаените актери како Русија и земјите на НАТО, Кина сè повеќе учествува. Имено, информатичките системи станаа приоритет во работата на разузнавачките служби пред се поради технолошките, воените и економско-политичките податоци. Познат факт е дека владите на многу земји, свесни за нивната зависност од напредните технологии, ги насочуваат своите разузнавачки служби кон добивање на напредни технологии со сите потребни средства. Хакерите сè повеќе се користат за упад во туѓи информатички системи за кражба на деловни тајни. Американската армија смета дека соработката со компјутерски хакери и надгледувањето на Интернет ќе бидат од суштинско значење за постигнување супериорност на информациите над непријателот.

Базите на податоци на државите, како воено така и технолошки претставуваат сеф со информации кои доколку се откријат можат да направат голема штета на одредена држава. Во модерното време објавувањето на тие податоци е направено да биде многу полесно со појавувањето на интернетот, што се докажува со случајот на Асанж, аферата Викиликс и случајот Сноуден со кој се откриени многу тајни на Пентагон. Во овој момент може да се каже дека се случува нова компјутерска војна[23] во која се вклучени, не само Русија и Обединетите нации, туку и Кина со се повеќе ресурси бидејќи е јасно дека најлесен начин за добивање на какви било податоци (воени, технолошки). Исто така е

[22]Janusz Piekalkiewicz, World history of espionage: : Agents, systems, operations, National Intelligence Book Center, Washington USA 1998.god. стр 341.
[23]http://lat.rtrs.tv/vijesti/vijest.php?id=135279

важно да се спомене дека и владите на многу држави во овој момент имаат насочено големи ресурси во напредокот на технологиите, свесни за нивната голема улога во модерниот свет. Војската на Соединетите Држави е уверена дека преку соработка со хакери и надгледување на интернетот тие ќе бидат супериорни во добивање на информации пред нивните противници.[24]

### 2.6. Компјутерска саботажа

Саботажата е инкриминација блиска до диверзијата, се разликува по тоа што не се работи за отворен непријателски мотивиран напад врз економските потенцијали, туку за прикриено, подмолно делување ,,од внатре". Суштината на делото е загрозување на економските основи со посебен начин на прикриено, подмолно делување на сторителот во самиот процес на работата. Покрај предизвикувањето на штетните последици, сторителот повредува и еден посебен однос на доверба, покрај објективните моменти на предизвикувањето значителна штета, подеднакво се важни тие субјкетивни моменти што се однесуваат на побудите на сторителот и начинот на извршување на делото. Прикриен, подмолен или друг сличен начин е постапување при кое сторителот или во целост не ги извршува или ги извршува своите обврски погрешно или во значително помал обем, од што треба и може, а притоа создава надворешен впечаток на уредно, вредно и совесно исполнување на своите задачи. Притоа сторителот настојува на нештата да им даде изглед на случај или резултат на туѓа грешка, така што е тешко да се открие вистинската причина на оштетувањето. Последицата е предизвикување на значителна штета за 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.[25]

Саботажата како криминално дело има повеќе појавни облици и форми, а со компјутеризацијата на скоро сите државни органи, значајни економски субјекти и на сите витални објекти во Државата се менуваат и начините и користените средства за

[24] http://edition.cnn.com/2015/08/31/politics/china-sanctions-cybersecurity-president-obama/
[25] Камбовски В. *„Казнено право, посебен дел"*, Просветно дело АД Скопје, 2003, стр. 460 - 461

извршување на саботажа. Во компјутеризираниот свет постојат во основа два типа на саботажа и тоа:[26]

- Физичка саботажа под која се подразбираат оштетувања на опрема, како што е посипувањето на електронските елементи со кафе, густи сок или со уфрлување на спојалки или парчиња од алуминиумска фолија во апаратите заради предизвикување на краток спој, предизвикување на високи – екстремни температури за саботирање на апаратите за разладување, сечење на комуникациски кабли или некоректно поврзување, носење на силни магнети во близина на магнетни медии, исклучување на струјата во време на работа на компјутерските системи, промена на лабелите на магнетните полиња и сл.
- Логичката саботажа подразбира бришење, оштетување или модифицирање на компјутерски податоци, програми или делови на оперативниот систем. Тоа најчесто се прави со користење на стандардни услужни програми, сопствени програми или со користење на техники како што се логичка бомба или компјутерски вируси.

Сторителите на компјутерска саботажа ги користат информатичките знаења и потпомогнати од мотивите за извршување на делото, а тоа се најчесто воени, економски или политички мотиви вршат саботажа и предизвикуваат огромни последици во материјална смисла, но предизвикуваат и револт и гнев кај граѓаните. Но, саботажата како дело се користи и од економските и стопанските конкуренти посебно со запирање или оневзможување на производство еден поголем период поради дефект на компјутерскиот систем, бидејќи целокупното производство е автоматизирано. Саботажата може да биде и компјутерско кривично дело посебно ако се знаат можностите на добивање на компјутерски податоци и програми кои се неопходни за да се планира и изврши саботажата. Или тоа би значело да се приберат сознанија и податоци за поставеноста и функционирањето на компјутерскиот систем, компјутерските програми кои се во функција со цел да се планира каде да се нападне, дали тоа да биде физичка

[26]Петровиќ С. *„Полицијска информатика“*, Криминалистичко – полицијска академија, Београд, 2007. (2) стр. 104

или логичка саботажа. Она што е во тенденција да се развива, се логичките саботажи или со изработка на соодветни компјутерски вируси напад на компјутерски систем на софистициран начин за тоа да може да се смета дека е техничка грешка или ,,пад во системот“ сомневањата да не бидат насочени кон тоа дека станува збор за кривично дело.[27]

### 2.7. Компјутерска порнографија

Објект на заштита при ваквото незаконско однесување е достоинството на личноста и сексуалната слобода.[28] Токму поради фактот што порнографските материјали сериозно го нарушуваат моралот и покрај постојаната работа на надлежните органи и борбата против нив, несфатливо е зошто пазарот на порнографски материјали постојано се шири. Компјутерската технологија даде клучен придонес во тоа. Благодарение пред се на интернетот, порнографијата е достапна низ целиот свет во различни форми како што се слики, видеа, текст, анимација и слично.

Конвенцијата за високотехнолошки криминал го криминализира делото Детска порнографија на следниов начин:

1. производство на детска порнографија;
2. нудење или на друг начин овозможување на детска порнографија преку компјутерски систем;
3. дистрибуција или емитување на детска порнографија преку компјутерски систем;
4. набавување детска порнографија за себе или за друг преку компјутерски систем;
5. Поседување на детска порнографија на компјутерски систем или на медиум за пренос на компјутерски податоци.[29]

Со наглото проширување на користењето на интернетот доаѓа до појавување на компјутерската порнографија, чија употреба е толку проширена што веќе е секојдневна и

[27]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр. 263-264

[28]V.ĐurĆić, D.Jovašević – Krivično pravo: posebni deo, Niš, 2013, стр.79

[29]D.Prlja, M.Reljanović, Z.Ivanović – Krivična dela visokotehnološkog kriminala, Beograd, 2011. стр.8.

во поконзервативните земји како што се Саудиска Арабија, Кина и Турција. Трговијата со сексуално експлицитни материјали е една од најраспростанетите и најупотребуваните активности на интернет. Во Азија исто така се појавува и недозволен облик на порнографија, децката порнографија каде поединци во обид за поголема заработка сексуално искористуваат деца. Големата сума на пари, многу често е главната причина за децата да прифатат такво искористување, но исто така многу често и родителот се појавува како оној кој го продава телото на своето дете за парична заработка. На повеќе меѓународни конференции е констатирано дека тие сајтови и педофилски мрежи треба да се спречат и отстранат.[30]

### 2.8. Компјутерска пропаганда

Интернетот на голем број на држави им служи како масовен медиум за формирање на мислење на народот. Компјутерската пропаганда исто така може да се користи и за низа кривични дела како:

- Повикување на насилство;
- Предизвикување на верски, расни или национални немири и омраза;
- Ширење на лажни вести;

Голем број од корисниците кои преку компјутерски систем се поврзани со интернетот и различни интернет страници и социјални мрежи, можат по пат на пропаганда да вршат негативни активности со идеолошки, расни, верски, национални содржини, но и омраза преку интернет и овозможување на терористички групи да имаат свое влијание.

Исто така компјутерските технологии како и интернетот се многу важни за државните органи за контролата на јавното мислење и народот. Тоа е вообичаена активност на државните органи во многу светски земји, поради тоа што интернетот во овој момент е најголемото средство на реклама и ширење на сите политички кампањи.

[30] www.blic.rs/Vesti/Svet/438405/Na-Filipinima-zbog-decje-pornografije-uhapseno-11-ljudi - 01. 08. 2015. god

Социјалните мрежи претставуваат едно од најбитните места во вршењето на компјутерската пропаганда. Така министерството за информатичко општество на Украина за време на војната имало ангажирано голем број на вработени кои за задача имале да насочуваат про-Украински вестите на сите Украински сајтови и да коментираат во врска со новостите поврзани за војната во Украина на сите поголеми светски интернет сајтови, како и рушењето на интернет страните кои им припаѓале на руските сепаратисти.[31]

Коментарите напишани на вестите од најчитаните интернет страници во светот претставуваат многу евтин начин за ширење на политичка пропаганда и формирање на јавно мислење, не само во одредена држава туку и во целиот свет.[32]

Социјалните мрежи исто така се покажале како многу важно средство за ширење на политичка пропаганда за време на избори и така денес се сметаат како главни делови на секоја политичка кампања за прибирање на приврзаници од помладите категории на гласачи.[33]

### 2.9. Компјутерски тероризам

Тероризмот влегува во редот на најакутелните проблеми на современиот свет, тој е толку алармантен проблем, што според некои со право може да се стравува дека ќе и удри темен печат на целата наша епоха. По својата мултидимензионалност на мотиви и облици, овој феномен успешно ги избегнува многуте национални и меѓународни обиди за негова поимна определба, правна регулатива и воспоставување на инструментариум за ефикасно сузбивање.[34]

---

[31] http://www.bbc.co.uk/monitoring/ukraines-new-online-army-in-media-war-with-russia
[32] http://www.usatoday.com/story/news/world/2013/08/14/israel-students-social-media/2651715/
[33] http://www.pbs.org/newshour/bb/media-july-dec12-download_11-16/
[34] Петровиќ С. *„Полицијска информатика“*, Криминалистичко – полицијска академија, Београд, 2007. (2) стр. 106 – 107

Разновидноста на делата што може да се подведат под поимот тероризам, го прават овој безбедносен проблем тежок за дефинирање, особено правно дефинирање. Се чини дека после нападите на кулите во САД во септември 2001 година, светот сè повеќе ја сфаќа опасноста од тероризмот и прави бројни меѓународни обиди, како за негово правно дефинирање, со меѓународните правни акти, така и за систематизација на дејствија кои се сметаат за дела на планирање, подготвување, финансирање, реализација или прикривање на терористички акт. Несомнено е дека сè уште постојат структури во светот кои тероризмот го третираат како борба за национални и човекови права, за слобода на одредени територии, но насилството не може да се оправда, особено насилството над цивилното население. Постои една изрека ,,тој што напаѓа знае и да се брани, а невиниот човек не знае ниту да напаѓа, ниту да се брани, тој е затечен од насилството на некој друг“. Пример терористички акт во Бугарија, нападот на терорист самоубиец врз туристи од Израел, во Бургас, укажува на тоа дека терористите ги бираат и жртвите со цел да влеат страв, несигурност на определена категорија на граѓани, во случајот израелски туристи.[35]

Како дејствија на тероризам се сметаат општо опасни дејствија или акт на насилство. Општоопасно дејствие или актот на насилство треба да се такви да создаваат чувство на лична несигурност или страв кај граѓаните. По тоа тероризмот се разликува од другите дела на насилство. Дејствијата на извршување треба да предизвикаат чувство на лична несигурност или страв кај повеќе граѓани. Нема значење тоа што таквото чувство фактички е создадено само кај едно лице. Група на граѓани се повеќе граѓани собрани на едно место по било кој основ – улица, село, шеталиште и сл.[36]

Тероризмот и неговиот развој го следат и технолошките процеси. Криминалните или терористичките активности од крајот на седумдесетите години се осовременети, односно терористите сè повеќе ја користат информатичката технологија како во процесот на организирање – регрутирање на лица, планирање на терористички акти, бирање или

[35]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр. 266

[36]Камбовски В. „*Казнено право, посебен дел“*, Просветно дело АД Скопје, 2003, стр. 458.

