ПРИРАЧНИК ЗА КОМПЈУТЕРСКИ КРИМИНАЛ

Јануари 2014

Автори:

Марко Зврлевски, *Јавен обвинител на Република Македонија*

Спасенка Андонова, *Јавен обвинител во Основното јавно обвинителство за гонење на организиран криминал и корупција*

Владимир Милошески, *Јавен обвинител во Основното јавно обвинителство за гонење на организиран криминал и корупција*

Уредник:

Ана Новакова Жикова, *Национален офицер за владеење на правото, Мисија на ОБСЕ во Скопје*

Игор Ристески, *Програмски асистент, Мисија на ОБСЕ во Скопје*

Тираж: *800 примероци*

Печати: *Скенпоинт, Скопје*

CIP - Каталогизација во публикација
Национална и универзитетска библиотека „Св. Климент Охридски", Скопје

343.533.9:009.7(035)

ЗВРЛЕВСКИ, Марко

Прирачник за компјутерски криминал / Марко Зврлевски, Спасенка Андонова, Владимир Милошески. - Скопје : OSCE, 2014. - 48 стр. : илустр. ; 21 см
Фусноти кон текстот
ISBN 978-608-4630-71-5
1. ,Рбет. ств. насл. 2. Андонова, Спасенка [автор] 3. Милошески, Владимир [автор]
а) Компјутерски криминалитет - Софтверски измами - Прирачници
COBISS.MK-ID 95899146

Поддржано од:

OSCE Organization for Security and Co-operation in Europe
Mission to Skopje

СОДРЖИНА

ВОВЕД 5

1. ИСТОРИСКИ РАЗВИТОК НА ЗАКОНОДАВСТВТО 7

2. МЕЃУНАРОДНА ПРАВНА РАМКА И СОРАБОТКА 13

3. НАЈЧЕСТО УПОТРЕБУВАНИ ТЕРМИНИ ВО ОБЛАСТА НА КОМПЈУТЕРСКИОТ КРИМИНАЛ 14

4. МЕМОРИЈА И СКЛАДИРАЊЕ НА ПОДАТОЦИ **21**

4.1. МЕРНИ ЕДИНИЦИ ЗА ПОДАТОЦИ 21
4.2. СКЛАДИРАЊЕ НА ПОДАТОЦИТЕ 22

5. МРЕЖА **23**

5.1 ПОИМ ЗА МРЕЖА 23
5.2 ДРУГИ МРЕЖНИ ПОИМИ 24
5.3. КАНАЛСКИ КОМУТИРАН НАСПРОТИ ПАКЕТСКИ КОМУТИРАН СООБРАЌАЈ 25
5.4. ИНТЕРНЕТ ПРОТОКОЛ (INTERNET PROTOCOL - IP) 25
5.5. ПОВРЗУВАЊЕ НА ИНТЕРНЕТ 26

6. СЕРВЕРИ **29**

7. ВИДОВИ КОМУНИКАЦИЈА МЕЃУ КОРИСНИЦИТЕ **31**

8. ВИДОВИ ИНТЕРНЕТ ИЗМАМИ **34**

9. ШТЕТНИ СОФТВЕРИ **35**

10. ЗАВРШНИ СОГЛЕДУВАЊА НА АВТОРИТЕ **39**

ПРИЛОГ 1: ОДРЕДБИ ОД КРИВИЧНИОТ ЗАКОНИК КОИ СЕ ОДНЕСУВААТ НА КОМПЈУТЕРСКИ КРИМИНАЛ 40

ПРИЛОГ 2: ПРОЦЕСНИ ОДРЕДБИ ОД КОНВЕНЦИЈАТА ЗА КОМПЈУТЕРСКИ КРИМИНАЛ 48

ВОВЕД

Обвинителството има значајна улога во истражување, откривање и изведување на поедници или групи кои сториле кривични дела пред лицето на правдата. Во услови на рапиден пораст на противправни дејствија, особено оние кои во себе имаат компјутерски (cyber) елемент, се понеопходна е потребата од соодветна едукација за да може да се сфати вистинската природа на овој вид криминал.

Во време на сè поголема употреба на компјутерите и електронските апарати во секојдневното живеење, јуриспруденцијата, на глобално ниво, сè повеќе почнува да става акцент на овој феномен.

Фокусот на овој Прирачник е насочен кон повеќе аспекти, а пред сè на феноменологијата на елекронската комуникација и замената на конвенционалниот систем на проследување на податоците со нов, кој на побрз и поефикасен начин овозможува трансфер на голема количина на податоци на големо растојание. Сето ова, неспорно, го подобрува квалитетот на живеење, но од друга страна преставува поле на кое на многу поедноставен начин може да се извршуваат илегални дејствија. Токму овој втор сегмент побудува голем интерес во јавноста која се занимава со кривично правната материја. Имено, сега се отвараат нови прашања уште во најраните фази на кривичното постапување и прибирањето на доказите. Сторителите на овој вид на криминал воопшто не се лимитирани со државни граници, а со тоа и надлежноста на секоја од државите се става под знак прашање во момент на прибирање на податоците. Сето ова претставува многу потежок предизвик за јавните обвинители во текот на постапувањето. Комплексноста на овој вид на криминал, особено постојаното еволуирање на начините и формите на извршување на противправните дејствија, бара постојана агилност и подготвеност на обвинителите во секојдневното практично постапување.

Овој Прирачник нема интенција да даде инструкции за постапување чекор по чекор, туку идејата е да се понуди една корисна алатка - водич кој ќе содржи поими кои ќе ја олеснат идентификацијата на средствата со кои се извршува овој вид на криминал, видот на докази кои треба да се обезбедат како и правилниот начин на нивно обезбедување, со што ќе се олесни процесот на докажување.

Традиционалните докази имаат физички облик, на пример: разни документи, фотографии, предмети и други траги кои физички се видливи и лесно може да се лоцираат и приберат како доказ. Електронските докази пак, иако немаат ваква видлива форма, по својата доказна сила не се поразлични од оние кои се сметаат за традиционални. Тие многу често се наоѓаат на места на кои само посебно обучени лица можат да ги детектираат и обезбедат и на тој начин да добијат релевантна вредност пред правосудните органи. Една од спецификите на дигиталните податоци е можноста истите да се обезбедат

во неограничен број и притоа секој примерок всушност е оригинал. Секоја електронска направа има свои специфични карактеристики што ја наметнува потребата да се примени и специфична процедура со цел да се обезбеди влез во меморијата каде се чуваат електронските докази, а притоа истите да останат неконтаминирани.

Меѓуинституционалната соработка претставува значаен сегмент на кој треба да се посвети посебно внимание, пред сè заради поедноставување и операционализирање на потребите на јавниот обвинител за прибирање на релевантни докази и можноста истите во најкраток рок да му бидат доставени.

Оттука произлезе и основниот мотив за изготвување на еден ваков Прирачник во кој ќе бидат внесени основните параметри кои треба да се имаат предвид при одлучување во кривично-правни предмети во кои се обработуваат кривични дела од областа на компјутерскиот криминал, но и за сите останати кривични дела каде што е потребно да се прибават докази кои оригинерно или дериватно се во електронска форма.

1. ИСТОРИСКИ РАЗВИТОК НА ЗАКОНОДАВСТВТО

Потребата за воедначување и систематизирање на глобално ниво на материјалните и процесните норми од областа на компјутерсиот криминал и електронските докази, свој одраз најде во Конвенцијата за компјутерски криминал[1] на Советот на Европа (во понатамошниот текст: Конвенцијата). Иако претходно постоеја обиди за дефинирање на материјалните норми кои ја регулираат меѓународно правната соработка, сепак Конвенцијата по својата сеопфатност, флексибилност и можност за лесно инкорпорирање во националните законодавства, иако првично наменета за државите во Европа, стана препознатлив механизам за лесна комуникација меѓу државите од целиот свет.

На Конвенцијата за компјутерски криминал подоцна се надоврзуваат и Конвенцијата за заштита на личните права при автоматизиран процес на обработка на личните податоци[2] со амандманите и Дополнителниот Протокол за авторизиран проток на лични подотоци надвор од државата[3], Дополнителен Протокол на Конвенцијата за компјутерски криминал за заштита од расизам и ксенофобија[4], Конвенција за заштита на децата од сексуална експлоатација и сексуално злоставување[5] и Директивите на ЕУ.

Советот на Европа ја усвои Конвенцијата за компјутерски криминал во Будимпешта на 23.11.2001 година. Вкупно 58 држави се потписнички на Конвенцијата, од кои 28 со ратификација. Конвенцијата беше потпишана од страна на нашата држава на 23.11.2001 година, ратификувана на 15.09.2004 година, а влезе во сила на 01.01.2005 година.

Конвенцијата содржи материјални, процесни и норми за меѓународна соработка. Одредбите од областа на материјалното право се однесуваат на: недозволен пристап, недозволено пресретнување, упад во податоци, упад во систем, злоупотреба на уред, фалсификување поврзано со компјутер, измама поврзана со компјутер, дела поврзани со детска порнографија, дела поврзани со повреда на авторски и други сродни права.

Вака дефинирани одредби се внесени и во македонското материјално законодавство и тоа во делот на општите одредби каде што се дефинирани основните поими за овој вид на криминал, како и специфични конкретни кривични дела. Домашната правна рамка која ја регулира областа на компјутерскиот криминал ги вклучува:

---

[1] Види: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
[2] Види: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
[3] Види: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&CM=8&NT=181
[4] Види: http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm
[5] Види: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=201

- Кривичниот Законик (КЗ)[6]
- Законот за кривичната постапка (ЗКП)[7]
- Законот за електронските комуникации[8]
- Законот за следење на комуникациите[9]
- Законот за електронска трговија[10]
- Законот за електронско управување[11]
- Законот за парнична постапка[12]
- Законот за податоците во електронски облик и електронски потпис[13]
- Декларација за побезбеден интернет

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

Домашното законодавство го задржува континенталниот пристап и нормите кои ја регулираат оваа материја се внесени во постојните закони, притоа водејќи сметка за заштитата на основните човекови права во врска со правото на слободно изразување и слобода на мислата и правото на приватност.

И покрај тоа што компјутерскиот криминал претставува материја која постојано се менува и има новитети кои неможе едноставно да се дефинираат (нови технологии во мобилната телефонија, примена на посебни истражни мерки итн), а особено кога станува збор за транснационална комуникација, сепак Конвенцијата во целост е инкорприрана во нашето законодавство. На овој начин се овозможува полесна меѓународна соработка, како и можност за лесно прилагодување на соодветните одредби на новите облици на овој вид на криминал.

