Југослав Ачкоски

СИГУРНОСТ НА КОМПЈУТЕРСКИ СИСТЕМИ, КОМПЈУТЕРСКИ КРИМИНАЛ И КОМПЈУТЕРСКИ ТЕРОРИЗАМ

- Скопје, 2012 -

Резиме

Основна намена на скриптата е запознавање на студентите со општествено негативните појави – компјутерски криминал и тероризам и штетните последици кои ги предизвикуваат.

Пратејќи ги линковите и користената литература, кои имаат едукативен и информативен карактер, студентот во голема мера може да се самоедуцира, а со тоа да ја подигне својата безбедносна култура на повисоко ниво, а со цел на самозаштита од овој вид на криминално делување.

СОДРЖИНА

9. ОСНОВИ НА ЗАШТИТА ОД КОМПЈУТЕРСКИ ВИРУСИ, ЦРВИ И ТРОЈАНЦИ
   - 9.1 Компјутерски вируси
   - 9.2 Антивирусни програми
   - 9.3 Заштита од вируси
   - 9.4 Тројанци
     - 9.4.1 Како се уфрлуваат тројанците?
     - 9.4.2 Заштита од тројанци
     - 9.4.3 Помошни програми за листање на активни процеси
     - 9.4.4 Firewall
   - 9.5 Црви
   - 9.6 Основни правила на заштита од вируси, црви и тројанци

10. СТРАТЕГИИ ЗА ЗАШТИТА ОД КРИМИНАЛНИ ДЕЈСТВА
    - 10.1 IT (*engl.*Information Technology) методи на заштита на компјутерските системи
      - 10.1.1 Класификација на информациите
      - 10.1.2 Правила на документирање
      - 10.1.3 Администрација и персонал
      - 10.1.4 Идентификација и авторизација на корисниците
        - А. Идентификација
        - А.1 Системи со лозинки
        - Б. Авторизација
        - Б.1 Логирање
        - Б.2 Back-up
        - Б.3 Firewalls
        - Б.4 Систем за детектирање на натрапници (нелегални влегувања) Intrusion Detection Systems (IDS)
        - Б.5 Справување со инциденти

11. ЗАШТИТА НА ДИГИТАЛНИТЕ ПОДАТОЦИ
    - 11.1 Криптографија
    - 11.2 Шифрирање со симетричен клуч
    - 11.3 Шифрирање со јавен клуч
    - 11.4 Дигитални потписи
    - 11.5 Дигитални сертификати
    - 11.6 Дигитални водени жигови
    - 11.7 Шифрирани обвивки

ЗАКЛУЧОК

ЛИТЕРАТУРА

ПРИЛОЗИ

ВОВЕД

Отсекогаш во технолошкиот развој, иновацијата имала силно влијание на сите сегменти во човековиот живот и работа, па во таа смисла информатичка технологија не е исклучок. Со оглед на случувањата во потесното и поширокото опкружување во минатото и сегашноста и нивните трендови, нема ни најмалку сомнеж дека информатичката технологија влијае на секој аспект на нашиот живот, сега и во иднина. Соочувајќи ги поединците, групите и нациите со предизвикот на адаптирање, иновации и реагирања на приликите и можности кои им се укажуваат од информатичка технологија, се врши неопходна трансформација, под заедничко име наречена *информатичка револуција*, од *индустриско во информатичко општевство*, најавувајќи нов *дигитален* период во кој нулите и единиците ќе бидат во знаење и вештина, алат и оружје, валута и роба, наука и уметност, забава и спорт... Таквата храбра констатација е изведена врз база на факти кои можат да се опишат и на следниот начин: *Се што се работи – се автоматизира и се што вреди - се дигитализира*. Понатаму, скоро во секоја работа ќе се вклучи користење на сметач, а најразновидните општествени вредности, во развој од мали до екстремно големи, ќе се трансформираат во т.н. *сајбер-добра*. Сето тоа се одвива и наоѓа во еден огромен новокреиран виртуелен простор означен со префикс *сајбер,* кој е превземена од зборот **engl.***cybernetics* (наука за управување) и кој треба да укаже на целата технолошка сложеност, зависност и проблематичност кои се присутни во тој нов, ама сеуште неуреден информатички амбиент, амбиент кој се разликува од обичниот и физичкиот свет на материјата и енергијата, во кој владеат знаењето, електронските импулси и дигитални броеви.

Што е сајбер-простор? Прашањето не е лесно, ниту пак одговорот е незначаен. Ако истото би се поставило на десетмина познавачи на проблематиката, сигурно би се добиле исто толку различни одговори. Сајбер-просторот е термин кој прв го вовел Вилијам Гибсон (William Gibson) 1984. година во својата позната новела *Neuromancer*. Во оваа новела, Гибсон го опишува сајбер-просторот како акумулирана можност на светот на компјутерскиот систем. Сајбер-просторот е, теориски простор во кој податоците можат да бидат складирани, пренесени и реконфигурирани.[1] Има уште многу други, покасно настанати, дефиниции и опис на овој термин. Авторот се определил за дефиниција која сајбер -просторот го толкува како виртуелен свет обележен со компјутери, компјутерски мрежи, информатички настани и информатички содржини во дигитална форма.

Новиот паралелен свет во виртуелниот простор, во кој настануваат под влијание на бурниот развој и се поширокота и обемната примена на информатичката технологија која е во состојба на рапидна револуција, станува арена за одвивање на најразличн активности и процеси, меѓу кои позначајно место им припаѓа на криминалните активности, со потенцијал кој предупредува и загрижува. Наведената констатација е всушност и клучна основа на оваа работа.

Индустрискиот свет влезе во фаза на технолошки промени и инвации кои влијаат на сите аспекти на животот и кои водат кон воспоставување на она шо се нарекува информатичко општевство. За да се достигне визијата Република Македонија да биде напредно информатичко општевство, многу прашања треба да бидат земени во предвид и дискутирани. Сепак, само неколку од нив се практично поврзани со влијанието на воведувањето на електронската комуникација кои треба да бидат дискутирани.

---

[1] Clarke R., *Information Technology & Cyberspace: Their Impact on Rights and Liberties*, Mietta's, Melbourne, January 1996, The Australian National University, http://www.anu.edu.au/people/Roger.Clarke/II/index.html

Денешниот свет се соочува со голем број на предизвици во борбата со феноменот на организираниот криминал, посебно „сајбер криминалот и сајбер тероризмот“ како нови модели на закани во 21 век. Колку повеќе информатичката технологија станува софистицирана, толку повеќе стануваат комплексни методите и средствата кои се употребуваат за борба за борба против криминалните активности посебно кај сајбер тероризмот.

Република Македонија не претставува исклучок од земјите кои зголемено се соочуваат со овој софистициран вид на организиран криминал. Како земја, нашата цел е да бидеме дел од глобалната безбедносна мрежа во борба против перењето пари, организираниот криминал, финансирањето на тероризам и влегувањето на „валканите пари“ во економијата. Република Македонија треба да превземе сериозни мерки за да го заштити својот безбедносен систем, посебно државните владини (институции), со цел од кражба на личните податоци, високо безбедносни тајни, воени планови и измамнички активности т.е. „крадењето пари“ од кредитните/дебитните картички. Сајбер тероризмот и криминалните активности имаат видливо неповолно влијание врз земјата т.е нејзината економија, безбедноста на граѓаните, јавниот живот и човековите права и слободи.

Поради сите горенаведени причини, овој нов облик на организиран криминал треба да биде спречен од понатамошно ширење не само на нашата територија туку и во целиот свет.

1. ИСТОРИСКИ ПРЕСВРТ

Се е почнато така неодамна во 1969 година кога за првпат повеќе компјутери биле поврзани во единствена компјутерска мрежа. Интернетот, тогаш познат како ARPAnet, зачнат е со иницијална конекција со четири главни компјутери со унииверзитетите од југозапад САД (University of California, UCLA – Los Angeles, Stanford Research Institute, SRI, University of California, UCSB – Santa Barbara, University of Utah – Salt Lake City).

Предисторијата на овој настан го опфаќа пронаоѓањето на адекватен одговор од заканата за потенцијален нуклеарен напад. Според тоа, ARPAnet бил дизајниран да овозможи комуникација и во услови на нуклеарен напад и ако една или повеќе мрежни локации бидат уништени. Понатаму, развојот на Интернетот е започнат како проект на американското Министерство за одбрана за креирање на националната компјутерска мрежа која би продолжила да функционира во можно пост-апокалиптично време, дури и ако нејзиниот поголем дел би биде уништен во нуклеарна војна или природна катастрофа.[2]

За разлика од денешниот ден, кога милијарди луѓе имаат пристап до Интернет, ARPAnet служел само за компјутерски професионалци, инжењери и научници кои го познавале неговиот комплексан начин на функционирање. Меѓутоа, од ова „семе“, со брзина и во обем во кој беа надвор од сите предвидувања и очекувања, никнаа нови компјутери на нови мали, средни и големи мрежи, кои меѓусебно се поврзувале, создавајќи разновидни информатички инфраструктури, соединување во една огромна мутант мрежа позната под името Интернет.

Посебно е значајно да се укаже дека многу од компјутерските мрежи, а посебно оние кои ги покриваат националните сајбер простори и формираат национална информатичка инфраструктура, поради податоците кои ги имаат и функциониите кои ги извршуваат, стануваат критични од аспект на националните интереси. Самиот термин национална информатичка инфраструктура се однесува на таков збир на компјутерски систем, база на податоци и телекомуникациски мрежи кои го покриваат целиот национален сајбер простор и кој ги чини електронските податоци и сервиси да се широко расположливи и достапни на сите оните кои се наменети.

После повеќе од еден век на постоење на електронската технологија, луѓето успеале да ги прошират електронскиот нервен систем и со глобално опфаќање, надминувајќи ги границите на просторот и времето, успеале да ја покријат нашата планета се до каде што се простираат нејзините физички граница. Интернет го направи тоа што визионерот на комуникацијата Маршал Меклуан (Marshall McLuhan) го нарече *глобално село,* конечно да стане реалност.[3] Имено, Меклуан уште во 70-те години на минатиот век го креирал концептот на *глобалното село*, чии делови меѓусебно се поврзани со електронски нервнен систем значајно пред тоа да се случи стварно.[4] Тој бил прв човек кој го популаризирал концептот *глобално село* и ги набљудувал неговите социјални ефекти. Неговото осознавања и согледувања биле револуционерни во тоа време бидејќи фундаментално се изменил начинот на кој до тогаш многу размислувал за медиумите, технологијата и комуникацијата. Тој внимателно ја избрал фразата *глобално село* се со цел да го истакне своето запазување дека електронскиот нервен систем (медиумот) рапидно *интегрира* на планетата – случувањата во еден дел од светот кои би

[2] Petrović R. S., *Kompjuterski kriminal*, Vojnoizdavački zavod, Beograd 2004, III izdanje, str. 66–73.

[3] *Internet Growth Statistics – Global Village History*, http://www.internetworldstats.com/emarketing.htm

[4] *Marshall McLuhan Foresees The Global Village*, http://www.livinginternet.com/i/ii_mcluhan.htm

можеле да бидат осознаени и доживеани во другите делови на светот во реалното време, што е слично на оноа што луѓето го доживуваат кога живеат во малите села.

Денес Интернетот продолжува да расте секојдневно се до моментот на создавање да *глобалното село* биде вистинито. Големината и брзината на промените, кои ги изненадиле и најоптимистичните футурологисти, најлесно е да се согледаат преку бројни покажувачи. Во врска со тоа значајно е да се укаже дека е пресудна улога во тие промени имало влијанието на промената на брзина на преносот на податоците.

Брзиот развој на информациско-комуникациската технологија континуирано секогаш ја потикнува големата брзина со која податоците би можеле да бидат пренесени. Затоа брзината на пренесување на податоците низ компјутерските мрежи доживеала вистински бум. Со почетните 50 килобајти во секунда (Kbps), брзина која била веќе присутна кај ARPAneta која иницијално поврзува четири компјутера во 1969 година, а во 1996. година достигнала 622 мегабајти во секунда (Mbps), така да во 1999. Година достигнува веќе 2,5 гигабајта во секунда (Gbps), а 2003. година во САД создадена е брзина од 10 гигабајта во секунда (Gbps). Наредната (2004) година, првата широкопростарана (backbone IPv6) мрежа во Кина (China Education and Research Network (CERN)), која поврзува 25 универзитета во 20 града, иницирана е со брзина од 1 до 10 гигабајта во секунда (Gbps).[5] Брзината на преносот од 10 Gbps во однос на почетната брзина од 50 Kbps представува фантастично зголемување од приближно 210,000 пати.

Таква промена на брзината на пренос на податоци и информации воделе до феноменален раст на Интернетот, еден од важните елементи на информатичката инфраструктура. Во 1969. година претходник на Интернетот стартуваше со само четири компјутера кои чиниле една единствена есенцијална мрежа. Денес поврзани компјутери има преку 350 милиони. Следната табела ја покажува неверојатна брзина на еволуција на Интернетот од 1995. година до денес, со аспект на зголемување на бројот на хостови и бројот на корисници на Интернетот[6]:

Во табелата 1 прикажано е зголемување на бројот на хостови (компјутери кои имаат регистрирано Интернет адреса) за десетте последни години.[7] Тоа зголемување од 5,846,000 хостови во јануар 1995. година на 353,284,187 во декември 2005. изнесува околу 60 пати, односно око 6000%. Слична е ситуацијата и со бројот на корисници, кои од 16 милиони во 1995. година се зголеми на повеќе од една милијарда, односно за исто така неверојатни 64 пати или за околу 6400%. Проектиран број на корисници на Интернет за 2010. година е 1.8 милијарди.

Табела 1. Зголемување на бројот на хостови

Датум	Број на хостови	Датум	Број на хостови
01/1995.	5,846,000	01/2001.	109,574,429
01/1996.	14,352,000	01/2002.	147,344,723
01/1997.	21,819,000	01/2003.	171,638,297
01/1998.	29,670,000	01/2004.	233,101,481
01/1999.	43,230,000	01/2005.	317,646,084
01/2000.	72,398,092	12/2005.	353,284,187

[5] *Hobbes' Internet Timeline, v8.1*, http://www.zakon.org/robert/internet/timeline/

[6] *Internet Growth Statistics – Global Village History, op. cit*.; *Hobbes' Internet Timeline v8.1*, op. cit.

[7] *Population Explosion!*, November 3, 2005, http://www.clickz.com/stats/sectors/geographics/print.php/5911_151151

Табела 2. Интернет корисници

Датум	Интернет корисници	% светска популација
12/1995.	16,000,000	0.4 %
12/1996.	36,000,000	0.9 %
12/1997.	70,000,000	1.7 %
12/1998.	147,000,000	3.6 %
12/1999.	248,000,000	4.1 %
12/2000.	451,000,000	7.4 %
08/2001.	513,000,000	8.6 %
09/2002.	587,000,000	9.4 %
12/2003.	719,000,000	11.1 %
12/2004.	817,000,000	12.7 %
12/2005.	1,018,000,000	15.7 %

Во наредната табела изложени се бројчани покажувачи на клучните региони на светот (табела 3, состојба 31. 3. 2006).

Табела 3. СВЕТ (состојба: 31. 3. 2006)

РЕГИОНИ	Популација (проценка за 2006)	% светска популација	% светска популација	Зголемување (2000–2005)
Африка	915,210,928	14.1 (23,649,000	2.6	2.3 (423.9
Азија	3,667,774,066	56.4(364,270,713)	9.9	35.6 (218.7)
Европа	807,289,020	12.4(291,600,898)	36.1	28.5 (177.5)
Европска унија	462,371,237	7.1(230,396,996)	49.8	22.5 (147.3)
Средњи исток	190,084,161	2.9(18,203,500)	9.6	1.8 (454.2)
СевернаАмерика	331,473,276	5.1 (227,303,680)	68.6	22.2 (110.3)
Латинска Америка	553,908,632	8.5 (79,962,809)	14.4	7.8 (342.5)
Австралија/Океанија	33,956,977	0.5 (17,872,707)	52.6	1.7 (134.6)
ВКУПНО	6,499,697,060	100.0 (1,022,863,307)	15.7	100.0 (183.4)

Интересно е да се воочи дека во сите набљудувани региони порастот на корисниците на Интернетот во периодот 2000–2005. изнесува повеќе од 100%. Најмал пораст е забележен во Северна Америка 110.3%, што е и разбирливо затоа што бројот на корисници на Интернет во однос на вкупната популација на регионот веќе достигна 68.6%, а најголем е на Средниот исток 454.2% и во Африка 423.9%. Бројот на корисници на Интернетот во однос на популацијата во регионот на Средниот исток изнесува 9.6%, а за Африка само 2.6%.

Исто така интересно е дека бројот на корисници на Интернет во два од набљудуваните региони во однос на нивната сопствена популација веќе надмина 50%: Северна Америка 68.6% и Австралија/Океанија 52.6%, додека Европската унија е на самиот праг да достигне 50% (49.9%). Од сето тоа произлегува дека бројот на корисници на Интернет е најголем во најразвиените делови на светот, што може да се толкува како и една од причините за нивната развиеност.

Бројот на веб сајтови јуни месец 1995. године изнесувал 23,500, а десет години покасно (август 2005) тој број изнесува 70,392,567, што е зголемено за 2,995.5 пати.[8] Понатаму, се се одвива и ќе се одвива со брзина и во обем кој тешко е разбирлив за обичниот човек.

[8] *Hobbes' Internet Timeline, v8.1, op. cit*.

2. ЕФЕКТИ ОД ИНФОРМАЦИСКАТА РЕВОЛУЦИЈА

Новиот милениум јасно најавува дека современата општествена заедница тешко може да функционира без информацискатa технологија, солидната информатициска инфраструктура и граѓани со доволно технолошко познавање и нивно користење. Ефектите од огромното влијание на информатичката технологија врз општевството се воочуваат преку трајни промени во начинот на комуницирање, учење, работа и забава. Тоа што секако треба добро да се воочи и запамти е дека трендот на овие промени подразбира трансформација на работата *од физичка на ментална, од сила на мускулите кон силата на умот* – а такви промени се, мора да се признае, навистина и драстични и драматични, и од нив произлегува и ќе произлегува многу широк опсег на национални и меѓународни политички, економски и социјални прашања, сега и во иднина. Јасно е дека многу тековни информатичко-технолошки трендови ќе продолжат, барем во наредните 15 до 20 години: компјутерите ќе постојат минијатурни, брзи, моќни и поефтини, комуникациска пропусност ќе се зголеми, а компјутерските мрежи се повеќе ќе ја прекриваат нашата планета. Меѓутоа, иднината не е потребно да се чека затоа што нам информатичката револуција веќе ни донесе многу нови погодности и можности кои ќе може да се користат во секојдневниот живот, а клучен алат за тоа користење е секако Интернетот. Збор е за една светска распространета можност, механизам за дисеминација информација и медиум за соработка и интеракција на поединачна и групна основа, без оглед на географската локација на учесниците. Клучен концепт на *Интернетот* е дека тој не ни бил дизајниран за само една апликација, туку како генерална инфраструктура на која можат да се развијат нови меѓусебно независни апликации.

Ова во најголема мерка го овозможила општата природа на сервисот кој ја пружа фамилијата на интеракцискиот протокол *TCP/IP*. Понатака, за разлика од другите компјутерски мрежи, Интернетот е збир на многу делови и се состои не само од еден туку од повеќеструки системи на податоци кои се развиени независно. Најпопуларни и најзначајни системи се:

- World Wide Web;
- Електронска пошта (e-mail);
- Дискусиони групи (USENET newsgroups);
- File Transfer Protocol (FTP);
- Gopher;
- Telnet;
- Internet Relay Chat (IRC);
- CU-SeeMe.

Сите наведени, ама и други системи пружаат и нудат на корисниците бројни и разновидни услуги и можности влијаејќи директно или индиректно на начинот на одвивања на најразновидни активности и работи во лепеза од тривијални до најобемни и најсложени. Поради илустрацијата да ги спомнеме само оние области кои се клучни за функционирање на секое општевство и во која примена информатичка технологија може да има импресивни економски и социјалние ефекти:

- Државна управа;
- Работење;
- Научно-истражувачка работа;
- Едукација;
- Здравствена заштита;
- Национална безбедност;

- Одбрана.

2.1. Државна управа

Познат е фактот дека отвореност на работењето на државната администрација е основа на секоја модерна демократска држава. Само во таква држава граѓаните можат да остварат едно од своите основни права и да знаат што и како државната администрација работи, како и од да нејзе бараат во интерес на граѓаните. Во тој контекст од администрацијата со право се очекуваа поефикасни, транспарентни и одговорни јавни услуги, поблиску до граѓаните и со пониски трошоци. Од друга страна, исто така е познато дека, ако не во сите, туку во повеќе држави, повеќето граѓани сметаат дека нивната државна управа е *преголема, неефикасна и многу скапа*.[9] Поради тоа, од тие причини се прават континуирани обиди да со разни типови на реорганизација на државната администрација ситуацијата значително да се подобри. На жалост, сите тие обиди воглавно завршуваат со несакани резултати.

Појавата на информацискатa технологија овозможува голема шанса и можност да конечно и во оваа област се остварат позитивни ефекти. Ако правилно информатичката технологија се применува би можела да биде есенцијални дел од решението, кое за секоја државна заедница е потребно како многу значајно решение, бидејќи владите на индустрискиот период (огромен државен апарат), кој е организиран да првенствено ги задоволи барањата и потребите на бирократските структури, се трансформири во една виртуозна, ефикасна и ефтина влада на информатички период, организиран по функциите и потребите на граѓаните. При тоа, значајно е да се свати дека оваа трансформација не подразбира само просто автоматизирана влада, туку нејзино потполно реобликување.[10] Имајќи ја во превид можноста на информатичката технологија, како и познатиот заклучок дека *доверлив тест на добра влада е нејзина способност да создаде добра администрација*, шансата да се приближи на граѓаните и да го зголеми квантитетот и квалитетот на своте услуги, да ја зголеми ефикасноста и да ги намали трошоците во јавниот сектор, го стимулира воведувањето на новите и подобрување на постоечките сервиси, ни една влада, по се изгледа, немала желба да пропушти. Во високо развиените земји најистакнати напори во оваа област биле насочени на изградување на електронска влада *(e-government)*. Ова име во себе ги обединуваше потребите, желбите и намерите на државната администрација да ја изврши сопствената трансформација согласно технолошките промени и барањето на времето. Изградбата понатака, се потпираше на иницијативата која ја користи информатичката технологија да ја редуцира канцелариската работа и модернизација на административниот процес. Во многу земји работите на големо се одминати и веќе почнале да се покажуваат првите значајни резултати во смисла на владината ефикасност, брза обработка на податоци, поголема точност, зголемено ниво на услуга и редуцирање на административните трошоци.