планирање на терористички цели, собирање податоци и информации преку компјутерските мрежи за витални објекти, голема фреквенција на луѓе, слаби точки на виталните објекти со цел извршување на терористички напади. Но, компјутерските мрежи се користат и за прикажување на ,,нивните успеси и достигнувања“ или успешно реализирани терористички акции.[37]

Постојат три основни начини со кои терористите може да ги користат компјутерите за координирање, планирање и извршување на своите активности во остварување на своите цели:[38]

- Прв основ е користење на компјутерот како алат или средство на извршување. Терористичките групи го користат Интернетот за пропагирање на своите идеи преку веб-сајтовите и собираат финансиски средства, најчесто во вид на доброволни прилози, како и собирање и размена на разузнавачки податоци.
- Втор основ е тоа што терористите можат да ги користат компјутерите за планирање и организирање на своите работни програми. Тие во компјутерите ги држат своите финансиски книги, терористичките планови, потенцијалните цели, дневниците на набљудување, плановите за напад, листите на придружните конспиратори и сл.
- Трет основ е тоа дека сајбер – терористите може да ги користат компјутерите за неовластен пристап до владини и приватни информациски системи со цел предизвикување на доста сериозни, дури и катастрофални последици.

Сајбер тероризмот претставува еден вид адаптација на тероризмот чии цели се компјутерските ресурси, а преку тоа и предизвикување на страв за жртвите, може да бидат предизвикани дури и поголеми материјални последици, но и човечки жртви. Нападите на компјутерските системи на витални објекти или компјутерски системи кои служат за управување најчесто се терористички напади пришто главна цел се компјутерските системи, а со тоа се предизвикуваат последици карактеристични за

[37]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр. 267

[38]Петровиќ С. *„Полицијска информатика“*, Криминалистичко – полицијска академија, Београд, 2007. (2), стр. 110.

терористички акт. Нема класичен напад со оружје или експлозив, но со нападот на компјутерскиот систем се предизвикуваат исто такви, дури и поопасни дефекти. На пример напад над компјутерскиот систем на аеродром и ќе се направат огромни последици во управувањето на летовите, дури и до последици на неправилно давање на команди за слетување, а сето тоа предизвикува пад на авионот и големо материјални и човечки жртви. Сè повеќе терористичките напади во иднина ќе имаат карактер на сајбер тероризам, бидејќи терористите сè повеќе користат технички капацитети како цел на напад, но капацитети кои се од витално значење, но и кои ќе го свртат вниманието на јавноста и тоа е целта на терористите, покрај директните напади влевање страв од идни напади.[39]

Сајбер тероризмот подразбира незаконски напади и закани за напад против компјутери, мрежи и информациите складирани во нив. Тоа се прави со цел да се заплашат или на некој начин да се уценуваат владините претставници за да се направат одредени политички отстапки за одредена групација која со закани од терористички акти, сака да се стекне со одредени политички права во Државата.

За еден терористички акт да се квалификува како сајбер тероризам треба нападот да биде против компјутерски систем на витални економски и државни органи и институции или значајни објекти од сообраќајот или објекти кои обезбедуваат вода, струја, гас за нормален живот на граѓаните. Но, како сајбер тероризам се сметаат и дејствијата на обезбедување компјутерски податоци за витални објкети кои може да бидат цели на терористички напад, обезбедување на средства преку повик од терористичките групи – се мисли на финансиски средства кои се неопходни за целиот процес на било кој терористички акт, но се смета дека сајбер тероризмот спаѓа во поскапите терористички акти. Во поширока смисла на зборот сајбер тероризам значи напад и закана насочени спрема компјутери, компјутерски мрежи и информатичка опрема со цел застрашување и влијание на владејачките структури и јавноста во политичкиот и социјалниот живот. Нападите се насочени спрема персонални компјутери и

[39]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр. 267-268

компјутерски системи, а најчест начин на криминален напад е преку програмирање и пуштање на опасни компјутерски вируси. Сепак, за сајбер тероризмот да се оквалификува како напад, треба да предизвика насилство против население и вредности, или барем да предизвика доволно штета за да предизвика страв и ужас кај населението. Нападот на небитни цели или цели со кои не може да се предизвика страв, нетреливост, но и обрнување на внимание на структурите на власта, не би можел да се третира како сајбер тероризам. На пример далечински упад во компјутерска мрежа на воздухопловен или друмски сообраќај, кој предизвикува губење на човечки животи, сериозна материјална штета и предизвикува страв, секако се дефинира, односно квалификува како информатички тероризам, додека влегувањето во некој помалку значаен компјутерски систем со што се оневозможува негово функционирање и комуникација со други системи не може да се смета за терористички напад, туку само компјутерски кривично дело, тоа се најчесто неовластени упади во туѓ компјутерски систем и предизвикување на штета во неговото функционирање или се третира како техничка грешка или пад на системот.[40]

Македонскиот законодавец предвидел во повеќе кривични дела да бидат предвидени криминални дејствија кои може да се опфатат со поимот на сајбер тероризам или класични терористички дејствија кои доколку се извршат со користење на информатичка технологија или против компјутерските системи и мрежи ќе бидат квалификувани како сајбер тероризам и постапката на обезбедување на докази се разликува од класичниот начин на обезбедување на докази, бидејќи покрај доказите и трагите од последицата (траги од крв, материјални траги и сл.) треба да се обезбедат и електронските траги, а тоа подрзбира расветлување на користење на одредена компјутерска техника, код или лозинка на логирање, или од каде е нападнат одреден компјутерски систем и кои компјутерски техники се користени.[41]

[40]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр. 269

[41]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр. 272

## 2.10. Хакирање

За хакирање во основа се смета нарушувањето на системот за заштита и навлегување во информатички системи без овластување. Изразот хакирање или на англиски hacking потекнува од англискиот јазик што во превод значи човек против компјутер.[42]

Извршувањето на ова кривично дело може да се направи на неколку начини. За успешно влегување во компјутерските системи и извршување на кривичните дела хакерите се служат со најразлични техники за информациите кои се потребни за извршување на тоа дело, но исто така користат и посебни програми кои се создадени со цел да се олесни извршувањето на тоа дело и да се заобиколат вообичаените заштити на компјутерските системи.

Како основни карактеристики на хакирањето се сметаат:

- Неовласениот пристап до компјутерските системи;
- Рушењето на системот за заштита и насилното влегување во компјутерсиот систем;
- Хакирањето секогаш се извршува преку влегување во компјутерските системи;
- За успешно извршување е потребно компјутерско големо знаење;
- Местото од каде се извршува нападот и местото каде е извршен нападот се секогаш оддалечени;
- Преку хакирање можат да се извршат и други дела како шпиунажа, измама, проневера, саботажа, дистринбуција на вируси и други;
- Хакерите можат да работат самостојно или во поголеми групи;[43]

Како последици на хакерските напади се појавуваат:

- Нарушување на заштитните системи;
- Успорување на работата или целосно прекинување на работа на системите;

[42] http://en.wikipedia.org/wiki/Hacker_%28computer_security%29
[43] Drakulić M., Osnovi kompjuterskog prava, Beograd, 1996. god ;стр. 449.

- Штета;
- Оштетување на податоците или нивна измена;
- Крадење;
- Распростанување на вируси;[44]

Хакирањето претставува многу сериозен проблем поради сериозните последици кои може да ги предизвика. Темната бројка кај овој вид на криминал е огромна од причина што жртвите најчесто не се свесни дека се има извршено хакирање врз нивните уреди и тоа не го пријавуваат. Поради тоа стравот од хакерски напади е многу висок, но во последно време почнуваат да се појавуваат нови фирми чии цели се заштитата на податоците и навремено пронаоѓање и спречување на хакирањето.

### 2.11. Пиратерија на софтвери

Софтверската пиратерија како кривично дело ја обележува користењето или мултиплицирањето на некој софтвер кој е стекнат на незаконски начин. Како две основни форми на овој криминал се сметаат користењето на нелегалните копии и доставувањето на ваквите копии. Така со зголемувањето на бројот на корисници на компјутери, се зголемила и потребата од заштита од создавање на пиратски софтвери.

Првпат пиратеријата како поим се појавува во почетокот на 1980-тите години и се претставува како дејство кое го прават поединец или група луѓе со препродажба на софтвери кои не се нивни. Подоцна пиратеријата како термин почнува да се користи и за крадење на софтверите, а не само нивна препродажба. Вредноста на софтверот може да биде многу голема, и преку пиратерија на сопствениците на софтверот да им биде нанесена голема штета како на угледот, така и на финансискиот профит кој требало да го стекнат од продажбата на тој софтвер доколку бил продаден на легален начин.

[44] Petrović R. S., Kompjuterski kriminal; Ministarstvo unutrašnjih poslova Republike Srbije : Uredništvo ĉasopisa"Bezbednost" i lista "Policajac",Beograd 2000.godina, стр.180.

Пиратеријата и мотивите за нејзино користење и производство се разликуваат од профит па се до спротивставување на законот, па така со проширувањето на пиратеријата профитот на компаниите кои го произведуваат тој софтвер се намалува и тие не можат да вложуваат во негова надградба и подобрување. Така за пример можеме да ја земеме цената на софтверските пакети, кој во просек се по околу 50 евра, и доколку 100 корисници, барем еднаш месечно преземаат по еден ваков пиратски софтвер загубите кои компанијата ги претрпува би биле огромни.

Големата распространетост на пиратеријата во светски рамки можеме да ја видиме и преку процентот на неговото користење во светски рамки каде 42% од софтверите кои се употребуваат се пиратски, а во Европската унија таа бројка е намалена на 33%.[45] Тоа се огромни загуби кои софтверските компании ги чинат многу.

Интернетот, и начините кои тој ги нуди за превземање на ваков пиратски софтвер ја прават неговата употреба да изгледа како нешто нормално и легално, со што софтверските компании се принудени да почнат со бесплатна понуда на основните софтверски пакети, па потоа да наплаќаат за нивните додатоци и надградби.

Microsoft како компанија која е една од најстарите и најголемите информатички компании во светски рамки почнала да се служи со тој начин, со цел намалување на големите загуби и се докажало дека по ова дејство многу од корисниците почнале да ги купуваат надградбите и дополнителните алатки. Но, и во овој случај заработувачката која фирмата ја има сега, за разлика од предходно е намалена од 70% на помалку од 15% од вкупните нејзини приходи.