[6] Службен весник на РМ бр.37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 50/2006, 60/2006, 73/2006, 87/2007, 7/2008, 139/2008, 114/2009, 51/2011, 51/2011, 135/2011, 185/2011, 142/2012, 143/2012, 166/2012, 55/2013, 82/2013
[7] Службен весник на РМ бр.150/2010, 100/2012
[8] Службен весник на РМ бр.13/2005, 14/2007, 55/2007, 98/2008, 83/2010, 13/2012, 59/2012, 123/2012, 23/2013.
[9] Службен весник на РМ бр.121/2006, 110/2008, 4/2009, 116/2012
[10] Службен весник на РМ бр.133/2007, 17/2011
[11] Службен весник на РМ бр.105/2009, 47/2011
[12] Службен весник на РМ бр. 79/2005, 110/2008, 83/2009, 116/2010
[13] Службен весник на РМ бр.34/2001, 98/2008

➢ ***Материјално право***

- *Кривичен Законик*[14]

Материјалните одредби за кривичните дела од областа на компјутерскиот криминал се содржани во КЗ и се однесуваат на:

- член 144 – Загрозување на сигурноста
- член 147 - Повреда на тајноста на писмата или други пратки
- член 149 – Злоупотреба на лични податоци
- член 149-а – Спречување на пристап кон јавен информатички систем
- член 157 – Повреда на авторско право и сродни права
- член 157-а - Повреда на правото на дистрибутерот на технички посебно заштитен сателитски сигнал
- член 157-б – Пиратерија на аудиовизуелно дело
- член 157-в – Пиратерија на фонограм
- член 193 – Покажување на порнографски материјал на дете
- член 193-а - Производство и диструбуција на детска порнографија
- член 193-б - Намамување на обљуба или друго полово дејствие на малолетник кој не наполнил 14 години
- член 251 - Оштетување или неовластено навлегување во компјутерски систем
- член 251-а - Правење и внесување на компјутерски вируси
- член 251-б - Компјутерска измама
- член 271 – Правење, набавување или отуѓување средства за фалсификување
- член 274-б - Изработка и употреба на лажна платежна картичка

[14] Интегралниот текст на одредбите од Кривичниот Законик кои се однесуваат на компјутерски криминал е даден како посебен Прилог 1 на овој Прирачник (види стр.34)

- член 279-а - Компјутерски фалсификат
- член 286 - Повреда на правото од пријавен или заштитен пронајдок и топографија на интегрални кола
- член 394-г - Ширење на расистички и ксенофобичен материјал по пат на компјутерски систем
- член 122 - Дефинирање на основни сегменти на компјутерскиот криминал:

точка 15 **платежни картички -** Под платежни картички се подразбира секаков вид на средства за плаќање издадени од страна на банкарски или други финансиски институции кои содржат електронски податоци за лица и електронски генерирани броеви со кои се овозможува вршење на каков било вид на финансиска трансакција;

точка 24 **детска порнографија** - Под детска порнографија се подразбира порнографски материјал кој визуелно прикажува очигледни полови дејствија со малолетник или повозрасно лице кое изгледа како малолетник, или го прикажуваат малолетникот или повозрасното лице кое изгледа како малолетник во очигледна сексуална положба, или реални слики кои прикажуваат очигледни полови дејствија со малолетник или го прикажуваат малолетникот или повозрасното лице кое изгледа како малолетник во очигледна сексуална положба;

точка 26 **компјутерски систем -** Под компјутерски ситем подразбираме било каков уред или група на меѓусебно поврзани уреди од кои еден или повеќе од нив, врши автоматска обработка на податоци според одредена програма;

точка 27 **компјутерски податоци -** Под компјутрески податци се подразбираат презентирање на факти, информации или концепти во облик погоден за обработување преку компјутерски систем, вклучувајќи и програма подобна компјутерскиот систем да го стави во функција

Покрај КЗ, материјалното право кое ги регулира различните казниви аспекти на компјутерскиот криминал исто така се сретнува и во други закони кои најчесто содржат посебна глава која се однесува на прекршочни одредби. Такви посебни закони *(lex specialis)* кои регулираат специфични прашања од областа на електронските комуникации, се наведени погоре.

➢ ***Процесно право***

- *Закон за кривичната постапка*

Процесниот аспект на прашањата поврзани со компјутерски криминал се однесува на мерките и дејствијата кои се применуваат специфично за овој вид на криминал, како и на мерките и дејствијата кои се применуваат при конвенционалниот криминал. Па така, овде би ги споменале одредбите од ЗКП за пребарување на компјутерски ситем и компјутерски податоци (член 184) и привремено одземање на компјутерски податоци (член 198), како и одредбите од Глава XVII – Мерки за пронаоѓање и обезбедување на лица и предмети, понатаму цел и видови на посебни истражни мерки (член 252) особено посебните мерки таен увид и пребарување во компјутерски систем и увид во остварени телефонски и други електронски комуникации итн.

Компјутерскиот криминал, како и конвенционалниот криминал, претпоставува прибирање на докази кои и покрај нивното физичко присуство бараат и прибирање на податоци кои не се видливи[15] и се во форма која што претпоставува претходно нивно детектирање и фиксирање преку физичкиот облик (компјутер, работна станица, телефон и сл.) па потоа превземање на дополнителни процесни дејствија кои претпоставуваат индиректен контакт со докази во електронска форма и места каде што истите се складиирани.

При прибирањето на доказите од особено значење е:

- Потврда за привремено одземање на предмети
- Кои предмети може да се одземат
- Начини на привремено одземање на предметите
- Услови и принципи на зачувување на веродостојноста на одземените предмети

Во ексклузивни случаи прибирањето на доказите се врши далечински со примена на одредбите од член 32б од Конвенцијата за компјутерски криминал.

Во ситуации кога е потребно да се направи увид во компјутери кои во моментот работат, од исклучителна важност е да нема прекин во електричното напојување бидејќи RAM-от ги чува податоците се додека има напојување, во спротивно истите може да се изгубат.

[15] CASX – податоци што се наоѓаат во активната меморија на компјутерот

- *Конвенција за компјутерски криминал – процесни норми*[16]

Како што беше наведено погоре, покрај материјалните норми, Конвенцијата за компјутерски криминал содрзи низа процесни норми:

- Член 14 – Опфат на процесните одредби
- Член 15 – Услови и гаранции
- Член 16 - Експедитивно зачувување на складирани компјутерски податоци
- Член 17 - Експедитивно зачувување и делумно откривање на преносни податоци
- Член 18 - Наредба за производство
- Член 19 - Претрес и запленување на складирани компјутерски податоци
- Член 20 - Собирање на преносни податоци во реално време
- Член 21 - Пресретнување на содржински податоци
- Член 22 - Јурисдикција

[16] Интегралниот текст на процесните одредби од Конвенцијата за комјутерски криминал е даден како посебен Прилог 2 на овој Прирачник (види стр.42)

2. МЕЃУНАРОДНА ПРАВНА РАМКА И СОРАБОТКА

Mutual Legal Assistance (MLA, меѓусебна правна помош) – претставува единствен основ за прибавување докази кои се наоѓаат во друга држава кои можат да имаат соодветна доказна сила пред надлежниот суд.

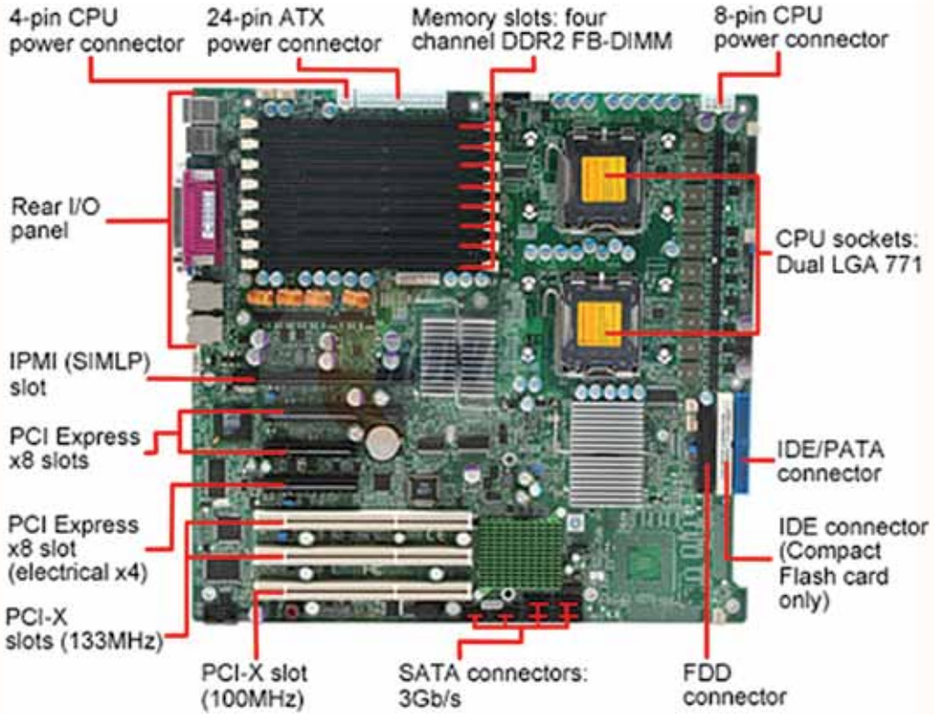
Second additional protocol of the European Convention Mutual Assistance in Criminal Matters (од 08.11.2001 година) - овозможува брза и директна комуникација меѓу овластените државни органи при добивање на спонтани информации поврзани за одреден кривично правен настан и со тоа примарните докази се добиваат директно без примена на MLA. На ваков начин, се постигнува поголема ефикасност на кривична постапка, особено во случаи кога се знае дека електронските докази може многу лесно и брзо да се изгубат, изменат или на кој било начин да се контаминираат.

Point 24/7 (Точка 24/7) - согласно член 35, Конвенцијата за компјутерски криминал поставува нов инструмент кој мошне ефикасно ја регулира меѓународната правна помош на институционално ниво. Ова дава можност да се приберат односно замрзнат податоците во период кој ни овозможува ефикасно предистражно решавање на основните постановки за следење на движењето на податоците во различни Internet Service Providers (ISP, интернет провајдери) во различни земји, но и податоци кои се наоѓаат во државни органи, институции, правни субјекти и физички лица, а без притоа да се користат конвенционалните методи и користење на државните органи (Министерството за правда и Министерството за надворешни работи) кои би можеле да ја забават постапката на лоцирање и замрзнување на податоците.

Точка 24/7 не значи и замена на конвенционалните начини на меѓусебна правна помош. Ваквиот институт е само подршка за отпочнување на меѓусебната правна помош, при што нема да се губи драгоцено време за зачувување на бараните податоци кои, кога станува збор за електронски докази, се подложни на брзо менување или уништување. Ова значи дека протокот на време е есенцијален за прибавување и докажување на оригиналноста на доказот како и можноста надлежниот државен орган навремено да го има соодветниот доказ како би можело да се води кривичната постапка.

3. НАЈЧЕСТО УПОТРЕБУВАНИ ТЕРМИНИ ВО ОБЛАСТА НА КОМПЈУТЕРСКИОТ КРИМИНАЛ

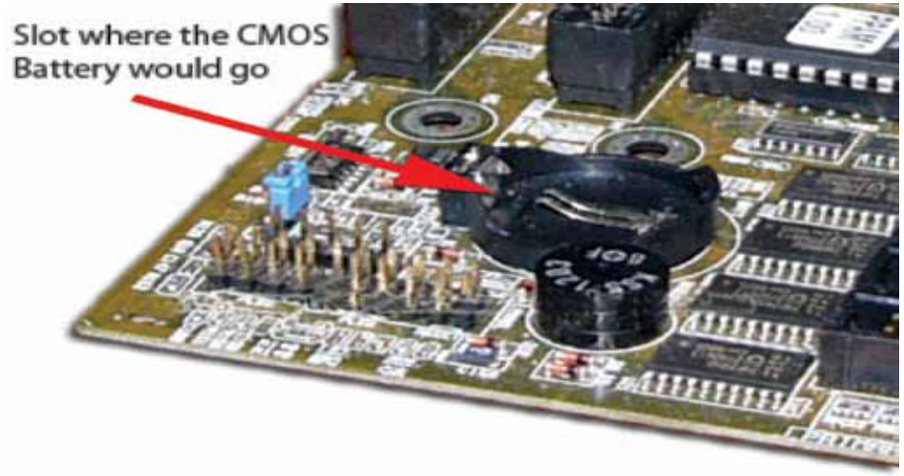
Матична плоча **-** Исто така, позната како главна плоча или системска плоча на компјутерот. Матичната плоча е централната шема на компјутерот. Сите останати делови и периферни уреди се вклучуваат во неа. Работата на матичната плоча е да ги поврзе информациите помеѓу сите останати уреди. Во матичната плоча се наоѓа BIOS (basic input/output system[17]) – основниот систем за влез/излез кој го управува компјутерот кога првично ќе се вклучи. На матичната плоча директно се приклучуваат другите составни делови, како на пример: меморијата, централната единица за обработка на податоци, графичката картичка, звучната картичка, хард дискот, диск уредот, видео картичка, заедно со различни порти и периферии.



Слика 1 – матична плоча

[17] Кратенката најчесто се изговара"*bye*-oss".

CMOS (Complementary Metal Oxide Semiconductop[18], дополнителен метално оксиден полупроводник) - претставува хардверот на компјутерот кој изведува фукнции на ниско ниво и основни компјутерски рутини при стартување на истиот. CMOS-от и BIOS-от честопати се користат наизменично. На BIOS-от можеме да гледаме како на софтвер, а на CMOS-от како на хардвер кој го употребува.

