UDK 343.326:004.738.5.056.53
DOI 10.7251/ZRSNG2223031S

ПРОБЛЕМИ У ПОСЛОВАЊУ И ФУНКЦИОНИСАЊУ РАЗВОЈА КОМПЈУТЕРСКЕ ТЕХНОЛОГИЈЕ И ПОСЛЕДИЦЕ ИЗАЗВАНЕ САЈБЕР КРИМИНАЛОМ

др Жељко Стевановић, Министартво одбране, Оружане снаге БиХ

Сажетак – **Нарушавање безбедности како личне тако и колективне у већини случајева може да буде угрожена од стране људског фактора. У оквиру тренутног стања и дешавања у свету, те последица које су изазване економском кризом, негативни утицаји су видљиви како у привредном тако и у безбедоносном сектору. У задње време под утицајем глобализације видљиве су промене у свим сверама живота. Глобализација се све више намеће са својим добрим и лошим странама. Нагли развој технологије те утицаји савременог ратовања имали су за последицу развој многих техничких достигнућа као директан утицај на привредни, друштвени те безбедоносни сектор већине развијених земаља. Борба у јачању својих позиција наметнула је у већем делу ЕУ велике проблеме које се рефлектују на друштвену заједницу. У свери појаве и наглог развоја компијутерске технике, те развојем паметних телефона долазимо до једног новог проблема који такође има утицај на друштво у глобалу а односи се на високо технолошки криминал познати као сјбер криминал.**

Кључне речи: глобализам; криминал; заштита; развој; технологија

Summary - Violation of both personal and collective security can in most cases be threatened by the human factor. Within the current situation and events in the world, and the consequences caused by the economic crisis, the negative impacts are visible both in the economic and in the security sector. Recently, under the influence of globalization, changes are visible in all areas of life. Globalization is increasingly imposing itself with its good and bad sides. The rapid development of technology and the effects of modern warfare resulted in the development of many technical achievements as a direct impact on the economic, social and security sectors of most developed countries. The struggle to strengthen their positions imposed major problems in most of the EU, which reflect on the social community. In terms of the emergence and rapid development of computer technology, and the development of smartphones, we come to a new problem that also has an impact on society globally, and it refers to high-tech crime known as cybercrime.

Keywords: globalism; crime; protection; development; technology

I Увод

Светски процес који је изазван глобализацијом незаустављиво напредује има утицај на већину светских земаља. Оне земље које су занемаривале глобализацију или су покушале у неком облику да јој се успротиве имале су успорен развој[1].

Овим утицајем можемо рећи да се ствара један нови економски поредак који ће за циљ да има убразан раст и развој земље у свим сферама како би држале примат за водећим.

Прилагођавање некадашњих структура које су настале на националним начелима сада се морају сагледавати новим глобалним начелима.

Глобални развој има велики утицај на технолошку развијеност како државе тако и људске свести у напредку и потрагом за бољи развој. Глобализација доводи до стварања трговачких блокова, глобалних компанија и глобалне економије. На тај начин свет постаје једна организација док би светско тржисте било доступно свима.

Развојем глобализације код многих земљама отвара се низ могућности од економског, безбедоносног до самог друштвеног развоја где би се могло напредовати и развијати у свим грана те могу послужити као добар пример другим земљама.

Да би земља у сваком погледу напредовала пред њу се стављају разни изазови и „препреке“, које мора да пређе и буде јака. Глобалним развојем економије долази и до потребе за већим развојем технологије. Нагли развој компијутерске технологије те интернет

[1] Здрилић, І.; Пувача,М.; Росо, Д.: Утјецај глобализације пројенеу начину пословања и организацијској култури, Економски Вјесник , 2010

комуникација који има вели значај у савременом ратовању, има јак утицај и на земље које се убрзано развијају. Развијена технологија омогућава унапређење пословања где долази некада до недостижних тржиста те се убрзава сам развој и напредак у појединим структурама.

Сам развој технологије са собом носи одговарајуће потешкоће и проблеме које се манифестују кроз високотехнолошки криминал познат као сајбер криминал.

Овај вид криминала је све више заступљен у свету а велики утицај има на економију, безбедност те на личну заштиту људи њихове приватности и функционалности. У све већим случајевима потенцијалне жртве су малолетници.