Не разбирањето или несакањето да се разбере дека производството на овие софтвери одзема големо време и ресурси и пиратеријата исто така ја понижува целата работа која ја направиле самите програмери за да ни го претстават конкретниот софтвер ја прави пиратеријата толку голема индустрија во светски рамки. Загубите кои се

[45] http://www.politika.rs/rubrike/Ekonomija/Piraterija-odnosi-milijarde-dolara.lt.html

направени на Американската економија преку овој вид на криминал чинат околу 200 милијарди долари, што претставува огромна бројка.[46]

### 2.12. Создавање и дистрибуција на вируси

Создавањето и дистрибуцијата на вируси како форма е застапена во сите поделби на компјутерскиот криминал. Како нејзина карактеристика се вирусите кои се многу мали програми, со големина од неколку килобајти, и нивна цел е загрозување и правење штета врз компјутерскиот систем.

Во мрежите на компјутерски системи доколку еден компјутер е заразен, многу лесно може да се пренеси вирусот на другите компјутери и да направи измени или штета на податоците во тие компјутери. Така, вирусот се дефинира како програма која извршува дејства кои се недозволени во компјутерскиот систем, и без знаење и дозвола од него.[47]

За една програма да биде сметана за компјутерски вируси, таа треба да ги има следните карактеристики:

- Да се активира сама и да го внесува својот код во кодот на извршување на друга програма;
- Да се размножува самата и да ги заменува другите програми со програми кои се создадени од вирусот со цел штета или кражба на информации и да наштетат и на персонални компјутери, а и на серверски системи;
- Вирусот мора да има одреден носител кој ќе му дава можност дополнително да се размножува доколку стапи во контакт со друг систем;[48]

[46] http://www.poslovni.hr/hrvatska/privreda-sad-a-godisnje-gubi-vise-od-200-mlrd-dolara-zbogpiratstva-52710

[47] Petrović R. S., Kompjuterski kriminal; Ministarstvo unutrašnjih poslova Republike Srbije : Uredništvo ĉasopisa"Bezbednost" I lista "Policajac",Beograd 2000.godina, стр. 44.

[48] Prlja D., Reljanović M., Ivanović Z., Krivična dela visokotehnološkog kriminala, Beograd, 2011год.,стр. 157.

Како облици на ова дело се земаат, создавањето на вирусот, кое без исклучок е секогаш свесно, и дистрибуцијата на вирусот која може да се направи и несвесно без намера за да се наштети на некој компјустерски систем.

Штетите кои компјутерските вируси можат да му ги нанесат на компјутерскиот систем можат да бидат најразлични, но најчесто се среќаваме со:

- Промена на големина на програмата;
- Успорување на системот и на самите програми во системот;
- Промена на начинот на извршување на програмата;
- Онеспособување на системот и негово оневозможување за нормално функционирање;
- Измени во датотеките на програмите;
- Бришење на податоци од системот;
- Намалување на просторот кој е слободен во компјутерскиот систем;[49]

Вирусите првпат се појавуваат во средината на 1980-тите години на Универзитетите во САД, каде се создаваат. Но, нивното најголемо проширување и масовно производство се случува со наглото зголемување на знаењето за работа со компјутери и развивањето на компјутерските науки. Во овој момент за создавање на еден вирус, не е потребно никакво посебно знаење, туку всушност едно лице со просечно компјутерско знаење може да создаде вирус.

Се верува дека компјутерските системи дневно барем еднаш се цел на напад на некој компјутерски вируси, и баш затоа се создадени посебни програми за заштита на компјутерските системи (antivirus), кои имаат за цел да ги пронајдат вирусите и да ги избришат што би ги направило овие напади незабележителни.

Една од овие компании кои произведуваат програми за заштита на компјутерските системи, во своите податоци ги спомнува најпознатите и најраспространети вируси до сега:

[49] Petrović R. S., Kompjuterski kriminal; Ministarstvo unutrašnjih poslova Republike Srbije : Uredništvo ĉasopisa"Bezbednost" i lista "Policajac",Beograd 2000godina, стр. 185.

- MYDOM, вирус кој е еден вид на црв и се пренесува преку е-поштата. Во 2004 година овој вирус направил штета од 38 милијарди долари, преку заразување на околку 2 милиони компјутери;
- Sobig.F е вирус тројанец кој влегува во компјутерскиот систем незабележано и го напаѓа од внатре. Штетата која овој вирус ја има предизвикано е околку 37 милијарди долари и повеќе од 2 милиони компјутери;
- I LOVE YOU е сличен вирус на MYDOM, кој се шири преку е-пошта и има вклучено порака во меилот кој го испраќа. Штетата која во 2000 година овој вирус ја има предизвикано е околку 15 милијарди долари и околу половина милион компјутери;
- CORE RED е вирус црв кој е наменет за компјутерси системи кои го користат Windows 2000, кој поради големите проблеми со овој оперативен систем е наменет за нив и штетата која овој вирус ја има предизвикано од појавата на Windows 2000, па до сега се смета дека е околку 1 милион компјутери и 2.6 милијарди долари.
- SLAMMER или SAFIR е посебен тип на вирус кој за цел има успорување на работата на компјутерските системи, и штетата која тој ја има предизвикано се смета дека е околу 200 илјади компјутери и 1.2 милијарди долари.

Како најдобрата заштита против компјутерските вируси се препорачува едукација за превенција на сите корисници и добри заштитни програми во компјутерскиот систем.

Неколку други начини кои доколку би се презеле би го намалиле ризикот компјутерските вируси се:

- Блокирање и непосетување на страни каде најчесто се наоѓаат вирусите;
- Бришење, блокирање и неотворање на е-пошта која е од непознат извор;
- Надградување и одржување на програмите за заштита;
- Редовна проверка и заштита на податоците во компјутерскиот систем;

- Да не се отвораат или превземаат датотеки или програми од непознати извори од интернет;[50]

### 2.13. Нарушување на приватноста преку информатичко-комуникациска технологија

Брзиот технолошки напредок кој се случува во целиот свет, создава потреба на државните органи да се обезбеди поголема сигурност, а и контрола на тоа што луѓето прават во светот. Времето кога информациите кои се собирале за луѓето биле преку следење, набљудување и разговори со нив полека одминува, а се заменува со следење на интернет, прислушкување на мобилните разговори, набљудување на твојата активност на интернет и твоите пребарувања.

Во поновото време исто така, се отвора можност и за чување и собирање на многу поголем број на податоци во споредба со минатото. Тие податоци се прикачуваат на електронски бази кој компаниите или државите ги користат и многу лесно можат да ги преработат и подоцна да ги најдат доколку им треба некој таков податок. Така, најразвиените земји имаат сопствени системи кои овозможуваат следење, прибирање податоци, складирање на тие податоци и многу лесно пронаоѓање доколку постои некоја потреба за тоа.

Всушност во САД, е потврдено дека 64-тата федерална агенција на САД има сајтови кои прибирале неовластено податоци за лица, кои се вршеле за контрола следење и набљудување на тие лица што е големо нарушување на приватноста. Исто така службите за безбедност, на скоро сите држави секојдневно ја нарушуваат приватноста на граѓаните. Најдобар пример за тоа е Националната агенција за безбедност на САД (НСА), која со специјален софтвер ги прелистува и ги пребарува сите емаилови кои се пратени или примени од и во територијата на САД, со посебни клучни зборови како што се оружје, бомба и слично, за да се најдат и да се отстранат потецијални опасни лица по безбедноста

[50] Ivanović Z., Prlja D., Reljanović M., Krivična dela visokotehnološkog kriminala, Beograd, 2011год.,стр. 168. i 169.

на САД и лицата кои живеат во САД, по што тие податоци се складираат и чуваат за понатамошни потреби.[51]

Така напредокот на информатичката технологија дава можност за дополнително рушење на приватноста на луѓето и на сето тоа кога ќе се додадат социјалните мрежи, тоа нешто е премногу едноставно и лесно за да не биде искористено. Социјалните мрежи се како рудник на податоци за секој кој има потреба од нив. Многу луѓе несвесно оставаат секакви податоци на социјалните мрежи и со тоа дозволуваат многу лесно искористување на нивните податоци. Внесувањето на податоците како име, презиме, датум на раѓање, место на раѓање, фотографии, телефонски броеви, е-маил, твои ставови кои ги објавуваш на тие социјални мрежи, на луѓето кои тоа сакаат да го искористат за противправни дела им ја прави работата многу лесна.

Најголемите интернет компании во светот (Google, Yahoo, Facebook) имаат огромна бројка на податоци во нивните бази на податоци исто како и развиените држави, преку кои следењето и набљудувањето на луѓето е олеснето и зголемено драстично.

Исто така базите на податоци можат да се користат за цели како продажба или реклама, исто како и за некои кривични истраги. Многу често продавањето на овие податоци може често да се забележи, на пример Google своите податоци за луѓето им ги продава на други компании за тие подоцна да можат своите продукти и реклами да им ги понудат баш на оние луѓе на кои им треба, и така да го зголемат своето финансиско заработување.

### 3. Начин на извршување на компјутерски криминал

Како начини преку кои компјутерите се користат за извршување на кривични дела можеме да ги одделиме:

- Компјутерите како предмет врз кој се извршува кривичното дело;
- Компјутерите како средство за извршување на кривичното дело;
- Компјутерите како средство за планирање на кривичното дело;

[51] http://www.theguardian.com/commentisfree/2013/aug/11/nsa-internet-surveillance-email

- Компјутерите како средство за раководење или прикривање на компјутерскиот криминал;[52]

Во првиот случај, кога компјутерите се предмет врз кој се извршува делото, над нив може да се извршат најразлични кражби на датотеки, податоци или програми, но и компјутерски компоненти и вршење на компјутерски саботажи.

Кога се користат како средство за извршување на компјутерскиот криминал, тие служат за крадење на лични податоци и начините кои се користат за извршување на тоа кривично дело се напредни и детално испланирани. Како еден пример на користење компјутери за извршување на кривично дело кражба на податоци можеме да ја одделиме сугестивната комуникација и манипулацијата која има за цел да ја натера потенцијалната жртва да остави лични податоци, и да се олесни начинот на добивање на тие податоци на извршителот на ова дело кој ако не би ги добил на овој начин би требало да изврши друго кривично дело (хакирање).[53] Тие украдени податоци можат да се користат за најразлична злоупотреба од името и презимето на жртвата, па се до матичниот број или пасошот, личната карта и кредитните картички.

Како средство за планирање, раководење или прикривање на компјутерскиот криминал, компјутерите најчесто се користат од страна на организирани криминални групи или терористички организации. Тие можат да служат за перење на пари, книговодство и најразлични измами и банкарски прикривања.

Исто така компјутеритерскиот криминал се користи и за измами, уцени и проневери, кои поради големата раздалеченост меѓу извршителот и жртвата и анонимноста која постои со работата преку компјутерски ситеми овозможува олеснето и поуспешно и извршување на тие дела.

Но, иако компјутерите им даваат толку голема слобода и можност на криминалците за извршување на овие кривични дела, од друга страна им даваат и голема помош на одговорните органи кои можат да ги користат за расчистување на тие дела и нивно

[52] D. Littlejohn Shinder, M.Cross,*Cybercrime*Burlington, MA, United States,2002, стр. 2.
[53] M.Budimlić, P.Puharić – *Kompjuterski kriminalitet – kriminološki,krivičnopravni, kriminalistički i sigurnosni aspekt* – Fakultet za kriminalistiku, kriminologiju i sigurnosne studije Sarajevo 2009 godina,стр. 10.