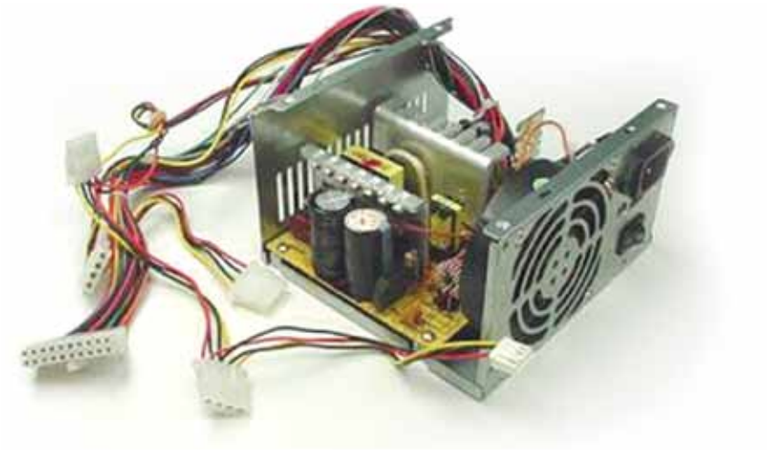


Слика 2 – Место каде се наоѓа CMOS-от

BIOS (Basic Input/Output System, основен систем за влез/излез) - претставува меѓу-уред кој му дозволува на корисникот да прави елементарни (low-level) функции во матичната плоча, CPU, меморијата и другите уреди. Првичните BIOS лежишта најчесто се поставени правилно. Една од најчестите промени кои му се прават на BIOS-от во форензичен капацитет е кога се менува редот по кој компјутерот ги пребарува уредите на кои може да биде сместен оперативниот систем (на пример: еден компјутер може да се стартува од USB уред, CD ROM или хард диск и редоследот на проверка на овие уреди може да се промени).

Напојување на компјутерот - Единицата за напојување со електрична енергија или т.н. Power Supply Unit (PSU) во компјутерот ја регулира и ја пренесува енергијата кон составните делови во кутијата. Стандардното електрично напојување ја претвора дојдовната енергија од 110V или 220 наизменична струја во еднонасочна струја, која сега е погодна да ги напојува компјутерските составни делови.

[18] Кратенката најчесто се изговара"*see*-moss".



Слика 3 – Напојување на компјутерот

Central Processing Unit (CPU, централна обработувачка единица/процесор) - е хардвер во рамките на компјутерот кој ги извршува инструкциите на компјутерските програми за вршење основни аритметички, логички и влезно/излезни операции на компјутерскиот систем. Луѓето најчесто ја мешаат со кутијата или шасијата на компјутерот. Меѓутоа процесорот претставува внатрешна компонента и не може да се види надвор од системот. Без разлика за каков тип компјутер се работи, процесорот работи со изведување серии складирани инструкции кои се познати како програма.

Слика 4 – CPU/процесор

Random Access Memory (RAM, меморија со произволен пристап) – Компјутерската меморија претставува форма на електронско складирање на податоци, иако најчесто се опишува како привремена форма за складирање податоци кои ги користат активните програми со цел побрзо да се пристапи до нив. Процесорот бара податоци од RAM-от, тие се обработуваат и обработени се впишуваат во RAM-от. Ова се случува милиони пати во секунда.[19]

Слика 5 - RAM

Universal Serial Bus (USB) - USB конектори можат да се најдат на повеќето современи компјутери и овозможуваат едноставно додавање голем број уреди на компјутерот како што се глушецот, печатачи, надворешни складишта на податоци и мобилни телефони. Во моментот ова е најчестиот метод за поврзување надворешни уреди кон компјутерот. Во праксата постои можност за поврзување повеќе од 127 уреди со еден компјутер преку користење УСБ. Леснотијата со која можат да се користат USB уредите, значи дека тие се истакнуваат како најчесто употребувани во многу дигитални форензични истраги/ вештачења[20].

Слика 6 - USB конектор

[19] при спроведувањата на законот повообичаени се обидите да се фатат податоците во РАМ-от пред да се прекине електричното напојување додека копјутерот пребарува.
[20] Во рамките на МВР постои Сектор за компјутерски криминал и компјутерска форензика

Hard disk drive (HDD, хард диск) **-** Претставува електромеханички уред кој содржи вртечки дискови и движечки глави за впишување/читање податоци. Дисковите имаат плочи во кои се запишани информациите и податоците лесно можат да бидат избришани или повторно запишани при што се зачувува структурата на дискот што ги прави одржливи на подолг временски период. Податоците се складираат на површината на плочата во т.н. сектори и патеки. Патеките се концентрични кругови, а секторите се сегменти на патеката. Податоците се складираат во хард дискот во вид на датотеки кои едноставно претставуваат „битови"[21]. Програмите претставуваат датотеки и процесорот ги третира како такви за да може да ги искористи. Повеќето компјутери имаат барем еден хард диск, а има и многу компјутери со повеќе од еден. За поголемите компјутери, како што се main frame[22] (мејн фрејм) компјутерите, нормално е да имаат повеќе хард дискови. Денес, вообичаено е и други уреди освен компјутерот како што се CCTV (затворените ТВ системи) и музичките уреди, да имаат хард дискови за да можат да сочуваат поголема количина податоци.

Слика 7 – хард диск

[21] Види подолу, „Меморија и складирање на податоци "

[22] Main frame komznjутерите ги користат претежно големи компании или владини институции за извршување суштински апликации, обработка на опсежни податоци (на пример, статистички податоци) и обработка на трансакции.

Solid-state drive (SSD) - претставува уред за складирање податоци кој користи полупроводничка меморија, т.е. микрочипови кои содржат мобилни делови. Овој уред ги складира постојаните податоци со цел обезбедување пристап до нив на истиот начин како во случај на традиционалниот хард диск. Понекогаш се нарекува и solid-state disk или електронски диск. Во споредба со електромеханичките дискови, SSD се помалку чуствителни на физички удари, тивки се, со пократко време на пристап и поголема тајност, но имаат повисока цена. SSD-ите употребуваат исти уреди за поврзување како и хард дисковите, па според тоа лесно се заменуваат во повеќето апликации. Бидејќи во SSD уредите податоците се складираат на сосема поинаков начин, тие носат нови предизвици кон дигиталните вештачења.

Слика 8 – SSD уред

CD/DVD/BD[23] **дискови -** Овие дискови можат да содржат различна количина податоци и обично се користат за складирање музика, видео или компјутерски датотеки за употреба на различни уреди. На пример, DVD има исти димензии како и CD, а може да содржи седум пати повеќе податоци од истиот. BD е оптички диск за складирање податоци со капацитет кој е и до десет пати поголем од оној на DVD. Со други зборови, овие дискови можат да складираат повеќе податоци отколку што беше возможно да се складира на хард дисковите од пред неколку години. Сите тие ги складираат податоците на различен начин од хард дискот и податоците кои се чуваат на нив не се толку непостојани како оние кои се складирани во хард-дискот.

[23] CD – Compact Disc (компакт диск), DVD – Digital Versatile Disc (дигитален повеќенаменски диск), BD – Blu ray Disc (диск со син зрак)

Слика 9 - CD/DVD/BD

Оперативен систем (OS) - претставува софтверска програма (платформа) која му овозможува на хардверот да комуницира со софтверските програми/апликации. Без оперативен систем компјутерот нема да може да функционира. Постојат различни видови оперативни системи (Windows, iOS, Android) во зависност од типот на компјутерот или дигиталниот уред (таблет, мобилен телефон). Повеќето компјутерски апликации се специфично создадени за одредени оперативни системи, иако сега е вообичаено да бидат достапни на повеќе од една платформа.

4. МЕМОРИЈА И СКЛАДИРАЊЕ НА ПОДАТОЦИ

4.1. Мерни единици за податоци

Bit – бит е основна единица за информација во компјутерите и дигиталните комуникации. Може да има само една од две вредности и, затоа, може физички да биде применет во уреди кои имаат две состојби (пр., „вклучено" и „исклучено"). Најчесто, овие вредности се означуваат со 0 и 1. Терминот „бит" е кратенка од **bi**nary digi**t** (бинарна цифра).

Byte – бајт е единица за дигитални информации во компјутерската технологија и телекомуникациите која, најчесто, се состои од осум бити.

Важно е да се напомне дека метричките префикси кои се користат со единицата бајт се идентични како метричките префикси во SI24 системот, но разликата е што компјутерската меморија е дизајнирана врз основа на бинарната логика, т.е. умножените вредности се со основа 2 (пр. 210, 220), а не 10 (пр. 103, 106).

Име (изговор)	Вредност	Кратенка
Bit (бит)	0 или 1	/
Byte (бајт)	8 бити (2^3)	B
Kilobyte (килобајт)	1,024 B (2^{10})	KB
Megabyte (мегабајт)	1,048,576 B ($2^{20} = 1024^2$)	MB
Gigabyte (гигабајт)	1,073,741,824 B ($2^{30}=1024^3$)	GB
Terabyte (терабајт)	1,099,511,628,000 B ($2^{40}=1024^4$)	TB

[24] Le Système international d'unités – меѓународен систем за мерни единици

4.2. Складирање на податоците

Капацитет на носачи на податоци:

- *CD* - вообичаено имаат капацитет од 650MB или 700MB
- *DVD* - Моментално достапно со 4.7GB или 8.5GB, а HVD е дизајниран со капацитет од 3.9 TB (830 пати поголем капацитет од обично DVD)
- *Хард драјв* - Моментално достапно со 4 Terabytes
- *Интернет* - поимот ИНТЕРНЕТ претставува кованица од зборовите INTER connected NETwork (МЕЃУ поврзана МРЕЖНА работа).

Онлајн складирање

- Дозволиво – Онлајн складирањето обезбедува сервис, особено корисен при водење на бизнис и патување, затоа што до складираните податоци може да се пристапи преку Интернет и да се најдат и споделат фајловите.
- Недозволиво – Истото се применува кон фајловите, фолдерите, сликите или кој било тип на податоци кои може да се најдат на секој компјутер кој е конектиран за Интернет и да се сподели од страна на секој кој ги има податоците за логирање.

Пример на недозволиво онлајн складирање претставува "dead letter box". Ова значи дека се отвора сметка на кој било бесплатен веб-мејл, потоа се пишува порака која вклучува и "тајна" содржина и се додаваат прилози (attachment) – ако има потреба од нив. Пораката не се испраќа, туку само се зачувува како draft (нацрт) верзија. Потоа се споделуваат логин детали со некој друг. Лицето со кое се споделени деталите се логира, ја чита, а потоа и ја брише пораката. Пораката не била никогаш испратена, туку била чувана само нејзина драфт верзија во некој од фолдерите на корисничката сметка – без можност виртуелно да се следи истата.

5. МРЕЖА

5.1. Поим за мрежа

Local Area Network (LAN, локална мрежа) - Компјутерска мрежа која покрива мала географска област, како што е домот, канцеларијата, група на згради, како на пример училиште. Карактеристиките кои го дефинираат *LAN*-от ја вклучуваваат високата брзина на преносот на податоци, помалиот географски опсег и недостатокот на изнајмени телекомуникаациски линии.

Wide Area Network (WAN, мрежа за поширoки области) - Компјутерска мрежа која покрива широка област (т.е секоја мрежа чии комуникациски линкови поминуваат метрополитски, регионални или национални граници) или на поедноставен-неформален начин, мрежа која користи рутери и јавни комуникациски линкови. ИНТЕРНЕТОТ преставува пример за оваа мрежа.

Мрежите можат да бидат ограничени:

- Според бројот на корисници на кои им припаѓаат,
- Според максималниот географски опсег на мрежната покриеност како што се, на пример, мрежите Ethernet или Wireless.

Интернетот дозволува/овозможува поврзување на овие мали мрежи во една, чија големина е неограничена. Исто така не е важно за каков тип на мрежа станува збор се додека TCP/IP е прифатена како комуникациски медиум.

World Wide Web (www, светска мрежа) – За првпат се појавува 1991 година кога HTML (Hyper Text Markup Language) беше измислен од Сер Тим Бернерс-Ли. HTML создаде платформа за комбинирање на зборови, слики и звуци на веб страните. Веб стандардите се развиваат од страна на **World Wide Web Consortium (W3C)** кој претставува меѓународна заедница која развива стандарди за да се обезбеди долгорочен развој на Мрежата. За пребарување на мрежата се користат т.н. **Web Browser-и (пребарувачи)** кои претставуваат посебни софтверски програми кои се направени да лоцираат и прикажуваат различни веб страни, меѓу кои најпознати се: Internet Explorer, Mozilla Firefox, Google Chrome, Safari, Opera итн. Пребарувачите и серверите за да можат да комуницираат меѓусебе на интернет користат заеднички протокол кој се нарекува **HTTP (Hyper Text Transfer Protocol)**.