---

[9] *E-Government guideline*, The World Bank, http://siteresources.worldbank.org/ INTEGOVERNMENT/ Resources/e-Gov_guideline.pdf; *E-Government Handbook*, CDT/infoDev, http://www.cdt.org/egov/handbook/; Stearns W. R, *Revolution in the U.S. Information Structure: The Promise of the National Information Infrastructure*, National Academy of Sciences, 1994, http://www.nap.edu/readingroom/books/newpath/chap3.html ;

[10] *Benefits of e-Government*, Asia-Pacific e-Government Portal, Last modified 2004, http://egovaspac.apdip. net/topics/benefits/; *E-Government Handbook*, op. cit. ; Horrigan B. J., *How Americans Get in Touch With Government*, Pew Interne & American Life Project, May 24, 2004, www.pewinternet.org;

2.2. Работење

Континуираното значање на информатичката технологија за работењето толку е големо да не може да биде пренагласено. Согласно напред изнесената констатацијата дека е избор за трансформација од сила на мускулите кон снагата на умот – знање и стручност на работната сила, стануват доминантни сторители на новиот начин на работење и веројатно ќе биде најзначаен детерминантен успех и во иднина.

Сите работни организации, во услови на се појака и бројна конкуренција и на брзи промени на барања на потрошувачи, во најмала или најголема мера вложуваат напори да откријат како да со користење на информатичка технологија побрзо и најдобро да се искористат приликитее и можностите кои таа несебично им ги дава. Современото работење базирано на информатичката технологија има можност да ги намали трошоците на производството и да го зголеми приходот на креирање на новите пазари за стари производи, да креира нови производи на основа на собрани информации за потребите и желбите на потрошувачите за истите и да формира нови можности на давање на услуги на своите клиенти.[11]

Новото работење на барањата и новите методи на управување се однесуваат, пред се, на управување со знаеење. Таквото управување подразбира поинаква организациона структура, а особено информатичката технологија има револуционерни импликации на промена на структурите на организацијата. Таа ја суспендира хиерархијата елиминирајќи го нивото на средни раководители чија улога би била да собира информации и да ги пренесува на највисоко или најниско во организациона пирамида. Новите организациони структури користат тимови на извршители поврзани преку информатички мрежи со оние кои ја обликуваат политиката, редуцирајќи на овој начин потребата за интерни посредници. Потреба за екстерни посредници исто така се редуцира. Производителите и потрошувачите производители и снабдувачи се поврзани директно, независно од географската локација, значајно редуцирајќи ги трошоците и на големо зголемувајќи корисност и оптек на информација која двосмерно се разменува.[12]

Дистрибуираните организации поврзани со електронски врски овозможуваат работа и од дома, па канцеларијата ќе биде таму каде може да се изврши работата, а тоа географски значи многу дислоцирано. Во такви случаи информатичката технологија има потенцијал не само да значајно ги смалува трошоците на работа, туку да дозволи подобар баланс помеѓу куќното и работното живеење. Телекомуницирањето дозволува на вработените да трошат повеќе време дома со семејството, што сигурно стимулативно ќе делува на нивното извршување на работните задачи.

Потикнување и иницијатива со новите можности и атрактивни сервиси ги потискуваат бариерите на *on-line* пристап во сметководствените сметки и продолжуваат да го менуваат лицето *on-line* на банкарството. Ракување и размена на паричните средства, посебно на оние кои ги вршат банките и другите финансиски институции, се повеќе се извршуваат на електронски начин. За тоа најдобро зборуваат бројчаните покажувачи. Банкарското *on-line* работење се зголемило на околу 40 милиони корисници до последниот квартал на 2005. година. Бројот на сметките се зголемил за 27% во однос на последниот квартал на 2004. година. Плаќањето на сметките преку банкарските *on-line* сметки сега изнесува скоро четвртина од сите плаќања на сметки на *on-line*.[13]

---

[11] Stearns W. R., *op. cit.*

[12] *An introduction to e-business optimisation*, http://www.weboptimiser.com/resources/index.html; *Introduction to E-business*, http://www.bgateway.com/bg-home/bg-services.htm

[13] *Online Banking Spikes, then Slows*, April 11, 2006, http://www.clickz.com/stats/sectors/

Интерактивното рекламирање преку Интернет достигна износ од 3,6 милијарди долари во четвртиот квартал на 2005. година, што е зголемување од 17% во однос на претходниот квартал, односно зголемување од 35% во однос на истиот период во 2004. година. Се проценува дека годишниот приход од рекламирање за 2005. е поголем од 12,5 милијарди долара, што во однос на 2004. година представља увеќање од 30%.[14]

Потрошувачката преку Интернет за 2005. година се зголемила за 22% во однос на претходната (2004) година. Вкупната потрошувачка, вклучувајќи и патувања, достигнала во 2005. година износ од 143.2 милијарди долари. Од тоа 60.9 милијарди долари потрошено е на патувања, а остатакот од 82.3 милијарди долари на останатото.[15] Понатаму, очигледно е дека работењето рапидно се преселува во сајбер-простор.[16]

2.3. Научно-истражувачка работа

Информатичката технологија има остварено неизмерно јако влијание во областа на научно-истражувачката работа. Интернетот, најзначајната форма на информатичката технологија, посебно е популарна меѓу научниците и веројатно представува најзначаен научен инструмент на новиот век. Моќен, софистициран пристап кој тој го обезбедува во собирање, средување, складирање, ажурирање, обработка, пребарување и размена на податоци и информации, како и поволностите на електронската документација која ја карактеризира едноставноста на документирање, леснотија на управување, модификација, ажурирање, чување и дистрибуција, пристапност и мали трошоци (хартијата се користи само за финална верзија), и најпосле, разновидни, ефикасни и ефтини можности на меѓусебни комуникации на електронски пораки, моментални пораки, со размена на електронски документи и видеоконференции, моментални пораки, олеснуваат, подобруваат и ги забрзуваат научните истражувања. Според тоа, Информатичката револуција е изнесена потполно во новите области на изучувања (на пр. компјутерски науки), нови интердисциплинарни домени (на пр. комплексни системи), како и драматичен напредок внатре во постоечките научни области (на пр. компјутерска лингвистика).[17]

А кога веќе станува збор за наука, право место е да се укаже дека поради доменот, длабочината и големината на влијанието на информатичката технологија научниците имаат обврска да истражуваат не само во внатрешното користење на информатичката технологија, дури и да превземаат истражувања од оваа технологија и нејзини импликации на нашата работна активност, нашата култура и нашата правна, политичка, економска и социјална политика и релација. Тоа е секако ново и многу обемно и сложено поле на истражување.

---

finance/print.php/3598231

[14] *Internet Ad Revenues Continued to Grow in the Fourth Quarter*, ClickZ News, March 1, 2006, http://www.clickz.com/news/print.php/3588506

[15] *Online Retail Sales Grew in 2005*, January 5, 2006, www.clickz.com/stats/sectors/retailing/article.php/3575456

[16] Hakman K., *E-Commerce Tutorial*, http://www.webmonkey.com/webmonkey/99/04/index0a.html

[17] Davidson T., Sooryamoorthy R., Shrum W., *Kerala Connections: Will the Internet Affect Science in Developing Areas?*, 2002, http://worldsci.net/EVERY4.pdf ; Finholt A. T., *Collaboratories: Science over the Internet*, 2002, http://www.aaas.org/spp/yearbook/2002/ch31.pdf ; Guice J., Duffy R., *The Future of the Internet in Science*, USRA Research Institute for Advanced Computer Science, NASA Ames Research Center, USA, http://ase.arc.nasa.gov/publications/pdf/2000-0174.pdf

2.4. Едукација

Како и во многу други области тако и во областа на едукацијата информатичката технологија овозможува бројни можности и шанси кои сигурно ќе предизвикаат големи промени во нашите едукациони системи. Можат да се најдат бројни примери на некои типови и промени за кои може да се очекува дека ќе станат пошироко распространети. На пример, се поголем број на школи бараат од своите ученици и студенти да постигнат базична компетентност во користењето на информатичкото-технолошки алатки, како што се обработка на текстови, табели, база на податоци и графика.[18] Непознавање на кодот на овие алатки во информатичко време најверојатно ќе биде етикета за неписменост. За наставниците е излишно да се зборува. Нивното технолошко образование значително е од неколку причини.

Прво, секако е шанса и можност да сами на себе си ја олеснат, подобрат и забрзаат сопствената активност, друго е да бидат обучени во применатата технологија и да можат без тешкотии да се вклучат во современата метода и техниката на едукацијата при тоа значително подобрувајќи го нејзиниот конечен исход и да бидат нејзини промотери, а не кочничари, и трето поради осетливи позитивни ефекти информатичката технологија на вкупните трошоци на образование со своето вклучување во тој процес даваат и личен придонес.[19]

Учениците и студентите веќе имаат на својот десктоп светски признати речници, прирачници и енциклопедии. Достапни им се во дигитална форма најнови прикази, расправи, студии, извадоци, учебници и монографии на светски автори, затоа што дигиталната врата на најпознатите светски библиотеки, научно-истражувачки установи и стручни списанија им се широко отворени. Тие најпросто речено нема да имаат повеќе желби, време и трпение да на класични предавања слушаат други, понекогаш конфузни и бескорисни, тиражи преполни со фрази, од кои често се вон памтењето оставање на обем кој може да се искаже со едноцифрен процент. Заблагодарувајќи се на информатичката технологија, се поголем број на ученици и студенти ќе поминуваат дел од своите „школски денови“ во виртуелни училници, групирани *on-line* со други кои делеле нивни интереси, вештини и квалификации.[20] Наставниците при тоа можат да бидат, не преносувачи на знаења, туку помагачи и усмерувачи кои помагаат на студентите ноасочувајќи ги во нивната насока на учење.

Понатаму, информатичката технологија нас неосетно не ослободува од традиционалното, ама стар модел на учење *(„искусен“ наставник пред класот насочен е на пружање знаења на заробените групи на студенти)*, затоа што потикнува други модели на класно учење. За разлика од индустриското време во информатичкото време наставниците и студентите не мора да бидат на исто место во исто време, ама затоа, благодарејќи на информатичката технологија, може и да се видат и да се слушнат. Исто така, од иста причина, учењете не мора да се прекине кога студент ќе се придружи на вработените, туку ќе може да продолжи до крајот на нивниот живот (индивидуално доживотно учење).

---

[18] *The Future of Information Technology in Education***,** An ISTE Publication, http://www.uoregon.edu/~moursund/FuturesBook1997/index.html

[19] Mоursund D., Smith I., *Five Research Summaries on IT in Education*, International Society for Technology in Education, 2000, http://darkwing.uoregon.edu/~moursund/dave/Free.html; Stearns W. R, op. cit.

[20] *Recommendations for Research and Development in Information Technology in Education,* Learning and Leading with Technology 2000-2001, ISTE (the International Society for Technology in Education, http://www.iste.org/

При тоа, клучно прашање се постаува што студентите треба да учат ментално, во однос на тоа што треба да учат потпомогнати едноставно со помошни средства, како што се книги и хартија, и во однос на тоа што треба да учат потпомогнати со софистицирани помошни средства како што се калкулатори, компјутери и други информатички технологии. Ова е тешко прашање, посебно имајќи ги во предвид константните промени на состојбата на технологијата. Спороста во прифаќање на рачни калкулатори во наставната програма сугерира дека софистицираните помошни средства за решавање на проблемите ќе наидат на обемно сопирање. Разликата помеѓу расположивите алати и алатите кои се користат во едукација најверојатно бројчано ќе се, зголемуваат.

Сепак, користењето на информатичката технологија во образовниот процес во многу земји ќе биде толку значајно колку што ќе го налага нивната национална политика. Така американскиот председател Клинтон уште во 1996. година најави акција со цел да секое дете во Америка биде технолошки образувано на почеткот на 21.век. Клинтон ги означи „четирите потпорни елементи“ за својот програм *„технологија во школите“*:[21]

- *Компјутери.*
  Опремување на секоја училница со модерни компјутери и средства за учење, кои се достапни на секој студент;
- *Конекција.*
  Поврзување на сите училници во Америка меѓусебно и со надворешниот свет;
- *Едукациона содржина.*
  Обезбедување на богат спектар на интересни инструктивни материјали и едукационен софтвер;
- *Обука на наставниците.*
  Обезбедување сите наставници да имаат обука и помош која им е птребна да остварат потполно користење на новата технологија.

Не постои ни најмалку сомнеж дека компјутерот е корисен и сестран едукационен алат кој може да се користи да помогне во решавање на проблемите и извршување на задачите кои се во центарот на различитите академски дисциплини.

Прогресот и развојот на многу и подобри апликативни пакети, како и подобри интерфејси помеѓу човекот и машината, причинува поголем раст на користење на алати на информатичка технологија. Исто така, научниците на полето на вештачката интелигенција ги развиваат апликативните пакети кои се наменети за решавање на многу тешки и сложени проблеми кои бараат повеќе човечко знање и вештина. Таквите апликативни програми ќе предизвикаат да нема дилеми, конечно да ги менуваат поголемите школски тематски содржини на сите нивоа и образувања.

2.5. Здравствена заштита

Секоја сериозна дебата за здравствената заштита представува голема можност за осовременување и рационализација на нејзините услужни и административни аспекти. Информатичката технологија има потенцијал фундаментално да ја подобри и усоврши врската на релација пациент – медицинска установа и овозможи на пациентот да биде информиран и активен конзумер на здравствените услуги. Покрај тоа, информатичката технологија содржи и ветување за значајна редукција на овој тип на трошоци. Затоа не изненадува фактот дека областа на здравството представува многу погодно тло за многу обемна примена на информатичката технологија. Оваа технологија ја менува

[21] The Future of Information Technology in Education, op. cit.

здравствената заштита многу радикално: го менува начинот на кој лекарите меѓусебно комуницираат, вклучувајќи консултации на специјалистите; го трансформира начинот на кој пациентите пристапуваат и делат информации; нудат дополнителни канали низ кои негата може да биде достапна на пациентите; и најпосле, значително ги намалува трошоците. [22]

Телемедицината е друга значајна апликација. Оваа технологија им овозможува на руралните средени пристап до специјалистите во водечките медицински центри. Користејќи ги системите за видео-конференција на големи брзини на пренесување и со висока резолуција на сликите, специјалистите на раздалечени локации, со кои се консултираат лекарите на пациентите, прегледувајќи ги рендгенските снимки, интервјуирајќи го пациентите, нудат експертски совети на опции со третмани. Во местата каде овие системи биле тестирани, корисниците потврдиле дека технологијата донесува подобра медицина до раздалечените зони, исто така го збогатува животот во руралните средини при тоа на лекарите давајќи им пристап на знаење и совет со специјалистите од светската класа. [23]

На крајот, потребно е во ист контекст да се укаже на вклучување на информатичката технологија и здравствената заштита, покрај другите области, во класдата на се поголема зависност од таа технологија.

2.6. Национална безбедност

Терминот *национална безбедност*, околу чија дефиниција, поради екстензивно менувачките карактеристики на безбедносниот амбиент, не постои општа согласност, во описната форма би подразбирало обезбедување на заштита на поединците, друштва и држави од екстерни и интерни закани на политичката, економската, социјалната, војната, еколошката, информатичката и друга природа во светло на постоечките ресурси и потенцијали. Еден од најзначајните инструменти за реализација на овие задачи на повеќето држави е нивна *тајна служба*, која, од една страна, има обврска да користи легални и илегални методи на присобирање, средување, проучување и користење и разузнавачки (јавни и тајни) податоци од областа на војниот, политичкиот, економскиот, научниот, културниот и техничкиот живот на другите земји, посебно на оние за кои е наведената држава посебно заинтересирана (разузнавачка работа), а од друга страна, да организира и непосредно се ангажира на заштита на тајните податоци на сопствената нација и во таа смисла открива, прати и оневозможува делување на разузнавачките служби на противникот (контраразузнавачка работа).[24]

Информатичката револуција на овие служби им дала нови и огромни можности на делување, посебно во областа на разузнавањето, а истовремено ја креирала и новата многу озбилна, сложена и одговорна задача и обврска за контраразузнавачко делување. Клучна улога во овие новини има Интернетот, кој во буквална смисла представува

---

[22] Advocat J., *Internet clinical trials: examining new disciplinary experiments in health care*, Monash University, Australia, Anthropology Matters Journal 2005, Vol 7 (1), http://www. anthropology matters.com; Robinson C. J., *Financing The Health Care Internet*, Health Affairs ~ *Volume 19, Number 6*, 2000,http://content.healthaffairs.org/cgi/reprint/19/6/72.pdf; Warren M., *The Internet and rural communities: implications for health care?*, http://www.plymouth.ac.uk/ files/extranet/docs/HSC/abstract 2003 - Feb 13 health of rural communities.pdf

[23] *CPME guidelines for Telemedicine*, Standing Committee of European Doctors, 2002, http://cpme.dyndns.org:591/database/Telemedecine_2002.pdf; *Health Information Online*, Pew Internet & American Life Project, November 2004, http://www.pewinternet.org; Stearns W. R, op. cit.; *What is Telemedicine?*, April 1998, http://www.med.und.nodak.edu/depts/rural/pdf/whatistele.pdf

[24] Copeland E. T., *The Information Revolution and National Security*, Strategic Studies Institute, August 2000, http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB225.pdf; Freeh J. L., *Threats to*

огромна ризница во најразноразните (јавни и тајни) податоци и информации кои би можеле да ги задоволат најразличините желби и потреби. Воедно, тој е во непрекинат прогрес и секој ден се менува по запрепастувачки стапка на раст.

За многу поединци, групи и организации, па со самото тоа и за многу тајни служби пошироко во светот, Интернетот станува примарен начин да се обезбеди и истражат јавните информации, на начин и во мера која до скоро не ни можело да се замисли, затоа што многу од тоа што е потребно да ги задоволи корисниците на разузнавачките информации се наоѓа на јавно достапните извори. Единствено што е потребно се *брзо реакциски собирачи* и *високостручни аналитичари* способни да на начин што одговара и во вистинска смисла да соберат, обработат и брзо пласираат адекватен извештај на основа на која авторитетот може да донесе правилна одлука.

Истовремено, Интернетот е и многу јак инструмент за собирање на тајни податоци и информации (наводно, на илегален начин), со обзир на факитите дека се повеќе тајните податоци од сефовите, металните ормари, плакари фиоки масовно се дигитализираат и се пренесуваат на заштитените компјутерски системи.

Тешко е и да се замисли која тајна служба не би сакала да ваквата можност максимално да се искористи.[25]

Посебно треба да се потенцира фактот дека денешните корисници на разузнавачките податоци имаат толку многу нови извори и избор при што тешко кој се снаоѓа и во физичкиот и во виртуелниот свет, така да поради многобројноста и разновидноста неможе успешно да се експлоатираат без адекватна примена на технолошките можности. Земајќи го во предвид фактот дека истите можности ги користат и противници, јасно е дека заштитата добива првокласно значење.

2.7. Одбрана

Експлозивното ширење на информатичката технологија го поткрена виртуелниот бран и промената која длабоко и мултидимензионално делуваат на поединци, организации и општевства во целина. Во таа смисла ни армиите не биле „поштедени“. Промените кои ја предизвикуваат информатичката технологија, а кои очигледно се и видливи, се однесуваат првенствено на начинот на собирање, обработка и презентирање на информациите. Самиот факт дека оваа технологија овозможува да се обезбеди комплетна, точна и благовремена информација на донесувачите на одлуки, од воен аспект е од првокласно значење. Од друга страна, информатичка технологија значајно допринесува да трошоците на обработка и комуницирање во се повеќе и повеќе ситуации силно паѓаат, што за сите армии на светот, како исклучително големи потрошувачи на финансиските средства, представува повеќе него доволна причина да се прифати и применува оваа технологија.

Поради сето тоа повеќе армии, посебно најразвиените земји, на пат се да станат организации на информатичкото време, што во воениот информатички амбиент фундаментално ќе го промени начинот на кој армијата ќе ја спроведе својата операција во мир, конфликт или во војна.[26]

---

[25] *U. S. National security*, Congessional Statement, FBI, January 28, 1998, http://www.fbi.gov/pressrm/ congress/congress98/threats.htm; *IC21: The Intelligence Community in the 21st Century, Staff Study*, Permanent Select Committee on Intelligence House of Representatives, One Hundred Fourth Congress, Washington, 1996, http://www.fas.org/irp/congress/1996_rpt/ ic21/ index.html

[26] Metz S., *Armed Conflict In The 21st Century: The Information Revolution And Post-Modern Warfare*, Strategic Studies Institute, April 2000, http://www.strategicstudiesinstitute.army.mil/ pdffiles/

На крајот на ова поглавие за ефектите на информатичката револуција секако е потребно да се укаже дека поради ограниченият простор изложени се само најнужните фрагменти на она каде информатичката технологија остварува осетливо влијание, додека во многу други значајни области, како што се воздушни, железнички и градски сообраќај, сложени хемиски процеси, снабдување со вода и електрична енергија, нафта и гас..., би морале да бидат исклучени.

PUB225.pdf 226; Sullivan R. G., M. Coroalles M. A., *The Army In The Information Age*, Strategic Studies Institute, March 31, 1995, http://www.strategicstudiesinstitute.army.mil/ pdffiles/ PUB268.pdf

3. ИМПЛИКАЦИИ НА ИНФОРМАТИЧКАТА РЕВОЛУЦИЈА

Неспорно е впечатокот дека информатичката технологија, многу агресивно го освојува човековиот животен простор не оставајќи ни најмал дел од тој простор надвор од сопственото влијание. Меѓутоа, трансформацијата која на бурен начин се одвива пред нашите очи пропратена е со одредени импликации и консеквенции чии се главни одредници како растечката зависност на општествената заедница од новата технологија и, со самото тоа, нејзината растечка осетливост, односно ранливост на пореметувањата кои од тоа можат да произлезат.

3.1. Зависност на општествената заедница

Од изложеното не е тешко да се заклучи дека експлозивното ширење на информатичката технологија драматично го менува начинот на кој работите се одвиваат, државна управа функционираше и спровоедуваше национална одбрана, затоа што функционирњето на секоја држава, во целина и сегментарно, се повеќе се потпира на информатичката, како национална така и глобална инфраструктура, чинејќи го општеството екстремно зависно од тие инфраструктури на скоро сите нивоа на секојдневниот живот – индивидуално, комерцијално и државно.

Ширење на комуникација и зголемување на електронска поврзаност, која со тоа доаѓа без сомнеж, ќе се зголеми со поефикасен проток на добрата, сервисот, знаењата и идејата внатре во општествената заедница. Во исто време, меѓутоа, оваа потполно иста електронска поврзаност исто така ќе ја зголеми зависноста на општествата од нови форми на загрозување. А ќе биде ли оваа структура загрозена или озбилно „раздрмана“, многу од критичните функции на општествата би можеле да крахираат или да ги подлегнат на значајните пореметувања. Тоа што бара посебно внимание е фактот дека таквата денешна зависност на општествата од информатичката инфраструктура ќе расте во годините кои доаѓаат.

