AGENCIJA ZA INFORMACIONO DRUŠTVO REPUBLIKE SRPSKE

Odjeljenje za informacionu bezbjednost

oib.aidrs.org

Krivična djela protiv bezbjednosti računarskih podataka

Saša Vojnović

Oznaka dokumenta	OIBRS-PUB-E1-01
Urednik izdanja	mr Srđan Rajčević [srdjan.rajcevic@aidrs.org]
Autor	Saša Vojnović [sasa.vojnovic@aidrs.org]
Datum izdavanja	2.6.2015.
Lokacija objave	https://oib.aidrs.org

SADRŽAJ

1. UVOD

Visokotehnološki (sajber) kriminal predstavlja jednu od najmlađih grana odnosno vrsta kriminala. Jednu od najboljih i najpreciznijih definicija visokotehnološkog kriminala dale su Ujedinjene nacije: Sajber kriminal u užem smislu (računarski kriminal) predstavlja svako ilegalno ponašanje obavljeno elektronskim putem koje za cilj ima sigurnost računarskih sistema, kao i podataka koje oni obrađuju dok sajber kriminal u širem smislu (kriminal vezan za računarsku tehnologiju) je svako ilegalno ponašanje obavljeno pomoću ili u vezi sa računarskim sistemom ili računarskom mrežom, uključujući i takve aktivnosti kao što su ilegalno posedovanje i/ili nuđenje i distribucija informacija pomoću računarskog sistema ili računarske mreže.[1]

Radi se u stvari o krivičnim djelima gde se kao objekat izvršenja krivičnog djela *(computer crime*) i kao sredstvo za izvršenje krivičnog djela (*computer related crime*) javljaju računari, računarske mreže, računarski podaci, kao i njihovi produkti u materijalnom i elektronskom obliku. Treba spomenuti da u visokotehnološki kriminal ne spadaju sva krivična djela u kojima se kao sredstvo izvršenja pojavljuje računar, već samo ona djela gdje je upotreba računara bitna za biće[2] krivičnog djela. Tako na primjer krivično djelo falsifikovanja novca neće biti tretirano kao visokotehnološki kriminal bez obzira da li se počinilac prilikom falsifikovanja novca služio računarom – biće tog krivičnog djela je izrada lažnog novca a računar, skener i printer se tu pojavljuju samo kao tehničko sredstvo za lakše počinjenje krivičnog djela.

Broj i vrste krivičnih dijela iz oblasti visokotehnološkog kriminala, kao i ekonomsku štetu koja nastaje izvršenjem ovih krivičnih dela, veoma je teško procjeniti. Prema nekim istraživanjima i procjenama, preko 1 milion ljudi dnevno je žrtva nekog od oblika visokotehnološkog kriminala. Načini izvršenja krivičnih djela, zbog same prirode savremenih informacionih tehnologija, veoma su raznoliki i sve sofisticiraniji. Počinilac ovakve vrste djela ne mora nužno da bude pojedinac. Sve su češći napadi samih država koje putem svojih obavještajnih službi koriste informacione tehnologije za prikupljanje informacija i špijunažu. Takođe preduzeća i korporacije (nekad i u saradnji sa organizovanim kriminalnim grupama) često sprovode industrijsku špijunažu. Bez obzira ko ih čini, ovakva vrstu krivičnih djela uglavnom je usmjerena na ugrožavanje odnosno prijetnju po:

- **integritet** (cilj je mjenjanje, uništavanje ili neki drugi način kompromitovanja integriteta podataka)
- **dostupnost** (cilj je sprečavanje pristupa podacima koji su inače dostupni)
- **povjerljivost** (cilj je prikupljanje povjerljivih podataka i informacija često u svrhu kriminalnih ciljeva kao što je krađa identiteta, krađa ličnih podataka, prevara...)

Kada se gleda tip, krivična djela visokotehnološkog kriminala mogu biti **politička** (sajber špijunaža, sajber terorizam kao sve češći oblik terorizma, sajber ratovanje); **ekonomska**

[1] Tenth UN Congress On The Prevention Of Crime And The Treatment Of Offenders, Beč, Austrija, 2000

[2] Pod bićem krivičnog djela podrazumijeva se skup posebnih elemenata koji predstavljaju posebna obilježja jednog krivičnog djela i koja ga razlikuju od drugih krivičnih djela

(internet prevare, piraterija softvera i baza podataka, sajber industrijska špijunaža); ona koja se odnose na **proizvodnju i distribuciju nedozvoljenih sadržaja** (dječija pornografija, širenje rasne i vjerske mržnje); ona koja se odnose na **povredu privatnosti** (prisluškivanje, nadgledanje pošte, fišing, spam...)i dr.