5.2. Други мрежни поими

Ports - се крајни точки (излези) или канали за комуникација низ мрежа. Повеќе излези на една сметачка машина овозможуваат во исто време да се добиваат податоци од различни мрежи или носители на податоци без притоа да има конфликт на приемот и излезот на информациите. Ports се виртуелни точки и не се влезови во сметачката машина на која се вклучуваат надворешни единици или комуникациски кабли.

Media Access Control (MAC) address - е единствен идентификационен број кој го содржат најголемиот број адаптери или мрежни картички внесени од страна на производителот и истите даваат единствени податоци за постоење на комуникација низ некој адаптер или мрежна картичка. Овој идентификационен број се сретнува кај сите уреди кои можат да бидат носачи на податоци (компјутерите, печатачите, скенерите, мултифункционалните уреди поврзани со компјутер, фото апаратите, видео камерите итн).

Botnet – овој поим е поврзан со збир IRC автоматизирани компјутерски програми за интернет комуникација, кои се поврзани и можат да комуницираат меѓу себе без да бидат попречувани од несакани корисници. Ова е основниот поим за botnet кој се користи за легална комуникација. Од друга страна, нелегалната комуникација преку botnet системот на авоматизирано насочена комуникација меѓу компјутери чија безбедност е компромитирана со помош на малициозни програми претставува начин на трансфер на информации низ некој компјутер без знаење на корисникот на компјутерот.

Encryption - е посебна програма која овозможува одделни податоци да бидат заштитени. Заштитата се врши со внесување посебни шифри кои оневозможуваат достапност до содржината на одреден дел од компјутерската меморија. Најчесто користени програми за инкрипција на податоците се: Microsoft Bitlocker, Truecrypt и Steganos.

Network Interface Controller (NIC) - познат и како network adapter или LAN adapter, е дел од хардверот (како составен дел на матичната плоча или пак во вид на мрежна картичка инсталирана во компјутерот) преку кој компјутерот комуницира со другите уреди во една компјутерска мрежа.

Network Switch - е уред за вмрежување кој овозможува повеќе уреди да се поврзат во компјутерска мрежа.

Router - е уред кој ја детерминира следната мрежна точка каде што пакетот на податоци треба да биде пренесен како негова следна или крајна дестинација.

Server – е компјутер или уред кој овозможува информации или сервиси за или на друг компјутер преку мрежа. Со користење на соодветен програм секој компјутер врзан на мрежа може да биде сервер. Во најголем дел од случаите тоа е "посветен" компјутер кој цело време е достапен за останатите

компјутери. Еден таков компјутер може да извршува повеќе сервиси и тоа web server, e-mail server, print server и слично.

Мрежен приклучок - компјутерски мрежен уред кој ги поврзува мрежните делови.

Bandwidth (ширина на опсег) **-** Количина на информации кои можат да бидат пренесени преку телефонска линија, кабелска, сателит итн. Колку е поголема ширината на опсегот, толку ќе биде и поголема брзината на конекцијата, како и пристапот кон Интернет, побрзи префрлања, ТВ искуство.

Network Interface Controller (NIC, Мрежна карта) **-** претставува кружна табла или карта која е инсталирана во компјутерот и овозможува конектирање на одредена мрежа.

Network Hub (Ethernet Hub, мрежен уред или концентратор) - претставува уред за поврзување на повеќе Ethernet уреди заедно со што тие делуваат како единствен мрежен сегмент. Хабовите работат на физичкиот слој (прв слој) од моделот OSI и терминот „приклучок на првиот слој" често се употребува наизмечнично со хабот. Со ова уредот претставува форма на мулти влезен повторувач. Мрежните хабови исто така се одговорни за препраќање на сигналот кон сите порти доколку детектира судир.

5.3. Каналски комутиран наспроти пакетски комутиран сообраќај

Во "каналски комутираните" мрежи, постои дефинирана конекција помеѓу испраќачот и примачот на податоците за време на комуникациската сесија. Пример за каналски комутирана мрежа е телефонската мрежа.

Поголемиот дел модерни податочни мрежи, како Интернет, се опишуваат како "неконекциски-ориентирани" или "пакетски комутирани". Кај нив, податоците кои се пренесуваат се делат на мали пакети без оглед на содржината, видот или структурата во блокови со соодветна големина кои се нарекуваат пакети и кои го наоѓаат својот пат од испраќачот до примачот преку посебен протокол.

5.4. Интернет протокол (Internet Protocol - IP)

Различни апликации и услуги користат протоколи за да комуницираат преку мрежи. Некои од поважните се: HTTP – Hyper Text Transfer Protocol; SMTP – Simple Mail Transfer Protocol; FTP – File Transfer Protocol; NNTP – Network News Transfer Protocol, TCP – Transmission Control Protocol, IP – Internet Protocol.

Интернет протоколот е еден од двата основни протоколи во интернет моделот

(познат како TCP/IP). Тој е главен протокол за комуникација, т.е. за пренос на датаграми (основни податочна единица која се пренесува во една пакетска мрежа). Неговата основна функција го овозможува вмрежувањето и, во суштина, го воспоставува интернетот. Задачата на IP, како основен протокол во интернет моделот, е да испорачува пакети од изворот до дестинацијата единствено врз основа на IP адресите во заглавието на пакетот податоци кој се пренесува. Тој ги дефинира и методите на адресирање кои се користат да се означи датаграмот со информација за изворот и дестинацијата.

Интернет протокол адресата (IP адреса) е нумеричка ознака која се доделува на секој уред (компјутер, печатач) кои се приклучени на компјутерска мрежа и кои користат IP протокол. IP адресата има две главни функции: идентификација на мрежниот интерфејс и адресирање на локацијата. Нејзината улога е опишана на следниот начин: „името покажува што бараме, адресата покажува каде тоа се наоѓа, патот покажува како се стигнува до целта". IP адресата, всушност, може да се сфати како интернет „телефонска линија". Без IP адреса не е можно да се пристапи кон Интернет. IP не претставува секогаш егзактен начин за идентификација. IP адресите спаѓаат во две категории, во зависност од понудата на провајдерот:

- Статички – остануваат исти при секој пристап на интернет.
- Динамички – се менуваат секој пат кога корисникот пристапува кон Интернет

За утврдување на корисникот на IP адресата во критичниот момент од исклучително значење претставува точното време на пристап до интернет. Податоците за точното време на пристап, како и временската зона ги обезбедува провајдерот на услугата.

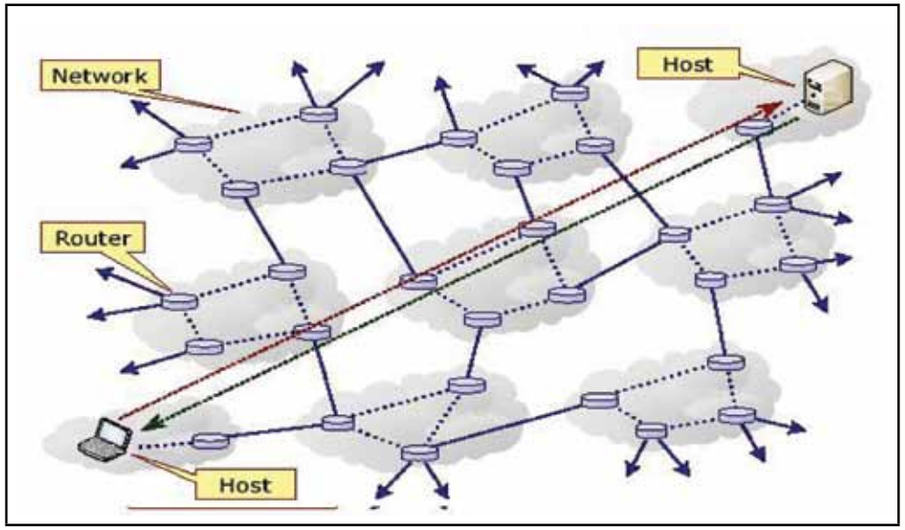
5.5. Поврзување на Интернет

Повеќето корисници се поврзуваат користејќи услуги на одреден снабдувач на интернет услуги (Internet Service Provider – ISP). Поврзувањето може да биде преку телефонска (Dial-up) линија, широкопојасен (Broadband, ADSL), дигитална мрежа за интегрирани услуги (Integrated Services Digital Network – ISDN), провајдер на Кабловска ТВ, безжична мрежа (WiFi), или сателитска врска.

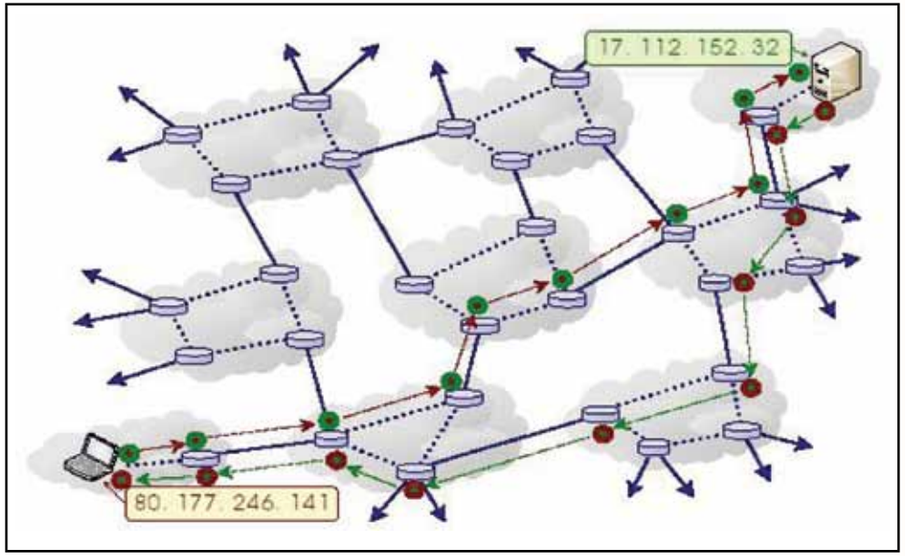
- *Снабдувачи на интернет услуги*

Internet Service Provider (ISP) се комерцијални организации кои овозможуваат/изнајмуваат пристап до Интернет. Се проценува дека ги има повеќе од 14,000 низ светот. ISP водат евиденција за користењето на интернетот под услови кои се различни во различни национални законодавства. Според легислативата во Република Македонија, ISP се должни да ги чуваат податоците во рок од две години.

Интернет - идеален приказ



Интернет - реален приказ



- *Униформни локатори за ресурси - URL*

URL претставува низа на знаци која е референца за одреден ресурс. На пример веб страницата http://www.jorm.org.mk

- *http://* - Се однесува на Интернет протоколот кој се користи (hypertext transfer protocol)
- *www.* - Се однесува на World Wide Web серверот
- *jorm.* – го претставува името на домејнот и се однесува на сопственикот на страницата
- *org.mk* - Се однесува на највисокото ниво на домејнот (Top Level Domain - TLD) кој се користи (најчесто кодот на земјата)

6. СЕРВЕРИ

Web servers (веб сервери) - претставуваат компјутери кои овозможуваат (даваат услуга на) пристап до веб страни. Секој веб сервер има IP адреса и евентуално домејн. На пример, доколку го внесете униформниот локатор за ресурси (URL) http://www.jorm.org.mk/index.html во вашиот пребарувач, се испраќа барање до веб серверот чиј домејн е jорм.org.mk. Серверот понатаму ја зема страницата насловена како index.html и ја испраќа до вашиот пребарувач.

Секој компјутер може да стане веб сервер доколку му се инсталира серверски софтвер и доколку се поврзе на интернет. Постојат повеќе софтверски апликации за веб сервери, како на пример: разни комерцијални пакети на Microsoft, Netscape итн.