3.2. Осетливост – ранливост на општествената заедница

Со зголемувањето на зависноста на **општествената** заедница од информатичката технологија, сразмерно се зголемува и осетливоста, односно ранливостана таа иста заедница на разни врсти на пореметувања кои од таа зависност можат да произлезат. Како пример може да се разгледаат накратко, поради илустрација, информациите и информатичката структура од воен аспект. Познато е да армиите на технолошки развиените земји, екстремно се зависни од компјутерскиот систем кој ги подржува во водењето на војна, разузнавачки и работни функции, поради што нивната заштита е есенцијална за национална одбрана на тие земји. Доволно е, како пример, да се спомене компјутеризираниот логистички систем на таква една армија која директно ги снабдува воените бази на различни локации со се што им е потребно, од средстава за лична хигиена до муниција, гас маски и друга опрема. Не е потребно да се има премногу мудрост за да се разбере дека потенцијалните последици доколку се случи паѓање на системот во време на кризи или војна со воени единици на теренот може да бидат наместо куршуми се пратат четки за заби. [27]

[27] *Security in cyberspace*, Staff statement, U.S. Senate, Permanent subcommittee on investigations, June 5, 1996, http://www.fas.org/irp/congress/1996_hr/s960605t.htm

Слична ситуација е и со податоците кои таа армија ги поседува и користи. Во времињата пред компјутерските системи податоците и информациите биле далеку подобро заштитени. Секоја картотека била во наменски ормар, кој бил добро обезбеден. Овие ормари биле сместени по канцеларииите кои се истотака заклучувале во државните згради во кои и по ходниците и околу зградите се наоѓала вооружена стража, подржана од најсовремените технички средства надзор и контрола на пристап и движење по зградите. Воедно, пристап до овие податоци, ормари или простории не бил дозволен на сите лица кои имале пристап во зградата, туку само посебно на одредени доверливи лица.

За да се пристапи до сите овие информации, непријателот би морал да влезе во воен комплекс и во секоја зграда, секоја просторија и пристапи на секој ормар. Потоа, напаѓачот би требало некако да ги однесе сите хартиени документи или да ги копира, а да не биде откриен. Класичните, скоро до совршенство развиените системи на заштита ова го чинеле скоро немовозможно.

Во виртуелниот свет сите овие документи можат да бидат лоцирани на еден сервер кој е виртуелно е поврзан со некои други компјутери било каде во светот. Напаѓачот би можел од дистанца од повеќе илјади километри електронски да ја „заобиколи стражата“ која го чува комплексот, да направи упад во системот и со неколку отчукувања на тастатурата да направи на својот компјутер да пренесе дигитална копија на одбрани датотеки и да при тоа не биде откриен.

Меѓутоа, крадењето на информации не е единствена работа за која армијата мора да биде заинтересирана.

Кога еднаш ќе се најде во електронските датотеки, напаѓачот може и да ги модификува постоечките податоци. Промена на математичкките формули би можела да ја промени полетувачката патека на проектил или авион, а померување на децимални точки во финансискиот систем на некоја армија би можело да предизвика финансиски хаос со широки размери. Покрај тоа, напаѓачот може да инсталира „логичка бомба“ која би можела да ги уништи или промени информацијите во однапред одредено време или после некое случување. Сето ова го нарушува интегритетот на податоци и информации, а во нивна точност воените лидери би морале да имаат доверба.

Исто така, секоја армија по природа на своите обврски и задачи мора сето време да биде во состојба да пристапува до своите информации. Деструкција или одбивање на пристапот до извесни информации би можело да има опасни импликации на способност на единиците да ги извршуваат своите мисии.

Во физичкиот свет, ни една армија никогаш не би дозволила нејзините информации да бидат изложени на ризик на таков начин и во обем како во виртуелниот, електронскиот свет. Причина е што одговорните на сите нивоа добро ги разбираат заканите и опасностите кои егзистираат во физичкиот свет и познаваат можности на класичниот начин на заштита од нив. Воедно, на располагање им е и голем број на високо обучени и оштручени извршители – специјалисти за различити облици на овој вид на заштита. Меѓутоа, заканите и опасностите во виртуелниот свет дури сега отпочнуваат да се откриваат, сваќаат и разбираат, а со можност на заштитата тек треба да се запознаваат. Што се однесува на стручната поддршка, ниту ја има доволно, ниту со тоа со што располага се користи на адекватен начин. Понатаму, проблемот станува се повеќе отворен.

Конечно, следи констатацијата која мора дословно да се уважи: *Оноа што важи за армијата и нејзиниот информатички простор во потполност важи и за сите други*

општествени сегменти, уклучувајќи го во целина и јавниот и приватниот сектор,како и академската средина.

Согласно на тоа, идентификувањето и означувањето на осетливости-ранливости за било кои од овие сегменти е критично. Што се тогаш главни осетливости, односно точки на ранливост на информатичката инфраструктура? Бројните извршени анализи укажуваат на три клучни зони:

- Недостаток на безбедносна култура;
- Човечки слабости;
- Софтверско-хардверски недостатоци.

Секоја од овие слабости може да бидат експлоатирани од злонамерни извршувачи на начин и во мера која многу озбилно може да ја загрози националната информатичка инфраструктура, нејзините функции и содржини, како и институциите кои она ги поддржува, со последици кои не е тешко да се предвидат. Недостаток на простор оневозможува сите овие зони детално да се образложат.

3.3. Закани и опасности

Тоа што е до сега познато за потенцијалните закани и опасности, чии причинител е првенствено човекот со атрибути со намера, екстремно е вознемирувачки. Бројните и разновидните можности на напад во сајбер простор формираат широк спектар на закани-опасности кои се, поради полесно и подобро согледување и разбирање на суштината, обемот и сложеноста на поставениот проблем, со многу малку исклучоци, можат да се класифицираат во една од четирите следни категории:

- Компјутерски криминал;
- Сајбер тероризам;
- Разузнавачко делување;
- Информатичко војување

Основен критериум за оваа класификација е мотивот на остварување на одредена цел. Така да, најкратко, компјутерскиот криминал како главен мотив за своето делување има материјална добивка.[28] Кај сајбер тероризмот мотивот е најчесто тежнеење да се оствари некоја политичка цел.[29] Разузнавачкото делување како мотив има откривање на туѓи и чување на сопствени тајни.[30] И на крај, кај информатчката војна мотив е остварување на информатичка доминација над противникот. [31]

Од аспект на националните интереси категориите се рангирани во растечки редослед по значење, имајќи ги во вид степенот на општествените опасности кои се појавуваат. При тоа, мора да се знае дека секоја од овие категории представува сложен поим, од аспект и начин на реализација, потекло (изворот), извршителите, мотивот, употребените ресурси и крајната цел, како и активностите на секоја категорија во дадени моменти, зависно од потребите и околностите, станат составен дел на повеќе – надредени

[28]Petrović R. S., Kompjuterski kriminal, op. cit.
[29]Petrović R. S., *Kiberterorizam*, Vojno delo, god. LIII, br. 2/2001, str. 100-122.
[30] Petrović R. S., *Neki aspekti nacionalne bezbednosti u informacionom dobu*, **N**auka, **T**ehnika, **B**ezbednost (NTB), Rad po pozivu, UDC: 681.324; 65.012.8, Godina XI, Broj 1, Septembar 2001, str. 7-27
[31] Petrović R. S., Globalno informaciono ratovanje, Zbornik radova (CD-ROM), YU INFO '99, Kopaonik, 22–26.marta 1999; Petrović R. S., *Kiber prostor - peta dimenzija ratovanja*, Vojni informator, br. 4, jul-avgust 2001, str. 29-50.

категории. Секако, се поставува и прашање кои се потенцијални извршители и од каде доаѓаат нападите. Да ли е опасен напаѓачот дванаестогодишен „сајбер-шетач“, кој, на изглед, нема право ни на возачка дозвола, или е тоа добро платен припадник на странска разузнавачка служба, анархист или индустриски шпиун? Дали заканата доаѓа од странски или домашни извори? За жал, тоа може да биде било кој или дури и мешавина од напред набројани, кои имаат пристап до Интернетот, одредено техничко знаење и зла намера, независно од полот, боја на кожата, раса, образование, политички убедувања, староста и вероисповеста. Сите тие можат да нападнат и однадвор и одвнатре, во секој момент, без оглед на одалеченоста, годишното време временските зони, време на ден или ноќ и временските прилики, односно неприлики.

4. ПОИМНО ОПРЕДЕЛУВАЊЕ И ДЕФИНИРАЊЕ НА ТЕРМИНИТЕ

4.1 Компјутерски криминал

Глобалните компјутерски мрежи овозможуваат создавање на нов облик на криминал. Се појавува посебен, софистициран, продорен, технички едуциран, бескруполозен, опседнат, понекогаш одмазднички настроен поединец со кого справувањето е многу тешко. Тој често не сака да биде сам, при што му е потребно друштво, а исто така и публика. Лесното движење низ сајбер просторот му ја зголемува самодовербата. Тоа чувство не е без причина, бидејќи е многу тешко да се открие во моментот на извршувањето на делото, при што тоа представува виситинскиот момент за негово фаќање и идентификување. Од друга страна, интернетот кој е толку ранлив и несигурен заради големиот број на корисници (се проценува дека од 2004 година, бројот на корисниците на Интернет се зголемил на 888,681,131 на 25 март 2005 година, односно 13,9% од вкупната светска популација), отвореноста и големиот број нерегулирани области за безбедно користиње, преставува идеално скривалиште за криминалци од различен тип.

Во такво опкружување и со такви поединци, се почесто се прават најразлични обиди не само за добивање на поголеми национални права, преку меѓународнити организации и асоцијации, туку цел на ваквите поединци е и приватниот сектор при што се предизвикуваат голем број на негативни последици поради неспречувањето на криминалните активности. Така на пример, финасискиот сајбер криминал, Австралија во 2003 година се соочи со загуба од 3,5 милиони долари, а вирусите, црвите и тројанците преку 2 милиони. Следната година финасњискиот сајбер криминал се намалува на 2 милиони долари, но последиците од од вирусите се зголемуваат преку 7 милиони. Исто така и Британците не поминуваат ништо подобро, бидејќи во 2003 година, финасискиот сајбер криминал ги коштал 120 милиони фунти, а вирусите 27,8 милиони. Приватниот сектор и корисниците почнуваат да преставуваат значаен фактор во создавањето на услови за заштита на приватните компјутерски мрежи и нивната поврзаност со глобалната интернет мрежа. Развојот на безбедна интернет инфраструктура не може да се замисли без заеднички активности на секој од овие актери, бидејќи сајбер криминалот постанува глобален проблем. Што е всушност сајбер криминал?

Голем временски период бил потребен за да се воспостават дефинициите за компјутерски криминал во текот на неговите зачетоци, но додека процесот на дефинирање се развива, во исто време се појавува нов феномен - сајбер криминал. Обидите за разјаснување на размерите на овој криминал и неговата опасност во документот „Криминал во спрега со компјутерски мрежи“(**engl.** *crime related to computer networks*) од десетиот конгрес на Обединетите Нации посветен на превенцијата од криминал и третирањето на сторителите од април 2000 година, Експертската работна група под овој криминал подразбира „ криминал кој се однесува на било кој облик на криминал кој може да се извршува **со** компјутерски системи и мрежи, **во** компјутерски системи и мрежи или **против** компјутерски системи и мрежи“. Тоа е криминал кој во суштина се одвива во електронска околина. Ако под компјутерски систем се подразбира “секој уред или група меѓусебно поврзани уреди со кои се врши автоматска обработка на податоци(или било која друга функција) “, како што е дефинирано во Конвенцијата за сајбер криминал(***engl.*** Convention on Cyber crime), Совет на Европа, тогаш е јасно дека без електронска околина нема да постои ваков тип на криминал. Тој е комплексен, при што се смета дека е чадор - термин што ги покрива разновидните криминални активности

вклучувајќи ги нападите на компјутерските податоци и системи, нападите поврзани за компјутерите, содржини или интелектуална сопственост. Поради тоа, компјутерските мрежи односно информациско-комуникациската технологија се појавува во повеќекратна улога, односно како:

• **Цел на напади** - се напаѓаат сервиси, функции и содржини кои се наоѓаат на мрежа. Се извршува кражба на услуги, податоци или идентитет, се оштетуваат или се уништуваат поединечни делови на мрежата или цела мрежа и компјутерски системи или се спречува правилно извршување на работата на функциите. Во секој случај целта на сторителот е мрежата во која се вметнуваат вируси или црви, се хакуваат сајтови, упаѓаат хакери, се извршува „одбивање на услугите“.

• **Алатка** - криминалците од памтивек користат камен, нож, отров, пиштол и слични оружја и орудија, а денска модерните криминалци не ги „валкаат“ рацете, користејќи ја мрежата во реализирање на својата намера и извршување на делата. Некогаш користењето на мрежата представувало потполно нова алатка, додека во друга прилика веќепостоечките алатки се толку усовршени дури е тешко и да се препознаат(при што се појавуваат две варијанти: нова дела со нови алатки и стари дела со нови алатки). Користењето на ова ново вооружување особено е популарно кај детската порнографија, злоупотребата на интелектуалната сопственост или електронската продажба на недозволена роба (дрога, човечки органи, деца, жени, оружје и сл.)

• **„Околина“** во која нападите се ивршуваат. Најчесто таа оклина служи за прикривање на криминалните дела, како што многу вешто успеваат тоа да го направат педофилите, при што може да се заклучи дека и останаттите криминалци не се ништо помалку успешни.

• **Докази** како што во класичниот криминал се појавуваат, нож, отров, пиштол или некое друго средство за извршување на делата, така мрежата и ICT (***engl.*** Information Communicatin Technology) се појавуваат во доказната постапка за сајбер криминалот.

Истовремено компјутерската мрежа служи како мрежа за поврзување на разни субјекти, при што таа е поддршка и симбол. Последната улога е поврзана за заплашување и попречување.

Неоспорно е дека на сајбер криминалот му е признато „својството“ криминал (при што не треба да се занемарува фактот дека и пред овој термин се појавувале и други термини: Интернет криминал, е-криминал, криминал на високи технологии, мрежен криминал и сл.) како „облик на однесување кој е противзаконски или ќе биде криминализиран за кротко време“. Земајќи во предвид дека постојат значајни разлики помеѓу земјите како и во документите на меѓународните организации и асоцијации, малата „бариера“ за однесувањето кое што треба да биде криминализирано за краток временски период, представува преседан со кој се овозможува намалување на последиците од несинхронизираноста и неускладената правна регулатива.

Имајќи го претходно наведеното во предвид, може да се констатира дека сајбер криминалот како облик на криминално однесување каде што сајбер просторот е околина во која компјутерските мрежи се појавуваат како средство, цел, доказ или симбол или околина за извршување на кривична дела. Поради тоа под сајбер простор се подразбира или вид на “заедница“ составена од мрежно поврзани компјутери во која елементите од традиционалното општевство се наоѓаат во облик на бајт или бит или “простор во кој се креираат компјутерските мрежи“. Терминот сајбер простор прв го употребил Вилијам

Џибсон во научно-фантастичната новела *Neuromancer* од 1984 година. (“ *Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding …*”) **.**

Тој е вештачка творба која бара висока техничка опременост, добра информациска инфраструктура и која е ничија и сечија својина, во која паралелно коегзистираат виртуелно и реално и во кој комуникацијаљта се одвива колективно и поединечно. Во таква околина, исклучително е тешко да се зборува за криминал од национални размери и општествена опасност, особено не во конвеционална смисла. Наведеното се темели на тоа дека општествениот, социјалниот и економскиот контекст на овој криминал не се поистоветува со класичниот трансационален криминал, бидејќи за сајберпросторот важат други правила - врз основа на Глобалната студија за организиран криминал(***engl.*** Global studies on organized crime), Центар за превенција од меѓународен криминал и Институтот за истражување на интерегионалниот криминал, Обединетите Нации.

Иако постојат бројни потешкотии во дефинирање на ваквиот тип на криминал, како што постои и изразена тенденција да не се признаваат специфичностите кои го пратат криминалот воопшто, сепак е јасно дека таквите ставови не може да бидат прифатливи бидејќи не можат да се занемарат ниту застрашувачките начини на реализација на овој тип на криминал, како што ниту последиците повеќе не се мерат во мал број на жртви, ниту во десетици илјади долари или евра, туку во шестоцифрени броеви. Проблемите настануваат и заради новите елементи за диференцирање на овој од другите облици на криминал. Поради тоа се појавува посебно прашање кои се видови на овој криминал.

4.2 Компјутерски тероризам

Во светот не постои унифицирана, единствена дефиниција за тоа како да се дефинира терминот **тероризам**. Иако зборот е комплексен по своето значење, одредени дефиниции се фокусираат на актерите на тероризмот, додека останатите се фокусираат на терористичките тактики и цели, како и методите кои се применуваат. Со цел да се гонат овие видови на терористички акти или да се направи од вооружените и други форми на насилство и криминал, националните и меѓународните институции, како и останатите структури, од пред извесно време бараа да се дефинира поимот тероризам. Една од најчесто користените дефиниции произлегува од правните акти од САД.

Според законот во САД, тероризмот е вграден условно во Годишниот извешта кој треба да биде поднесен од страна на државниот секретар до Конгресот секоја година. Тероризмот е дефиниран на следниот начин:

„претходно планирано, политички мотивирано насилство извршено против невоени цели од страна на суб – национални групи или тајни агенти“.[32]

Кога се зборува за поимот сајбер тероризам, според Федералното истражно биро – ФБИ овој феномен се дефинира како:

„предумислени, политички мотивирани напади против информации, компјутерските системи, компјутерските програми и податоци што резултираат со насилство против цели кои не се воени од страна на суб – националните групи или тајни агенти“.[33]

[32] Code Title 22, Ch.38, Para. 2656f(d)

Според друга дефиниција дадена од страна на американската комисија за заштита на критичната инфраструктура се вели дека: терористичките напади се креирани со цел да се предизвика физичко насилство или екстремна финасиска штета.

Исто така и терористите стануваат посовремени, при што го напуштаат традиционалниот начин на војување со пушки и друго вооружување, а воведуваат користење на софистицирана висока технологија. Кога станува збор за компјутерскиот тероризам денеска постои реална опасност информациските ресурси, а посебно глобалните информатички мрежи да станат многу ефикасно средство во рацете на терористите, овозможувајќи им начини за дејствување во кои порано не ни можеле да сонуваат.

Дека информациската инфрструктура е мета на терористичките организации, укажува фактот на упатените закани од ИРА во 1997 година,кога англиската јавност била шокирана со заканите дека покрај бомби, атентати и други облици на терористички акти ќе почне да користи елктронски напади на стопански и владини компјутерски системи.

Иако навидум терористите се познати како личности со психолошки профил на кои им недостасува соодветен талент и компјутерска вештина, искуствата со Al-Quade покажуваат дека припадниците на терористичката организација се служат со софистицирани техники за заштита на своите канали на комуникација на интернет, при што постојано поставуваат нови беб локации каде ги пропагираат своите фундаменталистички идеи, а кај некои од уапсените терористи се пронајдени компјутер со шифрирани фајлови.

Опасноста од терористички акти се зголемува кога станува збор тоа дека терористите во наредниот период се повеќе ќе користат висока технологија за остварување на своите деструктивни цели, а со помош на „извори на таленти“ кои може да обезбедат експерти или специјалисти кои се способни да извршат компјутерска саботажа или шпијунажа на високо ниво, така да од терористичките групи или организации се превземаат задачи по договор, или да обучуваат терористи за тални операции по пат на висока технологија и за стратегиски тероризам кој треба да се извршува од многу дисциплиниран и организиран кадар. Како „извори на таленти“ се појавуваат следните групи: технолошки платеници, незапослени технолошки експерти од земјите од третиот свет, западни технолошки експерти, високостручен кадар од бившите тајни служби и единици и сили за специјални намени од источниот блок (Штази, Секуритате, Спецназ, Ошназ.....).

Генерален заклучок кога се работи за компјутерски тероризам е дека со текот на времето кое доаѓа, терористите се повеќе ќе користат висока технологија како за шпијунажа и саботажа така и за пропагирање на своите идеи. Веројатни терористичи цели може да бидат:[34]

- банки на податоци;
- компјутерски системи;
- владини комуникациски системи;
- автоматизирани електроцентрали со кои управуваат компјутери;

---

[33] Според Федералното биро за истрага – ФБИ (http://searchsecurity.techtarget.com/sDefinition/0.,sid14_gci771061,00.html)

[34] Според Американска комисија за заштита на критичната инфраструктура (http://searchsecurity.techtarget.com/sDefinition/0.,sid14_gci771061,00.html)

- рафинерии за нафта;
- аеродромска инфраструктура и др.

4.3 Разлики помеѓу термините сајбер криминал и сајбер тероризам

Постојат многу дефиниции за тоа што претсавува сајбер криминал и сајбер тероризам. На времето постоела конфузија дали овие два термини се синоним или не. Некои автори се држат до тезата дека овие два поими се синоним, други пак не се застапници на оваат теза. Во глобални рамки, најрелевантни дефиниции кои се применуваат се дефинициите според терминологијата на САД. [35]

Во обид да се споредат терминте сајбер криминал и сајбер тероризам во понатамошниот текст ќе бидат истакнати разликите. Акривирањето на терминот за сајбер тероризам според наше разбирање е политичката мотивација. Примарна цел на сајбер тероризмот е да се инфилтрира во системот на одредена институција каде што има за цел да предизвика штета (финансиска загуба , жртви, оштетување на сопственоста...) со што ќе се предизвика дестабилизација на безбедноста на самата држава. [36]

Хакерите[37], кои обично го предизвикуваат сајбер криминалот, ова често го прават од забава и меѓусебно се натпреварууваат за поголем личен успех, како и за остварување на имотни и други цели. Додека хакерите (сајбер терористите) кои често се дел од терористичките организации, како на пример Ал Каеда, ЕТА, ИРА итн., ова го прават со одредена политичка цел. [4]

Исто така според некои автори може да се направи и поделбата дека хакерите кои извршуваат напади од забава може да се класифицираат во групата на обични криминалци, додека сајбер терористите треба да бидат класифицирани во делот на потежок облик на специфичен криминал. [4]

Сајбер терористите може да нападнат јасно дефинирани цели кои се од стратешко значење во одредени држави, што не зачни дека нападот мора да биде од поголеми размери со намера да се постигне одредената цел. На пример, цел на нападот може да биде една централа која обезбедува електрична енергија само за населението што живее во непосредна близина. Преку вршење на овој вид на напади може да се навлезе и во помал обем, а да се постигне поголем ефект. Ако дел од Скопје не функционира поради немање електрична енергија, самото тоа ќе влијае и врз останатите егзенстицијални потреби од населението. [4]

Како нреден пример за сајбер тероризам може да се нагласи и „хакерството во компјутерскиот систем на една болница, со менувањето на медицинските рецепти како смртоносна доза што може да се толкува како чин на одмазда“[38]. Секој може да биде жртва на одреден вид на терористички напад. [4]

Заедничко нешто за овие два термини (сајбер криминал и сајбер тероризам) е тоа што се користи компјутерот како заедничко оружје за вршење на кривичното дело.