U daljem teksu ću se osvrnuti na pojedinačna krivična djela protiv bezbjednosti računarskih podataka koja su propisana Krivičnim zakonom Republike Srpske.

2. KRIVIČNA DJELA PROTIV BEZBJEDNOSTI RAČUNARSKIH PODATAKA REGULISANA KRIVIČNIM ZAKONOM REP. SRPSKE[3]

Treba spomenuti da je Krivični zakon Republike Srpske, po ugledu na zakonodavstvo zemalja u okruženju, u oblasti visokotehnološkog kriminala u potpunosti prihvatio odredbe Budimpeštanske konvencije o vosokotehnološkom kriminalu kao najbitnijeg evropskog dokumenta u ovoj oblasti. Ova djela su regulisana Glavom 24. Krivičnog zakona:

- Oštećenje računarskih podataka i programa (član 292a)
- Računarska sabotaža (član 292b.);
- Izrada i unošenje računarskih virusa (član292v.)
- Računarska prevara (član292g.);
- Neovlašćeni pristup zaštićenom računaru, računarskoj mreži, telekomunikacionoj mreži i elektronskoj obradi podataka (član 292d.);
- Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (član 292đ.);
- Neovlašćeno korišćenje računara ili računarske mreže (član 292e.).

2.1. Oštećenje računarskih podataka i programa

(1) Ko neovlašćeno izbriše, izmjeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program, kazniće se novčanom kaznom ili zatvorom do jedne godine.

(2) Ako je djelom iz stava 1. ovog člana prouzrokovana šteta u iznosu koji prelazi 10.000 KM, učinilac će se kazniti zatvorom od tri mjeseca do tri godine.

(3) Ako je djelom iz stava 1. ovog člana prouzrokovana šteta u iznosu koji prelazi 30.000 KM, učinilac će se kazniti zatvorom od tri mjeseca do pet godina.

(4) Uređaji i sredstva kojima je učinjeno krivično djelo iz st. 1. i 2. ovog člana, ako su u svojini učinioca, oduzeće se.

[3]Krivični zakon Republike Srpske („Službeni glasnik Republike Srpske“, br. 49/03, 108/04, 37/06, 70/06, 73/10, 1/12 и 67/13)

Suština krivičnopravne zaštite računarskog podatka i programa je da se osigura zaštita integriteteta i cjelovitosti podataka i programa kao što tu zaštitu uživaju i drugi fizički predmeti odnosno pokretne stvari. Zato Krivični zakon pod pojmom pokretne stvari podrazumjeva i kompjuterski podatak ili program: *„Pokretna stvar je i svaka proizvedena ili skupljena energija za davanje svjetlosti, toplote ili kretanja, telefonski impuls, kao i registrovani podatak koji je rezultat elektronske obrade podataka (kompjuterski podatak ili program)“.* Bez obzira da li se radnja izvršenja sastoji od brisanja, izmjene, oštećenja ili prikrivanja podatka ili programa, krajnja posljedica ovog krivičnog djela je da se računarski podatak ili program ne mogu koristiti odnosno bivaju usljed izvršenja djela neupotrebljivi za obradu.

Klasičan primjer ovog krivičnog djela sastoji se u obaranju veb sajtova ili upadu na veb sajtove određenih firmi i preuzimanju administratorskih privilegija. To se dešava kada izvršilac, koristeći određene propuste u izradi veb sajta, preuzme administratorska prava, uradi preregistraciju domena kod drugog provajdera i time ostvari apsolutnu kontrolu nad sajtom. Na taj način je sajt postao neupotrebljiv za pravog vlasnika što može da ima teške posljedice. Zanimljiv slučaj iz sudske prakse desio se u Brčko distriktu gdje je izvršilac, koristeći svoje vještine, pristupio jednoj privatnoj veb stranici i izmjenio izvorni kod stranice što je dovelo do automatskog brisanja podataka čime je nanesena šteta vlasniku stranice.

Svi smo upoznati sa djelovanjem poznate hakerske grupe *Anonymous* koja vrlo često obara sajtove kako kompanija tako i državnih institucija (prije nekoliko godina ta grupa je oborila sajtove poznatih muzičkih kuća (Grand Produkcija, Siti Rekords i SOKOJ) i ostavila poruku: „Počelo je“.