Со цел да се конектирате кон некоја веб страница, морате да се логирате. Сите компјутерски системи креираат и чуваат записи од конекциите т.н. колачиња (cookies) кои содржат информации за:

- Идентитетот на корисникот (IP адресата)
- Датумот и времето кога е пристапено
- Содржината која е барана
- Колку долго е гледана бараната содржина
- Пребарувач од кој е пристапувано
- Оперативен систем кој го користел компјутерот
- Како е пристапено кон таа страница

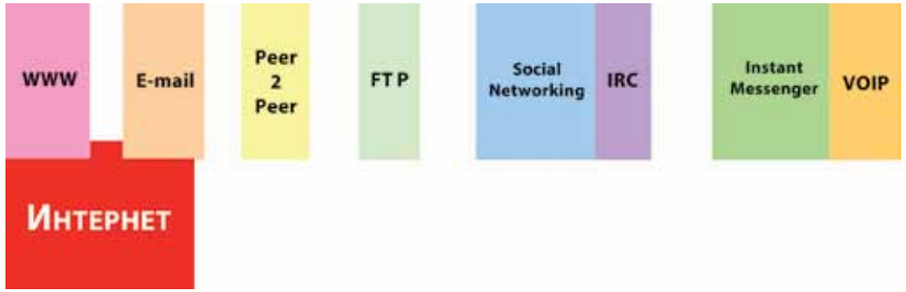
Proxy сервер - претставува сервер (компјутерски систем или апликација) кој делува како посредник за барањата од клиентите кои бараат ресурси (податоци, информација, документи итн) од други сервери. Ваквите сервери го контролираат барањето и овозможуваат пристап до бараниот ресурс. Денес повеќето proxy сервери се www proxy сервери кои обезбедуваат пристап на содржини на *www* и притоа му овозможуваат анонимност на корисникот.

Пример:

218.12.171.14 - [15/Feb/2009:16:08:43+0100] "GET/test.html HTTP/1.0" 200 1921 www.technologyrisklimited.co.uk "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)" "-"Ако е "анонимна" тогаш примачот ја гледа 218.12.171.14 и - Ако е 'транспарентна' тогаш примачот ја гледа 218.12.171.14 но и 212.99.110.242

Cloud Computing - претставува вид на сервис кој се заснова на заеднички (споделени) компјутерски ресурси, а не на услугата на локален сервер или личен уред при користењето на апликациите. При cloud computing, зборчето "cloud" се користи како метафора за "интернетот", па оттука фразата "*cloud computing*" значи "вид на комјутерско работење на интернет" каде различни услуги (сервери, складирање на податоци и апликации) се пренесуваат до компјутерите и уредите на организацијата или институцијата преку интернет.

7. ВИДОВИ КОМУНИКАЦИЈА МЕЃУ КОРИСНИЦИТЕ



Peer to Peer сервисите долго време обезбедувале трансфер на нелегални фајлови како и фајлови кои се предмет на правото на интелектуална сопственост. Peer to peer клиентите се познати помеѓу криминалните групи кои се инволвирани во овие активности. Првата генерација на peer-to-peer архитектура функционирала врз основа на принципот на користење на централизиран сервер за кој луѓето се конектирале со цел да симнуваат фајлови. На овој начин била извршена идентификација на лицата кои нуделе нелегални сервиси кои многу лесно можеле да се лоцираат и да се спречат. Втората генерација на peer to peer клиенти користеле поинакви методи за конектирање од оние кои имале листа на достапни фајлови кои се полесни за пребарување во однос на оние кои се однесувале како суперјазли со кои се вршело идентификација за достапните фајлови.

File Transfer Protocol (FTP) е протокол кој овомножува трансфер на фајлови од еден компјутер кон друг. Функционира врз основа на клиент/сервер логика со FTP програма која е инсталирана на клиентот овозможувајќи му на корисникот да комуницира со серверот со цел да добие пристап до сервисите и информациите на серверот. Кога корисникот сака да изврши трансфер на фајл, се креира TCP конекција до таргетниот систем. Корисничкиот ID и лозинката можат да се пренесуваат и корисникот може да изврши спецификација на фајловите и потребната активност. Кога е доделена дозвола за трансфер на фајлови, се креира уште една TCP конекција за податоците кои треба да се пренесат.

Internet Relay Chat Internet Relay Chat (IRC) е систем за телеконференција кој се уште постои, но најчесто се користи од страна на криминалците за комуникација и размена на фајлови. Функционира врз основа на серија од сервери кои се меѓусебно поврзани и делат текстуални пораки кои се испраќаат во "канали", виртуелни соби за состаноци. Наведени се темите за дискусија и клиентите кои имаат IRC клиент можат да се конектираат до еден или повеќе канали и да започнат дискусија со истомисленици. IRC не

е најчестиот "user friendly" сервис кој се користи на Интернет и најчесто го користат постари корисници со поголемо искуство.

VoIP (Voice over Internet Protocol) е алатка која обезбедува гласовна комуникација преку трансфер на data пакети со помош на интернет комуникација (Skype, Viber и сл.).

Social Networking Instant Messaging и Social Networking го завземаа местото на алатките за комуникација во последните години, со добро познати примери за брз и "user friendly" пристап до други корисници ширум светот. Главната функција на овие сајтови е можноста за креирање на личен профил и можноста за споделување на лични информации и запознавање на нови луѓе. Постои можност и за споделување на фотографии, музика и видео записи. Нивото на личните податоци кои лицата ги споделуваат, може да ги направи мета на криминалци, како на пример оние кои се вмешани во кражба на лични податоци и злоупотреба на деца. Страниците за Social Networking се многу корисно средство за спроведување на законот со собирање на информации за осомничените и нивните нелегални активности.

Instant messaging е форма на директна "real time" комуникација помеѓу две или повеќе лица кои користат делени клиенти. Овој тип на комуникација вклучува контакт помеѓу лица кои се знаат, за разлика од другите типови кои овозможуваат комуникација помеѓу непознати лица. Криминалците се познати по користењето на Instant messaging како метод за комуникација.

Twitter претставува социјално вмрежување и "micro-blogging" сервис кој им овозможува на своите корисници да испраќаат и да ги читаат "update"-те на другите корисници (попознати како tweet-ови), кои претставуваат текстуални пораки со максимална должина од 140 карактери. Има преку 5 милиони корисници во САД, Канада, Индија, Велика Британија и Јапонија.

Онлајн игра е игра која се игра преку некој вид на компјутерска мрежа. Ова речиси секогаш подразбира Интернет или некоја еквивалентна технологија, но игрите секогаш ја користат последната технологија; модемите пред Интернет и жичаните терминали пред модемите. Експанзијата на online gaming е одраз на целокупната експанзија на компјутерските мрежи од мали локални мрежи на Интернет и самиот пораст на пристап до Интернет. Онлајн игрите вариираат од едноставни текстуални игри до игри во кои се применува комплексна графика и виртуелни светови со многу играчи истовремено. Многу онлајн игри се поврзани со многу онлајн заедници, правејќи ги онлајн игрите како форма на социјална дејност.

Електронска порака (e-mail) – Вообичаено електронската порака поминува преку најмалку четири компјутери за време на нејзиното време на живот. Пораката се составува на корисничкиот компјутер, потоа се испраќа до

излезниот SMTP (Simple Mail Transfer Protocol[25]) мејл сервер на ISP. Излезниот ISP ја препраќа електронската порака до ISP SMTP мејл серверот (SMTP – SMTP) на примачот. Мејл серверот на примачот го пронаоѓа појдовниот мејл сервер на примачот (Post Office Protocol или POP3) и ја испраќа пораката кон "инбоксот (сандачето) на примачот". Корисникот се логира на својата корисничка сметка и пораката се наоѓа во неговиот инбокс (сандаче), која се брише во мејл серверот кој послужил во овој процес.

Електронската порака се состои од **Header (коверт) и Body (текст).** Header-от содржи информации за испраќачот, примачот IP адресите, мејл серверите, временски ознаки итн. Body-то ја претставува содржината на електронската порака и прилозите.

- *Различни видови на електронска пошта:*

Traditional e-mail (традиционален вид електронска пошта) – карактеристично е што се отвара со програма/апликација (на пр. Microsoft Outlook) веднаш по симнувањето, се наоѓа во компјутерот и до него не може да се пристапи од друг компјутер**.**

Web based e-mail (Веб-базирана електронска пошта) – се гледа преку компјутерот, но се наоѓа на оддалечен (remote) сервер. Ваквата електронска пошта може да се организира во папки, но единствено е видлива кога корисникот е онлајн.

Анонимни e-mail сервиси - Нудат можност за испраќање на анонимна електронска пошта. Сервисот е бесплатен и целосно анонимен, не врши проверка и зачувување на вашите податоци, не се зачувуваат копии од фајлови на серверот. Пример за вакви сервиси се: cotse.com; anonymizer.com; hushmail.com и слично.

[25] Мејл сервер – компјутер наменет за управување со е-пошта

8. ВИДОВИ ИНТЕРНЕТ ИЗМАМИ

Инвестициски шеми - користење на Интернет за давање финансиска поддршка за високи технички шеми како сајтови за виртуелен шопинг или провајдери на нови сервиси;

Шеми за кредитни картички - користење на незаконски добиени детали на кредитни картички за купување на производи со висока вредност преку Интернет;

Можности за бизнис/шеми за работа од дома - користење на Интернет за рекламирање на бизнис можности со кои жртвата плаќа однапред за информацијата или производот за работа;

Нигериска измама (т.н. Измами 419) - западно-африкански измами со променет начин на достава. Сега е електронска порака наместо традиционална пошта или факс. Останатиот пристап е ист и постои потенцијално голема можност за спамирање.

Интернет банкарство - се копира веб страната на некоја банка, во мала мера се менува веб адресата, се обезбедуваат линкови до легални банкарски сервиси и само еден или два линкови се за големи инвестиции кои бараат трансфер на значителни суми со цел да се осигура вклучување во вистински неверојатна можност за инвестиции.

Катастрофални повици за доброволни прилози - најголемиот дел од веб страните кои бараат помош за жртвите од цунамито на Далечниот Исток се лажни;

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

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

Добивки на лотарија - барање за исплата на добивки од лотарија или помош за освојување на победа (најчесто странски лотарии);

Phishing - електронска пошта која личи како да е од добро познат извор (на пример банка или интернет сервис провајдер) со која се бара да се потврдат личните податоци.

9. ШТЕТНИ СОФТВЕРИ

Малвер (malware) - кратенка од малициозен софтвер, е општ термин со кој се означува широк спектар непријателски или инвазивен софтвер, т.е. софтвер кој се употребува со цел да се попречи функционирањето на компјутерот, да се добијат чувствителни информации, или да се оствари пристап до приватни компјутерски системи. Може да биде во облик на код, скрипта, активна содржина и други видови софтвер.

Во малвер се вбројуваат компјутерските вируси, црви, тројанци, руткитови, спајвер, адвер, и други малициозни програми. Поголемиот дел активни малвер закани се, обично, тројанци или црви, а помал дел се вируси. Некои малвер програми можат да бидат маскирани да изгледаат како легитимен софтвер и дури може да дојдат од официјалната веб страница на некоја компанија во форма на корисна или привлечна програма во која е всаден малверот заедно со софтвер за следење кој прибира статистички податоци за маркетиншки потреби.

- *Најчести видови на малвери се:*

Компјутерски вирус е еден вид на малициозен софтвер кој, кога ќе се изврши, се реплицира со вметнување копии од себе (можеби модифицирани) во други компјутерски програми, датотеки со податоци, или boot секторот на хард дискот. Кога таа репликација успева за погодените области се вели дека се "заразени". Вирусите често претставуваат штетна активност на инфицираниот домаќин, на пример, кражба на простор на хард дискот или процесорот, пристап до приватни информации, corrupting податоци, прикажување на политички или хумористични пораки на екран на корисникот, спамирање на нивните контакти или влез нивните кратенки. Сепак, не сите вируси носат деструктивен елемент. Дефинирачката карактеристика на вирусите е дека тие се само-реплицирани компјутерски програми кои се инсталираат без согласност на корисникот.