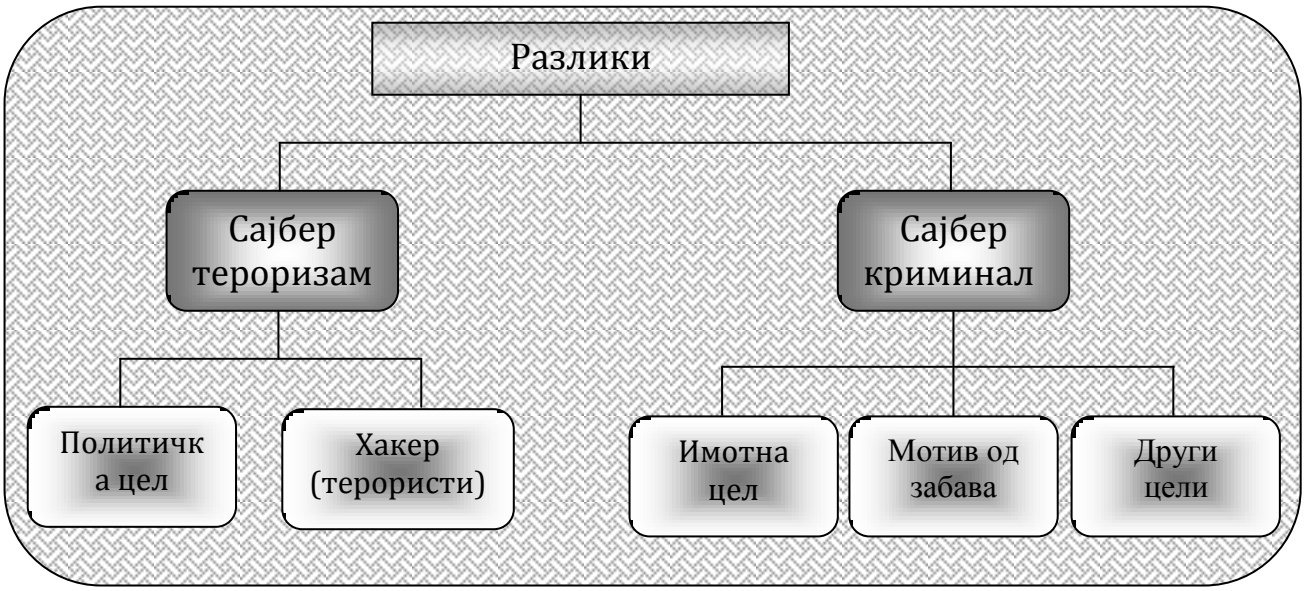
---

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

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

[37] „некој кој се обидува да се пробие во компјутерскиот систем“ (http://searchsecurity.techtarget.com/sDefinition/0.,sid14_gci212220,00.html)

[38] Cyber terrorism; Jimmy Sproles and Will Byars for Computer Ethics at ETSU 1998 (http://csciwww.etsu.edu/gotterbarn/stdntppr/)



Слика 1. Разлики помеѓу сајбер криминалот и сајбер тероризмот[39]

4.4 Компјутерски саботажи

Компјутерските саботажи се состојат во уништување или оштетување на компјутерите и другите уреди за обработка на податоци во рамките на компјутерските системи, или бришење, менување односно спречување на користење на информационите содржини во меморијата на информатичките уреди. Најчести видови на компјутерски саботажи се оние кои делуваат деструктивно на оперативно-информативните механизми и кориснички програми, пред се, оние кои имаат функција на чување на податоци.

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

5. ОБЛИЦИ НА КОМПЈУТЕРСКИ КРИМИНАЛ

Компјутерски криминал представува облик на криминално однесување, каде компјутерската технологија и информационите системи се искористуваат за извршување на кривичните дела, или компјутерот се употребува како средство или представува цел, каде се создава последици во кривично – правна смисла. Компјутерскиот криминал е исто така противзаконита повреда на податоците каде компјутерските податоци се менуваат со претходна замисла(т.н манипулација на компјутерите), разоруваат(т.н компјутерска саботажа), или се користат заедно со хардверот(т.н кражба на време).

Компјутерите и компјутерската технологија може да се злоупотребуваат на разни начини, а самиот криминал кој се реализира со помош на компјутер може да има облик како било кој од традиционалните видови на криминалитет, како што се кражби, затајување, проневери, додека податоците кои неовластено се собираат со злоупотреба на информациони системи, може на разни начини да се користат за стекнување на противправна корист.

Појавни облици на компјутерскиот криминал се:

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

5.1 Противправно користење на услуги и неовластено собирање на информации

Противправното користење на услуги се состои во неовластена употреба на компјутери или овластена употреба на истите од неавторизиран корисник.

Пример за новластена употреба на компјутерите е кога компјутерот се користи во било кои други цели, освен во цели кои представуваат намена на компјутерот во информациониот систем. Пример за овластена употреба на компјутерите за потребите на неавторизиран корисник, или заради остварување на други цели кои не се дозволени, како на пример, за случаи во кои вработениот собира податоци во една компанија за наредниот работодавач или кога расположливото компјутерско време се користи за завршување на приватни работи. Еден од најчестите облици на неовластеното користење на компјутерите со кои се среќаваат работодавачите ширум светот е е злоупотребата на Интернетот од страна на вработените.

Неовластеното собирање на информации представува своевидна кражба на податоци содржани во компјутерските системи, најчесто со цел за остварување на противправна имотна корист. Техничките и технолошките можности за неовластено собирање на информации со појавата Интернетот повеќекратно се зголемуваат така да крајна цел може да биде секој приватен компјутер или било кој друг поврзан или изолиран компјутерски систем.

5.2 Компјутерски кражби

Кражбите завземаат високо место во областа на компјутерскиот криминал, а во однос на разработената проблематика од посебно значење е представува кражбата на идентитетот. Овој вид на кражба има особено значење во општевство бидејќи покрај се останато, ја намалува довербата во интигритетот на комерцијалните трансакции и ја загрозува индивидуалната приватност. Проценките на експертите се дека компјутерските кражби ќе се зголемуваат со електронското тргување. Снабдени со индивидуални персонални информации, криминалците со украдениот идентитет може да отворат електронски сметки во банки, извршат купување, а во земјите каде се автоматизирани сервисните услуги за граѓаните, може да добијат документи за раѓање, пасош, кредит и сл., а се тоа во име на личноста за чии податоци се работи. Со лажен идентитет криминалците може да добијат кредити од банки, да купат автомобил, стан, и сл., при што на тој начин да предизвикаат финнасиско оштетување на жртвата, а во некои случаи на жртвата и се направи криминално досие. Жртвата во поглем број на случаи и не знае дека нејзиниот идентитет се „користи“ се додека не стигнат „сметки за наплата“. Значи и финасиската и „хуманата“ цена на кражбата за индивидуална жртва може да бидат многу високи, иако единствена причина за многу жртви може да биде тоа што нивните персонални податоци биле во некој фајл кој е украден или пак наивно давале информации на погрешни луѓе.

Иако поголемиот број на експерти тврдат дека потрошувачите се изложени на многу поголем ризик со користењето на кредитните картички во шопинг центрите при тргување, ресторaните или бензиските пумпи, отколку преку користењето на заштитените веб страници, бидејќи криптографската технологија и автентификациските процедури на веб страните ги штитат онлајн трансакциите на поголемиот број купувачи, додека прашањето за приватноста и стравот малверзација со кредитните картички во одредена мерка негативно влијае на онлајн трговијата.

5.3 Компјутерски измами

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

Бројот на облици на измами, како и начинот на нивната реализација е практично неограничен и во пракса се среќаваат од примитивни и „груби“ до измами за кои е користен висок степен на вештина и рафинираност. Но, во шемите за компјутерски измами секогаш се открива некој претходно постар користен облик на измама. Бидејќи во сите шеми на измами регистрирани на интернет се всушност преработени и прилагодени верзии на шеми, со кои некогаш и со векови се „ставани“ во заблуда невнимателни и лесноверни жртви.

Компјутерските измами се карактеризираат со многу големо продирање, заради голиминатa на интернетот како пазар, бидејќи брзо се шират со интернетот како медиум со кој се се случува многу брзо, а исто така и заради ниските трошоци за извршување на ваквиот вид на измами.

Компјутерските измамници ги злоупотребуваат карактеристиките на на Сајбер просторот допринесува раст на електронската трговија: анонимност, дистанца помеѓу продавачот и купувачот и моменталната трансакција. На тој начин тие ја користат и предноста на фактите дека измамата преку интернет не бара пристап до некој систем за исплата, како за тоа што бара секој друг вид на измама, а сито така и фактот дека дигиталниот пазар е сеуште недоволно уреден при што се создава одредена конфузаија за потрошувачите, што за компјутерските измамници се создаваат скоро идеални услови за компјутерски измами.

5.3.1 Измами со производи со „неверојатни карактеристики“

Големиот број на истражувања, како и одржаните семинари за измами со производи со „неверојатни карактеристики“ укажуваат дека една од најголемите на нелегални заработки на интернет се измамите со производи со „неверојатни карактеристики“. Врз основа на извештајот од Специјализираните агенции за заштита на купувачите на интернет Сиднеј, Австралија секои 44 секунди некој станува жртва бидејќи се одлучува да купи производ со „зачудувачки можности“ запознавајќи го преку интернет. Исто така наведените агенции извршиле истражување на Интернет при што откриле 1400 сомнителни сајтови само во областа на здравството, а како резултат на истражувањето се покренати тужби против 18 компании и детални истраги кои се во тек а опфаќаат уште 200 фирми во 19 земји ширум светот. Колкава штета е предизвикана од нелегална трговија во извештајот не е наведено, но доколку се знае дека таквите производи како серијата „Виолетова хармоија“ – од каде еден продукт наводно создава ново ниво на енергија во човечкиот организам – со цена од 30$ и 1095$, може лесно да се пресмета колку е заработувачката во милијарди долари секој ден. На врвот на листата на производите со „неверојатни карактеристики“ кои се продаваат на интернет се наоѓаат пилули кои овозможуваат на своите корисници да пијат пиво колку сакаат, а при тоа да не се здебелат (цена 71$ за 60 пилули) и појас за вежбање, кој кога не си во фотеља предизвикува исти ефект како направени 600 склекови за 10 минути (цена од 146$), потоа лушпи од јајца на птици кои наводно го зголемуваат либидито, течност која маснотијата од ткивото во текот на спиењето ја претвора во мускулна маса, хормони кои ја враќаат довербата во сопствената снага, магнети против несоница, вода која лечи аритритис, лекови за лечење на AIDS, а кои доаѓаат од Африка како решение на анегдотата зошто некои Афрички жени се имуни на оваа болест....

Наведените истражувања укажуваат дека „наивните купувачи“ односно жртвите најчесто се стари личности, болните, изнемоштените и сиромашните, кои бараат „трошка надеж за светлина во мрачниот бескраен тунел“.

6. ОБЛИЦИ НА РЕГУЛИРАЊЕ НА КОМЈУТЕРСКИОТ КРИМИНАЛ

Соодветна правна регулатива се користи за компјутерскиот криминал. Од првите појавни облици, на почетокот на 90 – тите години, до денес, многу меѓународни тела имаат посветено внимание на компјутерскиот криминал. Покрај меѓународната правна регулатива се е почесто правното регулирање на компјутерскиот криминал на национално ниво, особено на одредени облици. Правното регулирање на компјутерскиот криминал се одвива во повеќе правци, во зависност од облиците на појавување. Интересно е дека многу повеќе активности се случуваат на меѓунарпден план во однос на правното регулирање на компјутерскиот кримина на национално ниво. Тоа донекаде е природно, земајќи ги во предвид карактеристиките на делата и својствата на криминалците кои се извршители.

Најзначајните и најбројните меѓународни акти се донесенин во рамките на Европската Унија[40]: 1998 година изработена е посебна студија под наслов правни аспекти на компјутерскиот криминал во информациско општество (***engl.***Legal Aspects of Computer-related Crime in the Information Society – COMCRIME study), д-р Урлих Зибер, Универзитет во Вирзбург, која ги разработува основите на компјутерскиот криминал како возвивишен облик. Студијата во комбинација со останатите документи произлезени од Лисабонскиот состанок на Советот на Европа, 2000 –тата, каде е истакнато значењето на транзицијата во конкурентна, динамична и на знаење заснована екононимија, ги представува насоките на активностите поврзани за разбирање на феноменот компјутерски криминал. Акциониот план (***engl.*** e - Europe Action Plan) од истата година поврзан е со активности за обезбедување на сигурноста на мрежите и воспоставување на спработка на земјите членки и нивен заеднички пристап према компјутерскиот криминал до 2002 година. Во истата година е донесен и Предлог на Советот за правна рамка за одлучување поврзано за нападите на информационите системи (***engl.*** Proposal for a Council Framework Decision on attacks against information system). После една година, документото е дополнет со недозволен пристап во информационите системи и недозволено попречување на системите и податоците. Во 2000 година донесена е и Директивата за електронско работење (***engl.*** *Directive on electronic commerce*) во која посебно внимание е посветено на проблемот за злоупотреба.[41] Исто така, истата година се донесуваат различни документи поврзани со правното регулирање на компјутерскиот криминал: Одлука на Советот за спречување детска порнографија на интернет, Конвенција за меѓусебна помош во кривично – правната материја, Препорака за стратегијата во новиот Милениум за заштита и контрола на комјутерскиот криминал. Потоа следува документ кој треба да обезбеди сигурно информациско општевство низ безбедна информациска инфраструктура и борба против криминал поврзан за компјутерите (***engl.***) Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime)[42]. Важно е да се напомене дека наведената година има есенцијално значење, бидејќи се донесуваат голем број на документи со кои се регулира правната рамка за борба против компјутерскиот криминал или исто така познат како криминал на високи технологии.

---

[40] Legal Aspects of Computer-related Crime in the Information Society – COMCRIME study, http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf

[41] Directive on electronic commerce http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF

[42] Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, http://www.justice.gov/criminal/cybercrime/intl/EUCommunication.0101.pdf

Во 1983 година во рамките на OECD (***engl.*** Organization for Economic Cooperation and Development), усвоена е Студија за меѓународна примена и хармонизација на кривичното право поврзано за проблемите на компјутерскиот криминал и злоупотребата, а три години покасно излезена е Листа во рамките на документот Криминал врзан за компјутери: анализа и правна политика, а 1999 година е обележена како година во која се донесени цел сет на прирачници за сигурност на информационите системи со кои се воспоставуваат правила и правземаааат соодветни мерки за постигнување на сигурноста.

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

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

Во рамките на групата Г8 од 1997 година (кога е предложен акциониот план за борба против компјутерскиот криминал, а усвоен 1998 година), на предлог на експертската група за соработка на полето правда и внатрешни работи, министрите за правда и внатешни работи во повеќе наврати во повеќе наврати расправале за принципите на таа борба, како и за потребите за меѓународна соработка во спроведување на истраги и фаќање на извршителите како и прифаќање на стандарди дефинирани со конвенцијата на Советот на Европа.

Исто така, оваа организација ги има донесено следните документи:

- ✓ Recommendations for Enhancing the Legal Framework to Prevent Terrorist Attacks ;

- ✓ Recommendations on Special Investigative Techniques and other Critical Measures for Combating Organized Crime and Terrorism ;

- ✓ Recommendations for Sharing and Protecting National Security Intelligence Information in the Investigation and Prosecution of Terrorists and Those Who Commit Associated Offenses: Best Practices for Network Security, Incident Response and Reporting to Law Enforcement , и други.

Обединетите Нации (ОН), исто така имале бројни активности, при што донеле соодветни акти кои директно или индиректно биле поврзани за решавање на проблемот за компјутерски криминал. Покрај ОН со одредени аспекти или типови на овој криминал се занимаваат и други меѓународни организации каква што е WIPO, Меѓународна стопанска комора, Светска трговска организација, Азиско-пацифичка организација за економска соработка.

Материјалните права стануваат „бесмислени“ во однос на процесните, кои треба да ги опфатат сите постапки кои се врзани за кривичните, граѓанските, управните, арбитражните и други работи и активности. Овие права треба да им олеснат на правосудните и истражните органи во собирањето на податоците во доказната постапка за извршените дела и извршителите. Истовремено наведените одредби би требало да ја олеснат институционалната соработка, која мора да се воспостави помеѓу соодветните органи од различни земји, како и меѓународните полициски органи. Врз основа на претходно наведеното Европската Унија во 2000 -тата година донесува Конвенција за меѓународна помош во криминалната материја (***engl.*** *Convention on Mutual Assistance in Criminal Metters*), со која не се предвидува само соработка туку и усклaдување на правните и правосудните системи на земјите членки. Соработката се очекува и со релевантни институциски корисници, органи за супервизија за заштита на податоците, како и индустријата. Истакнувањето на воспоставувањето на ефикасност, транспаретност и рамнотежа меѓу сите актери кои кои треба да допринесат во борбата за спречување и санкционирање на сајбер криминалот, представува оправданост на Конвенција за меѓународна помош во криминалната материја. Во однос на компјутерскиот криминал ниту групата Г8 не изостанува во решавањетро на практичните прашања за соработка и интернационализација на активностита врзани компјутерскиот кринал. Воспоставена е мрежа која 24 часа 365 дена во годината обезбедува адекватна примена на принципите за борба против криминалот на високи технологии. На нив се придружуваат и земји кои не се членки. Со тоа што кругот се шири а очекуваните ефекти треба да бидат подобри. Создаден е и експертски тим кој треба да ги идентификува методите и техниките, како и да ги дефинира стандардите кои може да се применуваат во борба против компјутерскиот криминал, како и пружањето на помош на специјализираните тела за негово откривање. Експерскиот тим ја сочинува Меѓународната организација за компјутерски докази (***engl.*** *IOCE*) како организација на која и се пиклушуваат тимови од Европската Унија и нејзините земји членки. На тој начин е воспоставена мрежа со цел да се олесни реализицијата на програмата за истражување и следење на овој вид криминал.

Во Р. Македонија санкционирањето на овие кривични дела е регулирано со член 251 од Кривичниот законик, член 251 од КЗ на (навлегување во компјутерски систем) службен весник бр. 37/1996 година. Кај нас ова кривично дело е внесено во КЗ во 1996 година и од то гашпа наваму се применува овој член во практика. Спаѓа во глава 23,

Кривич ни дела против имотот од КЗ на Р.Македонија. Став 1 од овој член вели: Тој којшто неовластено ќе внесе измени, објави, скрие, избрише или уништи компјутерски податоци или програми, или на друг начин ќе на влезе во компјутерски систем со на мера за себе или за друг да прибави противправна имотна корист или да оштети друг - ќе се казни со парична каз на или со затвор до три години. [43]

Во Германија тоа е регулирано со Закон за сузбивање на стопански криминал од 1986, Компјутерска шпионажа член 202, компјутерска измама чл. 263, Промена на податоци чл. 302, компјутерска саботажа чл.303. Во Австрија регулирано е во1989 година, чл. 126 оштетување на податоци. Англија во 1990 со Закон за злоупотреба на компјутери кој предвидува повеќе кривични дела ја регулира оваа проблематика. Во Република Словенија - Казнен закон од 1999 година со чл. 225 - Противзаконски влез во заштитена база на податоци; чл. 242 – Навлегување во компјутерски систем, додека во Република Хрватска компјутерскиот криминал е регулиран во 1996 година со член 223 - Оштетување и употреба на туѓи податоци.[44]

6.1 Превземање на други мерки за регулирање на компјутерскиот криминал

Адекватноста и ефикасноста во регулирањето на компјутерскиот криминал сериозно се доведува во прашање доколку не се превземат други мерки. Студиите и останатите материјали содржани во рамките на меѓународните организации и асоцијации, како и одговорните национални институции предвидуваат реализација на мерки во рамките на постојаните консултански процеси. Така на пример во рамките на COMCRIME студијата е предвидено:

- формирање на посебни единици на специјализирана полиција на национално ниво;
- воспоставување соработка помеѓу правосудните органи, индустријата, организацијата на потрошувачи и телата за заштита на податоци;
- „охрабрување“ во создавањето на специјализирани продукти кои служат за зголемување на сигурноста на компјутерските системи и мрежи.

Се разбира, никако не треба да заборави на исклучителното значење на енкрипција, како основна алатка за обезбедување на сигурноста на нови услуги, осбено во електронското работење, а кој треба да овозможи ефикасна борба против криминалот на интернет. Сепак, воспоставувањето на специјализираните единици за откривање, пратење и фаќање на сајбер криминалците, представува чекор напред од кој се очекува поголема успешност и посигурен излез на во сајбер просторот на корисникот. Како пример на работа на таквите тела представува воспоставувањето на „жешка линија“ помеѓу големиот број на земји од САД, Велика Британија, Германија, Норвешка, Австрија, Холандија до Ирска во рамките на таканаречената ***Daphne*** програма и поврзаните провајдери во Европскиот Форум. Овие активности се поддржани и од експерти кои поради произлезената обврска од договорот за воспоставување на конкретни мрежи на „жешки линии“ или симболично наречени „електронска кула на стражари“ под покровителство на организацијата на УНЕСКО се состанале во Париз во 1999 година. На нив треба да им се додат и екипите собрани окулу проектот Екскалибур (***engl.*** *Excalibur*) кој е развиен од Шведското разузнавачко одделение за криминал и со кое се воспоставува

[43] Македонско сонце 501/ 06.02.2004
[44] Македонско сонце 501/ 06.02.2004

соработка помеѓу полициите на Германија, Велика Британија, Холандија и Белгија заедно со Европол и Интерпол.

Овие специјализирани единици мора перманетно да се усовршуваат за да може да се спротистават на многу специјализираните криминалци. За таа цел Европол организира постојана обука на своите членови од специјализираните групи, а повремено и посебни семинари за оние кои се насочени во областа на одреден вид на сајбер напад. Како пример може да се наведе семинарот одржан за одредена група инспектори организиран од Европол кој се однесувал на спецификите за детска порнографија на интернет и методите и техниките за откривање на „изворите", како и начините за собирање и обезбедување на докази. Слично на Европол, исто така во рамките на Интерпол, а ниту посебната група на експерти во рамките на Г8 не изостанува со континуирано усовршување. ФБИ (***engl.*** *Federal Bureau of Investigation*) во 2000 –тата имало 16 (шестнаесет) специјализиарни станици на територијата на федералните држави со над 190 (стоидеведест агенти) групирани во единици од 3-4 инспектори. Потребно е во бројката да се додадат и бројните универзитетски професори и соработници, како и експертите од институтите, индустријата, компаниите и разни други организации и институции и сите оние кои се вклучуваат по повик за откривање, следење и собирање на докази, но за пружање на консултански услуги на службените единици. За да се согледа во колкав размер е овој феномен и идентификуваат карактеристиките на појавните облици се формирани посебни тимови за анализа (во ФБИ популарно се наречени ***engl.*** *Computer Analysis and Response Teams* – CART, кои имаат трострука улога, да пронаоѓаат и анализираат податоци неопходни за подршка на инспекторите од ФБИ, да бидат техничка и советодавна поддршка и да помогнат во развојот на софтверските и другите производи за обезбедување на сигурноста на компјутерските системи и мрежи). Во денешницата бројот на тимови е многу поголем.

Воспоставувањето на соработката помеѓу правосудните органи, индустријата и разноразните организациц и асоцијации посебно е потенцирана во 1997 година, кога во Вашнгтон е одржан состанок на министрите за правда и внатрешни работи од земјите членки на Г8 и кога се утврдени 10 точки на Акционинен план за борба против сајбер криминалот меѓу кои посебно место е посветено на соработката во индустрискиот сектор кој дизајнира, развива и приозведува компоненти од глобалните мрежи но исто така и кој треба да биде одговорен за изградба и примена на технички стандарди за сигурност. На тој начин е воспостевена соработката со произведувачите на специјализирани хардверски исофтверски производи наменети за сигурноста. Комисијата на Европската Унија има донесено Одлука за развој на посебен програм (EU R&D Framework Programme, Internet Action Plan, i Programs STOP i Daphne) кој има за цел да ги утврди правците за борба против поединци и групи кои се здружени со цел злоупотреба на електронското работење во рамки кога бројни субјекти се потенцијални и стварни жртви.