Poznati su i slučajevi radnika koji su, iz revolta prema poslodavcima, odnijeli službene laptope kući i izbrisali sa njih podatke i sadržaje koji su bili neophodni za poslovanje poslodavca, što je imalo određene štetne posljedice za poslovanje firme.

2.2. Računarska sabotaža

> ***Ko unese, uništi, izbriše, izmijeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program ili uništi ili ošteti računar ili drugi uređaj za elektronsku obradu i prenos podataka sa namjerom da onemogući ili znatno ometa postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte, kazniće se zatvorom od šest mjeseci do pet godina.***

Ovo krivično djelo je, može se reći, samo jedan teži oblik krivičnog djela oštećenja računarskih podataka i programa. Razlog zbog čega je izdvojeno kao posebno djelo je namjera izvršioca da omete postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe, javne službe i ustanove. Najpoznatiji slučajevi računarske sabotaže odnose se na upade i obaranje veb sajtova državnih institucija. Već spomenuta hakerska grupa *Anonymous* sve više

pravi probleme državnim institucijama upadom na njihove veb stranice i stavljanjem poruka sa različitim značenjem.

Imamo u Srbiji zabilježen slučaj računarske sabotaže gdje je izvršilac, koji je u jednom državnom organu bio zaposlen kao analitičar za izvještavanje i informisanje, u namjeri da onemogući postupak elektronske obrade podataka, sa službenog računara izbrisao preko 5000 dokumenata koji su bili od značaja za rad njegove službe i koji su bili klasifikovani kao službena tajna.

Računarska sabotaža se danas sve više koristi kao jedan od savremenih oblika ratovanja za kojim posežu države (sajber ratovanje).

2.3. Izrada i unošenje računarskih virusa

(1) Ko napravi računarski virus u namjeri njegovog unošenja u tuđi računar ili računarsku mrežu ili telekomunikacionu mrežu, kazniće se novčanom kaznom ili zatvorom do šest mjeseci.
(2) Ko unese računarski virus u tuđi računar ili računarsku mrežu i time prouzrokuje štetu, kazniće se novčanom kaznom ili zatvorom do dvije godine.
(3) Uređaj i sredstva kojima je učinjeno krivično djelo iz st. 1. i 2. ovog člana oduzeće se.

Računarski virus se može definisati kao program koji ugrožava ili mjenja funkcije računarskog sistema, odnosno program koji ugrožava ili neovlašćeno koristi računarske podatke. Iz odredbi se vidi da je kažnjivo samo pravljenje računarskog virusa. Onog trenutka kada je virus napravljen, smatra se da je djelo izvršeno, uz postojanje namjere unošenja uz tuđi računar ili mrežu. Drugi oblik krivičnog djela je unošenje virusa u tuđi računar ili mrežu, bez obzira da li je učinilac sam napravio virus ili je na neki drugi način došao do njega. Ovde je bitno da je nastala šteta bilo koje vrste (imovinska šteta, gubitak nekog podatka...). U slučaju izvršenja ovog krivičnog djela i procesuiranja izvršioca, sud će u svakom konkretnom slučaju uz pomoć vještaka cjeniti da li se nešto smatra računarskim virusom.

U sudskoj praksi Njemačke postoji slučaj osamnaestogodišnjeg hakera koji je svojim virusom zarazio preko 20 miliona računara za veoma kratak vremenski period, od svega par dana. Na taj način je na jednom broju računara onemogućio dalji rada a na određenom broju je došlo do uništenja svih podataka. Izvršilac je osuđen na 21 mjesec zatvora.

U postupku koji je vođen pred sudom u Beogradu, jedno lice je osuđeno za krivično djelo pravljenja i unošenja računarskog virusa. Radi se o učiniocu koji je na svom personalnom računaru, pomoću jedne programske aplikacije napravio računarski virus, a u namjeri njegovog unošenja u tuđe računare. Virus je imao funkcije slikanja aktivnog monitora zaraženih računara drugih korisnika, postavljanje sadržaja na zaražene računare drugih korisnika kao i skidanje sadržaja sa tih računara. Viruse je izvršilac slao putem elektronske

pošte sa različitih adresa i aktivacijom virusa od strane korisnika, izvršilac je imao uvid u sadržaj aktivnog monitora i snimao sadržaje koje korisnik unosi na računar i na taj način prouzorkovao štetu korisnicima.