Тројански коњ (Trojan horse) или „тројанец" е малициозен софтвер кој не се реплицира самиот и кој изведува дејства одредени од неговата природа, па вообичаено резултира со губиток или кражба на податоци и, веројатно, оштетување на системот. Овој вид малвер честопати функционира преку т.н. „социјален инженеринг", претставувајќи се како рутинска, корисна или интересна програма или код со цел да се убедат жртвите да ја инсталираат на нивните компјутери. Често, тројанецот делува како заден влез, по што неговиот креатор може да оствари неавторизиран пристап до инфицираниот компјутер. Тројанците не се лесно препознатливи но, доколку изведуваат значителни компјутерски или комуникациски активности, можат забележително да ја забават работата на компјутерот. Тројанците не се обидуваат да се всадат во други програми или податоци како вирусите и не се реплицираат како црвите.

Дистрибуиран напад за одбивање услуга (DISTRIBUTED DENIAL-OF-SERVICES - DDoS) или DDoS напад е обид компјутерот или одреден мрежен ресурс да се направи недостапен за целните корисници. Иако средствата за извршување на DDoS напад, како и мотивите и целите можат да варираат, овој вид на напад обично се состои од напорите привремено или на неодредено време да го прекинат или суспендираат давањето услуги на уредот кој е поврзан на интернет. Извршителите на DoS напади, обично, ги имаат за цел сајтовите или услугите сместени на веб сервери од висок профил како што се банките, порталите за исплата од кредитни картички, па дури и серверите одговорни за TLD. Оваа техника денес најшироко се употребува кај одредени игри или се користи од страна на сопствениците на серверите или, пак, од страна на незадоволните конкуренти. Сè почесто, DoS нападите, исто така, се користат и како облик на отпор. За DoS се вели дека е алатка за изразување несогласување или, според некои аналитичари, DoS е форма на "улични протести на интернет". Терминот генерално се користи во врска со компјутерски мрежи, но не е ограничен само на ова поле. На пример, тој се користи и во однос на управувањето со ресурсите на главниот процесор. Вообичаен метод на напад вклучува „заситување" (сатурација) на целната машина со надворешни барања за комуникација во толкав обем што таа не може да одговори на легитимните барања за сообраќај или, пак, реагира толку бавно што, во суштина, станува недостапна. DoS нападите, обично, доведуваат до преоптоварување на серверот. Во општи црти, DoS нападите се изведуваат така што се принудува целниот компјутер да се ресетира или да ги конзумира своите ресурси така што повеќе не може да ги обезбеди своите наменети услуга или се попречува медиумот за комуникација помеѓу легитимните корисници и жртвата , така што тие не комуницираат соодветно. Denial-of-service нападите се сметаат за прекршување на правилната политика за користење на интернет креирана од страна на Одборот за интернет архитектура (Internet Architecture Board - IAB), а ги повредуваат и политиките за прифатливо користење на, речиси, сите интернет провајдери. Тие, исто така, најчесто претставуваат и повреда на законите во некои земји.

Worms (Црви) – се малициозни програми кои се разможуваат во ситемот. Нивната цел е да овозможат неправилно работење на системот согласно желбата на лицето кое го креирало овој малициозен код, односно да пропуштаат одредена информација која би влегла или излегла од системот без негова дозвола.

Firewall - е хардвер уред или софтвер програма која овозможува да се добие поголем степен на сигурност во мрежата. Неговата задача е да блокира или овозможи движење на податоците низ мрежата. Најчеста задача му е да го блокира влезот на податоци низ портови кои не се наменети за тие податоци, односно да овозможи сообраќајот на податоците да биде низ точните портови, а останиот сообраќај да го блокира.

- *Најчесто користени термини за платежни картички*

Skimers се апарати кои се користат за неовластено прибирање на податоци од платежни картичи и тоа податоци кои се наоѓаат на магнетната лента на платежната картичка и податоци за ПИН (Personal identification number) кодот од картичката. Постојат два вида на скимери: а) фиксни кои се монтираат на АТМ-и (банкомати) и б) мобилни кои го читаат само записот од магнетната лента. Скимерите во себе содржат повеќе компоненти и тоа:

- читач на податоците од магнетната лента,
- видео камера за видео запис од видео надзорот на делот на апаратот на кој се користи платежната картичка, а е во делот каде што се внесува ПИН кодот (авторизационен клуч) за употреба на платежната картичка.

Скимерите во себе содржат медиум за зачувување на податоците кои се добиени од останите негови делови. Читачот на податоци од магнетната лента на платежната картичка е во облик на влезниот сегмет на АТМ-от и низ него незабележано минува платежната картичка. Читањето на податоците може да биде:

- аудио читање (кога при влезот на платежната картичка во АТМ-от, се слуша звук на отчитување кој всушност претставува аудио комуникација меѓу АТМ-от и платежната картичка и во тој момент се слуша кодот кој е запишан на платежната картичка) и
- кога на скимерот директно се впишува содржината од платежната картичка и се зачувува на медиум кој е составен дел од скимерот. Вториот дел е видео камера насочена кон тастатурата каде што се внесува кодот за авторизација при што визулено се детектира и се запишува на медиумот овој код.

Потоа, овие податоци се внесуваат во компјутер и со посебна програма податоците од магнетната лента добиваат формат погоден за внесување на друга магнетна лента како магнетен запис. Следниот чекор е споредба со видео записот за бројот кој е внесен како авторизација.

Мобилните збирачи на податоци (mobile skimmers) се уреди кои криминалците ги инсталираат во терминали за плаќање или исплата (point of sale – POS терминали) или банкомати и кои ги копираат податоците за сметката на корисникот на вметнатата платежна картичка од магнетната лента на задната страна на картичката. Доколку корисникот користи дебитна платежна картичка, заедно со споменатите податоци се копира и личниот идентификациски број на корисникот (personal identification number - PIN). Копираните податоци подоцна се користат за изработување фалсификувани кредитни или дебитни платежни картички за повлекување пари од банкомати.

Plastic е секоја пластична картичка која има стандардна големина и на која има внесена магнетна лента, на која може да се внесе магнетен запис. Не е од значење предната страна на пластичните катички да биде пополнета и дизајнирана доколку истата се користи за АТМ.

MSR 206 е апарат со кој се внесуваат податоци од платежна картичка на магнетната лента на пластичната картичка.

Магнетна лента на платежната картичка е лента на која се внесуваат податоците на банката издавач на платежната картичка, бројот на сметката во банката и името на лицето кое е носител на платежната картичка. Интересно за неа е што може да бидат впишувани и бришени податоци во неограничен број пати.

10. ЗАВРШНИ СОГЛЕДУВАЊА НА АВТОРИТЕ

Правото на фер и правично судење е неповредливо и затоа обвинителот има обврска и одговорност за навремено обезбедување, заштита и презентирање на електронските докази пред судот. Тоа ја детерминира проактивната улога на обвинителот, кој сега, имајќи ја предвид неговата нова позиција во текот на истрагата, мора да поседува соодветни познавања и од областа на компјутерскиор криминал.

Обвинителот мора да знае како функционираат компјутерот и интернет мрежите, како да ги разбере извештаите на експертите од оваа област и мора да знае во која насока и на кој начин ќе ја води истрагата и какви задолженија ќе упатува до правосудната полиција. Во текот на целата постапка, обвинителот треба да поседува знаење и вештина за начинот на кој ќе врши супервизија на собраните докази, како да ги заштити и обезбеди, особено ако доказите се обезбедувани надвор од нашата јурисдикција. Од обвинителската подготвеност и стручност ќе зависи и исходот на постапката.

Токму затоа обвинителот, работејќи заедно со правосудната полиција мора да ги максимализира напорите за обезбедување на електронските докази кои ќе бидат основа за градење на силен и добро претставен случај во судот.

Напредната технологија подразбира и зголемување на бројот на уреди кои можат да содржат електронски докази. Затоа секој кој е вклучен во процесот на откривање на овој вид криминал мора да знае дека листата на потенцијални докази, опрема и уреди кои содржат електронски информации и кои можат да функционираат поединечно или споено со компјутерскиот систем секојдневно се проширува.

Ваквиот процес подразбира постојано осовременување на законските прописи кои мора да го следат брзото темпо на развивање на нови форми на овој криминал, а со тоа и нивно соодветно нормирање и санкционирање.

Овој прирачник е основно помагало при секојдневното постапување кој содржински опфаќа основни - општи поими од областа на компјутерскиот криминал, но тоа не значи и континуирана обврска за едукација на обвинителот.

Прилог 1

Одредби од Кривичниот законик кои се однесуваат на компјутерски криминал

Член 144

Тој што по пат на информатички систем ќе се закани дека ќе стори кривично дело за кое е пропишана казна затвор од пет години или потешка казна против некое лице поради неговата припадност кон определена национална, етничка или расна група или верска определба

Член 149

(1)Тој што спротивно на условите утврдени со закон без согласност на граѓанинот прибира, обработува или користи негови лични податоци, ќе се казни со парична казна или со затвор до една година.

(2) Со казна од став 1 се казнува тој што ќе навлезе во компјутерски информатички систем на лични податоци со намера користејќи ги за себе или за друг да оствари некаква корист или на друг да му нанесе некаква штета.

Член 149-а

(1) Тој што неовластено спречува или ограничува друг во пристапот кон јавен информатички систем, ќе се казни со парична казна или со затвор до една година.

(2) Ако делото од став 1 го стори службено лице во вршење на службата или одговорно лице во јавен информатички систем, ќе се казни со парична казна или со затвор од три месеци до три години.

(3) Ако делото од став 1 го стори правно лице, ќе се казни со парична казна.

(4) Гонењето се презема по приватна тужба.

Член 157

(1) Тој што во свое име или во име на друг неовластено ќе објави, прикаже, репродуцира, дистрибуира, изведе,емитува или на друг начин неовластено ќе посегне по туѓо авторско право или сродно право,односно авторско дело, изведба или предмет на сродно право, ќе се казни со парична казна или со затвор до една година.

(2) Тој што со делото од став 1 прибавил поголема имотна корист, ќе се казни со затвор од три месеци до три години.

(3) Тој што со делото од став 1 прибавил значителна имотна корист, ќе се казни со затвор од шест месеци до пет години.

(4) Обидот е казнив.

(5) Примероците на авторските дела и предметите на сродните права, како и средствата за репродуцирање се одземаат.

(6) Ако делото од став 1 го стори правно лице, ќе се казни со парична казна.

Член 157-а

(1) Тој што без одобрение од овластениот дистрибутер на технички посебно заштитен сателитски сигнал произведува, увезува, дистрибуира, изнајмува или на друг начин става на располагање на јавноста, односно дава услуги на поставување на материјален или нематеријален уред или систем заради пробивање на таков сигнал, ќе се казни со затвор од шест месеци до три години.

(2) Ако со делото од став 1 е прибавена значителна имотна корист или е предизвикана значителна штета, ќе се казни со затвор од една до пет години.

(3)Тој што прима технички посебно заштитен сателитски сигнал чија заштита е пробиена без одобрување на неговиот овластен дистрибутер или врши натамошна дистрибуција на таквиот сигнал, ќе се казни со затвор од шест месеци до три години.

(4) Ако со делото од став 3 е прибавена значителна имотна корист или е предизвикана значителна штета, ќе се казни со затвор од една до пет години.

(5) Ако делото од овој член го стори правно лице, ќе се казни со парична казна.

(6) Предметите кои биле наменети или користени за сторување на делото или кои настанале со сторувањето на делото се одземаат.

Член 157-б

(1) Тој што без одобрение на филмскиот продуцент или овластениот дистрибутер на кој филмскиот продуцент му го пренел своето право на аудиовизуелното дело произведува, увезува, репродуцира, дистрибуира, ускладиштува, изнајмува, пушта во промет или на друг начин става на располагање на јавноста, или презема други дејствија заради дистрибуција,

изнајмување, јавно прикажување, пуштање во промет, ставање на располагање на јавноста или на друг начин противправно го користи аудиовизуелното дело, односно видеограмот или неговите неовластено умножени примероци, ќе се казни со затвор од шест месеци до три години.

(2) Ако со делото од став 1 е прибавена значителна имотна корист или е предизвикана значителна штета, ќе се казни со затвор од една до пет години.

(3) Ако делото од овој член го стори правно лице,ќе се казни со парична казна.