Можеби најзначајна активност е обидот за операционализација на соработката помеѓу овие актери со формирање на ЕУ Форум, кој ги ипфаќа разните агенции, провајдерите на интернет услуги, операторите за телекомуникации, организацијата за човечки права, представниците на организациите за заштита на потрошувачите, телата за заштита на податоците и сите други заинтересирани кои сакаат да воспостават соработка во борбата против компјутерскиот криминал на европско ниво.

Форумот треба да овозможи:

- развој на 24/7 врска помеѓу државните органи и индустријата;

- дефинирање на стандардни барања за кои провајдерите треба да обезбедат информации за користење на интернет;
- изградба и примена на етички кодекс со дефинирање „добри работни навики“ на сите учесници, а посебно во меѓусебните односи помеѓу државните органи и индустријата;
- поттикнување за размена на информации за трендовите на криминалот за високи технологии помеѓу различните партнери, посебно во рамките на индустријата;
- воспоставување на посебни концерни за развој на нови технологии;
- развој на менаџмент механизмот со кој се дава заштита, олеснува идентификацијата и се совладуваат пречките врзани информационата инфраструктура;
- воспоставување на цврсти облици за експертска соработка помеѓу различните меѓународни организации, тела и асоцијации (на пример Совет на Европа и Г8);
- развој на принципи за соработка (***engl.*** *Memorandum of Understanding, Codes of Practice in line with the legal framework*)

6.2 Начини на дознавање,мерки за откривање на сторителите и докажување на компјутерскиот криминал

Редоследно постапката е следна: пријава од оштетен, откривање од страна на администраторите на информатичките системи, истрагата и докажувањето мора да го прават стручни лица со посебни, стручни и практични знаења и компјутерска форензика. Еден од најчестите начини за дознавање на кое било кривично дело, па така и на кривични дела од областа на компјутерскиот криминал, е секако пријавата од оштетениот. Во оваа смисла под поимот оштетен можат да бидат физички и правни лица, државни органи и институции. [9]

На пример, кога стручните лица кои ги одржуваат и администрираат информатичките системи ќе забележат дека дошло до неовластено навлегување во системот кој тие го одржуваат однадвор и дека настанала одредена штета во смисла на губење на податоци или на целокупното работење на системот, секако дека ова неовластено навлегување треба да го пријават до соодветен државен орган кој е надлежен понатаму да постапи, со цел пронаоѓање и санкционирање на сторителот.[45]

Стручните овластени лица на овој орган ќе го проценат видот и обемот на настанатата штета и ќе преземат понатамошни мерки. Истражувачите на овој вид криминал понекогаш користат оригиналнса апликациска програма, а понекогаш специјален софтвер за анализа и алатки за истражување. Истражувачите најдоа начини за собирање траги од оддалечен компјутер до кој тие немаат непосреден физички пристап, спроведувајќи пристап преку телефонска линија или мрежна конекција. Дури е можно да се следат активностите на компјутерска мрежа преку интернет. Овие про цедури формираат дел од она што е наречено компјутерска форензика, па некои луѓе исто така го користат овој термин при употреба на компјутерот за анализа на комплексни податоци

[45] Македонско сонце 501/ 06.02.2004

(на пример конекции помеѓу индивидуи со испитување на телефонско логирање или трансакции преку банки). Другата употреба на терминот е кога компјутерите се искористени во судот во форма на компјутерска графика за да илустрираат комплексна ситуација, или како замена на голем волумен на лис тови - базирани на истражувања и состојби. [9]

Што е всушност компјутерска форензика? Компјутерска форензика е доказ од компјутер кој треба да биде издржан, убедлив и доволен за судот да може да го прифати. Во форензичко-информатички постапки без разлика колку и да се внимателни луѓето кои имаат за цел да крадат електронски информации тие оставаат траги од нивните активности. Исто кога сторителите се обидуваат да го уништат доказот кој е на компјутер тие позади себе оставаат траги. Во двата случаи може да се докаже дека овие траги може да се пронајдат и да се презентираат пред судот. Компјутерските форензички специјалисти прават повеќе од вклучување на компјутерот и листање на фолдери и пребарување на фајлови. [9]

Тие треба да бидат способни да извршат комплексни "evidence recovery procedures" со вештина и експертиза која ќе го држи кредибилитетот на електронските докази пред судот. Во основа овие постапки опфаќаат: копирање на податоци, барање на докази од електронска пошта и друга интернет комуникација, враќање на податоци, пребарување на документи и други податоци. [9]

7. ОБЛИЦИ НА РЕГУЛИРАЊЕ НА САЈБЕР ТЕРОРИЗМОТ

Во Република Македонија не постои одредена законска рамка за борба против сајбер тероризмот. Многу луѓе и институции во Република Македонија наемаат идеја што всушност преставува поимот сајбер тероризам и каков сериозен проблем би преставувал овој вид на тероризам. Иако тероризмот како појава е широко распространет низ целиот свет и низ сите медиуми, сепак постои одреден сериозен недостаток од истражувања и дебати за влијанието кое би го имал овој облик на тероризам – сајбер теорзмот. [4]

Сепак, во текот на последните неколку години Македонија направи мал чекор во да се ангажира за прашањата поврзани за сајбер тероризмот. Поточно, сето ова започна кога станаа алармантни нападите врз веб сајтовите[46], како предмет на напад од страна на хакарите кои доааѓаат однадвор.[47] Како илустрација, во 2008 година, официјалната веб страница на бившиот Претседател на Република Македонија Бранко Црвенковски беше нападната од страна на група хакери од Косово, Албанија и Грција.[48] [4]

Република Македонија ја инцираше борбата против тероризмот со учевство на разни семинари и конференции кои се поврзани на темата сајбер тероризам. [49] Македонија исто така има ратификувано и голем број на меѓународни конвенции кои се однесуваат на сајбер криминалот. Во 2004 година Македонија ја ратификуваше и Конвенцијата за компјутерски криминал донесена во 2001 година од стрна на Советот на Европа, како и допол нителни протоколи за криминални акти од расиситичка и ксенофобична природапреку компјутерските системи. Значи,овие меѓународни правни акти се инкорпорирани во домашното законодавство. [4]

Македонските државни власти стануваат се посвесни за фактот дека официјалните веб страници на државните институции се ранливи на сајбер напади, а поради слабата заштита, по правило лесна цел. Државните веб сајтови најчесто се нападнати од страна на хакерите кои доаѓаат од заемјите во соседството. [4]

ИТ (***engl.*** *Information Technology(IT)*) специјалистите треба да ги преземат сите неопходни мерки и да ги користат сите методи кои им стојат на располагање се со цел да ги заштитат податоците на организациите (државните, јавните и приватните). Тие треба да ги посетуваат сите обуки, да ги применат сите апликативни методи за да го обезбедат и заштитат целокупниот систем на организацијата. [4]

Државните власти, исто така, без двоумење и без никакви одложувања, треба да го ажурираат Кривичниот законик на РМ со посебна одредба која ќе го регулира терминот сајбер тероризам. [4]

7.1 Република Македонија во борбата против сајбер тероризмот

Во Република Македонија нема посебни специјализирани институции кои се занимаваат со сајбер тероризам и кои легално го истражуваат. Тоа е така бидејќи во Македонија сајбер тероризмот не е легално дефиниран, регулиран и прифатен.

---

[46] Веб сајтови на: Претседател Ѓорѓи Иванов (www.president.gov.mk); Бившиот Претседател Бранко Црвенковски 2004-2009(www.president.gov.mk); А1 (www.a1.com.mk); Телма (www.telma.com.mk); Музеј на Македонија (www.musmk.org.mk)

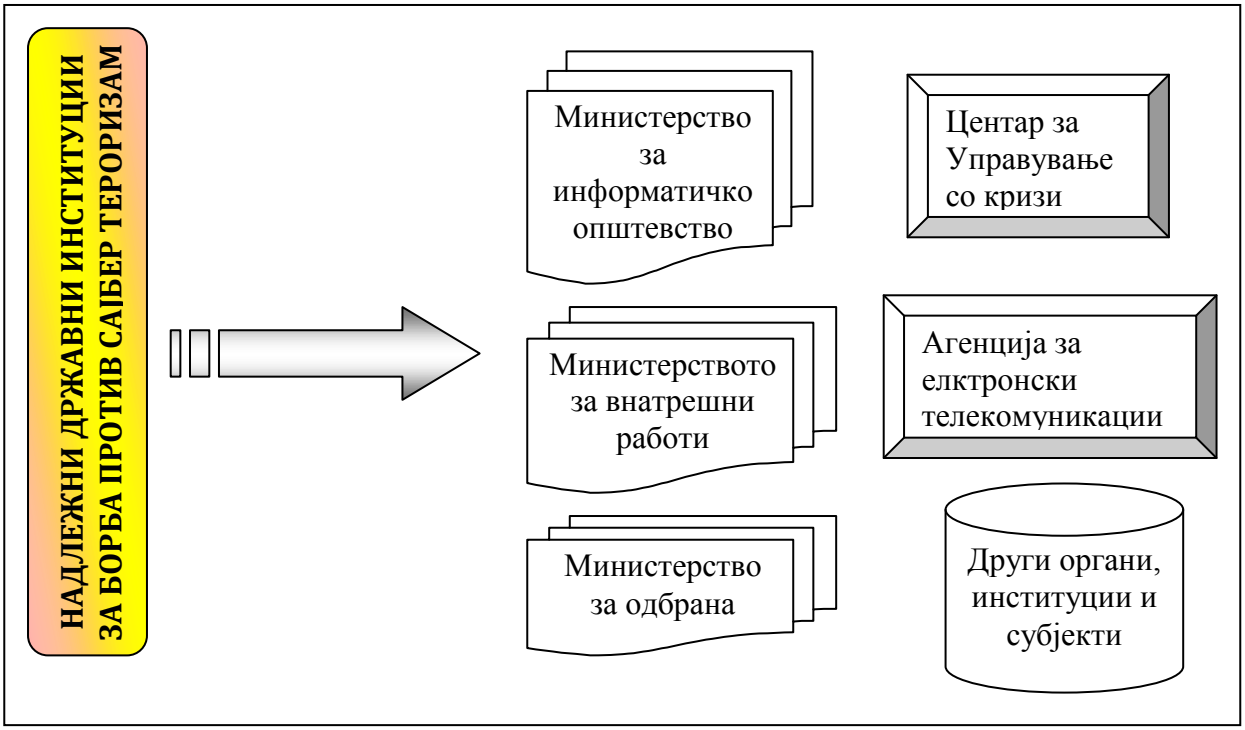
[47] Македонските сајтови се супер за хакирање; Вест

[48] Македонските сајтови се супер за хакирање; Вест http://www.vest.com.mk/?ItemID=B8658BB6CF4BDE48B575FF9B62084C09

[49] Активности за превенција и справување со последици од сајбер тероризам. Министерство за информатичко општество http://www.mio.gov.mk/?q=node/1911

Меѓутоа постојат државни институции одговорни за одредени аспекти на сајбер тероризмот, како на пример заштитата на информатичката технологија и безбедноста во целина. Овие институции ги сочинуваат: Министерство за информатичко општевство, Бирото за јавна безбедност, кое е во рамките на Министерството за внатрешни работи, Министерство за одбрана, Центар за управување со кризи и Агенција за електронски комуникации. Овие институции се согласија да ги координираат активностите и да ја определат институционалната основа за градење норми и интензивна меѓународна соработка за борба против сајбер тероризмот. Земајќи го сето ова во предвид, важно е да се потенцира дека за да започне да се применува еден функционален систем против сајбер тероризмот, потребна е поголема проактивна ангажираност и соработка со други државни институции, како и измена, дополнување на веќе постоечкиот Кривичен законик и соодветни прописи.

Следува графички приказ на надлежните државни институции, кои треба да го решат прашањето за борба против сајбер тероризам.



Слика 2. Надлежни институции во Р. Македонија

8. УПАД ВО КОМПЈУТЕРСКИТЕ СИСТЕМИ

Иако изразот „упад“ асоцира на примена на одредено механичко движење, заради влегување во „затворен“ простор, како што е извршувањето на класична кражба, но кога станува збор за компјутерски криминал, зборот представува суптилно, по електронски пат извршено нарушување на тајноста на одреден компјутерски систем, односно неовластен електронски упад во централниот компјутерски систем, односно неовластен електронски упад во централниот компјутерски систем и неговата база на податоци. Овие дела претежно ги извршуваат хакери, кои преку персоналните сметачи вклучуваат и други инфомациони системи, при што првенствено се користи интернет. Извршителите на ваквите дела, многу вешто ги заобиколуваат заштитните механизми, при што делата не ги извршуваат од злонамерни побуди, туку настојуваат јавно да ги демонстрираат своите информатички вештини со кои располагаат или да укажат на постоечките слабости во механизмот за заштита на компјутерскиот систем. Затоа на мета на извршителите на вакви дела се компјутерските мрежи, од кои се очекува да бидат максимално заштитени од електронски упади, а се работи за следноте: воени компјутерски комуникации, инфорамациони системи на безбедносните служби, државните институции и други.

Иако незлонамерноит упад во компјутерските системи, вообичаено се третира како најлесен вид на компјутерска деликвенција, тој во ниеден случај не е безопасен. Со тоа, ваквите упади претставуваат потенцијална опасност за виталните компјутерски мрежи предизвикувајќи непоправливи штети. Поради тоа, во кривично правна смисла со овие дела, доколку не се предизвикани одредени конкретни штетни последици, обично се врши повредување на тајноста на податоците, во заштитените компјутерски банки на информации.

8.1 Криминал врзан за компјутерски мрежи

Криминалот врзан за копмјутерските мрежи е облик на криминално однесување каде што сајбер просторот е околина во која компјутерските мрежи се појавуваат во трострука улога: како средства и алатка, цел или окружување во кое се извршуваат кривичните дела.

- **Компјутерски мрежи како цел на напад –** се напаѓаат сервиси, функции и содржини кои се наоѓаат на мрежа. Се крадат податоци и услуги, се оштетуваат или уништуваат делови или цели мрежи и копмјутерски системи, или се попречува работата на функциите. Во секој случај цел на извршителите е мрежата во која се уфрлуваат malware, се извршуваат DOS напади и др.
- **Компјутерските мрежи како средство и алат –** денес модерните криминалци ги користат се повеќе компјутерските мрежи како оружје за реализација на своите намери. Користењето прво на новото вооружување особено е популарно кога станува збор за детската порнографија, злоупотреба на интелектуалната сопственост, или онлајн продажба на недозволени стоки (дрога, човечки органи и др.)
- **Компјутерските мрежи како околина во која нападите се реализираат.** Најчесто тоа опкружување служи за прикривање на криминалните работи, особено тоа важи за педофилите, а ни другите криминалци не се ништо многу помалку успешни. Исто така постојат и други облици, како што е на пример користење на мрежата за застрашување, разноразни вплеткување, кои што некогаш се повеќе изразени кај компјутерскиот отколку кај сајбер криминалот. Важно е дека на

сајбер криминалот му е признато „својството“ на криминал како „облик на однесување кој е противзаконит или ќе биде криминализиран за кратко време“.

Во зависност од типот на извршените дела сајбер криминалот може да биде:

I. Политички:

- сајбер шпијунажа и сајбер саботажа;
- хакирање;
- сајбер тероризам;
- сајбер војување.

II. Економски

- сајбер измами;
- хакирање
- крадење на интернет време и услуги;
- пиратство на софтвер и микрочипови;
- сајбер индустриска шпијунажа;
- спам;
- злоупотреба на жени и деца;
- манипулација со забранети производи, сустанци и стока – дрога, човечки органи и оружје;
- повреда на сајбер приватноста – надгледување на електронска пошта, прислушкување, снимање, пратее на е-конференции, прикачување и анализа на шпијунските софтвери и „cookies“;
- производство и дистрибуција на недозволени штетни содржини како што се детска порнографија, педофилија, верски секти, ширење на расистички, нацистички и слични идеи и ставови.

8.2 Сајбер напад врз информациско-комуникациската инфраструктура на Естонија

Естонскиот случај преставува еден од најгоелмите кои некогаш се случиле во историјата. Овој случај вклучува серија на сајбер напади кои започнале на 27-ми април 2007 година. Тие нападите се извршени врз информациско-комуникациските системи на Естонскионскиот парламент, во банките, министерствата, медиумите, всушност, во сите значајни државни институции при што предизвикале дестабилизација на државната безбедност.[50]

Нападот се случил во време на затегнати односи , после една дипломатска расправија помеѓу Естонија и Русија за дислоцирање на воениот споменик на Советскиот

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

Сојуз во Талин, кога новинарите од Естонија во медиумските извештаи ја обвиниле Руската влада за отпочнување на нападот.[51]

По бранот на напади врз виталните институции на Естонија, таа побарала помош од НАТО со цел да развие заедничка стрегетија против „сајбер терористите".

Иако имало обвинувања испратени врз Кремљ од страна на медиумите во целина, на 6-ти септември 2007 година, Министерот за одбрана на Естонија признава дека нема докази кои што ги поврзуваат сајбер нападите со руските хакери со следната изјава:

„Се разбира, во моментов јас не можам со сигурност да тврдам дека сајбер нападите биле организирани од Кремљ или други руски владини органи", рекол Џек Авиксо во интервју на Естонскиот втор теевизиски канал. [52]

Русија ги отфрлила обвинувањата и ги нарекла неосновани, бидејќи тие имале за цел да ги дестабилизираат добрите соседски односи помеѓу двете земји.

Од друга страна, ниту НАТО, ниту експертите на Европската комисија не успеале да најдат докази за вмешеност на руските службеници во тие настани.

И покрај направените напори, на 10-ти март 2009 година целата ситуација станува појасна со изјавата дадена од страна на Константин Голоскоков, комесар во Кремљ поддржан од малдинската група Наше, во која изјавил дека ја превзема одговорноста за сајбер нападите.[53]

Со цел да се заштити Естонија превзема поинакви безбедносни мерки за одбрана од сајбер нападите и прави јасна поделба на задачите помеѓу владините институции и ги ангажира актерите од секторите како што се приватните безбедносни агенции да работат на подобрување на критичната инфраструктура.[54]

Естонскиот парламент од неодамна се занимава и со ревизија на Кривичниот закон[55], се со цел да почнат да се применуваат поригорозни методи, да се обезбеди поголема сигурност за сите витални институции во државата и да се спречи нејзината понатамошна реализација. .[56]

8.3 Последици од компјутерски криминал

Штетите што настануваат со извршување на компјутерските дејанија, во зависност од облиците во кој се појавуваат на компјутерскиот криминал, може да се поделат на:

[51] Cyber terrorism: The World's First Internet War?: Stefan Nicola; August 8, 2007; (http://www.govtech.com/dc/articles/12966)
[52] Estonia has no evidence of Kremlin invlment in cyber attacks; Ria Novosti; 2008 (http://en.rian.ru/world/20070906/76959190.html)
[53] Kremlin-backed group behind Estonia cyber blitz; Charles Clover; March 11, 2009; (http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html)
[54]Надица Мирчевска, научен труд Сајбер тероризам – современ облик на тероризмот колку Република Македонија е ранлива од сајбер тероризам
[55] Council of Europe; Cyber terrorism – the use of the internet for terrorist purposes, Strassbourg,2007,p.161
[56]Надица Мирчевска, научен труд Сајбер тероризам – современ облик на тероризмот колку Република Македонија е ранлива од сајбер тероризам

- **финансиски** – кои може да настанат кога извршителот го врши делото со цел за стекнување на противправна материјалнакорист;
- **нематријална** – се оденсува на неовластено откривање на туѓи тајни или друго штетно постапување;
- **комбинирани** – кога со откривање на одредени тајни или повреда на авторските права, по пат на злоупотреба на компјутер или информациска мрежа се наруши нечив углед, а истовремено се предизвика и конкретна финансиска штета.

8.4 Превенција од сајбер криминалот

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

Тенденција за зголемување на овој облик на криминал покажуваат и некои статистички податоци. Врз основа на податоците претставени од експертите на компанијата Sophos, во текот на 2007 година биле откриени 6.000 заразени веб страници, од кои 83% припаѓале на компании. Бројот на имејл заканите има тенденција на опаѓање, но обратнопропорционално се зголемува бројот на имејли кои содржат линкови кои водат до малициозни интернет страни.[57]

Голем проблем во сузбивањето на сајбер криминалот претставува фактот дека цел на извршителите е се што се поврзува на интернет, односно освен персоналните сметачи, тука се вбројуваат и мобилни телефони, iPhone, iPod Touch, терминали и други уреди кои се конектираат на интернет постојано или повремено. Според одредени сознанија, постојат и обвинувања, дека одредени држави се појавуваат како нарачатели на сајбер криминалот.[58] Врз основа на претходно изнесеното, може да се заклучи дека сајбер криминалот во иднина се повеќе ќе биде застапен, во однос на останатите видови на криминал.[59]

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

- заради општествената оправданост и целисходност, како и заради следење на општествените трендови и приклучување кон западноевропските држави, потребно е забрзување на активностите за донесување и усвојување единствени основи за заштита на автоматизираните информациони системи;
- од аспект на заштитата, една од најважните активности на која би требало да се посвети посебно внимание е изградба и развој на етички норми и принципи во доменот на информатиката;

[57]Интернет страница http://www.maturskiradovi.net/forum/Thread-kompjuterski-kriminal
[58]Интернет старница http://www.nezavisne.com/nauka-tehnologija/internet/Potrebni-ostriji-zakoni-za-sajber-kriminal-69298.html
[59]Интернет страница http://www.maturskiradovi.net/forum/Thread-kompjuterski-kriminal

- ревизија на кривичниот закон и негово прилагодување на новите појавни облици на општествено опасно однесување предизвикано од информацискатa технологија;
- нова систематизација и трансформација на телата или органите кои ја пратат состојбата во оваа област, извршуваат анализи на појавите, ги истражуваат причините, извршителите и методите и предлагаат соодветни мерки и акции за спречување, откривање, разјаснување и докажување на овие видови на кривични дела.[60]

[60]Sajber krize, Akademija za Bezbednost i Diplomatija, Beograd, 2009, http://www.scribd.com/doc/35038693/Cyber-Krize

9. ОСНОВИ НА ЗАШТИТА ОД КОМПЈУТЕРСКИ ВИРУСИ, ЦРВИ И ТРОЈАНЦИ[61]

9.1 Компјутерски вируси

Компјутерските вируси се мали програми, од неколку килобајти, кои имаат исклучиво за цел да направат штета на заразен компјутер. Се размножуваат воглавно на начини што се „вгнездуваат“ кај други фајлови, а штета предизвикуваат така што ги бришат или менуваат фајловите на дискот. Во случај доколку се работи за информациони системи, вирусот од заразениот компјутер може да зарази друг копмјутер во компјутерска мрежа, со цел да измени или оштети фајлови од оперативниот сисмет на компјутерот.