полесно спречување и докажување, како и идентификување на лицата кои ги извршуваат тие дела.

## ГЛАВА ТРЕТА

## ПРАВНА РЕГУЛАТИВА НА КОМПЈУТЕРСКИОТ КРИМИНАЛ

### 1. Меѓународна правна регулатива

Меѓународната заедница го спознава компјутерскиот криминалитет во осумдесетите години од минатиот век со почетокот на масовната компјутеризација на сите сфери од општетствениот живот во сите земји во светот. Чудото на 20 - тиот век, предизвикувачот на третата револуција на информатичката технологија и привилегија на генијалните умови, покрај непроценливите вредности за севкупен развој на општетството, претставува и потенцијална опасност за загрозување на севкупната безбедност во светот.Гениите на информатичката технологија претставуваат и потенцијална опасност за искористување на знаењата во насока на злоупотреба на нивните знаења, вештините со кои располагаат во компјутерските програмирања, манипулациите во размена и пресретнување на податоци со цел стекнување на противправна имотна корист, ширење на расна и верска дискриминација, но и ,,натпревар“ помеѓу вештите компјутерџии во улога на сторители на кривични дела кои тешко може да бидат откриени.Откривањето, расветлувањето и докажувањето на постоење компјутерски криминал претставува потешкотија, бидејќи националните законодавства немаат систематизирано кривични дела каде што компјутерот ја игра главната улога и дава квалитет на класичниот криминал на еден нов појавен облик на криминалитет каде и доказниот материјал е тешко обезбедлив, речиси секогаш е ,,невидлив“ за откривачите кои немаат знаења од областа на компјутерската технологија. Опасноста од можните масовни последици за загрозување на безбедноста во рамките на една држава е огромна, бидејќи станува збор за криминалитет кој има квалитет на транснационален криминал, меѓународната заедница во повеќе наврати се обидува најпрво да го дефинира овој проблем, за потоа да се изнаоѓаат начини, да се даваат препораки до националните законодавстава за инкриминирање на повеќе криминални појави кои имаат обележја на компјутерски

криминалитет. Уште во 1976 година во Конвенцијата на Советот на Европа во Стразбург за криминолошките аспекти на економскиот криминалитет се прави категоризација на компјутерскиот криминалитет како дел од економскиот криминалитет.[54]

Историски развој:

Поважни меѓународни акти донесени за цел регулирање на компјутерскиот криминалитет:

- Во 1998 година е изработена студија насловена како Правни аспекти на компјутерскиот криминал во информациско општество (engl.Legal Aspects of Computer-related Crime in the Information Society – COMCRIME study), од д-р Урлих Зибер, Универзитет во Вирзбург
- Акциониот план (engl. e - Europe Action Plan), донесен е истата година, за цел обезбедување на сигурност на мрежите и воспоставување соработка меѓу земјите членки.
- Директивата за електронско работење (engl. Directive on electronic commerce ), донесена во 2000 година.
- Во 2000 година се донесени и други документи: Одлука на Советот за спречување детска порнографија на интернет, Конвенција за меѓусебна помош во кривично – правната материја, Препорака за стратегијата во новиот Милениум за заштита и контрола на комјутерскиот криминал.

Советот на Европа на крајот на 1998 година отпочнува со подготовки за донесување на Конвенција за сајбер криминал, а во 2000-тата година пуштен е во процедура на јавна расправа. Конвенцијата денеска е еден од најзначајните документи кои покрај еврпоските земји ја прифатиле и Јапонија, САД, Канада и Јужна Африка. Конвенцијата која стапила на сила во јули 2004 година ја пратат бројни документи донеснеи во рамките на Советот[55]:

[54]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр. 42-43

[55]Ачкоски Југослав, Сигурност на компјутерски системи, компјутерски криминал и компјутерски тероризам, Скопје, 2012 година, стр.32-33

- Trust and Security in Cyberspace: The Legal and Policy Framework for Addressing Cybercrime (2002);
- Cyber-Rights & Cyber-Liberties, Advocacy Handbook for NGOs (2003);
- Racism Protocol to the Convention on Cybercrime (2003);
- The Protocol to the Cybercrime Treaty (2002);
- Additional Protocol to the Cybercrime Convention Regarding "Criminalization of Acts of a Racist or Xenophobic Nature Committed through Computer Networks ";
- Report Revised draft of the Protocol on Racist Speech (2002);
- Background Materials on the Racist Speech Protocol ;
- Draft Protocol on Racist and Zenophobic Speech: Prelimiary draft (2001);
- Second Protocol on Terrorism (2002).

**Конвенција за компјутерски криминал**

Конвенцијата за компјутерски криминал е донесена од Советот на Европа на 23 ноември 2001 година во Будимпешта со цел водење заедничка политика насочена кон заштита на општеството од компјутерски криминал, меѓу другото, преку усвојување на соодветно законодавство и негување на меѓународната соработка на земјите потписнички на овој документ, Потребата од донесување на оваа Конвенцијата е предизвикана од темелните промени што настануваат со дигитализацијата, конвергенцијата и континуираната глобализација на компјутерските мрежи, но и поради ризикот што компјутерските мрежи и електронските информации можат да бидат искористени за извршување на кривични дела и дека доказите поврзани со извршувањето на таквите дела можат да бидат сочувани и пренесени преку овие мрежи. Придонесот од Конвенцијата би требало да биде поефикасна борба против компјутерскиот криминал, но и заштита на легитимните интереси за користење и развој на информациските технологии. Исто така, се смета дека оваа Конвенција е неопходна за одвраќање од актите насочени противтајноста, 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 воведување овластувања потребни за ефикасна борба против таквите кривични дела, со овозможување на нивно откривање, спроведување истрага и подигнување обвинение на национално и меѓународно ниво и преку обезбедување аранжман за брза и сигурна меѓународна соработка.[56]

Првото поглавје претставува збир на дефиниции и основни термини што се користат во Конвенцијата. Второто поглавје на Конвенцијата ги регулира материјалните и процесните одредби за кои потписниците на Конвенцијата се обврзуваат да ги вметнат во своето законодавство. Материјалниот дел е поделен на:

1. Дела против доверливоста, интегритетот и достапноста на компјутерските податоци и системи: нелегален пристап; незаконско следење; крадење на податоци; крадење на системи; злоупотреба на уредот.

2. Дела поврзани со компјутер: фалсификување поврзано со компјутер; компјутерска измама.

3. Дела поврзани со содржина: прекршоци поврзани со детска порнографија.

4. Дела поврзани со повреда на авторските права и сродните права.

5. Други форми на одговорност: обид, помагање и поддршка; одговорност на правно лице; санкции и мерки.

Конвенцијата пропишува минимум стандарди за криминализација на овие кривични дела, а со неа создадена е и основа за соработка меѓу надлежните органи на државите потписнички.

Третиот дел од Конвенцијата е посветен на меѓународната соработка, каде одредбите ги регулираат начините за надминување на пречките во спроведувањето на националното законодавство, кои по правило вклучуваат учество на повеќе земји, а често и поединци од повеќе земји. Повеќето одредби од Конвенцијата ја регулираат соработката на државите во врска со можната размена на информации за сторени

[56]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр. 51-52

кривични дела, како и екстрадиција на сторители. Во посебни случаи, може да се воспостави директна соработка помеѓу судските органи на двете земји, како и Интерпол,без никакво посредување од извршната власт.

**Дополнителен Протокол на Конвенцијата за спречување на компјутерскиот криминал кој се однесува на казнување на акти на расизам и ксенофобија извршени преку компјутерски систем**

Дополнителениот Протокол на Конвенцијата за спречување на компјутерскиот криминал кој се однесува на казнување на акти на расизам и ксенофобија извршени преку компјутерски систем е донесен во Стразбург на 28 јануари 2003 година, со цел истакнување и подобрување на слободите на граѓаните, без разлика на нивната националност, вера, припадност и сл. Се нагласува потребата за обезбедување полна и ефикасна примена на сите човекови права без било каква дискриминација или разлика како што тоа е загарантирано со европските и другите меѓународни документи, убедени дека делата на расизам и ксенофобична природа претставуваат кршење на човековите права и опасност на владеење на правото и демократската стабилност. Се смета дека националното и меѓународното право треба да обезбедат соодветни легални одговори на пропагандата на расистичката и ксенофобична природа извршени преку компјутерските системи, а земајќи ги во предвид техничките и комуникациски олеснувања за пренесување на информации ширум земјината топка, за краток временски период.Со наведениот протокол е направено дефинирање на поимот ,,расистички и ксенофобичен материјал“ кој претставува секаков пишуван материјал, секоја слика или секоја друга презентација на идеи или теории кои помагаат, промовираат или поттикнуваат омраза, дискриминација или насилство, против било кој поединец или група на поединци, базирани на раса, боја на кожа, наследно, национално или етничко потекло, како и верско потекло ако се користи како изговор за било кој од тие фактори. Мерки кои би требало да се преземат на национално ниво се: инкриминирање на поведенија кои се направени намерно или ненамерно и противправно по пат на дистрибуција и ширење на расистички

и ксенофобичен материјал во јавноста, по пат на компјутерски систем, потоа инкриминирање на намерни и противправни поведенија со заканување преку компјутерски систем спрема лица кои припаѓаат на група чија разлика во расата, бојата на кожата, наследството или националното или етничко потекло се изговор за таквото криминално дело спрема било кое од наведените лица, со било која припадност; инкриминирање на поведенија сторени намерно и противправно со елементи на навреда мотивирана со расизам или ксенофобија.[57]

## 2. Правна регулатива на компјутерскиот криминал во Република Северна Македонија

Правната регулатива на компјутерскиот криминал во Република Северна Македонија е опфатена во Кривичниот законик, и преку него се уредени и предвидени кривичните дела кои спаѓаат под компјутерски криминал.

### 1. Компјутерски кривични дела предвидени со Кривичен законик од 1996 година[58]

Со донесувањето на Кривичниот законик на Република Македонија во 1996 година предвидени се типични инкриминации како компјутерски кривични дела, но и во одредени класични инкриминации се воведени одредби за можноста од извршување со компјутер или ако е нападната компјутерска мрежа или систем.

Систематски ги прикажуваме инкриминациите со елементи на компјутерски криминал по Глави од Кривичниот законик, а тоа се:

- **Кривични дела против слободите и правата на човекот и граѓанинот**

1. Повреда на тајноста на писмата или други пратки Чл. 147;

[57]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр. 57

[58] Сл. весник на РМ бр. 37/96

2. Злоупотреба на лични податоци – чл. 149;
3. Неовластено прислушкување и тонско снимање Чл. 151;
4. Повреда на авторско и на други сродни права Чл. 157;

- **Кривични дела против половата слобода и половиот морал**

1. Прикажување на порнографски материјал на дете – Чл. 193.3

- **Кривични дела против имотот**

1. Навлегување во компјутерски систем Чл. 251.

Со измените и дополнувањата на Кривичниот законик од 1999 година нема значајни промени во однос на компјутерските кривични дела.[59]

**2. Компјутерски кривични дела предвидени со Кривичен законик од 2004 година[60]**

Измените и дополнувањата на Кривичен законик на РМ од 2004 година внесоа значајни промени со изменување на содржината и дополнување на инкриминациите и креирани се нови инкриминации и тоа во:

- **Глава XV - Кривични дела против слободите и правата на човекот и граѓанинот**

1. Загрозување на сигурноста – Чл. 144 ст. 4;
2. Повреда на тајноста на писмата или други пратки – Чл. 147;
3. Злоупотреба на лични податоци- Чл. 149;
4. Спречување на пристап кон јавен информатички систем – Чл. 149 – а;
5. Неовластено прислушкување и тонско снимање – Чл. 151;
6. Неовластено снимање – Чл. 152;
7. Повреда на авторско право и сродни права – Чл.157.