Koliko štete može da napravi računarski virus može da se ilustruje na primjeru Irana gdje je 2010.godine računarski virus *Staksnet* ugrozio iranski uklearni program. Virus je napadao uređaje koji kontrolišu centrifuge uranijuma, nastojeći da obustaci rad tih centrifuga.

Vrlo često se uz krivično djelo izrade i unošenja računarskog virusa pojavljuje i krivično djelo računarske prevare, gdje je izvršilac zarazio virusom računar nekog korisnika, a svu u cilju pribavljanja ličnih informacija o korisniku (lični podaci, brojevi bankovnih računa i dr.)

2.4. Računarska prevara

(1) Ko unese netačan podatak, propusti unošenje tačnog podatka ili na drugi način prikrije ili lažno prikaže podatak i time utiče na rezultat elektronske obrade i prenosa podataka u namjeri da sebi ili drugom pribavi protivpravnu imovinsku korist i time drugom prouzrokuje imovinsku štetu, kazniće se novčanom kaznom ili zatvorom do tri godine.

(2) Ako je djelom iz stava 1. ovog člana pribavljena imovinska korist koja prelazi iznos od 10.000 KM, učinilac će se kazniti zatvorom od jedne do osam godina.

(3) Ako je djelom iz stava 1. ovog člana pribavljena imovinska korist koja prelazi iznos od 30.000 KM, učinilac će se kazniti zatvorom od dvije do deset godina.

(4) Ko djelo iz stava 1. ovog člana učini samo u namjeri da drugog ošteti, kazniće se novčanom kaznom ili zatvorom do šest mjeseci.

Ovo krivično djelo, može se reći zauzima centralno mjesto u grupi krivičnih djela protiv bezbjednosti računarskih podataka i predstavlja najrašireniji oblik ovih djela. Ono se posmatra kao jedan poseban oblik krivičnog djela prevare.

Radnja izvršenja ovog krivičnog djela sastoji se u unošenju nekog podatka, brisanju nekog podatka, propuštanju da se unese neki podatak ili se, na bilo koji drugi taj podatak prikrije ili lažno prikaže, a da ta radnja koja se preduzima i da taj podatak koji se na taj način uništava, prikriva, lažno prikazuje, utiče na rezultat elektronske obrade u onom izvornom smislu. Posljedica ovih preduzetih radnji jeste da se dobije određeno stanje na računaru ili u računarskom sistemu koje ne bi bilo dobijeno, niti bi se do njega moglo doći a da nije taj podatak unijet, izbrisan, promijenjen. Da bi bilo izvršeno ovo krivično djelo, mora postojati namjera (umišljaj) pribavljanja protivpravne imovinske koristi. Postoji i privilegovani oblik ovog djela kod kojeg nema namjere da se pribavi imovinska korist već samo postoji namjera da se nanese šteta drugom licu.

Danas veoma raširen oblik računarske prevare je tzv „Nigerijska prevara“. Radi se o prevari koja se vrši pomoću lažnih email poruka o dobicima na igrama na sreću, lažnih poruka vezanih za dobrotvorne priloge, humanitarnim akcijama i dr. Izvršenje „Nigerijske prevare“ uglavnom počinje ubjeđivanjem „žrtve“ da učestvuju u podeli određenih novčanih fondova, i to ako unapred uplate određeni novčani iznos. Taj novčani iznos je u najvećem broju slučajeva neuporedivo manji od onog iznosa koji bi trebali da dobiju kao korist od nekog fonda, odnosno od pošiljaoca poruke. Jednom kada se uplati iznos pošiljaoci maila nestaju bez traga.

Još jedan od raširenijih načina računarske prevare je tzv Phishing (pecanje) koji ustvari predstavlja način krađe povjerljivih podataka (ličnih podataka, brojeva računa, pin kodova..). Najčešće se izvršava tako što lice primi (lažnu) elektronsku poštu od svoje banke da postoje izvjesni problemi sa računom i koja sadrži uputu da se lice obrati banci odnosno da se uloguje na sajt banke (lažni) i unese podatke o sebi i svom računu. Izvršilac koje je uputilo poruku je istovremeno napravio i lažni sajt banke i ostavljajući svoje podatke lice se „upecalo“ i otkrilo svoje bankovne podatke izvršiocu.