Државе које су у глобализацији напредовале у овој врсти заштите боре се против овог вида криминала и покушавају сузбити утицај истог.

Имају добро развијене сајбер центре који се у већини случајева налазе у склопу полицијских структура а чешће су заступљени и у војном сектору.

II Високотехнолошки криминал и његов утицај

Напредак и развој земље у технолошком смислу за последицу има развој високотехнолошког криминала или како све чешће употребљавамо израз сајбер криминал.

Појам високотехнолошки **криминал** и сајбер криминал се изједначававају а сам појам "сајбер криминал" први пут је употребио писац **Вилијам Гибсон** у свом научно фантастичном роману "**Неуромансер**".[2] Појава сајбер криминала изазива велику пажњу како владиног тако и невладиног сектора из разлога што на мети истог су како правна тако и физичка лица док и деца нису изузета. Сајбер криминал јавља се у разним облицима који за намјеру имају експлатацију података али и наношење штете посредством сајбер простора.

Најчешће се реализује путем малициозних програма који су штетни а који користе сајбер криминалци како би приступили туђим рачунарима и нанели одговарајућу штету. Они се могу јавити у више облика као што су:

- Вируси, који су препознатљиви по промени рада рачунара и разним искакућим прозорима.
- Праћења и шпијунирања активности док је лице на интернету (spyweare).
- Превара на начин да се кориснику саветује да купи антивирус који уопште и не постоји, јер је његов компијутер напао одређени вирус **(**Scareware).
- Крађа идентитета, у последње време је начешћи а жртве су обично корисници друштвених мрежа где се за циљ има прибављање материјалне користи.
- Преваре путем мејла (phishing**)** где сајбер криминалци покушавају да добију поверљиве информације као што су лозинке, бројеви рачуна, корисничко име и сл.
- Сајбер избуда, је нешто озбиљни облик где губимо контролу над нашим информацијама.

Сви ови облици могу да се јаве код праваних и физичких лица а појавом било ког облика код великих компанија дошло би до одређених губитака. У пословању стјбер криминал се разликује тј. његови типови и последице у зависности о каквим нападима се ради.

Ако чувамо неке значајне информације клијената које приликом сајбер напада могу бити угрожене и субјекат тим поводом претрпи штету може доћи до покретања законског поступка против компаније услед сајбер напада.

Приликом ових радњи дођиће до повећања трошкова самог поступка али и трошкова на име одштете.

Када говоримо о компанијама и предузетницима потребно је предузети све неопходне мере како би се спречио напад на податке и податке о клијентима.

Потребно је искористити све програме који нам стоје на располагању као и додатне мере како би спречили и ојачали безбедност података који су поверљиви од потенцијалних сајбер напада.

Свака компанија која је на удару сајбер криминала или је потенцијални циљ истог потребно је да правовремено потражи помоћ професионалаца за сајбер безбедност.

Компанија може да се заштити и на начин да се осигура у осигуравајућим кућама од сајбер криминала под условом да те куће нуде такав вид услуга али то је реткост. Немогуће је данас заштитити своју приватност у сајбер свету јер телефон рачунар или неки други уређај су потенцијални приступи приватном животу корисника истих али се ризик итекако може смањити уколико се предузму мере заштите података[3].

[2] https://vib.rs/sajber-kriminal/

[3] Заштита приватности у сајбер свету, Стручни чланак

III Конвенција о компијутерском криминалу

Државе чланице Вијећа Европе те државе потписнице, дана 23.01.2001. године у Будимпешти, усвојиле су Европску конвенцију о компјутерском криминалу а Босна и Херцеговина је дана 25.03.2006. године је донијела Одлуку о ратификацији ове Конвенције.