„Заразувањето“ на фајловите од оперативниот систем на компјутерот со вирус, црв или тројанец, настанува на неколку начини:

- преку разни медиуми кои се носачи на информации кои се заразени од компјутер со вирус, црв или тројанец;
- преку фајлови добиени преку имејл;
- преку фајлови превземени од интернет;
- посета на веб страна на која е поставен вирус, при што таквите сајтови се воглавно поставени на бесплатен сервер, имаат долги адреси (http://members.tripod.com/~ludnica/cool.html) и содржат скрипта со која се уфрлува вирус или тројанец;
- сигурносни дупки односно безбедносни пропусти во самите софтвери и оперативни системи кои овозможуваат пенетрација на вирусите, тројанците или црвите.

9.2 Антивирусни програми

За борба против вирусите се користат Антивируси – програми кои спречуваат компјутерот да се инфицира и кои ги уништуваат вирусите, доколку дојде „инфекција“ на копмјутерот.

Антивирусните програми спрчуваат „зараза“ така што ги скенираат фајловите кои се употребуваат во барање на кодот (со програма внатре во програмата) и доколку најдат код кој дава присуство на вирус, тие го спречуваат стартувањето на програмата. Фалловите кои се заразени се чистат така што едноставно внатре во заразениот фајл го бришат кодот за кои се сигурни дека е вирус. **Антивирусите имаат база на кодови од вирусути за кои производотилите на Антивирусите успеале да набават.**

Доколку Антивирусот е постојано уклучен, за мануелното скенирање е непотребно бидејќи активниот антивирус го скенира секој фајл кој се стартува.

Освен што е потребно да на компјутерот има инсталирано антивирус, исто така е потребно за антивирусот да се обзбедуваат нови дефиниции односно бази на податоци за новите вируси за да може да се откриваат новите вируси.

Начинот на кој се обезбедуваат новите дефниции се нарекува апдејтување (***engl.*** update), при што е потребно додека е компјутерот конектиран на интернет на иконата на

[61] Интернет страница (http://www.apisgroup.org/sec.html?id=7)

прозорот од Антивирусот да се кликне на „Update“, после тоа антивирусот автоматизирано ги повлекува новите дефниции од производителот на антивирсот.

9.3 Заштита од вируси

Универзалната заштита од вируси се состои во тоа секој да секој нов фајл кој ќе се сними на дискот (преку USB, CD, ICQ[62] итн.) потребно е обавезно да се скенира со некој антивирусен програм пред да се стартува.

Исто така како заштитна мерка е недозволувањето на снимање или копирање на фајлови и фолдери од друго лице освен од сопственикот односно корисникот на компјутерот.

Антивирусот, во согласност со мерки за заштита од вируси, потребно е да биде апдејтуван, така да со новите дефиниции се спречи инфицирање на компјутерот.

9.4. Тројанци

Тројанци се прогами кои кога ќе влезат во некој компјутер, ги праќаат сите шифри, лозинки во сандачето на електронската пошта на оној кој ги уфрлил, при што му овозможуваат на лицето кое ги уфлило тројанците, да пристапува на заразениот диск, што значи дека оној кој ги уфрлил тројанците може да чита, пишува, брише или менува фајлови на заразениот компјутер, дури и да добие потполн пристап на целокупнта меморија на заразениот компјутер. Тоа значи и како најчест случај се јавува гасење на заразениот компјутер или пак користење на истиот за напад на друг компјутер, а истото се извршува без знаење на сопствениокот на компјутерот.

Тројанците своето име го добиле по познатиот коњ за време на опсадата на Троја, која грците безуспешно ја напаѓале 10 (десет) години, за да на крајот се повлечат оставајќи пред нејзиниот влез огромен коњ како знак за признавање на поразот. Тројанските воини, воодушевини од победата, го внесле коњот внатре во градот и се посветиле на прославувањето на својата голема победа. Меѓутоа кога сите троајнски воини заспале пијани, од коњот се отворила добро скриена врата и од неа излегол одред на грчки воини, кој ја отворил вратата на тврдината, пуштајќи внатре да влезат останатите Грци, кои повлекувањето го исценирале и го чекале моментот кога ќе се отворат вратите да влезат. После тоа, Троја многу лесно ја зазеле.

На исти начин денес е возможно неовластено да се пристапи во други компјутери, и да се украдат потребните фајлови, интернет лозинки и слично. Накратко речено можно е злоупотреба на одреден компјутер без притоа сопственикот да е свесен, дека некој друг со програмата наречена „Тројански коњ“ има корисничка привилегија во неговиот компјутер.

Последиците кои може да бидат катастрофални се однесуваат на уништување на документи на дискот или некој проект на кој е работено со години од страна на оној што извршил уфрлување на тројанец или пак од истиот да се очекува префрлување на

---

[62] ICQ (***engl***. *Seek You* - „те барам“) е компјутерски прогарам наменет за размена на текстуални пораки помеѓу неговите корисници, преку користење на Интернет. Првата верзија е излезена во 1996 година, а називот е создаден од играта со англиските зборови. Со текот на времето се појавиле и можности за пренос на фајлови, слики, како и онлајн играње помеѓу корисниците. http://en.wikipedia.org/wiki/ICQ

документите на друг компјутер, потоа да го троши платениот интернет сообраќај, со што резултира со намлување на брзината на интренет сообраќаојот, дури и можно е да се изврши напад од компјутер во кој е уфрлен тројанец, на сервер од банка.

9.4.1 Како се уфрлуваат тројанците?

Можни се два начина:

- првиот начин е некој да инстилира на компјутрерот; тројанец, без знаење на сопственикот;
- вториот начин е преку интернет – ако некој испрати електронска порака во сандачето од електронската пошта во која има вметнато фајл (кој е тројанец) и притоа се бара истиот програм да се стартува, а освен програма може да се прати и игра, слика и слично.

Истото важи и за ICQ, како и за сите останати програми кои служат за комуникација преку интернет.

9.4.2 Заштита од тројанци

Универзалното правило за заштита од тројанци се однесува на неотворање на фајлови кои се испратени во сандачето од електронската пошта или ICQ, а истите се непознати за сопственикот на сандачето. Во наведениот случај заштитата се однесува на отворањето на фајловите од електронската пошта кои се познати или претходно договорени со сопственикот на сандачето.

Исто така , возможна е и заштита преку Start up и MSCONFIG.

Секој „Back Door“ тројанец се пројавува во Start up на Windows-от. За да се провери кои програми се сетирани во Start up, се притиска на Start, потоа се кликнува на Run, и се пишува MSCONFIG и се притиска на OK. Доколку се појави порака дека програмот не постои, тогаш наместо MSCONFIG, треба да се напише REGEDIT, при тоа да се дојде до стеблото HKEY_LOCAL_MACHINESOFTWARE / MicrosoftWindowsCurrentVersionRun

Кога се стартува MSCONFIG и се притисне на копчето на Start Up, ќе се појави список на програми кои се подесени секогаш да се стартуваат кога Windows ќе се статува. Од наведената листа на програми потребно е да се направи разлика на за некој сомнителен фајл со назив како што се EXPLORER.EXE, PICTURE.EXE, име на програма која е сомнителна (тројанецот Kuang2.c е препраќан како Setup.exe кој се наоѓал во фајлот fport.zip) или со некое друго име за кое постои сигурносnт дека не е корисничка програма, при што е потребно да се исклучи, односно избрише доколку се користи REGEDIT. Но, доколку наведениот програм е кориснички, се излегува од DOS (Start/Shut Down) и со командата RENAME променува името на на фајлот. Од тука произлегува препорака до корисниците на Windows, сите сомнителни програми е потребно да ги избришат или да ги исклучат, а се остваат само оние програми кои се потребни. Доколку се потребни исклучените програми за работа на оперативниот систем тогаш е потребно истите да се вклучат.

Програмите како што се SysTray, LoadPowerProfile, ScanRegistry и TaskMonitor се остваат постојано да работат. Најдобро е пред стартувањето на сомнителните програми, некаде во Start Up да се запишат сите имиња на фајлови, и притоа да се стартува програмата и после тоа да се изврши споредба во Start Up пред и после стартување на

сомнителниот програм. Доколку во Start Up се појави ново име на фајл тогаш е во прашање „тројанец“ и истиот се исклучува при што се се решава.

9.4.3 Помошни програми за листање на активни процеси

Помошните програми овозможуваат да се види листата на активни процеси, потоа истите да се исклучат или моментално да се стопираат. Овие програми овозможуваат да се види дали е активен некој сомнителен програм (тројанец или вирус) при што овозможува да се види адресата на програмата во меморијата и адресата на дискот.

Може да се најдат голем број на вакви програми од различни производители на Web, при што најчесто се бесплатни, но има и такви кои се комерцијални.

9.4.4 Firewall

Антивирусите не се идеални, од причина што ги откриваат само вирусите и тројанците кои производителот на антивирусната програма успеал да ги набави и да ги анализира, така да новите или домашните тројанци (кои воопшто не е тешко да се искодираат благодарение на програмските јазици VisualBasic ili Delphi) може да поминат и покрај антивирусната програма, а при тоа да не бидат откриени.

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

Универзален начин на заштита е да се избрише тројанец, а како приимер може да се наведе следното: преку имејл е добиена игра. Играта е стартувана од корисникот, потоа истата е искористена и корисникот потоа го користел сметачот да „сурфа“ на интернет. Доколку се претпостави дека при стартувањата на играта е инсталиран тројанец, тоа значи дека антивирусот не го заштитил оперативниот систем, но Firewall-те од различни производители кои се нудат може да го заштитат оперативниот систем. Тие ќе го известат корисникот дека има некој нов програм кој се обидува да пристапи на Интернет, при што истото е доволен показател дека дека хард дискот е инфициран. Во тој случај е потребно да се блокира трајно вирусот, на начин што треба да се влезе во DOS (преку Shut Down) и да се избрише програмата (тројанецот).

Претходно опишаното ја претстави вистинската улога на Firewall – от, мониторинг на излзниот сообраќај од компјутерот спрема интернет, (***engl.***Inbound Connection), сепак останува да се објасни, што се случува, кога некој пакет податоци доаѓа до компјутерот, т.е кога кога некој хакер ја пингува IP адреста на компјутерот (***engl.***Outbound Connection)

Хакерите ја пингуваат адресата на компјутерот, односно праќаат податоци на портот на тројанците, за да дознаат дали компјутерот е заразен. Доколку постои одговор од тројанецот, хакерите ќе знаат дали е инсталиран тројанец, при што на тој начин ќе навлезат во компјутерот. Ако пакетот на податоци е испратен према портот, кој во тој момент го „демне“ програмот кој не е авторизиран од корисникот, доколку е инсталиран Firewall-от, во зависност од производителот ќе пријави Outbound Connection и ќе ја објави IP адресата на хакерот и името на програмата која го сака да навлезе преку портот.

Доколку е програмата сомнителна, воспоставената конекцијата е потребно да се блокира засекогаш.

Но, доколку на програмата и се дозволи да воспостави конекција, Firewall-от нема да пријави ништо.

Ако пакетот на податоци биде насочен спрема портот во кој во тој момент не е резервиран за ниеден програм, Firewall-от ќе пријави Outbound connection, при што ќе објави "N/A", бидејќи ниеден програм не го „демне" тој порт. Во таква ситуација е потребно да се блокира конекцијата (не засекогаш), но доколку нападите и понатаму продолжат од страна на хакерите, тогаш конекцијата од таа IP адреса или портот кој моментално го користи хакерот е потребно засекогаш да се блокира.

Можно е да се постави прашањето, зошто да се блокира пакет на податоци ако е упатен спрема порт кој во ниеден момент не е резервиран. Блокирањето е потребно да се изврши од причина што ризикот е голем, бидејќи никогаш не се знае што има во позадина, односно пакетот на податоци може да отвори скриена врата во системот или да го блокира целиот систем.

Ако некој се обиде недозволено да пристапи на одреден компјутер (со цел блокирање или рушење на оперативниот систем) или некој програм на кој не му е дадена привилегија да пристапи на интернет и се обиде да воспостави конекција на некој порт, Firewall – от во истиот момент ќе го блокира сомнителниот порт и ќе го постави прашање до корисникот дали ја дозволува конекцијата, што значи дека Firewall-от не дозволува влез и излез од компјутерот без дозвола на корисникот.

Како заклучок може да се нагласи дека дека моментално е многу тешко да се заобиколи Firewall-от така да не постои програма која ќе успее да пристапи на интернет со заобиколување на Firewall-от. Тој е непробивен дури и за вештите хакери, па од таа причина истиот се користи на сите системи за кои е потребно многу високо ниво безбедност.

9.5 Црви

„Црв" е дел од софтвер кој „гризе" низ само еден компјутерски систем или низ мрежа на компјутерски системи, манипулирајќи, менувајќи или уништувајќи податоци или програмски кодови на местата до каде има пристап. „Црв" не се реплицира, туку се движи наокулу и остава штета на својот пат. Доколку биде откриено неговото присуство, може да го „одбегне" неговото „фаќање". Многу вируси имаат вградено „црви".

9.6 Основни правила на заштита од вируси, црви и тројанци

1. Потребно е скенирање на секој програм пред да се стартува
2. Потребно е скенирање на секој имејл или фајл кој ќе стигне преку ICQ или MIRC пред да се отвори, без разлика кој е испраќачот, бидејќи истиот не знае дека компјутерот е инфициран
3. Не посетување на страници чии адреси се добиваат од непознати лица.
4. Потребно е секогаш да се имаат нови антивируси кои ги откриваат вирусите во real time пред истите да се копираат на тврдиот диск, без разлика дали се истите компресирани, вградени или слично.

5. Потребно редовно да се врши update на новите дефиниции за антивирусните програми, за да може да се соберат информации за новите вируси и тројанци.
6. Задолжително користење на Firewall
7. Да се изврши енкрипција на датотеките за да се спречи нивната неовластена употреба.
8. Поставување и користење на password-е за влез во датотеки.
9. Недозволување на внесување на фајлови освен од сопственикот.
10. Користње на легални софтвери бидејќи во нелегалните софтвери се наоѓаат безбедносни пропусти или „bugs“, кои може да овозможат навлегување во копмјутерот. Ова важи и за најновите верзии на софтвер, бидејќи за секоја нова верзија излегува како подобрена, но сепак ненамерните безбедносни пропусти се појавуваа, а истите со секоја нова верзија се дектираат и исправаатЗато а е потребно редвно да се извршува update- вање.

10. СТРАТЕГИИ ЗА ЗАШТИТА ОД КРИМИНАЛНИ ДЕЈСТВА[63]

Воглавно секаде во светот за заштита од компјутерски криминал не се трга од тоа да се бркаат компјутерските криминалци, иако и тоа мора да се спроведува, туку многу повеќе се оддава заначење на заштитата на компјутерските системи пред да се случи било какво криминално дејство. Затоа понатаму ќе се даде повеќе акцент на заштитата на компјутерските системи од било какви криминални дејствија.

Едно од можеби најраспространетите криминални дејствија е ширењето на вирусите, тројанските коњи, црвите и логичките бомби. Најраспространето е можеби поради фактот што се пренесуваат на најразлични начини. Преку преснимување на податоци преку разни медиуми, по електронска пошта, FTP, итн. Секојдневно се појавуваат разни видови вируси. Некој од нив можеби и неопасни но се создаваат и вируси кој и тоа како можат да го „распарчат“ било кој незаштитен компјутерски систем.

Решение во најголем број случаи за овие проблеми се анти-вирус програмите кои во најголем број случаи ги „фаќаат“ вирусите, тројанските коњи, црвите и логичките бомби и ги бришат. Поради секојдневното појавување на нови би требало што почесто да се превземаат најнови вирус дефиниции од интернет страниците на вирус програмите.

За другите видови криминални дејствија понатаму се изложени некои од најраспространетите методи за заштита на компјутерски системи.

10.1 IT (*engl.*Information Technology) методи на заштита на компјутерските системи[64]

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

10.1.1 Класификација на информациите

Основно е да се класифицираат информациите според соодветното ниво на пристапност. На пример, „за читање“, „доверливо“, „тајно“. Оваа класификација е потребна и само тогаш може да се постават најдобри и најефективни мерки за заштита на информациите. Класификацијата би требало да биде направена од страна на сопственикот на информациите.

10.1.2 Правила на документирање

Сите системи, а особено системот за идентификација и авторизација, системот за класификација на информациите и Апликативните системи, мораат да бидат документирани и евидентирани. Во организациите според безбедносните правила и прописи, секое нелегално влегување и инцидент би трбало да се документира. Освен тоа, во организацијата би требало да се направи прирачник кој ќе содржи упатства за активности и мерки кои треба да се преземат во случај на инцидент.

---

[63] Стратегии за заштита од компјутерскиот криминал (Computer Crime Prevention Strategies) Александар Петрушевски

[64] Стратегии за заштита од компјутерскиот криминал (Computer Crime Prevention Strategies) Александар Петрушевски

10.1.3 Администрација и персонал

За успешна заштита на информациите важно е да се стекнат добри основни работни навики и да се воспостават процедури за оддржување на работните навики. Исто така и важно да се создаде работна атмосфера и воспостави дисиплиниран приод кон работата. При потреба за работа со доверливи информации, од голема важност е да се одберат луѓе кои се потполно адекватни и сигурни за таа работа. Тие треба да доверливи до ниво еднакво на доверливоста на информациите со кој работат. Пристапот до информациите треба да биде ограничен само до ниво кое е неопходно вработениот да ја заврши својата работата. Особено осетлива материја треба да се подели на повеќе делови, кои ќе се поделат на различни вработени така што ниеден од нив ќе нема пристап до целокупната материја.

Понатаму, безбедносните мерки, ќе бидат ефективни само во случај кога вработените се соодветно обучени. Многу е важно тие да ја разбираат работата и да го разбираат проблемот. Ова може да биде постигнато со обука во самата работна организација.

Секој вработен мора да биде обучен како да користи мрежа, како да се однесува со доверлива информација, да прави back-up, итн. На вработените треба да им се каже што да направат за да се спротистават на одредени закани, што не би требало да прават, на кого можат да јават во случај на нелегално влегување во системот и од кого да побараат помош. Исто така е многу важно вработените да се обучат да го пријавуваат секој инцидент, за да може да се превземат чекори за заштита и заштита од идни несакани навлегувања во системот.

Кога се работи за нови или пак привремено вработени, треба да им се даде воведна обука, во која ќе им се објасни за важноста на безбедноста на податоците. Би било корисно и да се стави член во договорот на вработениот за неговите обврски во однос на безбедноста и доверливоста.

10.1.4 Идентификација и авторизација на корисниците

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

Пристапот до компјутер може да биде ограничен со контролни процедури кои се базираат на различни типови на системи за идентификација и авторизација. Идентификација е процедура од два чекора: да се идентификува корисникот и да се потврди идентификацијата. Најпростите систем се базираат само на лозинки. Пософистицираните системи користат картички и/или „биометрични“ методи во комбинација со лозинки.

А. Идентификација

А.1 Системи со лозинки

Овие системи даваат мерки на заштита од повремени побарувања на податоци, но ретко запираат упорни криминалци. Компјутерските лозинки имаат улога на клуч на компјутерот.

Правила за креирање лозинки:

- секој да поседува своја лозинка и да не ја споделува со други.

- Лозинките би требало да бидат различни од корисничкото име
- идеална лозинка би била: алфанумеричка и најмалку 6 карактери долга
- Други идентификациони системи

Лозинките се нешто што го „знаеш“ и што лесно може да го открие некоја друга личност. Затоа системите базирани на нешто што се „знае“ (лозинки или пак PIN) и нешто што се „има“ како на пример авторизациски картички се многу позаштитени од првите. Некој и да ја дознае лозинката не „врши работа“ без картичката. Но денес најсилно заштитени системи се оние кои се базираат на нешто што се „знае_____“, нешто што се „има“ и нешто што „е“ самиот човек (биометрика).

Постојат два главни типа на картички:

- Магнетни картички, со магнетна лента која содржи доверливи податоци, и
- Чип картички, кои наместо магнетна лента содржат микрочип.

Биометричките системи користат специфични персонални карактеристики (биометрика) на личноста, на пример, отисок од прст, глас или ретина од око. Но овие системи се сеуште скапи и не многу користени.

Б. Авторизација

По идентификацијата на корисникот мора да постои правило за кој објект (податок, уред) секој корисник ќе има дозвола за работа. Ова се нарекува систем за контрола на пристап.

Б.1 Логирање

Најголемиот број на компјутерски системи поседуваат некаква процедура за логирање. Понекогаш и самостојните системи поседуваат системи за идентификација и авторизација, особено кога повеќе корисници со различно ниво на пристап го користат системот. Во системите со повеќе корисници секогаш има процедура за логирање. Посакувано ниво на заштита ќе се постигне само тогаш кога различни мерки на заштита правилне ќе бидат проследени со логирање.

Правилно логирање одговара на прашањата:

- Кој се логирал (корисник)
- Кога
- Од каде
- Што правел (активности)
- Додатни податоци (во зависност од активноста)

Б.2 Back-up

Денешните модерни компјутерски системи се осетливи, неретко „паѓаат“, и корисниците можат да направат грешки кои ќе доведат до ненадејни уништувања на податоци. За да се заштити системот од целосно губење на податоците под овие околности, неопходно е да се преземат процедури за правење на регуларни копии од

податоците. Податоците треба да се копираат во иста форма на back-up медиум и овој медиум да се чува на сигурно место.

Б.3 Firewalls

Едно од најчесто поставуваните прашања е „Како да се заштити внатрешна мрежа од надворешна (пример Интернет)?“

Едно решение е поставување на Firewall. Што е Firewall?

Firewall е систем или група од системи кои го контролираат пристапот помеѓу две мрежи. Firewall системите се типична прва одбрамбена линија помеѓу внатрешна (на некоја организација) или пак приватна мрежа и надворешниот свет, особено Internet. Firewall-от не само што треба да врши контрола на специфични операции како FTP, превземање електронска пошта, итн, туку треба и да му отежне или оневозможи на натрапникот или напаѓачот однадвор да пристапи кон внатрешната мрежа.

Воглавно постојат два типа на на firewall системи:

- packet-filtering firewall систем
- aplication-level firewall систем

Б.4 Систем за детектирање на натрапници (нелегални влегувања) Intrusion Detection Systems (IDS)

Дали има потреба од систем за детектирање на натрапници ако се поседува firewall?

- Да има потреба. Главната улога на firewall-от е да заштитува од надворешни влегувања. Но не заштитува од внатрешни натрапници.
- Меѓутоа понекогаш firewall-от „паѓа“ и од надворешни натрапници поради тоа што:
- многу тешко да се конфигурира коректно
- Хакерите и Кракерите можат да провлечат некои пакети низ скоро секој firewall систем
- Скоро секој софтвер содржи bugs, тоа е случај и со firewall софтверите.
- Постојат два типа на системи за детектирање на натрапници:
- Статистичко детектирање. Системот бара навлегувања од статистички податоци за да детектира необични однесување во системот.
- Детектирање по шема или потпис. Ваков систем споредува активности од колекција од познати видови напади или пак од група на правила. Значи гледа активности кој се случуваат по некоја шема или прекршување на некои правила. Поради овие работи би требало да се користи воедно и firewall системи и системи за детектирање на натрапници.