- **Глава XVIII – кривични дела против честа и угледот**

[59]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр 71-72
[60] Сл. весник на РМ бр. 19/04

1. Клевета – Чл. 172;
2. Навреда – Чл. 173;
3. Изнесување на лични и семејни прилики – Чл. 174;
4. Омаловажување со префрлување за кривично дело – Чл. 175;
5. Неказнување за кривичните дела од Чл. 172 – 175 и
6. Изрекување судска опомена или ослободување од казна за кривичните дела од Чл. 172 – 175.

- **Глава XIX - Кривични дела против половата слобода и половиот морал**

1. Прикажување на порнографски материјал на дете – Чл. 193

- **Глава XXIII - Кривични дела против имотот**

1. Оштетување и неовластено навлегување во компјутерски систем – Чл. 251;
2. Правење и внесување на компјутерски вируси – Чл. 251 – а;
3. Компјутерска измама – Чл. 251 – б.

- **Глава XXV - Кривични дела против јавните финансии, платниот промет и стопанството**

1. Неовластена употреба на туѓ пронајдок или софтвер – Чл. 286.

- **Глава XXXII - Кривични дела против правниот сообраќај**

1. Компјутерски фалсификат – Чл. 379 – а.

Со измените и дополнувањата на Кривичниот законик во 2004 година воведена е и одговорноста за правните лица кога кривичните дела се извршени од физички лица, но во име и за сметка на правното лице. Со измените и дополнувањата на Кривичниот законик

во 2008 година се воведени промени и нови дефинирања на поими и нови инкриминации од областа на компјутерскиот криминалитет.[61]

### 3. Компјутерскиот криминалитет со измените на Кривичниот законик од 2008 година[62]

Македонското материјално казнено законодавство ги имплементира препораките од Конвенцијата за компјутерски криминал така што најпрво ги дефинира значајните поими кои се користат при инкриминирање на нови кривични дела и при измените и дополонувањата на веќе постоечките кривични дела.

**Дефинирани се поимите : ,,жртва“ ; ,,детска порнографија“; ,,компјутерски систем“ и ,, компјутерски податоци“.[63]**

**Под жртва на кривично дело**се подразбира секое лице кое претрпело штета, вклучувајќи физичка и ментална повреда, емотивно страдање, материјална загуба или друга повреда или загрозување на неговите основни слободи и права како последица на сторено кривично дело.

**Под детска порнографија** се подразбира порнографски материјал кои визуелно прикажува очигледни полови дејствија со малолетник, или очигледни полови дејствија со лице кое изгледа како малолетник, или реални слики кои прикажуваат очигледни полови дејствија со малолетник.

**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.

---

[61]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр 72-73

[62] Службен весник на РМ бр. 07/2008.

[63] Чл. 122 ст. 21, 22 и 23, Службен весник на РМ бр. 07/2008

**Под компјутерски податоци** се подразбира презентирање на факти, информации или концепти во облик погоден за обработување преку компјутески систем, вклучувајќи и програма подобна за компјутерскиот систем да го стави во функција.

Направени се одредени измени и дополнувања во Глава XV - Кривични дела против слободите и правата на човекот и граѓанинот и тоа во Членот 157 ,,Повреда на авторско право и сродни права,, и воведени се три нови члена, нови инкриминации под наслов ,, Повреда на правото на дистрибутерот на технички посебно заштитен сателитски сигнал“ Чл. 157 – а; ,,Пиратерија на аудиовизуелно дело“ Чл. 157 – б и ,, Пиратерија на фонограм“ Чл. 157 – в.

Одредени интервенции се направени со измена и дополнувања на членот 193 (наместо терминот дете се става малолетник кој не наполнил 14 години) и воведен е нов член 193 – а со наслов ,,Производство и дистрибуција на детска порнографија преку компјутерски систем“ во Глава XIX - Кривични дела против половата слобода и половиот морал.

Измени и дополнувања има и во Глава XXXIII - Кривични дела против јавниот ред со воведување на нови инкриминации и тоа:

1. Терористичка организација Чл. 394 – а;
2. Тероризам – Чл. 394 – б и
3. Финансирање тероризам Чл. 394 – в.[64]

### 4. Компјутерскиот криминалитет со измените на Кривичниот законик од 2009 година[65]

Измените и дополнувањата на Кривичниот законик на Република Македонија од 2009 година донесуваат квалитативни промени во казненото законодавство, посебно со воведување на правни норми кои се однесуваат на попрецизна определност во одговорноста на правните лица, делот наконфискација на имот, направено е редефинирање на економските казнени дела и редефинирање на компјутерските

[64]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр 73-74

[65] Службен весник на РМ бр. 114/2009.

кривични дела и посебно дефинирање на значајните поими кои се користат во инкриминациите на кривичните дела од овие групации. Ова е доста битно во водењето на постапките за откривање, расветлување, докажување и превенција од компјутерскиот криминал, пред сé од причина што не е можно работење на криминални случаи и расветлување и докажување на криминал, ако во времето на извршувањето тие дејствија не биле предвидени како кривични дела.

Измените и дополнувањата на Кривичниот законик на Република Македонија од 2009 година, се во примена од март 2010 година и се во функција на редефинирање на економските казнени дела каде што спаѓаат и компјутерските кривични дела во согласност со Номенклатурата на Министерството за внатрешни работи на Република Македонија.

Направено е прецизирање на одредбите за одговорноста на правните лица, воведена е одговорност за правните лица кај повеќето инкриминации од областа на економскиот криминалитет, односно потесната групација на компјутерски криминалитет, а извршено е и дефинирање на некои поими кои се од значење за компјутерските инкриминации.

Дадени се следните дефинициии во членот 122 и тоа:

1. **Електронски пари** се пари кои врз основа на закон се во оптек во Република Македонија или во странска држава.
2. **Платежни картички** се секаков вид средства за плаќање издадени од банкарски или други финансиски институции кои содржат електронски податоци за лица и **електронски генерирани броеви** со кои се овозможува вршење на каков било вид финансиски трансакции.
3. Под **имот** се подразбира пари или други инструменти за плаќање, хартии од вредност, депозити, друга сопственост од секаков вид и тоа материјална или нематеријална, движна или недвижна, други права врз предметите, побарувања, како и јавни исправи и легални документи за сопственост и актива во пишан или во **електронски облик** или инструменти со кои се докажува правото на сопственост или интерес во таквиот имот.

Како битна квалитативна измена во Кривичниот законик секако е воведувањето на одредби за спроведување непосредна и проширена конфискација за сторителите кои се стекнале со противправна имотна корист со вршење на кривични дела.

Извршени се промени во одредени инкриминации, во повеќе групации на кривични дела, со што несомнено е зголемена листата на компјутерски кривични дела и тоа во:

- **Глава XVIII – Кривични дела против честа и угледот**
    - Навредата според Членот 173 ст. 2 се менува и гласи ,,Тој што друг јавно ќе го изложи на подбив по пат на компјутерски систем поради неговата припадност на група која се разликува според расата, бојата на кожата, националната припадност или етничко потекло, или ќе ја изложи на подбив групата на лица која се одликува со некоја од тие особености.
- **Глава XIX - Кривични дела против половата слобода и половиот морал**
    - Насловот на Членот 193 – а се менува во Производство и дистрибуција на детска порнографија, се менува и содржината на инкриминацијата.
    - - Се воведува нов Член 193 – б Намамување на обљуба или друго полово дејствие на малолетник кој не наполнил 14 години.
- **Глава XXIII - Кривични дела против имотот**
    - Во Членот 251 – Оштетување и неовластено навлегување во компјутерски систем се направени повеќе измени и дополнувања во смисла на опфаќање на повеќе криминални поведенија, повеќе начини на извршување и користење на посебни уреди за извршување на некое од криминалните поведенија опфатени со оваа инкриминација, а е воведена и одговорност за правните лица.
    - Во Членот 251 – а е воведен нов став за одговорност на правните лица.
    - Во Членот 251 – б се направени измени и е дополнет со став за предвидена казнена одговорност на правните лица.
- **Глава XXV Кривични дела против јавните финансии, платниот промет и стопанството**

- Во Членот 271, ставот 2 е сменет, а е додаден и нов став 3 со кој е предвидена одговорност за сторителите кои монтираат посебни уреди за снимање на банкарски податоци. - Воведен е нов Член 174 – б ,,Изработка и употреба на лажна платежна картичка“
- - Се менува Членот 286 со нов назив ,,Повреда на правото од пријавен или заштитен пронајдок и топографија на интегрални кола“ се менува и содржината на самата инкриминација.

- **Глава XXXIII Кривични дела против јавниот ред**
  - Направена е измена на Чл. 394 – б Тероризам во ставот 1 и 2 во квалитативна смисла со опфаќање на повеќе поведенија како криминални и казниви со елементи на тероризам.
  - Во Членот 394 – в се менува ставот 2 и се додаваат нови ставови каде меѓу другото е предвидена и одговорност на службените лица и одговорни лица во банка или во друга финансиска институција за непочитување на законските прописи со кои е санкционирано и се превенираат однесувања со елементи на финансирање на тероризам.

Воведена е нова инкриминација во Чл. 394 - г ,,Ширење расистички и ксенофобичен материјал по пат на компјутерски систем“.[66]

### 3. Правна регулатива на компјутерскиот криминал во други држави

Во Република Хрватска компјутерските кривични дела беа систематизирани во повеќе глави на Кривичниот закон и тоа[67]:

[66]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр 74-77

[67]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр. 62

- Во групацијата на кривични дела против имотот се предвидени кривичните дела: Повреда на тајноста, целокупноста и достапноста на компјутерските податоци, програми или системи; Компјутерски фалсификат; Компјутерска измама; Повреда на правото на авторот или уметнички изведувач; Недозволена употреба на авторско дело или уметничка изведба, Повреда на правата на производителот на аудиовизуелни снимки и правата во врска со радиодифузните емисии.
- Компјутерски казнени дела против половата слобода и половиот морал се: искористување деца или малолетни лица за порнографија и Запознавање на деца со порнографија.

Со измените и дополнувањата на Кривичниот закон од 2011 година дел од компјутерските кривични дела се систематизирани во посебна глава насловена како „Кривични дела против компјутерските системи, програми и податоци ” и се предвидени следните кривични дела: Неовластен пристап; Попречување во работата на компјутерските системи; Оштетување на компјутерски податоци; Неовластено пресретнување на компјутерскиподатоци; Компјутерско фалсификување; Компјутерска измама; Злоупотреба на уреди и тешки казнени дела против компјутерските системи, програми и податоци. Додека и во другите глави на кривичниот законик се предвидени повеќе компјутерски кривични дела и тоа во следните глави[68]:

- Кривични дела против човештвото и човечкото достоинство: Тероризам.

- Кривични дела против приватноста: Повреда на тајноста на писмата и други пратки; Неовластено тонско снимање и прислушкување; Неовластено снимање и Недозволена употреба на лични податоци.
- Кривични дела против честа и угледот: Навреда, Срамотење; Клевета.
- Кривични дела против полно злоупотребување и искористување на децата: Намамување на дете за задоволување на сексуални потреби; Искористување на

[68]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр. 62-63

деца за порнографија; Искористување на деца за детска порнографија; Прикажување на деца на порнографија.