Drugi način prikupljanja digitalnog zapisa bankovnih kartica, vrši se direktno na bankomatima i POS terminalima, gdje kriminalac fizički postavlja elektronski uređaj (*skimmer*) na mjesto gde se ubacuje bankovna kartica. Uloga *skimmera* je da sa magnetne trake koja se nalazi na poleđini bankovne kartice očita digitalni zapis i memoriše ga. Kasnije, tako prikupljeni digitalni zapisi se uz pomoć posebnih uređaja, koji su lako dostupni na tržištu, narezuju na bijelu plastiku, odnosno na *blanko* kartice. Pin kodovi se obično prikupljaju postavljajući male skrivene kamere na bankomate. Na ovaj način prave se duplikati originalnih bankovnih kartica.

Primjer računarke prevare imamo i u slučaju sportskih kladionica gdje lica koja rade u sportskim kladionicama mogu da izmjene u računaru podatak o vremenu na kojem je podešen računar i time ostvare veliku imovinsku korist.

Kakakterističan primjer internet prevare desio se u jednoj njemačkoj banci gdje je jedan službenik štedionice izdao naredbu svom računaru da, prilikom obračunavanja kamata, zaokružuje stotine i desetine pfeninga i ostatke do zaokruženog broja, automatski prebacuje na njegov račun. Tako je službenik u vrlo kratkom vremenu, sebi pribavio veliku imovinsku korist.

2.5. Neovlašćeni pristup zaštićenom računaru, računarskoj mreži, telekomunikacionoj mreži i elektronskoj obradi podataka

(1) Ko se, kršeći mjere zaštite, neovlašćeno uključi u računar ili računarsku mrežu ili neovlašćeno pristupi elektronskoj obradi podataka, kazniće se novčanom kaznom ili zatvorom do šest mjeseci.

(2) Ko snimi ili upotrijebi podatak dobijen na način predviđen u stavu 1. ovog člana, kazniće se novčanom kaznom ili zatvorom do dvije godine.

(3) Ako je usljed djela iz stava 1. ovog člana došlo do zastoja ili ozbiljnog poremećaja funkcionisanja elektronske obrade i prenosa podataka ili mreže ili su nastupile druge teške posljedice, učinilac će se kazniti zatvorom do tri godine.

Ovo krivično djelo se izvršava na način da se izvršilac neovlašćeno uključi u računar ili računarsku mrežu ili pristupi elektronskoj obradi podataka kršeći mjere zaštite. Radi se o „probijanju lizinke (*Passworda*)“ koja je u stvari tajni kod koji je vlasnik računara unio na računar kako bi samo on imao pristum računaru ili pojedinim servisima. Lica koja se bave ovim danas se nazivaju „hakeri“ Oni se iz različitih motiva bave ilegalnim pristupanjem računarskim sistemima i sposobni su da savladaju i najsloženije mjere zaštite koje određeni računarski sistemi posjeduju.

Jednom kada izvršilac uspije na taj način da pristupi podacima trećeg lica, te podatke može da zloupotrebi na razne načine. Može da te podatke prodaje pribavljajući određenu finansijsku korist za sebe i tada će postojati uz ovo i krivično djelo računarske prevare.
Zanimljim primjer se desio u jednoj susjednoj zemlji gdje je izvršilac, kršeći mjere zaštite, pristupio mreži pravodusnih institucija, kojoj su pristup imali samo sudije i tužioci, i neovlašteno ostvario uvid u informacije i podatke osjetljive prirode.

Takođe imamo primjer iz Srbije gdje su maloljetni hakeri neovlašteno pristupili bazi podataka jedne političke partije, snimili podatke i pradali te podatke redakcijama štampanih i elektronskih medija.
U Republici Srpskoj jedan izvršilac je upao u računarsku mrežu jedne firme i blokirao knjigovodstveni softver zahtjevajući određenu finansijsku isplatu.

Opšteprisutna je pojava upada u Facebook profile i zloupotrebe podataka dobijenih na taj način. Ovako se uz izvršenje ovog krivično djela mogu izvršiti i druga krivična djela: neovlašćeno korišćenje ličnih podataka, širenje mržnje...)