(4) Предметите кои биле наменети или користени за сторување на делото или кои настанале со сторувањето на делото се одземаат

Член 157-в

(1) Тој што без одобрение од производителот на фонограм или здружението за колективно остварување на правата на производителите на фонограми произведува, репродуцира, дистрибуира, ускладиштува, изнајмува, пушта во промет или на друг начин става на располагање на јавноста, или презема други дејствија заради дистрибуција, изнајмување, пуштање во промет, ставање на располагање на јавноста или на друг начин противправно го користи фонограмот или неговите неовластено умножени примероци, ќе се казни со затвор од шест месеци до три години.

(2) Ако со делото од став 1 е прибавена значителна имотна корист или е предизвикана значителна штета, ќе се казни со затвор од една до пет години.

(3) Ако делото од овој член го стори правно лице,ќе се казни со парична казна.

(4) Предметите кои биле наменети или користени за сторување на делото или кои настанале со сторувањето на делото се одземаат.

Член 193-а

(1) Тој што произведува детска порнографија со цел за нејзина дистрибуција или ја пренесува или ја нуди или на друг начин ја прави достапна детската порнографија, ќе се казни со затвор од најмалку пет години.

(2) Тој што набавува детска порнографија за себе или за друг или поседува детска порнографија, ќе се казни со затвор од пет до осум години.

(3) Ако делото од ставовите (1) и (2) на овој член е сторено преку компјутерски систем или друго средство за масовна комуникација, сторителот ќе се казни со затвор од најмалку осум години.

(4) Ако делото од овој член го стори правно лице, ќе се казни со парична казна.

Член 193-б

Тој што преку компјутерско-комуникациски средства со закажување средба или на друг начин намамува малолетник кој не наполнил 14 години на обљуба или друго полово дејствие или на производство на детска порнографија и ако со таквата намера е остварена непосредна средба со малолетникот, ќе се казни со затвор од една до пет години.

Член 251

(1) Тој што неовластено ќе избрише, измени, оштети, прикрие или на друг начин ќе на-прави неупотреблив компјутерски податок или програма или уред за одржување на информатичкиот систем или ќе го оневозможи или отежне користењето на компјутерски систем, податокот или програмата или на компјутерска комуникација, ќе се казни со парична казна или со затвор до три години.

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

(3) Со казната од ставот (1) на овој член ќе се казни тој што неовластено ќе пресретне, со употреба на технички средства, пренос на компјутерски податоци кој нема јавен карактер до, од и внатре во одреден компјутерски систем, вклучувајќи и електромагнетни емисии од компјутерски систем кој поддржува такви компјутерски податоци.

(4) Тој што делата од ставовите (1), (2) и (3) на овој член ќе ги стори спрема компјутерски систем, податоци или програми што се заштитени со посебни мерки на заштита или се користат во работењето на државни органи, јавни претпријатија или јавни установи или во меѓународни комуникации, или како член на група создадена за вршење такви дела, ќе се казни со затвор од една до пет години.

(5) Ако со делото од ставовите (1), (2) и (3) на овој член е прибавена поголема имотна корист или е предизвикана поголема штета, сторителот ќе се казни со затвор од шест месеци до пет години.

(6) Ако со делото од став (4) е прибавена поголема имотна корист или е предизвикана поголема штета, сторителот ќе се казни со затвор од една до десет години.

(7) Тој што неовластено изработува, набавува, продава, држи или прави достапни на друг посебни направи, средства, компјутерска лозинка, код за пристап и сличен податок со кој целината или дел од компјутерскиот систем се оспособува за пристап, компјутерски програми или компјутерски податоци наменети или погодни за извршување на делата од ставовите (1), (2) и (3) на овој член, ќе се казни со парична казна или со затвор до една година.

(8) Обидот за делото од ставовите 1 и 2 е казнив.

(9) Ако делото од овој член го стори правно лице, ќе се казни со парична казна.

(10) Посебните направи, средства, компјутерски програми или податоци наменети за извршување на делото ќе се одземат.

Член 251-а

(1) Тој што ќе направи или ќе преземе од друг компјутерски вирус со намера за внесување во туѓ компјутер или компјутерска мрежа, ќе се казни со парична казна или со затвор до една година.

(2) Тој што со употреба на компјутерски вирус ќе предизвика штета во туѓ компјутер, систем, податок или програма, ќе се казни со затвор од шест месеци до три години.

(3) Ако со делото од став 2 е предизвикана поголема штета или делото е сторено во состав на група создадена за вршење такво дело, сторителот ќе се казни со затвор од една до пет години.

(4) Обидот за делото од став 2 е казнив.

(5) Ако делото од овој член го стори правно лице, ќе се казни со парична казна.

Член 251-б

(1) Тој што со намера за себе или за друг да прибави противправна имотна корист со внесување во компјутер или информатички систем невистинити податоци, со невнесување на вистинити податоци, со менување, бришење или прикривање на компјутерски податоци, со фалсификување на електронски потпис или на друг начин ќе предизвика невистинит резултат при електронската обработка и преносот на податоците, ќе се казни со парична казна или со затвор до три години.

(2) Ако сторителот прибавил поголема имотна корист, ќе се казни со затвор од три месеци до пет години.

(3) Ако сторителот прибавил значителна имотна корист, ќе се казни со затвор од една до десет години.

(4) Тој што делото од став 1 ќе го стори само со намера да оштети друг, ќе се казни со парична казна или со затвор до една година.

(5) Ако со делото од став 4 е предизвикана поголема штета, сторителот ќе се казни со затвор од три месеци до три години.

(6) Тој што неовластено изработува, набавува, продава, држи или прави достапни на друг посебни направи, средства, компјутерски програми или компјутерски податоци наменети за извршување на делото од став 1, ќе се казни со парична казна или со затвор до една година.

(7) Обидот за делото од ставовите 1 и 4 е казнив.

(8) Ако делото од овој член го стори правно лице, ќе се казни со парична казна.

(9) Посебните направи, средства, компјутерски програми или податоци наменети за извршување на делото ќе се одземат.

(10) За делото од став 4 гонењето се презема по приватна тужба.

Член 271

(1) Тој што прави, набавува, продава или дава на употреба средства за правење лажни знаци за вредност, ќе се казни со парична казна или со затвор до една година.

(2) Тој што неовластено изработува, набавува, држи, продава или дава на употреба инструменти, предмети, компјутерски програми и други сигурносни заштити или компоненти кои служат за заштита против фалсификување, како и средства за неовластено прибавување на банкарски податоци, заради правење лажни пари или преправање на вистински пари или, други инструменти за плаќање, хартии од вредност или лажни платежни картички ќе се казни со затвор од три до десет години.

Член 274-б

(1) Тој што ќе направи лажна платежна картичка со намера да ја употреби како вистинска, или прибавува лажна картичка со таква намера, или ќе му ја

даде на друг на употреба или тој што лажната картичка ќе ја употреби како вистинска,ќе се казни со затвор од шест месеца до пет години и со парична казна.

(2) Со казната од ставот (1) на овој член ќе се казни и тој што прибавува банкарски податоци од вистински платежни картички и податоци за носители на тие платежни картички со намера да ги искористи за изработка и употреба на лажна платежна картичка или вака прибавените податоци ги дава на друг со таква намера.

(3) Ако сторителот од ставот (1) на овој член стекне поголема имотна корист, ќе се казни со затвор од една до осум години.

(4) Ако делото од ставовите (1), (2) и (3) на овој член е сторено од член на група, банда или друго злосторничко здружение, сторителот ќе се казни со затвор најмалку четири години.

(5) Ако делото од овој член го стори правно лице ќе се казни со парична казна.

Член 286

(1) Тој што со намера да оштети друг или да прибави противправна имотна корист неовластено ќе поднесе пријава на патент или во пријавата нема да го наведе или лажно ќе го наведе пронаоѓачот или ќе ја направи достапна на јавноста суштината на пронајдокот пред тој да биде објавен на начин утврден со закон, ќе се казни со парична казна или со затвор до три години.

(2) Со казната од ставот (1) на овој член ќе се казни и тој што со намера да оштети друг или да прибави противправна имотна корист неовластено ќе произведе, пушти во промет, увезе, извезе, понуди на продажба, складишти или користи производ или постапка која е предмет на заштита со патент или неовластено ќе употреби, репродуцира, увезе, извезе или дистрибуира заштитена топографија на интегрално коло или софтвер.

(3) Тој што со делото од ставовите (1) и (2) на овој член прибавил значителна имотна корист или предизвикал значителна имотна штета, ќе се казни со затвор од една до пет години и парична казна.

(4) Ако делото од ставовите (1) и (2) на овој член е сторено од организирана група или со делото е предизвикана опасност за животот и здравјето на луѓето, сторителот ќе се казни со парична казна или со затвор од најмалку три години.

(5) Ако делото од овој член го стори правно лице, ќе се казни со парична казна.

(6) Предметите кои се направени или употребени за извршување на кривичното дело ќе се одземат.

Член 379-а

(1) Тој што со намера да ги употреби како вистински неовластено ќе изработи, внесе, измени, избрише или направи неупотребливи компјутерски податоци или програми што се одредени или подобни да служат како доказ за факти што имаат вредност за правните односи или тој што таквите податоци или програми ќе ги употреби како вистински, ќе се казни со парична казна или со затвор до три години.

(2) Ако делото од став 1 е сторено во однос на компјутерски податоци или програми што се користат во работењето на државни органи, јавни установи, претпријатија или други правни и физички лица кои вршат работи од јавен интерес или во правниот сообраќај со странство или ако со нивната употреба е предизвикана значителна штета,сторителот ќе се казни со затвор од една до пет години.

(3) Тој што неовластено изработува, набавува, продава, држи или прави достапни на друг посебни направи, средства, компјутерски програми или компјутерски податоци наменети или погодни за извршување на делото од став 1, ќе се казни со парнична казна или со затвор до три години.

(4) Обидот за делото од ставовите 1 и 3 е казнив.

(5) Посебните направи, средства, компјутерски програми или податоци за извршување на делото, ќе се одземат.

Член 394-г

(1) Тој што преку компјутерски систем во јавноста шири расистички и ксенофобичен пишан материјал, слика или друга презентација на идеја или теорија која помага, промовира или поттикнува омраза, дискриминација или насилство, против кое било лице или група, врз основа на раса, боја на кожа, национално или етничко потекло, како и верско уверување, ќе се казни со затвор од една до пет години.

(2) Со казната од ставот (1) на овој член ќе се казни и тој што делото ќе го стори преку други средства за јавно информирање.

(3) Тој што делото од ставовите (1) и (2) на овој член го врши со злоупотреба на положбата или на овластувањето или ако поради тие дела дошло до безредие и насилства спрема луѓе или до имотна штета од големи размери, ќе се казни со затвор од една до десет години.

Прилог 2

Процесни одредби од Конвенцијата за компјутерски криминал

Оддел 2 - Процесно право

Наслов 1 - Општи одредби

Член 14 - Опфатот на процесните одредби

(1) Секоја Страна ќе усвои такви законодавни и други мерки кои се неопходни за да се воспостават овластувања и постапки предвидени во овој оддел со цел да се овозможи преземањето на посебни истражни дејствија и постапки.

(2) Освен во случаите кога изрично е предвидено поинакво постапување, како во случаите предвидени со одредбата од членот 21, секоја Страна ќе ги воведе овластувања и ќе ги спроведува процесни дејствија предвидени со став 1 од овој член во однос на:

а. кривичните дела предвидени во членовите 2 до 11 од оваа Конвенција;

б. останатите кривични дела сторени со помош на компјутерски систем; и

ц. прибирањето докази во електронска форма за одредено кривично дело;

(3)

а. Секоја Страна може да стави резерва во поглед на примената на мерките предвидени во членот 20 само во поглед на делата или видовите на дела кои се точно определени во нејзината резерва, под услов опсегот на тие дела или видови на дела да не е потесен во споредба со опсегот на делата во однос на кои ќе се применуваат мерките предвидени со член 21. Секоја Страна ќе ги разгледа ограничувањата содржани во нејзината резерва за да се овозможи широка примена на мерките предвидени во член 20.