- Кривични дела против бракот, семејството и децата: Повреда на приватноста на детето.
- Кривични дела против здравјето на луѓето: Фалсификување на лекови и медицински производи;
- Кривични дел против општата сигурност: Уништување или оштетување на јавни уреди;
- Кривични дела против економијата: Злоупотреба на повластени податоци; Злоупотреба на пазарот на капитал.
- Кривични дела против јавниот ред: Јавно поттикнување на насилство и омраза.

**Република Србија**

Во Република Србија има посебна глава во Кривичниот законик47 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 "со следните инкриминации[69]:

- Оштетување на компјутерските податоци и програми,
- Компјутерска саботажа,
- Правење и внесување компјутерски вируси,
- Компјутерска измама,
- Неовластено навлегување во компјутерскиот систем, во компјутерската мрежа и електронската обработка на податоците,

[69]Николоска Светлана, „Методика на истражување компјутерски криминалитет", Факултет за безбедност, Скопје, 2013 година, стр. 63

- Спречување и ограничување на пристапот до јавна компјутерска мрежа и
- Неовластено користење на компјутер или компјутерска мрежа.

Втора групација на компјутерски кривични дела се ,,Казнени дела против интелектуалната сопственост“ и тоа[70]:

- Неовластено користење на авторско дело или предмет од некое сродно право;
- Неовластено отстранување или менување на електронските информации кои се однесуваат на авторските и на другите сродни права.

Трета групација на компјутерски кривични дела се во рамките на кривичните дела против слободите и правата на човекот и граѓанинот, со следните инкриминации[71]:

- Повреда на тајноста на писмата и на други пратки,
- Неовластено прислушкување и снимање,
- Неовластено фотографирање и
- Неовластено прибирање лични податоци.

**Франција**

Францускиот – Code Penal има посебно поглавје со систематизирани дела кои претставуваат злоупотреба на личните права по пат на компјутерски програми или фајлови. Систематизирани се 15 законски одредби во кои е предвидена заштита од разни облици на повреда, но она што е забележливо во делот на санкционирањето се високите

[70]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр. 63-64
[71]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр. 63-64

казни и тоа од 300 000 евра или затвор во траење од 5 години.[72]Како криминални поведенија се издвоени следните:

- Неовластено презентирање,
- Автоматска обработка на податоци кои содржат имиња,
- Непреземање на потребните мерки на заштита кои имаат за цел зачувување на доверливоста на информациите и нивно пренесување на трети неповикани лица,
- Неовластено прибирање податоци,
- Автоматска обработка на податоци кои содржат имиња, а кои се наменети за медицински испитувања,
- Неовластено снимање или чување во компјутерска меморија податоци кои директно или индиректно овозможуваат откривање религиозна, расна, политичка припадност или сексуална ориентираност на лицето и
- Прибирање, класифицирање, пренесување или на друг начин откривање информации кои доведуваат до повреда на угледот и честа на засегнатото лице, неговиот приватен живот или соопштување на информации на трето неповикано лице.[73]

**Германија**

Германското казнено право познава шест казнени дела кои може да се класифицираат како компјутерски деликти, а тоа се:

- Во главата на кривични дела против половата слобода - Дистрибуција на порнографски материјал,

[72]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр. 64
[73]Тупанчевски Н. и Кипријановска Д. оп. цит , стр. 533.

- Во главата на кривични дела против измама и злоупотреба на довербата се: Кражба на податоци и Компјутерска измама,
- Во главата на кривични дела со елементи на Фалсификување на податоците е предвидено делото – Фалсификување на податоци со доказна сила и
- Во главата на кривични дела против имотот се: Промена на податоците и Компјутерска саботажа.[74]

**САД**

САД – Закон за компјутерски измами и злоупотреби (CFAA) по 11 септември и Закон за воедначување и засилување на соодветните инструменти за спречување и отстранување на тероризмот во 2001 година PATRIOT ACT 2001. Со измените на Законот за компјутерски измами и злоупотреби опфатени се компјутерските измами и други слични активности кои се вршат врз заштитен компјутер, или, пак оние кои настанале со нивната употреба. Кривичен законик на САД во 18 – то Поглавје (член 2510) прецизно ги дефинира делата кои се однесуваат на недозволено користење, дури и на вообичаена електронска опрема, во однос на лицата со оштетан слух, се разбира од страна на оние лица со нормален слух кои сакаат да прислушуваат туѓи разговори без притоа да постои законско оправдување за тоа, а не само во поглед на користењето на телефонските апарати.[75]

Во САД долги години наназад е санкционирано и делото ,,Користење на меѓудржавните уреди за трансфер на информации кои се однесуваат на малолетниците“ која доследно е поврзана со Поглавјето 110, каде што е регулирана сексуалната и другите облици на експлоатација врз децата. Исто така е предвидено во рамките на Глава 42, насловена како ,,Јавно здравје и грижа“ пропишана е обврска секоја Интернет провајдер

[74]Тупанчевски Н. и Кипријановска Д. оп. цит , стр. 533.
[75]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр. 65

мрежа да ги пријави забележаните забранети користења, односно користењата извршени со таква цел пласман на детска порнографија.[76]

Како позначајни би ги издвоиле следните инкриминации за компјутерски криминал во САД, а тоа се[77]:

- Компјутерска шпионажа;
- Неовластен пристап до информации од компјутери кои се користат од страна на една владина агенција;
- Штета или нарушување на компјутер кој се користи од страна на владината агенција;
- Измама со користење на компјутер;
- Измама од страна на лица со компјутерски лозинки или слични информации, под одредени околности;
- Закана, изнуда, уцена и други незаконски дела извршени со користење на компјутер;
- Трговија со украдени или фалсификувани пристапни помагала, кои можат да се користат за да се добијат пари, стоки или услуги;
- Намерни оштетувања на имотот, опремата, линиите и комуникациските системи;
- Следење и откривање на комуникациите од страна на телеграф, усно или по електронски пат;
- Прекршување на доверливоста на електронски и гласовни пораки;
- Намерно да се добие или модификува порака која се чува во компјутерска меморија, како и попречување на овластен пристап до таквите извештаи.

[76]Тупанчевски Н. и Кипријановска Д. оп. цит , стр. 534

[77]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр. 65-66

**Канада**

Во Канада казненото законодавство има класифицирано неколку кривични дела од областа на компјутерскиот криминал и тоа[78]:

- Неовластена употреба на компјутер ја санкционира кражбата на компјутерски услуги, ја штити приватноста, го инкриминира користењето на компјутерскиот систем со намера за извршување криминал, се однесува на лицата кои се занимаваат со промет, особено трговија со компјутерски лозинки.
- Штети нанесени врз компјутерските податоци, опфатени се повеќе криминални дејствија и тоа: уништување и измена на податоците, спречување, прекинување на пренос или попречување на законско користење на податоците и ограничување пристап до податоци од страна на овластените лица.

**Англија**

Во Англија се предвидени повеќе инкриминации кои се однесуваат на компјутерскиот криминалитет и тоа се[79]:

- Намерен незаконски пристап до компјутер или содржани во него компјутерски податоци или програми;
- Неовластен пристап до податоци за чување на компјутерски медиуми, во компјутерскиот систем или мрежа, или ако тоа резултира со уништување, блокирање, модификација или копирање на информации, нарушување на компјутер, компјутерскиот систем или мрежа;
- Откривање на лични податоци (вклучувајќи и користење на компјутерската технологија);

[78]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр. 66

[79]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр. 66-67

- Производство и дистрибуција на порнографски материјали, со користење на компјутерска технологија.

**Русија**

Руското законодавство предвидува кривична одговорност за компјутерскиот криминал во Глава 28 од Кривичниот законик која се состои од три статии и тоа[80]:

- Нелегален пристап до информации од компјутер (нелегален пристап до компјутерски заштитени информации, односно податоци за чување на медиуми), компјутерски систем или мрежа ако постои уништување, блокирање, модификација или копирање на информации, повреда на работата на компјутерот, компјутерскиот систем или компјутерските мрежи;
- Создавање, употреба и дистрибуција на компјутерски штетни програми (создавањето на компјутерските програми или измени на постојните програми, очигледно е водечко во неовластени уништувања, блокирања, модификации или копирање на информации, од компјутер, компјутерски систем или мрежа како и употреба или дистрибуцијата на таквите програми).
- Несоодветно користење на компјутер, компјутерски систем или мрежа (несоодветно користење на компјутер, компјутерски системи или мрежи од страна со пристап до компјутер, компјутерски систем или мрежа, што резултира со уништување, блокирање или модификација на законски заштитени компјутерски информации, ако овој чин предизвикува значителна штета.

Рускиот законодавец предвидел во Кривичниот законик можност за постоење елементи за извршување на криминал со помош на компјутер или да бидат нападнати самиот компјутер, компјутерскиот систем или мрежа. Такви одредби има во следните

[80]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр. 67

инкриминации: клевета – ширење лажниинформации преку компјутерски систем насочени против честа и угледот на некое лице; навреда – понижување на честа и достоинството на друго лице или оштетување на неговото реноме; нарушување на приватноста – нелегално прибирање, или дисеминација на информации за приватниот живот на поединци кои ги сочинуваат неговите или нејзините лични или семејни тајни, без негова согласност или ширење на оваа информација во јавна изјава, јавно покажува дела на нарушување на приватноста на друго лице или оштетување на неговото реноме, или на медиумите ако овие дела биле извршени за платен или други услуги а се предизвикува и повреда на правата и интересите на граѓаните; повреда на тајноста на писмата, телефонските разговори, поштенски, телеграфски и други комуникации; повреда на авторско право и сродни права – употреба на нелегални објекти на авторско право или сродните права, како и на именувањето авторство, ако овие акти предизвикаат голема штета; прекршување на правата на патент - незаконско користење на инвенција, нови модели или индустриски дизајн, откриени без согласност на авторот или барателот суштината на инвенција, нови модели или индустриски дизајн пред официјалното објавување на информации за нив, именувањето на авторство или присила во коавторство, ако овие акти предизвикаат голема штета; кражба - тајна проневера на друг имот; лага - кражба на друг имот или за купување на друг имот од страна на измама или злоупотреба на довербата; изнуда - барање за пренесување на друг имот или права на сопственост или други акти од материјална природа, под закана од насилство или уништување или оштетување на имот на други, како и под заканата од пролиферацијата на клевети кон неговите роднини или било која друга информација која може да предизвика значителни штети по човекот или на легитимните интереси на жртвата или неговите роднини; предизвикува штета на имот со измама или злоупотреба на довербата; намерно уништување или оштетување на имотот (доколку овие дела предизвикале значителна штета); уништување или оштетување на имотот, поради небрежност (во големи размери); нелегален бизнис (спроведување на бизнис, без регистрација или во прекршување на правилата за регистрација, како и застапување во органите на државата, за регистрација на правните субјекти на документи кои содржат лажни информации или