Циљ ове Конвенције је да реализира веће јединство између својих чланова и интензивирање сарадње са другим државама чланицама Конвенције у борби против сајбер криминала и потребу за заштитом легитимних интереса повезаних са развојем компјутерских технологија, спречавање злоупотребе компјутерских система, мрежа и података, те бржа и ефикаснија борба против кривичних дјела почињених у сајбер простору, олакшавајући њихово откривање, истрагу и гоњење како на унутрашњем тако и међународном нивоу. Конвенција разликује четири врсте кривичних дјела почињених у сајбер простору, и то:

- дјела против повјерљивости, интегритета и доступности компјутерских података и система, у која се убрајају: недозвољени приступ компјутерским системима, повреда интегритета података, повреда интегритета система и злоупотреба;
- компјутерска дјела, у која се убрајају компјутерско фалсификирање и компјутерска превара;
- дјела везана за садржај, у која се убрајају дјела која се односе на дјечију порнографију;
- дјела у вези са нападом на интелектуалну својину и односна права.[4]

Циљ Конвенције је да државе потписнице уврсте претходно наведена кривична дјела у национална кривична законодавства, уколико то већ нису учиниле. Конвенција је нарочито важна због брзине дјеловања страна у поступку.

Овом конвенцијом добијају се добри бенифити између земаља у циљу чувања и похране података путем ИТ сектора односно компијутерских система, јер нису све земље подједнако развијене у области сајбер криминала.

[4] CYBER CRIMINAL AND PRIVACY PROTECTION IN THE CYBER WORLD, Стручни чланак

IV Заштита деце у сајбер простору

Сам развој технологије и велика експанзија сајбер криминала у великој мери одразио се на децу. Све је више заступљености и утицаја сајбер криминала у овом сегменту а односи се на искоришћавању деце кроз дечију пормографију, сексуално искоришћавање.

Честа ухођења, крађе иденитета, преваре, претње, изнуде, те крађе деце само постављају низ питања и отварају велики број расправа на који начин деца која користе рачунаре, друштвене мреже и интернет могу да се заштите.

Акценат треба дати на јачању закона, законских регулатива те у великој мери ангажовања родитеља и њихова едукација.

Слобода кориштења интернета у свери развоја технологије код деце има добре и лоше особине а односе се на њихову информисаност, те бржи начин доласка до жељених информација и ону другу страну где дете није свесно у какву замку може да упадне и каква жртва може да постане.

Деца су најрањивија група интернет насиља за разлику од одраслих јер им не достаје свест, моугћности искоришћавања и последица које могу настати. Велики је број студија о сајбер нападима на децу, која су често завршавала трагично јер дечији несвесни начин и сватање подложно је већем степену искоришћања.

Потребно је у свери развоја науке и технологије у школама увести обавезно информисање како деце тако и родитеља јер штета када се начини последице су велике.

Многе развијене земље велики труд улажу у заштиту деце од сјабер напада чинећи све кроз едукацију. У будућности многе дебате биће вођене на ову тему са циљем здравијег развоја и безбрижне употребе информација у сфери експанзије бржег протока и прикупљања информација.

V Закључак

Развој земаља и нагла експанзија и развој технологије те нагла глобализација која има све већи примат утиче на све свере развоја.

Економија многих земаља зависи од низа фактора те утицаја брзог протока информација и заштите истих.

Велика експанзија и коресподенција пословања у копијутерском свету је много лакша, бржа и даје многе погодности али има и онај други утицај који негативно може да утиче на њихово пословање. Све већим утицајем сајбер криминала долази до низа проблема и наношења штете како појединцима тако и групама.

Велики губитци који могу да се десе утицајом сајбер криминала могу да утичу и на саму државу. Многе земље све више се баве усклађивањем законсих одредби и развијању свести које се односи на заштиту података и смањивању утицаја од стране сајбер криминала.

Деца која су најрањивија категорија подложна овом виду насиља и криминала морају адекватно бити заштићена где је потребно уложити велике напоре на њиховој заштити.

Потребно је отворити многа питања где би се дали одговори кроз информисаност друштва како би се у довољној мери ставила под контролу велика претња садашњице.

Литература

[1] Здрилић, I.; Пувача,M.; Роco, „Утјецај глобализације“

[2] CYBER CRIMINAL AND PRIVACY PROTECTION IN THE CYBER WORLD, Стручни чланак.

[3] Williams K. R., Guerra N. G. (2007) Prevalence and Predictors of Internet Bullying, Journal.

[4] Права и заштита деце у сјабер простору, правне последице сјбер криминала над децом,др Енис Омеровић, Научни рад

[5] https://vib.rs/sajber-kriminal/

[6] Стојановић З., Кривично право, посебни део, 2007. Београд