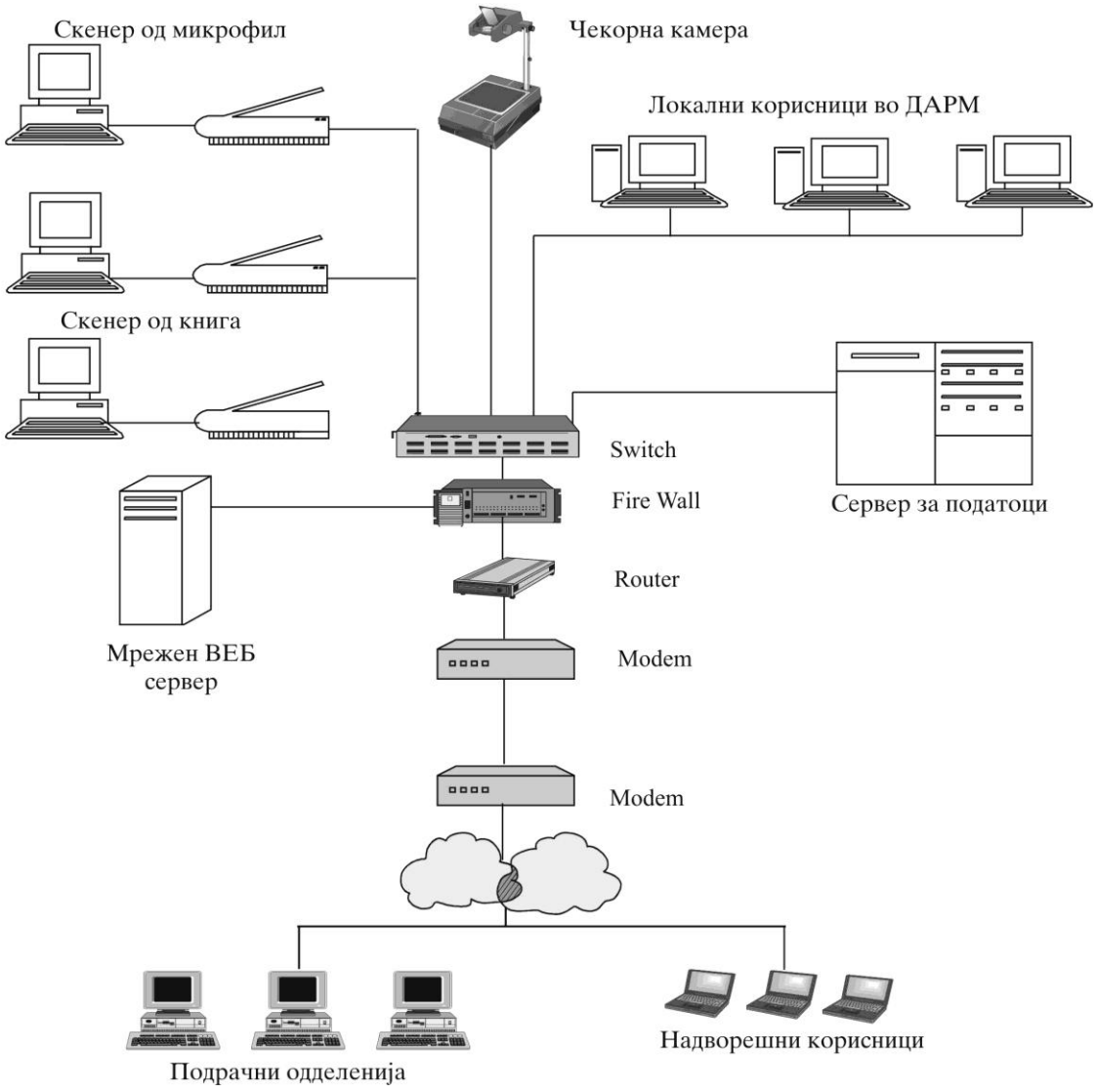
Б.5 Справување со инциденти

Иако на системот има инсталирано и firewall и систем за детектирање на натрапници, сепак некој треба да се грижи за него во случај на инциденти. Да се биде подготвен за инцденти е најдобар начин за да се справи со нив.

Некои попознати методи за справување на инциденти се состојат од следните фази:

- подготовка
- детектирање
- запирање на ширењето
- поправка
- проследување на инцидентот

Порака до сите кои се инволвирани во Информацискатa технологија Користете го своето знаење во позитивни, корисни работи. Не се трудете со своето знаење да наштетите некому и внимавајте со своето компјутерско однесување да не се втурнете во некои компјутерски криминални дејства. Последиците од нив се еднакво опасни како од било кое друго криминално дејство неповрзано со компјутер.



11. ЗАШТИТА НА ДИГИТАЛНИТЕ ПОДАТОЦИ

Дигиталините податоци се заштитуваат од: неовластен пристап, недозволено копирање и понатамошно дистрибуирање и докажување на автентичноста на податоците. Механизмите за заштита може да се поделат во неколку групи:

- механизми кои се однесуваат на заштитата и обезбедувањето на идентитетот на корисниците, според кои се врши доделување на права на пристап за одредени ресурси на ниво на системот;
- механизми поврзани со правата и привилегии на сопствениците и администраторите на ниво на системот кои одредуваат дали корисниците имаат дозвола да пристапат на одредена содржина без повреда на тие права;
- механизми на енкрипција, кои ја менуваат дигитализираната граѓа да биде читлива само на оние корисници кои легално набавиле клуч за декрипција;
- механизми за трајно шифрирање (*engl. persistent encryption*), кои овозможуваат употреба на граѓа за корисници, каде системот ги декриптира само оние делови кои се моментно потребни, а останатите остануваат криптирани;
- механизмите на дигиталните потписи и дигиталните водени жигови кои вградуваат информација за корисникот или сопственоста на дигитализираната граѓа.

11.1 Криптографија

Целта на криптографијата е заштита на дигиталните податоци од неовластено користење, при што содржината на информациите се менува и станува нечитлива. На тој начин се врши нивното заштитување сè додека не се изврши обратна операција и да се добијат оригиналните податоци. Процесот на енкрипцијата се користи за:

- осигурување на приватноста и тајноста на податоците;
- осигурување на интегритетот на податоците;
- можност за утврдување на автентичноста или идентификација - утврдување на идентитетот на личноста, компјутерскиот терминал, кредитна картичка и т.н.;
- можност за утврдување на автентичноста на пораката - утврдување на веродостојноста на изворот за информации;
- можност за вградување на дигитален потпис во пораката;
- можност за авторизација - можност за пренос на овластувањето на друго физичко или правно лице;
- можност за издавање на дигитално уверение - потврда дека информацијата доаѓа од проверен извор;

- можност за сведочење - потврда на создавање или постоење на одредена информација;
- можност за издавање на сметка - потврда за примање на информацијата;
- можност за потврдување - потврда за давање на одредена услуга;
- можност за доделување на сопственички права - доделување на доделување права на некое физичко или правно лице за користење и/или понатамошна продажба на граѓата;
- осигурување на анонимноста;
- осигурување на неможноста за одбивање на некоја, претходно договорена обврска;
- осигурување на можноста за отповикување на авторизацијата и уверението[65]

За да се изврши криптирање на податоците, потребно е тие да бидат во дигитализиран запис. За енкрипција на дигитализираниот запис се користи клуч за шифрирање, со кој се преобликува записот да не биде препознатлив, при што без познавање на клучот не може да се врати во својот изворен облик. Постојат два начини на шифрирање на дигиталините податоци: шифрирање со користење на симетричен клуч (*engl. symmetric - key encryption*) и шифрирање со користење на јавен клуч (*engl. public - key encryption*).

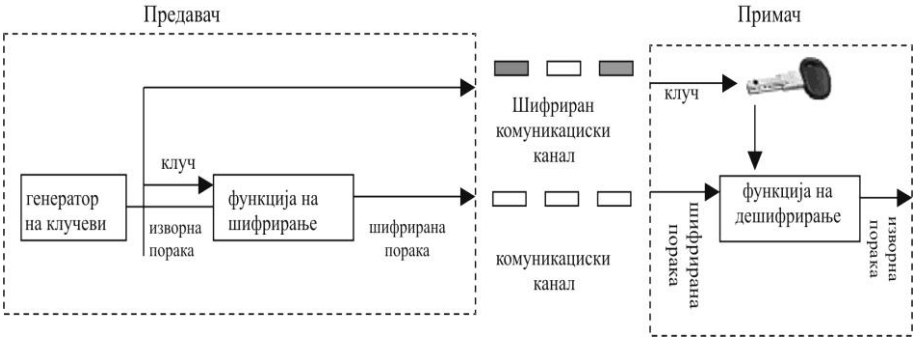
11.2 Шифрирање со симетричен клуч

Кај шифрирањето со симетричен клуч, истиот клуч се користи за шифрирање и дешифрирање на пораки, односно дигиталните податоци се праќаат по комуникациски канал. Таквиот систем се состои од три дела: генератор на клучеви, функции на шифрирање и функции на дешифрирање. Процесот се извршува на следниот начин. Прво предавачот го стартува генераторот на клучеви - програма која доделува единствен клуч за шифрирање на пораката. Секој клуч се користи за едно шифрирање. Потоа се стартуваат функциите за шифрирање, кои како влезни вредности ја имаат изворната порака и клучот за шифрирање. Таа функција ја преобразува пораката соодветно на клучот, а како резултат се добива шифрирана порака. Потоа, пораката преку комуникацискиот канал се испраќа до примачот. Примачот, кој треба да го познава клучот, во тој момент ги стартува функциите на дешифрирање, кои како влез ги имаат шифрираната порака и клучот за шифрирање. По внатрешното преобразување, функцијата резултира со изворна порака која за примачот е читлива.

Тајноста на клучот е многу важна, бидејќи секој кој знае може да ја дешифрира пораката. Врз основа на тоа, главен проблем претставува како да се достави клуч до одреден корисник, без опасност да се дознае при преносот. Еден од начините за доставување на клучеви може да биде по пат на заштитен комуникациски канал. Целата порака не се пренесува преку заштитен комуникациски канал заради брзината на преносот. Заштитениот

[65] Stancic, 'Digitalizacija grage"

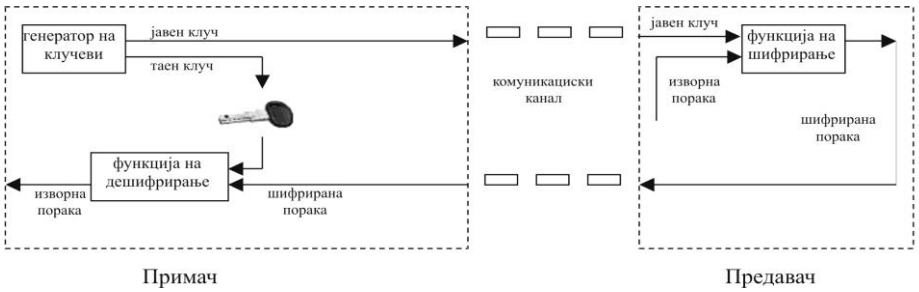
комуникациски канал е обично канал со помала пропусност. Од тие причини лесно може да се испрати клуч за шифрирање, заради малата големина и потоа целата порака по добивањето на клучот, може лесно да се препрати преку незаштитениот, јавен канал.



Слика 3.23: Постапка на шифрирање и дешифрирање со употреба на симетричен клуч

11.3 Шифрирање со јавен клуч

Оваа техника на шифрирање користи два вида на клучеви - јавен клуч и приватен клуч. Овие два клуча имаат единствено својство: пораката шифрирана со јавен клуч може да се дешифрира единствено со соодветен приватен клуч. Овој систем, исто така се состои од три дела: генератор на клучеви, функции на шифрирање и функции на дешифрирање. Процесот на шифрирање и дешифрирање се одвива на следниот начин. Прво примачот го стартува генераторот за клучеви - програма која доделува единствен пар на јавен и приватен клуч. Тогаш примачот јавно го објавува (на Интернет, во весници и сл.) или директно го доставува на предавачот својот јавен клуч, а приватниот клуч строго го чува. Предавачот ја стартува функцијата на шифрирање која како влезна вредност има изворна порака и јавен клуч на примачот. Шифрираната порака по пат на комуникациски канал се праќа на примачот. Така шифрираната порака може да ја дешифрира единствено сопственикот на приватниот клуч кој одговара на јавниот клуч со кој пораката е шифрирана. Примачот ја стартува функцијата за дешифрирање која како влезна вредност има шифрирана порака и приватен клуч, односно како резултат се добива изворна порака.



Слика 3.24: Постапка на шифрирање и дешифрирање со употреба на јавен клуч

Кога ќе се споредат методите за енкрипција со симетричен и јавен клуч може да се заклучи дека методата со јавен клуч е многу побезбедна, бидејќи

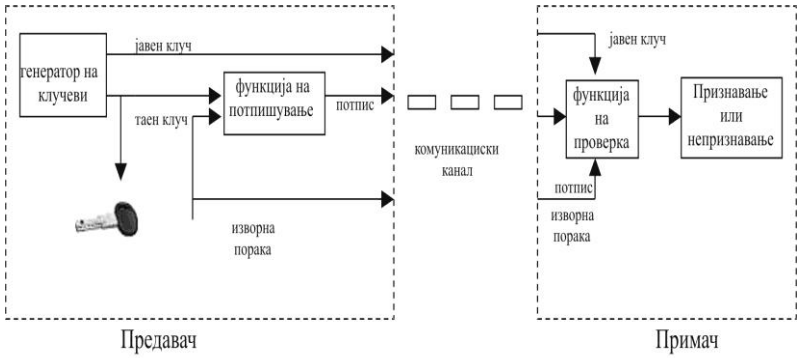
клучот за дешифрирање не се пренесува, при што можноста за негово откривање е многу помала. Тајниот клуч на некој начин е одреден со јавниот клуч, но за негово откривање врз основа на познавањето на јавниот клуч треба да се примени метода со „груба сила“ (*engl. brute force*), т.е. начинот на кој се испробуваат сите можни комбинации додека не се погоди вистинската, меѓутоа со денешниот развој на компјутерите тоа би барало многу време.

Заради тоа може да се направи комбинација на овие два методи, каде што, може да се употреби шифрирање со симетричен клуч, а клучот кој се доставува на примачот се шифрира со техника на јавен клуч. Со оглед дека техниката на шифрирање со јавен клуч бара повеќе процесорско време споредено со шифрирањето со симетричен клуч, со ваквата комбинација се добива на брзината и истовремено се зголемува сигурноста.

11.4 Дигитални потписи

Дигиталниот потпис го одредува идентитетот на учесникот во електронска размена на податоците и обезбедува интегритет на податоците. [66]Системот на дигиталните потписи се базира на технологијата на шифрирање со јавен клуч. Дигиталниот потпис е бинарна низа која се додава на документи за да се потврди неговата точност и исправност. Бинарната низа е изведена од тајниот клуч на потписникот на документот.

Дигиталните потписи функционираат на ист начин како и класичните потписи на хартиените документи. Така, во хартиен облик, одредената личност со својот потпис сведочи за точноста и исправноста на некој документ. Потписот е единствено обележје на секој човек и е зависен од личноста која потпишува. Наспроти тоа, дигиталните потписи може да се гледаат како функција на личноста која го потпишува и потпишаниот документ. Разликата се состои во тоа што кога една личност потпишува повеќе дигитализирани документи, сите потписи се разликуваат, додека за потпишувањето на хартиените документи не е тоа случај. Тоа мора да биде така зошто дигиталните потписи како бинарни низи, се праќаат со пораката, бидејќи ако истиот потпис би се користел за повеќе документи, секој кој добил од тие документи со дополнителна бинарна низа може да ја додаде на некој друг документ, т.е. да се потпише некој друг, и таквиот документ да се прати понатаму.



Слика 3.25: Постапка на дигитално потпишување

[66] Strategija razvitka Republike Hrvatske, “Hrvatska u 21. stoljecu ”, Informaciska i komunikaciska tehnologija, Vlada R. Hrvatske, 2000, <http://www.hrvatska21.hr>, 2001

Системот за дигитално потпишување се состои од три дела: генератор на клучеви, функции на потпишување и функции на проверување. Процесот се одвива на следниот начин. Личноста која сака да потпише некој дигитален документ најнапред го стартува генераторот на клучеви со што добива единствен пар на јавен и приватен клуч. Потоа ја стартува функцијата на потпишување, која како влезна вредност има дигитален документ и таен клуч, при што како резултат се појавува дигитален потпис. Така потпишаниот документ, со почеток на јавниот клуч, предавачот по пат на комуникацискиот канал го доставува на примачот или јавно го објавува. Примачот на документите кој сака да ја провери автентичноста на документите мора да ја стартува функцијата за проверка која како влезна вредност има документ, дигитален потпис и јавен клуч. Функцијата за проверка резултира со признавање или непризнавање на изворниот дигитален потпис.

11.5 Дигитални сертификати

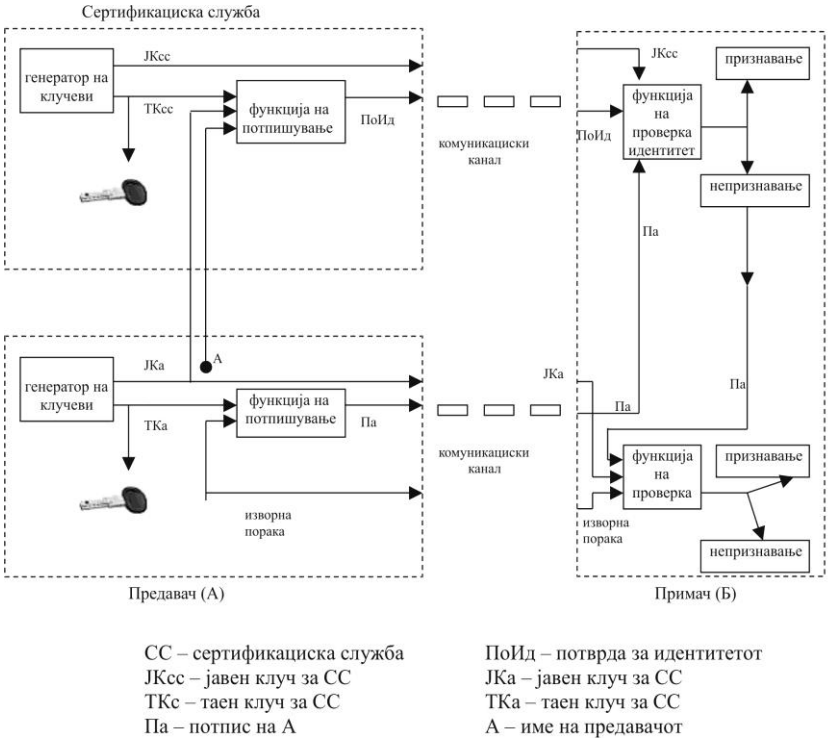
Со оглед на тоа, дека дигиталниот потпис го одредува идентитетот на учесникот во електронската размена на податоци потребно е издвојување на дигитални сертификати, т.е. дигитална потврда со која се докажува идентитетот (*engl. identity certificate*) за да примачот на податоците може да го провери идентитетот на предавачот. Сертификациониот авторитет (*engl. CA - certifying authorities*) е служба која издава дигитална потврда за идентитетот, таа поседува овластување со што дигиталните потврди имаа кредибилитет.

Проблемот на дигиталните сертификати и нивниот идентитет, се сведува на развој на инфраструктурата за управување на јавните клучеви. Сертификациониот авторитет издава потврда за идентитетот, при што ја потпишува со свој клуч за потпишување. Потврда за идентитетот на некоја личност, односно дигитално потпишан бинарен запис содржи јавен клуч и име на сопственикот, а може да содржи и некои податоци како “рок на употреба”, т.е. информација во кој временски период јавниот клуч е валиден. Кога примачот го има јавниот клуч од сертификациониот авторитет, тогаш може врз основа на довербата во авторитетот да верува во исправноста на потврдата за идентитетот која таа го издала, а препознавајќи го јавниот клуч на личноста која е во потврдата, може да верува во фактите дека таа личност му ги пратила податоците кои ги примил.[67]

На пример, примачот Б примил документ кој го потпишала личноста А заедно со потврдата за идентитетот во која се наведува името на А и соодветниот јавен клуч. Примачот тогаш го користи јавниот клуч издаден од авторитетот за може да ја провери вистинитоста на дигиталниот потпис на потврдата за идентитетот. Ако вистинитоста е потврдена, тогаш примачот може со целосна доверба да го искористи јавниот клуч на личноста А, со што се утврдува дека личноста А го потпишала применият документ. Довербата на примачот во авторитетот значи негова доверба за вистинитоста на нејзиниот јавен клуч, доверба со која се докажува дека авторитетот навистина и доделила јавен клуч на личноста А.

[67] National Academy of Sciences, ”The Digital Dilemma. Intellectual Property in the information Age”, USA, National Academy Press, 2000, http://books.nap.edu/html/digital _dilemma>, 2000

Сегментот за верифицирано управување со јавните клучеви, т.е. издавање на потврда дека зад одреден јавен клуч и име, е личност за која се потврдува нејзиниот идентитет. Многу е важно за проверката на примачот, дали наведената институција го доставила одредениот документ, може ли да се верува дека документот е идентичен на оригиналниот, т.е. дали некој неовластен не го променил. Овој сегмент е исто така важен при потпишувањето на дигиталните договори кога двете договорените страни можат да се наоѓаат во два различни града или пак на две различни страни на светот, а мораат да имаат доверба дека другата потпишана страна е таа вистинската.



Слика 3.26: Постапка за употреба на дигитални сертификати

11.6 Дигитални водени жигови

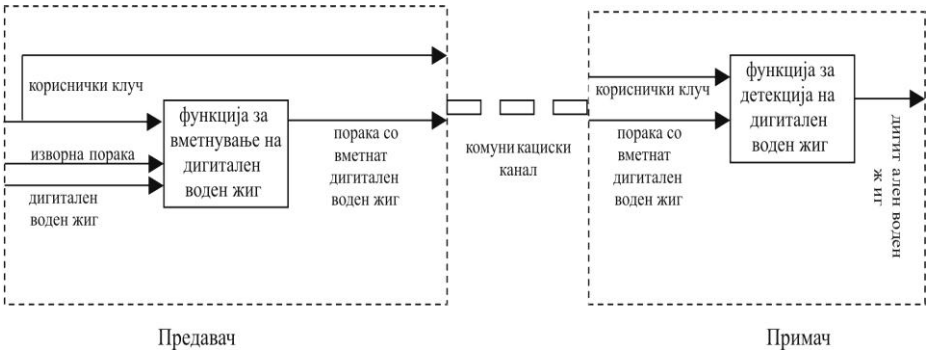
Дигиталниот воден жиг е сигнал кој е додаден на дигиталната граѓа со намера да се пренесе, одредена мала, количина на информација. Со детекција на присутност или неприсутност на воден жиг може да се докаже автентичноста или неавтентичноста на дигитализираната граѓа. Тие главно се користат за обележување на сликовната, звучната или видео граѓата. Постојат различни примени на дигиталните водени жигови кои најчесто се следните:

- докажување на сопственоста на некоја содржина;
- вметнување на податоци за примачот (*engl. fingerprinting*), за да може да се утврди од каде е потеклото на евентуалната нелегална копија;
- проверка на автентичноста и интегритетот;
- опишување на содржината (*engl. content labeling*);
- контрола на користење;

- заштита на содржината.[68]

Дигиталните водени жигови може да бидат видливи или невидливи за корисниците, а по обликот „меки“ (*engl. fragile*) или робусни (*engl. robust*). Видливите дигитални водени жигови се појавуваат во облик на логотип или порака на видливо или чујно подрачје од дигитализираната граѓа, кои на корисниците им служат како информација за сопственост или дозвола за користење. Некои институциите користат ваков вид на жигови за слободна дистрибуција на материјалот со низок квалитет за професионална употреба, а ја наплаќаат граѓата со висок квалитет. Невидливите жигови може да се користат како доказ за нелегално користење на дигиталните документи. Меките дигитални водени жигови не се постојани при обработка на дигитализираните документи, при што се користат за да се детектираат евентуалните измени на документите. Во моментот на преземање на дел од оригиналниот документ не е возможно да се докаже неговото потекло. Робусните водени жигови се провлекуваат низ целиот дигитален запис, при што неговите делови може да се детектираат и покрај тоа што се вградени и вклучени во некој документ.