извршување на претприемачки активности без посебна дозвола (лиценца) во случаи кога таква дозвола (лиценца) е потребна, или во прекршување на условите за лиценцирање, ако овој чин предизвика голема штета на граѓаните, организациите, или државата, или вклучува наплатата на приходите во големи размери); очигледно лажно рекламирање (употребата во рекламирањето лажни информации во однос на стоки, работи или услуги, како и нивните производители (уметници, продавачите), постојат елементи за обврски на себичен интерес и предизвикува значителна штета; нелегално стекнување и откривањето на комерцијални или банкарска тајна (собирањето на информации за конституирање на банкарските тајни, комерцијални или одкражба на документи, поткуп или закани, како и други нелегални средства за откривање или злоупотреба на информации); измама на потрошувачите (мамење на тежини, пресметки, карактеристики за квалитетот на стоките (услуги) или други измама на потрошувачите од организации ангажирани во продажба на стоки или услуги за населението, како и граѓаните кои се регистрираат како индивидуални претприемачи во трговијата (услуги), ако овие дела биле извршени во значителни количини; на дистрибуција на нелегални порнографски материјали или предмети (нелегално производство за дистрибуција или рекламирање, дистрибуција, рекламирање порнографски материјали или предмети, како и илегалната трговија во печатени публикации, филмови и клипови, слики или други предмети со порнографска содржина; шпионажа (пренос, како и собирање, кражба или поседување на странска држава, организација или странски претставници на информации кои претставуваат државни тајни, како и доставување или подигање на инструкциите на други странски разузнавачки информации за употреба во штета на надворешната безбедност на Русија, доколку овие дела се извршени од страна на странски државјанин или лице без државјанство; јавни апели за екстремистички активности; поттикнување на национална, расна или верска омраза (акции насочени кон поттикнување на национална, расна или верска омраза, понижување на националното достоинство, како и за пропаганда на ексклузивност, супериорност или инфериорност на граѓаните врз основа на нивниот однос кон религијата, националноста или расата; откривање на државни тајни (на откривање на информации кои претставуваат државна тајна од страна на лицето на кое му е доверена

во вршење на службата; јавни повици за агресивна војна.Листата на инкриминации е навистина доста широка, но со тенденција да се проширува, а во Русија се воделе и неколку посложени криминални случаи со елементи на компјутерски криминал.[81]

**Република Бугарија**

Во Кривичниот законик на Република Бугарија се прифатени препораките од Конвенцијата за компјутерски криминал, а направена е измена и дополување со воведување на повеќе казнени поведенија во повеќе членови кои се систематизирани во неколку глави. На тој начин се санкционирани поведенија кои се однесуваат на противзаконско дознавање на содржина на порака испратена по електронски пат, со користење на специјални технички средства, а истото се однесува и за порака испратена по телефон или телеграф. Потоа, се предвидува казнена одговорност за секоелице кое без дозвола на лицето кое е администратор ќе користи компјутер, ќе добие, промени, избрише или уништи компјутерска програма или податоци во голема мера, а предвиден е и квалификаторен облик ако е причинето значително оштетување или ако настанале други потешки последици, потоа ако делото е сторено со специјална цел – добивање на имотна корист, а во овој член предвидена е и одговорност за сторителот кога делото ќе го изврши во рамките на својата службена должност.Инкриминирани се и кривични дела за изработка и внесување на компјутерски вируси, злоупотреба на уреди, незаконска употреба на компјутерските или системските лозинки со што се доведува до откривање на лични податоци или информации кои претставуваат државна тајна. Инкриминирано е и кривично дело со елементи на компјутерски фалсификат и компјутерски измами. Инкриминирани се дела поврзани со компјутерска детска порнографија и дела за заштита на авторските права. Имено, воведени се неколку нови членови и тоа 319 а кој се однесува на следните криминални поведенија: остварување на незаконски пристап, умножување компјутерски податоци и користење на компјутерски податоци кога

[81]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр.67-69

дејствието е направено без дозвола, а како сторители се физички лица, државјани на Република Бугарија и странски лица.[82]

Предвиден е и организиран облик на извршување кога делото е извршено од страна на две или повеќе лица, договорени однапред за да извршат таков вид на кривично дело. Во овој член е предвидена и казнена одговорност доколку податоците имаат степен на државна тајна. Со членот 319 б заштитени се компјутерските програми и компјутерските податоци во случаите кога сторителот или сторителите ќе добијат, менуваат, бришат или уништуваат компјутерски програми или податоци, наведените дејствија треба да бидат реализирани без дозвола на лицето кое го администрира или употребува компјутерот и случајот да не е безначаен. Во Членот 319 в е предвидена казнена одговорност за сторител кој криминалните дејствија од претходниот член 319 б кога делото е поврзано со податоци кои се даваат по сила на закон по електронски пат или на магнетен носител, а тоа се податоци од социјално осигурување, даночни извештаи, трговија со хартии од вредност и друго. Воведување на компјутерски вирус е инкриминирано кривично дело со членот 319 г каде законодавецот предвидува одговорност за сторителот кој ќе воведе компјутерски вирус во компјутер или во информациона мрежа, а со член 319 г е предвидена казнена одговорност за сторителите кои незаконски ќе користат компјутерски или системски лозинки, но потребно е да настане и конкретен штетен резултат. Законодавецот со посебно кривично дело врши заштита на електронските документи и електронските потписи со чл. 319 е, а одговорни се физички и правни лица. Ова се типични компјутерски кривични дела предвидени во бугарското материјално казнено законодавство, но и во други кривични дела се инкриминирани поведенија кога сторителот делото ќе го изврши со употреба на компјутер или ќе нападне туѓ компјутер иликомпјутерски систем. Направена е заштита на електронската пошта, заштита на авторските права, заштитата на сопственоста од електронска измена на податоци и слчно. Кривично – правната регулатива на кривичните дела со елементи на компјутерски криминал, анализирана низ казнените законодавства

[82]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр.69-70

на неколку претходно наведени држави, одговара на состојбите со компјутерскиот криминал во национални и светски рамки и секако треба да се напомене дека светот навистина го согледал проблемот и опасноста од компјутерскиот криминал, а со тоа се налага потребата од имплементирање на препораките од меѓународните документи за кодификација на нови кривични дела, дополнувања кај класичните кривични дела.Останува проблемот со практичната примена на законските прописи во успешно расветлување и докажување на случаи со елементи на транснационален компјутерски криминал.[83]

[83]Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 година, стр.70-71

## ГЛАВА ЧЕТВРТА

## ПРЕВЕНТИВНИ МЕРКИ

### 1. Начини на превенција

Сајбер криминалот заради спецификите, општествената опасност што ја предизвикува и високата стапка на раст, во се поголема мера станува многу озбилен општествен проблем и тоа не само во национални туку и во меѓународни размери. Врз основа на наведените причини потребна е соодветна акција заради успешно спротиставување на новото општествено зло. Постојат три типа на механизми, кои може да помогнат во одговор на предизвиците на сајбер криминалот: алатки за заштита, етика и закони. Овие механизми имаат превентивен и репресивен карактер, при што во нивната примена изразита предност мора да се даде на превентивните во однос на репресивните мерки.[84]

Тенденција за зголемување на овој облик на криминал покажуваат и некои статистички податоци. Врз основа на податоците претставени од експертите на компанијата Sophos, во текот на 2007 година биле откриени 6.000 заразени веб страници, од кои 83% припаѓале на компании. Бројот на имејл заканите има тенденција на опаѓање, но обратнопропорционално се зголемува бројот на имејли кои содржат линкови кои водат до малициозни интернет страни.[85]

Голем проблем во сузбивањето на сајбер криминалот претставува фактот дека цел на извршителите е се што се поврзува на интернет, односно освен персоналните сметачи, тука се вбројуваат и мобилни телефони, iPhone, iPod Touch, терминали и други уреди кои се конектираат на интернет постојано или повремено. Според одредени сознанија, постојат и обвинувања, дека одредени држави се појавуваат како нарачатели на сајбер криминалот.[86]

---

[84]Ачкоски Југослав, Сигурност на компјутерски системи, компјутерски криминал и компјутерски тероризам, Скопје, 2012 година, стр.44

[85]http://www.maturskiradovi.net/forum/Thread-kompjuterski-kriminal

[86]http://www.nezavisne.com/nauka-tehnologija/internet/Potrebni-ostriji-zakoni-za-sajberkriminal-69298.html

Врз основа на претходно изнесеното, може да се заклучи дека сајбер криминалот во иднина се повеќе ќе биде застапен, во однос на останатите видови на криминал.[87]

Земајќи го во предвид претходно наведеното, потребно би било превземање на следните мерки[88]:

- заради општествената оправданост и целисходност, како и заради следење на општествените трендови и приклучување кон западноевропските држави, потребно е забрзување на активностите за донесување и усвојување единствени основи за заштита на автоматизираните информациони системи;
- од аспект на заштитата, една од најважните активности на која би требало да се посвети посебно внимание е изградба и развој на етички норми и принципи во доменот на информатиката;
- ревизија на кривичниот закон и негово прилагодување на новите појавни облици на општествено опасно однесување предизвикано од информацискатa технологија;
- нова систематизација и трансформација на телата или органите кои ја пратат состојбата во оваа област, извршуваат анализи на појавите, ги истражуваат причините, извршителите и методите и предлагаат соодветни мерки и акции за спречување, откривање, разјаснување и докажување на овие видови на кривични дела.[89]

Превенцијата и високото ниво на свеста при користење на Интернет мрежата во деловна комуникација е најдобриот начин за борба против компјутерсиот криминалитет.[90] Овој сектор регистрираше зголемен број на пријави и информации за сомненија за сторени кривични дела од областа на Интернет измамите, каде најчесто жртви се физички и правни лица од земјава. Поради комплексниот начин на истрага која ги вклучува меѓународните организации за полициска соработка и различните законски регулативи во

[87] http://www.maturskiradovi.net/forum/Thread-kompjuterski-kriminal
[88] Ачкоски Југослав, Сигурност на компјутерски системи, компјутерски криминал и компјутерски тероризам, Скопје, 2012 година, стр.44-45
[89] Sajberkrize, Akademija za Bezbednost i Diplomatija, Beograd, 2009, http://www.scribd.com/doc/35038693/Cyber-Krize
[90] Секторот за компјутерски криминал и дигитална форензика при Министерството за внатрешни работи.

државите каде се одлеваат "украдените" парични средства, најдобриот начин за борба против овој вид на криминал е превенцијата и високото ниво на свест при користење на интернет мрежата во деловната комуникација. Односно, од досегашната пракса со ваков вид на случаи, Одделението за истраги на компјутерски криминал при Секторот за компјутерски криминал и дигитална форензика ги дава следните совети: мејл адресите кои правните субјекти ги употребуваат за деловна соработка да се користат максимално професионално и од страна на ограничен број вработени во фирмата; корисничките лозинки на мејл адресите да содржат комплексни карактери и истите да се менуваат на одреден временски период; доколку е возможно, за деловни потреби да се избегнува користење на комерцијални мејл сервиси, а истите да се заменат со професионални ИТ фирми кои нудат вакви услуги и гаранции за квалитет на истите; задолжително да се прави телефонска или друг вид на потврда со деловниот соработник за договорените фактури/профактури, особено ако се воочи измена во банкарските податоци каде треба да се уплатат паричните средства; сомненијата за измами во истиот момент да се пријават до одговорните во Банката каде правниот субјект е клиент како би можело навремено да се превенира во извршувањето (процесирањето) на трансакцијата.