б. Кога Страната, поради ограничувањата предвидени со домашното законодавство кое е во сила во моментот на усвојување на оваа Конвенција, не е во можност да ги применува мерките предвидени со членовите 20 и 21 во однос на комуникациите кои се пренесуваат внатре во компјутерскиот

систем на одреден провајдер на услуги, кој систем:

i опслужува и се користи од мала група на корисници; и

ii кој не се однесува на јавните комуникациски мрежи и не е поврзан со друг компјутерски систем, било јавен или приватен, тогаш Страната може да го резервира правото да не ги применува овие мерки врз гореспоменатите комуникации. Секоја Страна ќе ги разгледа ограничувањата содржани во нејзината резерва со цел да се овозможи широка примена на мерките предвидени во членовите 20 и 21.

Член 15 - Услови и гаранции

(1) Секоја Страна ќе се залага воведувањето, имплементацијата и примената на овластувањата и постапките предвидени во овој оддел да подлежат на условите и гаранциите предвидени со домашното право со кои се обезбедува адекватна заштита на човековите права и слободи, вклучувајќи ги и правата кои произлегуваат од обврските што Страната ги презела со потпишувањето на Конвенцијата за заштита на човековите права и основни слободи на Советот на Европа од 1950 година, Меѓународниот пакт за граѓанските и политички права на Организацијата на Обединетите нации од 1966 година и другите меѓународни инструменти за заштита на човековите права, во кои е инкорпориран принципот на пропорционалност.

(2) Овие услови и гаранции, пропорционално на природата на постапката или овластувањето, меѓу другото, опфаќаат судска или друга независна контрола, основите кои ја оправдуваат нивната примена и ограничувањата на опсегот и времетраењето на овластувањето или постапката.

(3) Во обем кој е конзистентен со јавниот интерес, а посебно со интересот за темелно спроведување на правдата, секоја Страна ќе го земе предвид влијанието на овластувањата и постапките предвидени со овој оддел врз правата, одговорностите и легитимните интереси на трети лица.

Наслов 2 - Експедитивно зачувување на складирани компјутерски податоци

Член 16 - Експедитивно зачувување на складирани компјутерски податоци

(1) Секоја Страна ќе усвои такви законодавни и други мерки кои се неопходни за да им се овозможи на нејзините надлежни органи да наредат или на сличен начин да можат да обезбедат експедитивно зачувување на точно определени компјутерски податоци, вклучувајќи преносни податоци кои се складирани со помош на компјутерски систем, а посебно кога постојат основи да се верува дека компјутерските податоци се изложени на опасност од загуба или модификација.

(2) Кога Страната го применува ставот 1 од овој член со издавање наредба до одредено лице да ги зачува точно определените складирани компјутерски податоци кои ги поседува или кои се наоѓаат под контрола на тоа лице, Страната ќе воведе такви законодавни или други мерки кои се неопходни за да наметне обврска над тоа лице да го сочува и одржува интегритетот односно целовитоста на компјутерските податоци онолку време колку што е потребно, но не повеќе од деведесет дена, за да им се овозможи на надлежните органи да побараат нивно откривање. Страната може да предвиди таквата наредба да биде дополнително обновена.

(3) Секоја Страна ќе усвои такви законодавни или други мерки кои се неопходни за да се наметне обврска врз имателот или друго лице кое треба да ги сочува компјутерските податоци, преземените постапки да ги чува во тајност онолку време колку што е предвидено со домашното право.

(4) Овластувањата и постапките предвидени со овој член подлежат на одредбите содржани во членовите 14 и 15.

Член 17 - Експедитивно зачувување и делумно откривање на преносни податоци

(1) Секоја Страна ќе усвои во поглед на преносните податоци што треба да се зачуваат согласно член 16 такви законодавни или други мерки кои се неопходни:

а. за да се овозможи експедитивно зачувување на преносните податоци без оглед на тоа дали еден или повеќе провајдери на услуги биле инволвирани во пренесувањето на таа комуникацијата; и

б. за да се овозможи експедитивно откривање пред надлежните органи на Страната или пред лицето определено од надлежниот орган, доволно

количество преносни податоци за да може Страната да го идентификува провајдерот на услуги и патот по кој комуникацијата била пренесена.

(2) Овластувањата и постапките предвидени со овој член подлежат на одредбите содржани во членовите 14 и 15.

Наслов 3 - Наредба за производство

Член 18 - Наредба за производство

(1) Секоја Страна ќе усвои такви законодавни и други мерки кои се неопходни нејзините надлежни органи да бидат овластени да му наредат или наложат:

а. на лице кое се наоѓа на нејзината територија да достави точно определени компјутерски податоци кои се во владение или под контрола на тоа лице, а кои се складирани во компјутерски систем или во медиум кој служи за чување на компјутерски податоци; и

б. на провајдер на услуги кој нуди услуги на територијата на Страната да достави претплатничка информација во врска со тие услуги, а која се наоѓа во владение или под контрола на тој провајдер на услуги.

(2) Овластувањата и постапките предвидени со овој член подлежат на одредбите содржани во членовите 14 и 15.

(3) Во контекст на овој член, изразот "претплатничка информација" означува информација во облик на компјутерски податок или било каков друг облик кој го поседува провајдерот на услуги, а која се однесува на претплатниците на неговите услуги но не и на содржинските и преносните податоци врз основа на која може да се утврди:

а. видот на комуникациската услуга што се користи, техничките одредби и периодот во кој се дава услугата;

б. идентитетот на претплатникот, неговата поштенска или географска адреса, неговиот телефонски или друг пристапен број, како и информации за наплатата кои се достапни и видливи од договорот или аранжманот за давање услуга;

ц. било која друга информација што може да се добие на самото место каде што е инсталирана комуникациската опрема, а која информација е достапна врз основа на договорот или аранжманот за давање услуга.

Наслов 4 - Претрес и запленување на складирани компјутерски податоци

Член 19 - Претрес и запленување на складирани компјутерски податоци

(1) Секоја Страна ќе усвои такви законодавни и други мерки кои се неопходни нејзините надлежни органи да бидат овластени да вршат претрес или да преземат други дејствија со кои ќе обезбедат пристапат до:

а. компјутерски систем или дел од него, како и до складираните компјутерски податоци во него; и

б. медиум за складирање на компјутерски податоци во кој можат да се чуваат компјутерски податоци и кој се наоѓа на нејзината територија.

(2) Секоја Страна ќе усвои такви законодавни и други мерки кои се неопходни кога нејзините надлежни органи вршат претрес или преземаат други дејствија со кои пристапуваат кон точно определен компјутерски систем или дел од него согласно став 1.а. и кога постојат основи да се верува дека бараните податоци се чуваат во друг компјутерски систем или дел од него, кој се наоѓа на нејзината територија, да можат легално да им пристапат на тие податоци преку првиот компјутерски систем и да можат експедитивно да го прошират претресот или преземањето слични дејствија на пристапување до другиот систем.

(3) Секоја Страна ќе усвои такви законодавни и други мерки кои се неопходни нејзините надлежни органи да бидат овластени да ги запленат или на друг начин да ги обезбедат компјутерските податоци до кои пристапиле согласно ставовите 1 и 2. Овие мерки опфаќаат овластување:

а. да се заплени или на сличен начин да се обезбеди компјутерски систем или дел од него или медиум кој служи за складирање на компјутерски податоци;

б. да се направи или задржи копија од тие компјутерски податоци;

ц. да се сочува интегритетот на релевантните складирани компјутерски податоци;

д. да се направат непристапни или да се отстранат сите компјутерски податоци од достапниот компјутерски систем.

(4) Секоја Страна ќе усвои такви законодавни и други мерки кои се неопходни нејзините надлежни органи да бидат овластени да му наредат односно да му наложат на било кое лице кое има познавање за начинот на кој функционира компјутерскиот систем или за мерките кои треба да се преземат за да се заштитат компјутерските податоци, да ги даде, во мера колку што е разумно или потребно, неопходните информации за да може да се преземат мерките предвидени во ставовите 1 и 2.

(5) Овластувањата и постапките предвидени со овој член подлежат на одредбите содржани во членовите 14 и 15.

Наслов 5 - Собирање компјутерски податоци во реално време

Член 20 - Собирање преносни податоци во реално време

(1) Секоја Страна ќе усвои такви законодавни и други мерки кои се неопходни нејзините надлежни органи да имаат овластување да:

а. собираат или снимаат на нејзината територија со помош на технички средства; и

б. да му наложат на провајдерот на услуги, во границите на неговите техничките можности:

i да собира или да снима со помош на технички средства на територијата на таа Страна; или

ii да соработува со или да им помага на надлежните органи во собирањето или снимањето на:

преносни податоци во реално време (време на случување),поврзани со точно определени комуникации кои се пренесуваат на нејзината територија со помош на компјутерски систем.

(2) Кога Страната, поради важечките принципи на домашниот правен поредок, не може да ги воведе мерките предвидени со став 1.а., наместо тоа таа може да усвои законодавни и други мерки кои се неопходни за да се обезбеди собирање и снимање “во реално време-време на случување” на преносните податоци поврзани со точно определени комуникации кои се пренесуваат на нејзината територија, со помош на технички средства.

(3) Секоја Страна ќе усвои такви законодавни и други мерки кои се неопходни за да му се наложи на провајдерот на услуги да го чува како доверлив фактот на спроведување на овластувањата предвидени со овој член, како и да ги чува како доверливи така добиените информации.

(4) Овластувањата и постапките предвидени со овој член подлежат на одредбите содржани во членовите 14 и 15.

Член 21 - Пресретнување на содржински податоци

(1) Секоја Страна ќе усвои такви законодавни и други мерки кое се неопходни, во врска со серијата на сериозни дела што треба да се предвидат со домашното право, со кои нејзините надлежни органи ќе бидат овластени:

а. да собираат и снимаат преку примена на технички средства на територијата на таа Страна;

б. да му наложат на провајдерот на услуги, во границите на неговите техничките можности:

i да собира или да снима на територијата на таа Страна преку примена на технички средства; или

ii да соработува со или да им помага на надлежните органи во собирањето или снимањето на:

содржински податоци поврзани со точно определени комуникации, во реалното време, кои се пренесуваат со помош на компјутерски систем на нејзината територија.

(2) Кога Страната поради важечките принципи на домашниот правен поредок, не може да ги воведе мерките предвидени со став 1.а., наместо тоа таа може да усвои законодавни и други мерки кои се неопходни за да се обезбеди собирање и снимање "во реално време-време на случување" на содржински податоци за точно определени комуникации кои се пренесуваат на нејзината територија, со примена на технички средства на таа територија.

(3) Секоја Страна ќе усвои такви законодавни и други мерки кои се неопходни за да му се наложи на провајдерот на услуги да го чува како доверлив фактот на спроведување на овластувањата предвидени со овој член, како и да ги чува како доверливи така добиените информации.

(4) Овластувањата и постапките предвидени со овој член подлежат на одредбите содржани во членовите 14 и 15.

Оддел 3 – Јурисдикција

Член 22 – Јурисдикција

(1) Секоја Страна ќе усвои такви законодавни и други мерки кои се неопходни за да воспостави јурисдикција над делата предвидени со членовите 2 до 11 на оваа Конвенција, во случаите кога делото е сторено:

а. на нејзината територија;

б. на брод кој плови под знамето на таа Страна; или

ц. во воздухоплов кој е регистриран според законот на таа Страна; или

д. од нејзин државјанин, доколку делото е казниво според кривичниот закон онаму каде што е сторено, или доколку делото е сторено надвор од територија која потпаѓа под јурисдикција на било која Страна.

(2) Секоја Страна може да го резервира правото да не ги применува или да ги применува правилата за јурисдикција предвидени во став 1.б. до 1.д. од овој член или дел од нив само во точно определени случаи или услови.

(3) Секоја Страна ќе усвои такви законодавни мерки кои се неопходни за да воспостави јурисдикција над делата предвидени во членот 24, став 1 од оваа Конвенција, во случаите кога наводниот сторител се наоѓа на нејзината територија и таа Страна не планира да го екстрадира во случај кога барањето за екстрадиција се заснова единствено врз околноста на неговото државјанство.

(4) Оваа конвенција не ја исклучува кривичната јурисдикција на Страната воспоставена во согласност со нејзиното домашно право.

(5) Кога две или повеќе Страни тврдат дека имаат јурисдикција над одредено кривично дело предвидено со оваа Конвенција, доколку е тоа возможно, инволвираните Страни ќе се консултираат со цел да се определи најсоодветната јурисдикција за гонење на тоа дело.