Системот на дигиталните водени жигови се состои од два дела: функции за вметнување на жигот и функции за детекција на жигот. Процесот се одвива на следниот начин. Предавачот на дигитализираниот документ ја стартува функцијата за вметнување на жигот која како влезна вредност го има изворниот дигитален документ, дигиталниот воден жиг и корисничкиот клуч, а како резултат се добива документ со вметнат дигитален воден жиг. Потоа, заедно со клучот се проследува таквиот документ на примачот, кој ако сака може да го детектира жигот. За да може да го детектира, примачот мора да ја стартува функцијата за детекција на жигот. Таа како влезна вредност има кориснички клуч и примен документ, а како резултат се добива дигитален воден жиг со што потврдува неговата автентичност или пак се негира.

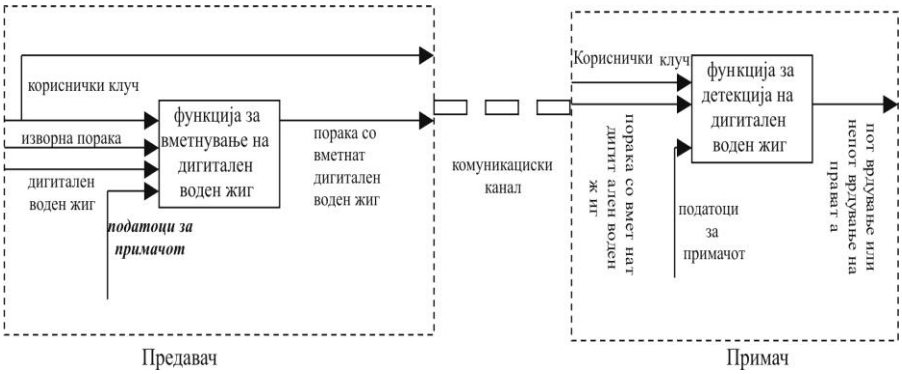


Слика 3.27: Систем на дигитален воден жиг

За процесите, каде што се вметнуваат податоци за примачот на дигиталниот воден жиг, постои дополнителна влезна вредност, односно шифра на корисник, со која на единствен начин се одредува примачот, т.е. корисникот на кој е дозволена употреба на одреден дигитализиран документ. Во тој случај како излезна вредност на функцијата за вметнување од жигот се добива

[68] National Academy of Sciences, ”The Digital Dilemma. Intellectual Property in the information Age”, USA, National Academy Press, 2000, http://books.nap.edu/html/digital _dilemma>, 2000

дигитализиран документ со вметнат дигитален воден жиг и податоци за примачот. Функцијата за детекција на жигот тогаш како дополнителна вредност има шифра на корисник, а резултира со потврдување или негирање на правата на користење на одреден примач. Процесот за вметнување на податоците за примачот е својствен за робусните дигитални водени жигови.



Слика 3.28: Систем на дигитален воден жиг со вметнување на податоци за примачот

11.7 Шифрирани обвивки

Шифрираните обвивки (*engl. cryptographic envelopes*) се создадени како систем за засилена заштита на пренос и користење на дигитализираната граѓа. Овој систем користи шифрирана дигитална меморија која содржи изворна порака, изјава за правата на пристап и користење на пораката, а исто така може да содржи дигитален воден жиг како и дигитален воден жиг со вметнати податоци за примачот.

Користењето на пораката од страна примачот, мора да биде одобрено од софтвер кој го проверува правото на користење. Таквиот софтвер се користи на сервер . Исто така треба да изврши дешифрирање само на оној дел од пораката кој моментално се прегледува, со што се зголемува заштитата. Со системот на шифрирани обвивки се овозможува лесна достапност до дигиталните податоци, без загрозување на финансиските интереси на институцијата, како сопственик на граѓата, заради можна неовластена дистрибуција на копии.

ЗАКЛУЧОК

Бројните и разновидни потенцијални закани кои ги загрозуваат информационите системи во институциите, организациите и компаниите, а посебно оние кои имаат карактер на криминални дела, недвосмислено ја наметнуваат потребата за изградба на соодветни системи за заштита на дигиталните податоци во компјутерските мрежи. Во ниеден момент не смее дасе заборави на фактот дека не постои апсолутна заштита и дека секој информационен систем е изложен на ризици, но со навремено дејствување, големината на постоечкиот ризик, можно е да се доведе во прифатливи граници.

Особено значаен е аспектот на едукација и обучување на персоналот како и оспособување на носителите на КИС, во спротивставувањето на појавните облици како и идентификувањето на феноменолошките и етиолошките карактеристики на компјутерскиот криминал.

Очигледно е дека информатичката технологија придонесува во современото општество безброј поволности, но исто така и создала и низ проблеми и ризици кои многу порано ни ни постоеле. Растечката зависност од информатичката технологија, која добива колосални размери, создала услови за настанување на бројни зони на осетливост со потенцијално многу озбилни консеквенци, кои можат да се протегаат поради губиток на контрола над нивната судбина, што укажува на фактот дека општествената заедница во се поголема мера станува изложена на новиот феномен – осетливост (ранливост) во информатичката ера.

Денес, повеќето држави веќе имаат суштински ресурси базирани на информатичка технологија. Оние кои тоа уште го немаат, прават се да на овој план создадат одредени резултати. Клучни сектори, како телекомуникациите, банкарството и финансиите, транспортот, електрична енергија, нафтата и гас, снабдување со вода, сервиси за вонредни ситуации и витални војни и цивилни операции, есенцијални за секојдневно успешно и несметано функционирање на економијата и државните органи, постануваат се позависни од оваа технологија. Како оваа зависност ќе се зголемува, истотака ќе се зголемува и осетливоста на општеството на секое нарушување или компромитацијата на информатички инфраструктури и автоматизирани активности и процеси.

Историски, критичната инфраструктура била физички разделена и раздвоена и нејзините елементи функционрале самостојно со релативно мала поврзаност и ниски или никаков степен на меѓузависност. Меѓутоа, со напредокот на технологијата, оваа инфраструктура прогресивно се обединува и станува поврзана, често и многу меѓузависна. Напредокот во технологијата исто така реултираше со високо и растечко ниво автоматизација во функционирање на критичната инфраструктура. Зголемено потпирање на оваква инфраструктура, комбинирано со нејзина растечка комплексност која произлегува од нејзината интеграција и автоматизација, прават од нејзините ентитетити многу осетливи и високо вредни потенцијални цели за разни врсти на атакување.[69] Затоа, како што е деструкцијата, на пример, на мостови, фабрики или централи закана на националната безбедност на индустриското

[69] Arquilla J., Ronfeldt D., *"Cyberwar is Coming"*, Comparative Strategy, Volume 12, no. 2, pp. 141–165., Copyright 1993 Taylor & Francis, ISSN 0149-5933/93, http://www.stl.nps.navy.mil/c4i/cyberwar.html; *"Information Operations (the cyber threat)"*, Canadian Security Intelligence Service, CSIS/SCRS 1999, http://www.csis-scrs.gc.ca/eng/operat/io2e.html

друштво, деструкцијата на информатичката инфраструктура сигурно ќе биде закана на националната безбедност на информатичкото друштво. Имајќи при тоа во вид дека индустриското друштво поврзано со заштита на физичкиот капитал и обезбедување на заштитените рута за транспорт на ресурси, информатичкото општество мора да биде поврзано со заштита на информации и трансферот на информации.

Понатаму, очигледно е дека постои и темна страна на информатичката технологија, која ни малку не е потценувачка и која, гледано од аспект на националните интереси, на глобално ниво ги вклучува и покрај другото и следните можности:[70]

- Одбиен пристап или реметење на информатичкиот сервис;
- Неовластено мониторирање на информатичкиот систем;
- Неовластено откривање на класифицирани податоци и информации кои се обработуваат,пренесуваат или се зачувани внатре во системот;
- Неовластена модификација или деструкција во мрежната база на податоци и податоци и информации кои се зачувани, во обработка или во пренос;
- Неовластена модификација или деструкција на компјутерски програми или компјутерски можности;
- Манипулација во информатичките сервиси, кои би резултирале со измама, финансиски загуби или други криминални дела.

Покрај сето ова, не би смеело да се занемари ни фактот дека заедно со ширењето на технологијата созреваат и нови генерации на потенцијални злонамерни актери. На жалост, и нивните информатиќчки алати се повеќе стануваат софистицирани и моќни, а исто така постануваат и зголемено кориснички прилагодени, побарувајќи многу малку стручност за нивна употреба. Поради тоа, како и поради се поголема зависност од информатичката технологија, информатичката инфраструктура практично станува *Ахилова пета* на современата општествена заедница.

Експертите се сложуваат дека заканите се бројни и сериозни, но и предупредуваат на тоа дека заканите со кои сме моментално соочени, може се многу поопасни од заканите со кои ќе се пресретнеме во блиска иднина. До кој обем сме во состојба да се браниме и заштитиме од овие закани сега и во иднина – тешко е да се процени, ама она што е извесно е императивната потреба да уште денес, затоа што може утре да биде касно, да се отпочне со неопходна акција во тој правец.

Наведеното е потребно да се примени многу брзо затоа што промените, сепак, неминовни, а клуч на успехот е во одговорот на прашање *како да се примени новата технологија на иновативен начин, а истовремено да се спречи нејзина злоупотреба?* За одговор на ова прашање неопходни се многубројни сериозни анализи да би се идентификувала *стратегија* со која би се добиле

[70]Awareness of National Security Issues and Response (ANSIR) Program, April 6, 1998., http://www.fbi.gov/hq/nsd/ansir/ansir.htm; Forno F. R., *Hidden Threats and Vulnerabilities to Information Systems at the Dawn of a New Century*, Special to EmergencyNet News; 11/22/98, http://www.emergency.com/techthrt.htm

одговори на поставените прашања. Стратегијата би морала да овозможи да се остварат две клучни работи:

- препознавање и капитализација на неочекувани прилики и можности кои ги пружа информатичката технологија;
- идентификација и избегнување на несаканите консеквенци поврзани со уклучување и примена на таа технологија.

Остварување на овие цели не ни лесно ни едноставно. Затоа, земајќи ги во предвид обемот, серизноста и сложеноста на овој проблем, чии димензии по сите критериуми достигнуваат не само национални, веќе и меѓународни размери, неговото разрешување не би смеело да биде препуштено на ентузијазмот на групата или поединците и нивните импровизирани и парцијални решенија, тука тоа е всушност проблем кој мора да се подигне на највисоко (државно) ниво, а носител на клучните активности би морала да биде владата, како и државни ентитет најодговорен за општата состојба во нацијата, кој истовремено има и најмногу авторитет неопходан за реализација на таквата задача.

Постојат барем три причини поради кои проблемот треба да се подигне на така високо ниво. Прво е секако фактот дека не можеме да чекаме да нашиот приватен сектор од ембрионалната состојба да се развие и зајакне до ниво на кој ќе му се овозможи, како што е пракса во развиените земји, на адекватен начин и рамноправно придружи на државната администрација во решавање на оваа задача и да на тој начин секој ги превземе своите делови од обврските и одговорностите.

Друга причина е исто така фактот, и тоа загрижувачки, е дека авториртетите кои можат да влијаат на решавање на проблемот, не се ни обидуваат да го запознаат и разберат.

Тие едноставно немаат време за „научна фантастика“, затоа што се занимаваат со „реални“ проблеми на денешницата. Нивното верување да проблемот нема да ескалира, барем додека се тие одговорни, ја зголемува нивната пасивност.

Оправданост на потребата за националната стратегија за заштита на сајбер просторот

Во врска со проблематиката која се разработува, како трета причина, не би требало да се занемари ни фактот дека во нашата средина уште е присутно многу непознавање и неразбирање, па и не прифаќање на погодностите што ги нуди новата технологија. Многу, кои за жал уште одлучуваат, тешко се одрекуват од старите и ненадминати начини на комуницирање, работа и учење. Ставот дека на нас новата технологија не ни е потребна се заснова на проверени факти дека се може и без оваа технологија, а со тоа и без нејзините потенцијални негативни импликации. Одговорот е краток и јасен: Точно е дека се се може и без информатичка технологија. Ама со нејзе, се тоа се може *побрзо, полесно, пообемно, поефтино и поквалитетно*. Покрај тоа, не би смеело да се дозволи да поради можните потенцијални опасности да се откажеме од расположивите можности, туку да тие можности контролирано и во интерес на поединци, групи или државата максимално да ги експлоатираме и да на тој

начин обезбедиме најлесен, најбрз и најсилен национален прогрес. Спротивното е обратно и не коренспондира на здравиот разум и сопствените интереси.

Со цел разрешување на наведениот проблем е неопходна долгорочна, фазна, силна, широко сеопфатна и повеќедимензионална акција која на национално ниво може да се предизвика само од „поголем“ авторитет, јасен е заклучокот дека во првата фаза на овој процес целиот терет мора да падне на владата и нејзините органи, моментално единствено компетентни и со доволно капацитет да го покренат разрешување на оваа, од општествен аспект, посебно значајна, озбилна и сложена задача.

Од наведеното се заклучува важноста за разрешување на проблемот пред се, поради тоа што сите корисници на информатичката технологија, сегашни и идни, со право *бараат и очекуваат* да во нашиот сајбер простор се креира амбиент во кој ќе се овозможи безбедно и тајно да се комуницира, рекламира, купува и продава, плаќа и наплатува, обучува и образува, креира и создава, забавува и релаксира ... Понатаму, на потег е владата, а нејзин прв чекор би требало да биде донесување на НАЦИОНАЛНА СТРАТЕГИЈА НА ЗАШТИТА НА САЈБЕР ПРОСТОРОТ.

РЕФЕРЕНЦИ

[1] Advocat J., *Internet clinical trials: examining new disciplinary experiments in health care*, Monash University, Australia, Anthropology Matters Journal 2005, Vol 7 (1), http://www.anthropologymatters.com

[2] *An introduction to e-business optimisation*, http://www.weboptimiser.com/resources/index.html;

[3] Arquilla J., Ronfeldt D., *„Cyberwar is Coming“*, Comparative Strategy, Volume 12, no. 2, pp. 141-165., Copyright 1993 Taylor & Francis, ISSN 0149-5933/93, http://www.stl.nps.navy.mil/c4i/cyberwar.html

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

[5] *Benefits of e-Government*, Asia-Pacific e-Government Portal, Last modified 2004, http://egovaspac.apdip.net/topics/benefits/

[6] Clarke R., *Information Technology & Cyberspace: Their Impact on Rights and Liberties*, Mietta's, Melbourne, January 1996, The Australian National University, http://www.anu.edu.au/people/Roger.Clarke/II/index.html

[7] Copeland E. T., *The Information Revolution and National Security*, Strategic Studies Institute, August 2000, http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB225.pdf

[8] *CPME guidelines for Telemedicine, Standing Committee of European Doctors*, 2002, http://cpme.dyndns.org:591/database/Telemedecine_2002.pdf;

[9] МАКЕДОНСКО СОНЦЕ 501/ 06.02.2004

[10] *E-Government guideline*, The World Bank, http://siteresources.worldbank.org/INTEGOVERNMENT/Resources/e-Gov_guideline.pdf

[11] *E-Government Handbook*, CDT/infoDev, http://www.cdt.org/egov/handbook/

[12] Finholt A. T., *Collaboratories: Science over the Internet*, 2002, http://www.aaas.org/spp/yearbook/2002/ch31.pdf

[13] Forno F. R., *Hidden Threats and Vulnerabilities to Information Systems at theDawn of a New Century*, Special to EmergencyNet News, 11/22/98, http://www.emergency.com/techthrt.htm

[14] Freeh J. L., *Threats to U. S. National security*, Congessional Statement, FBI, January 28, 1998, http://www.fbi.gov/pressrm/congress/congress98/threats.htm

[15] Guice J., Duffy R., *The Future of the Internet in Science*, USRA Research Institute for Advanced Computer Science, NASA Ames Research Center, USA, http://ase.arc.nasa.gov/publications/pdf/2000-0174.pdf

[16] Hakman K., *E-Commerce Tutorial*, http://www.webmonkey.com/webmonkey/99/04/index0a.html

[17] *Health Information Online*, Pew Internet & American Life Project, november 2004, http://www.pewinternet.org

[18] *Hobbes' Internet Timeline v8.1*, http://www.zakon.org/robert/internet/timeline/

[19] Horrigan B. J., *How Americans Get in Touch With Government*, Pew Interne&American Life Project, May 24, 2004, www.pewinternet.org

[20] *IC21: The Intelligence Community in the 21st Century*, Staff Study, Permanent Select Committee on Intelligence House of Representatives, One Hundred Fourth Congress, Washington, 1996, http://www.fas.org/irp/congress/1996_rpt/ic21/index.html
[21] *Information Operations (the cyber threat)*, Canadian Security Intelligence Service,CSIS/SCRS 1999, http://www.csis-scrs.gc.ca/eng/operat/io2e.html
[22] *Internet Ad Revenues Continued to Grow in the Fourth Quarter*, ClickZ News, March 1, 2006, http://www.clickz.com/news/print.php/3588506
[23] *Internet Growth Statistics - Global Village History*, http://www.internetworldstats.com/emarketing.htm
[24] *Introduction to E-business*, http://www.bgateway.com/bg-home/bg-services.htm
[25] *Marshall McLuhan Foresees The Global Village*, http://www.livinginternet.com/i/ii_mcluhan.htm
[26] Metz S., *Armed Conflict In The 21st Century: The Information Revolution And Post-Modern Warfare*, Strategic Studies Institute, April 2000, http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB225.pdf226;
[27] Moursund D., Smith I., *Five Research Summaries on IT in Education*, International Society for Technology in Education, 2000, http://darkwing.uoregon.edu/~moursund/dave/Free.html
[28] *Online Banking Spikes, then Slows*, April 11, 2006, http://www.clickz.com/stats/sectors/finance/print.php/3598231
[29] *Online Retail Sales Grew in 2005*, January 5, 2006, www.clickz.com/stats/sectors/retailing/article.php/3575456
[30] Petrović R. S., *Globalno informaciono ratovanje*, Zbornik radova (CD-ROM), YU INFO '99, Kopaonik, 22-26. marta 1999.
[31] Petrović R. S., *Kiber prostor - peta dimenzija ratovanja*, Vojni informator, br. 4, jul-avgust 2001, str. 29-50.
[32] Petrović R. S., *Kiberterorizam*, Vojno delo, god. LIII, br. 2/2001, str. 100-122.
[33] Petrović R. S., Kompjuterski kriminal, *Vojnoizdavački zavod*, Beograd 2004, III izdanje, 510 st.
[34] Petrović R. S., *Neki aspekti nacionalne bezbednosti u informacionom dobu*, **N**auka, **T**ehnika, **B**ezbednost (NTB), Rad po pozivu, UDC: 681.324; 65.012.8, Godina XI, Broj 1, Septembar 2001, str. 7-27.
[35] *Population Explosion!*, November 3, 2005, http://www.clickz.com/stats/sectors/geographics/print.php/5911_151151
[36] *Recommendations for Research and Development in Information Technology in Education*, Learning and Leading with Technology 2000-2001, ISTE (the International Society for Technology in Education, http://www.iste.org/
[37] *Revolution in the U.S. Information Infrastructure*, Copyright 1995 by the National Academy of Sciences, USA, http://www.nap.edu/readingroom/books/newpath/
[38] Robinson C. J., *Financing The Health Care Internet*, Health Affairs ~ Volume 19, Number 6, 2000, http://content.healthaffairs.org/cgi/reprint/19/6/72.pdf

[39] *Security in cyberspace*, Staff statement, U.S. Senate, Permanent subcommittee on investigations, june 5, 1996, http://www.fas.org/irp/congress/1996_hr/s960605t.htm
[40] Stearns W. R, *Revolution in the U.S. Information Structure: The Promise of the National Information Infrastructure*, National Academy of Sciences, 1994, http://www.nap.edu/readingroom/books/newpath/chap3.html
[41] Sullivan R. G., M. Coroalles M. A., The Army In The Information Age, Strategic Studies Institute, March 31, 1995, http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB268.pdf
[42] *The Future of Information Technology in Education*, An ISTE Publication, http://www.uoregon.edu/~moursund/FuturesBook1997/index.html
[43] Warren M., *The Internet and rural communities: implications for health care?*, http://www.plymouth.ac.uk/files/extranet/docs/HSC/abstract2003-Feb 3 health of rural communities.pdf
[44] *What is Telemedicine?*, April 1998, http://www.med.und.nodak.edu/depts/rural/pdf/whatistele.pdf
[45] *Awareness of National Security Issues and Response (ANSIR) Program*, *Слободан Р. Петровић*, April 6, 1998., http://www.fbi.gov/hq/nsd/ansir/ansir.htm
[49] Davidson T., Sooryamoorthy R., Shrum W., *Kerala Connections: Will the InternetAffect Science in Developing Areas?*, 2002, http://worldsci.net/EVERY4.pdf

ПРИЛОЗИ

Хакерски групи [71]

Hacker group
091 Labs
A
Advanced Persistent Threat
User:Angelixd/Pumping Station: One
C
Chaos Computer Club
Chaos Computer Club France
D
Digital DawgPound
Decocidio
User:Dweekly/HackerDojo
E
Electronic Disturbance Theatre
Electronik Tribulation Army
G
Electronik Tribulation Army
Goatse Security
H
HacDC
Hack Canada
Hacker Dojo
Hacktivismo
Hackweiser
HACP (hacker)
Helith
Honker Union
The Humble Guys
I
IPhone Dev Team
Infonomicon
K
Kiberpipa

L
L0pht
Level Seven
M
Metalab
Milw0rm
Moonlight Maze
N
NYC Resistor
Network Crack Program Hacker (NCPH) Group
P
P.H.I.R.M.
Phone Losers of America
Phrozen Crew
Port7Alliance
Pumping Station: One
R
Red Hacker Alliance
S
S0ftpj
Securax
Shmoo Group
T
TOG (hackerspace)
Team Elite
TESO
The 414s
Titan Rain
U
UXu
W
W00w00

71

http://en.wikipedia.org/wiki/Category:Hacker_groups