2.6. Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži

(1) ***Ko neovlašćeno sprečava ili ometa pristup javnoj računarskoj mreži, kazniće se novčanom kaznom ili zatvorom do jedne godine.***

(2) ***Ako djelo iz stava 1. ovog člana učini službeno lice u vršenju službe, kazniće se zatvorom do tri godine.***

Jedan od najraširenijih načina izvršenja ovog krivičnog djela sastoji se u sljedećem: odabere se određeni veb sajt, obično neke važne institucije u zemlji, kojem često pristupa veliki broj korisnika. Zatim se na taj sajt, odnosno server na kome se nalazi sajt, pošalje veći broj informacija ili zahtjeva za informacijama, što dovodi do zagušenja saobraćaja prema tom

serveru i na taj način se onemogući pristup sadržaju i uslugama sajta. Napad dolazi sa velikog broja računara tako da je vrlo teško spriječiti ovakvu vrstu napada. Ovakvi napada se nazivaju *DDoS* napadi.
Česti su slučajevi ovakvih napada na veb portale vlada zemalja u cilju onemoćavanja pristupa istim pa tako i portal Vlade Republike Srpske često biva predmetom napada.

2.7. Neovlašćeno korišćenje računara ili računarske mreže

(1) Ko neovlašćeno koristi računarske usluge ili računarsku mrežu u namjeri da sebi ili drugom pribavi protivpravnu imovinsku korist, kazniće se novčanom kaznom ili zatvorom do tri mjeseca.
(2) Gonjenje za djelo iz stava 1. ovog člana preduzima se po prijedlogu.

Ovde se radi o učiniocu koji neovlašteno koristi računarsku mrežu ili koristi određene računarske usluge u svrhu činjenja nekog od prethodno navedenih krivičnih djela. Ono što je bitno za izvršenje ovog djela je da učinilac ima namjeru da zloupotrebom sebi ili drugom obezbjedi određenu imovinsku korist.

4. PREVENTIVNO DJELOVANJE – PREPORUKE

U daljem tekstu dat je pregled korisnih savjeta za zaštitu računara i zaštitu ličnih podataka:

1. Uvijek treba na računaru imati aktiviran zaštitni (antivirus) program. Osnovna svrha antivirusnog programa je sprečavanje ubacivanja virusa u korisnikov računar. Antivirus program je potrebno redovno ažurirati.
2. Operativni sistem je potrebno redovno ažurirati kako bi se sigurnosni propusti na vrijeme uočili i otklonili
3. Računar treba gasiti kad korisnik nije kraj njega. Na taj način se sprečava preuzimanje kontrole nad njegovim radom.
4. Posebnu pažnju treba obratiti prilikom *download-a* (preuzimanja) sadržaja sa interneta jer se često dešava da su ti sadržaji zaraženi nekim virusom. Takođe obratiti pažnju na preuzimanje priloga koju dođu uz elektronsku poštu nepoznatih pošiljalaca. Takvu poštu nije preporučljivo otvarati.
5. Prilikom obavljanja plaćanja preko interenta stalno treba kontrolisati stanje na računu. Obavezno je potrebno kontrolisati izgled stranice i sigurnosne protokole koji se koriste na tim stranicama.
6. Izbjegavati korištenje ličnih podataka na internetu (datum rođenja, broj telefona, brojeve kartica, pin kodove...)
7. Lozinke za elektronske naloge za poštu i dr. nikada ne čuvati automatski u poljima za unos.
8. Važne podatke u elektronskom obliku poželjno je čuvati na uređajima bez internet konekcije ili na prenosivim medijima (prenosivim hard diskovima, USB stikovima...).

9. Prilikom registracije na razne sajtove obratiti pažnju na podatke koji se ostavljaju.
10. Izbjegavati postavljanje fotografija na internet koje bi mogle biti javno dostupne drugima

4. ZAKLJUČAK

Ova oblast kriminalnih aktivnosti je kod nas može se reći nova, ali svakim danom sve više prisutna. Ona zahtjeva konstantno praćenje zbog njene dinamičnosti koju joj pruža brz razvoj informacionih tehnologija. S jedne strane je potrebno stalno nadograđivati pozitivnopravne propise, odnosno učiniti zakonodavstvo u ovoj oblasti elastičnim i brzo promjenjivim u skladu sa promjenama tehnologija. Na taj način se može obezbjediti adekvatna sudska zaštita kao preduslov za sigurno korištenje računara i sigurno i kvalitetno obavljanje raznih računarskih usluga.

S druge strane, pojedinci treba da imaju određenu vrstu „kulture bezbjednosti“ i u svom ponašanju treba da poštuju određene principe jer se na taj način štiti i privatni i javni interes. Neophodno je vršiti stalnu edukaciju korisnika računarskih tehnologija o sajber kriminalu i njegovim pojavnim oblicima u cilju podizanja svijesti samih korisnika.