## 2. Статистички податоци за компјутерскиот криминал

### 2.1. Статистички податоци за регистрирани кривични дела и сторители по член 251, 251-а и 251-б од Кривичниот законик во периодот од 2006 година до Август 2019 година

| Период | Член 251 –*Оштетување и неовластено навлегување во компјутерски систем* | | Член 251-а – *Правење и внесување на компјутески вируси* | | Член 251-б – *Компјутеска измама* | |
|---|---|---|---|---|---|---|
| | Кривични дела | Сторители | Кривични дела | Сторители | Кривични дела | Сторители |
| *Јануари-Август 2019 година* | 42 | 24 | - | - | 9 | 7 |

| | | | | | | |
|---|---|---|---|---|---|---|
| *2018 година* | 53 | 28 | - | - | 14 | 10 |
| *2017 година* | 43 | 34 | - | - | 13 | 12 |
| *2016 година* | 70 | 40 | - | - | 12 | 3 |
| *2015 година* | 40 | 33 | - | - | 8 | 3 |
| *2014 година* | 76 | 22 | - | - | 4 | 5 |
| *2013 година* | 74 | 15 | - | - | 4 | 1 |
| *2012 година* | 31 | 14 | - | - | 7 | 5 |
| *2011 година* | 47 | 29 | - | - | 1 | 2 |
| *2010 година* | 36 | 43 | - | - | 5 | 6 |
| *2009 година* | 63 | 73 | - | - | 5 | 2 |
| *2008 година* | 20 | 30 | - | - | 4 | 10 |
| *2007 година* | 7 | 11 | - | - | 2 | 1 |
| *2006 година* | 2 | 4 | - | - | - | - |

## 2.2. Кривични дела и сторители за период од 2017 до 2019 година

| ***Членови од Кривичен законик*** | | **2017** | | **2018** | | **2019** | |
|---|---|---|---|---|---|---|---|
| | | КД | Сторители | КД | Сторители | КД | Сторители |
| 144 став 4 | Загрозување на сигурноста | 5 | 2 | 21 | 22 | 29 | 24 |
| 149 | Злоупотреба на лични податоци | 48 | 32 | 76 | 47 | 103 | 49 |
| 149-а | Повреда на авторско право и сродни права | / | / | / | / | / | / |
| 157 | Повреда на правата на дистрибутерот на технички посебно заштитен сателитски сигнал | / | / | 5 | 5 | 1 | 1 |
| 193 | Прикажување на порнографски материјал на дете | / | / | 2 | 1 | 4 | 2 |
| 193-а | Производство и дистрибуција на детска порнографија | 4 | 6 | 2 | 1 | 6 | 5 |
| 251 | Оштетување и неовластено влегување во компјутерски систем | 43 | 34 | 53 | 28 | 65 | 37 |
| 251-а | Правење и внесување на компјутерски вируси | / | / | / | / | / | / |
| 251-б | Компјутерска измама | 13 | 12 | 14 | 10 | 12 | 9 |
| 274-б | Изработка и употреба на лажна платежна картичка | 12 | 14 | 4 | 2 | 8 | 7 |
| 394-г | Ширење на расистички и ксенофобичен материјал по пат на компјутерски систем | / | / | 5 | 5 | 27 | 26 |
| ***Вкупно:*** | | **125** | **100** | **182** | **121** | **255** | **160** |

## Заклучок

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

Со овој труд сакаме да докажеме дека сигурноста на информатичките системи во нашата земја е од големо значење поради големото информатичко незнаење на граѓаните што ги прави идеални жртви и не се свесни за последиците во случај на напад на незаштитен информатички систем.

Како факт, за тоа сведочат безброј злоупотреби, како што е сега актуелниот скандал за јавна соба, каде што, личните податоци на многу жртви, припаднички на женскиот пол се злоупотребени, на начин што споделувани се нивни приватни слики, телефонски броеви и други лични податоци меѓу поголема група на луѓе креирана во апликацијата Телеграм.

Сакаме да докажеме дека сторителите на овие кривични дела се се потешки за откривање поради тоа што постои една позитивна врска помеѓу извршителите и новата технологија поради тоа што производителите на истата прибираат се помалку податоци за нивните корисници односно нудат се поголема приватност на нивните потрошувачи со што се зголемува ризикот за неоткривање на лицето кое го сторило тоа дело и неговата самодоверба за да стори повторно такво дело бидејќи предходно не бил откриен и не ја сносил одговорноста за тоа дело.

Новонастанатите услови во последнава година овозможија поинакви можности за развој на многу кривични дела, меѓу кои и компјутерскиот криминал. Светската пандемија предизвикана од Корона вирусот влијаеше значајно врз развојот на компјутерскиот криминал. Според Извештајот од Интерпол за влијанието на Ковид-19 врз компјутерскиот криминал две третини од земјите-членки на Европската Унија пријавиле значително зголемување на компјутерскиот криминал за време на светската пандемија, на начин што најчесто биле таргетирани луѓе кои што ги пребарувале клучните зборови „Ковид“ или „Корона“. Сајбер криминалците ја користат пандемијата за да извршат напад на податоци

против критичната инфраструктура и здравствени установи кои што се одговорни за справување со Ковид-19. Исто така значително е зголемено клонирањето на официјалните веб страни на владите, преку кои што се крадат чувствителни податоци за корисниците, кои што подоцна можат да се користат во идните сајбер напади.

Сајбер криминалците ги развиваат и ги зајакнуваат своите напади со алармантно темпо, искористувајќи го стравот и неизвесноста предизвикана од нестабилната социјална и економска ситуација низ целиот свет. Во исто време, поголема зависност од конекцијата и дигиталната инфраструктура поради глобалнотата пандемија и карантинот ги зголемува можностите за сајбер напади. Бидејќи КОВИД-19 продолжува да опстојува на глобално ниво, понатамошно зголемување на компјутерскиот криминале многу веројатно во блиска иднина. Привлечени од ранливоста поврзана сополитиките за работа од дома и потенцијалот за зголемена финансиска корист, се компјутерските криминалци при што голема е веројатноста да ги градат своите активности и да развиваат понапреден и софистициран режим на работа. Во иднина сајбер криминалците би ги детектирале работниците кои работат од дома и нивните напади би биле насочени кон основните компјутерски работни алатки и компјутерскиот софтвер кој го користат за работа нивните компании. Друг двигател на понатамошното проширување на скалата за компјутерски криминал е влијание кое што го врши карантинот врз други кривични дела и области, што резултира во криминалци кои бараат алтернативни приливи на приходи. Како што такви, некои криминалци најверојатно ќе ги искористат понудите на Dark net пазарот. Покрај тоа, кога е вакцината против КОВИД-19 ќе биде достапна, многу е веројатно дека ќе има уште еден скок на компјутерскиот криминал поврзан со овие медицински производи, како и мрежен упад и сајбер напади за кражба на податоци. Во иднина се очекува дополнителен пораст на компјутерскиот криминал, како и пренасочување кон компјутерскиот криминал на многу криминалци од останатите сфери. Потребно е да се делува брзо и ефикасно за со цел да се спречи, превенира и намали ширењето на овој криминал, бидејќи штетите кои може да ги предизвика се непредвидливи.

**Користена литература**


1. Ignjatović Đ., Pojmovno određenje kompjuterskog kriminala, Beograd, 1991 god.
2. B.Simonović, *Kriminalistika*, Pravni fakultet u Kragujevcu, Kragujevac, 2004 god.
3. T.Aleksić i M.Škulić, *Kriminalistika*, Beograd, 2007 god.
4. Zivkovski, Z. I., Otkrivanje i razjašnjavanje kompjuterskog kriminaliteta, 2012 god.
5. Gillespie, A. A., Cybercrime: Key Issues and Debates Florence, Kentucky (USA), 2015 god.
6. Jovašević, D., Hašimbegović T., Krivičnopravna zaštita računarskih podataka, 2008 god.
7. Šarkić N., Prlja D., Damnjanović K., Marić V., Ţivković V., Vodinelić V., Mrvić-Petrović N., Pravo informacionih tehnologija, Beograd, 2011 god.
8. Jovi̇ći̇ć D., Bošković M., Kriminalistika metodika, Banja Luka, 2002 god.
9. Petrović R. S., Kompjuterski kriminal; Ministarstvo unutrašnjih poslova Republike Srbije: Uredništvo ĉasopisa"Bezbednost" i lista "Policajac",Beograd 2000 god.
10. Toren J. P., Intellectual Property and Computer Crimes (Intellectual Property usiness Crimes Series) , New York USA, 2003 god.
11. Николоска Светлана, „Методика на истражување компјутерски криминалитет“, Факултет за безбедност, Скопје, 2013 год.
12. Петровиќ С. *„Полицијска информатика“*, Криминалистичко – полицијска академија, Београд, 2007 год.
13. Janusz Piekalkiewicz ;World history of espionage: : Agents, systems, operations, National Intelligence Book Center, Washington USA 1998.god
14. Камбовски В. *„Казнено право, посебен дел“*, Просветно дело АД Скопје, 2003 год.
15. V.ĐurĊić, D.Jovašević – Krivično pravo: posebni deo, Niš, 2013 god.
16. D.Prlja, M.Reljanović, Z.Ivanović – Krivična dela visokotehnološkog kriminala, Beograd, 2011 god.
17. Drakulić M., Osnovi kompjuterskog prava, Beograd, 1996. God god.
18. D. Littlejohn Shinder, M.Cross,*Cybercrime*Burlington, MA, United States,2002 god.
19. M.Budimlić, P.Puharić – *Kompjuterski kriminalitet – kriminološki,krivičnopravni, kriminalistički i sigurnosni aspekt* – Fakultet za kriminalistiku, kriminologiju i sigurnosne studije Sarajevo 2009 god.

20. Ачкоски Југослав, Сигурност на компјутерски системи, компјутерски криминал и компјутерски тероризам, Скопје, 2012 год.
21. Sajberkrize, Akademija za Bezbednost i Diplomatija, Beograd, 2009 god.

**Интернет извори**

1. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2001:0051:FIN
2. Hi-Teh crime: The Impect to UK Business, www.nhtcu.org
3. Australian Institute of Criminology, www.aic.gov.au
4. Robinson J., Internet as the Scene of Crime, International Computer Crime Conference, Oslo,2000., www.ccips.org
5. http://www.rtv.rs/sr_lat/evropa/milionska-kradja-lozinki-u-nemacko_454999.html
6. http://lat.rtrs.tv/vijesti/vijest.php?id=135279
7. http://edition.cnn.com/2015/08/31/politics/china-sanctions-cybersecurity-president-obama/
8. www.blic.rs/Vesti/Svet/438405/Na-Filipinima-zbog-decje-pornografije-uhapseno-11-ljudi
9. http://www.bbc.co.uk/monitoring/ukraines-new-online-army-in-media-war-with-russia
10. http://www.usatoday.com/story/news/world/2013/08/14/israel-students-social-media/2651715/
11. http://www.pbs.org/newshour/bb/media-july-dec12-download_11-16/
12. http://en.wikipedia.org/wiki/Hacker_%28computer_security%29
13. http://www.politika.rs/rubrike/Ekonomija/Piraterija-odnosi-milijarde-dolara.lt.html
14. http://www.poslovni.hr/hrvatska/privreda-sad-a-godisnje-gubi-vise-od-200-mlrd-dolara-zbogpiratstva-52710
15. http://www.theguardian.com/commentisfree/2013/aug/11/nsa-internet-surveillance-email
16. http://www.maturskiradovi.net/forum/Thread-kompjuterski-kriminal

17. http://www.nezavisne.com/nauka-tehnologija/internet/Potrebni-ostriji-zakoni-za-sajberkriminal-69298.html
18. http://www.maturskiradovi.net/forum/Thread-kompjuterski-kriminal