# Okvir za rješavanje problema cyber kriminala

Haris Hamidović
IT sektor – Odjel informacijske sigurnosti
MKF EKI Sarajevo
Sarajevo, Bosna i Hercegovina
haris.hamidovic@eki.ba

Amra Hamidović
Regionalni ured Tuzla
OSCE BiH
Tuzla, Bosna i Hercegovina
amrahamidoviciur@gmail.com

Mahir Zajmović
Fakultet informacijskih tehnologija
Sveučilište/Univerzitet „Vitez“
Vitez, Bosna i Hercegovina
mahir.zajmovic@unvi.edu.ba

*Sažetak*— **Unatoč svim pogodnostima koje je donijela informacijska tehnologija, njihovom svestranom korištenju i općem prihvaćanju, nisu izostale ni negativne posljedice. Pored novih oblika zloupotreba, informacijska je tehnologija omogućila da se već tradicionalni oblici kriminalnih dijela izvode na novi, kvalitativno i kvantitativno drugačiji način. U borbi protiv cyber kriminala postoje razni modeli, koji se koriste kako bi se opisale faze i postupci koji utječu na njegovo suzbijanje. U ovom radu predstavljamo jedan od praktično primjenjivih modela za suzbijanje cyber kriminala koji uključuje faze: sprječavanja, otkrivanja, istrage i procesuiranja cyber kriminala. Osim toga, predstavljamo i najznačajnije izazove s kojima se susreću javni i privatni subjekti u rješavanju problema cyber kriminala.**

***Ključne riječi- cyber kriminal; sigurnost; digitalni dokazi***

## I. UVOD

U svijetu nezakonitih društveno štetnih djelovanja cyber kriminal zauzima jedno od vodećih mjesta. Prema učestalosti, dosegu, negativnostima i štetnim posljedicama izbija u prve redove te uz ostalo postaje velika smetnja poželjnom informacijskom razvoju. Opravdana su stoga nastojanja da se mehanizmima samoobrane i pravnim propisima štiti informacijske sisteme od takvih protupravnih djelovanja i strogo kažnjava njihove počinitelje.

Unatoč svim pogodnostima koje je donijela informacijska tehnologija, njihovom svestranom korištenju i općem prihvaćanju, nisu izostale ni negativne posljedice. Pored novih oblika zloupotreba, informacijska je tehnologija omogućila da se već tradicionalni oblici kriminalnih dijela izvode na novi, kvalitativno i kvantitativno drugačiji način.

U borbi protiv cyber kriminala postoje razni modeli, koji se koriste kako bi se opisale faze i postupci koji utječu na njegovo suzbijanje. U ovom radu predstavljamo praktično primjenjiv model, koji uključuje faze: sprječavanja, otkrivanja, istrage i procesuiranja cyber kriminala. Osim toga, predstavit ćemo i najznačajnije izazove s kojima se susreću javni i privatni subjekti u rješavanju problema cyber kriminala.

## II. STVARNA OPASNOST

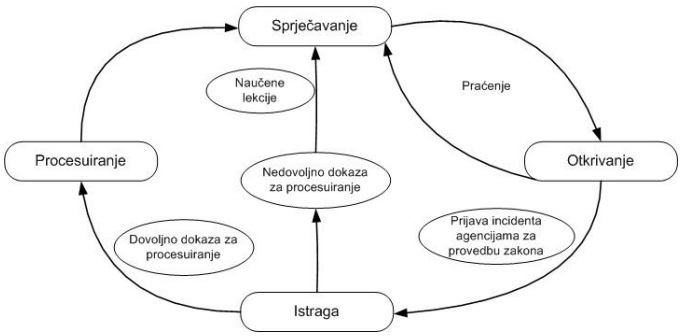
Sve se veći broj podataka i informacija o ljudima, njihovom imovinskom, zdravstvenom, radnom ili drugom stanju prikuplja, obrađuje i pohranjuje u informacijskim sistemima brojnih financijskih, zdravstvenih, upravnih, privrednih i drugih javnih i privatnih institucija i preduzeća. Otvorenost takvih sistema prema okolini, koje je nametnuo suvremeni način života i komuniciranja, učinio je takve podatke dostupnima onima koji su nadležni za njihovo korištenje, ali i svima drugima koji takav pristup ostvaruju neovlašteno radi ostvarivanja svojih nezakonitih i nemoralnih ciljeva. Posebno su ugroženi veliki vojni, vladini, privredni i drugi informacijski sistemi, na kojima se nalaze tajni i povjerljivi podaci, važni za pojednice, preduzeća i organizacije te nacionalne a nerijetko i šire društvene interese. I najzaštićeniji informacijski sistemi, unatoč golemim ulaganjima i naporima organizacija, ne mogu se othrvati od sve brojnijih napada i postići zadovoljavajući stepen svoje sigurnosti, koji će jamčiti tajnost, cjelovitost i dostupnost u njima pohranjenih podataka. O napadima na brojne informacijske sisteme i štetnim posljedicama koje oni snose radi toga, govore izvješća mnogih agencija i organizacija koje se bave pitanjem sigurnosti. [1]

Na temelju različitih studija i stručnih mišljenja, izravni negativni ekonomski utjecaj uzrokovan djelima cyber kriminala se procijenjuje na stotine miliona dolara godišnje. Naprimjer, projekcija ukupnih gubitaka koje su pretrpjele američke organizacije zbog cyber kriminala u 2014. godini je iznosila 800,492,073 dolara. [2] Procjene gubitaka rađene su na temelju izravnih i neizravnih troškova koji mogu uključivati:

- stvarno ukradeni novac;
- procjena troškova krađe intelektualnog vlasništva;
- troškovi povrata, popravke ili zamjene oštećenih mreža i opreme, te
- nematerijalni gubitak zbog izgubljenih poslovnih mogućnosti, uslijed nedostatka povjerenje kupaca u online trgovanje.

## III. MODEL ZA SUZBIJANJE CYBER KRIMINALA

U borbi protiv kompjuterskog kriminala postoje razni modeli, koji se koriste kako bi se opisale faze i postupci koji utječu na njegovo suzbijanje. Ured američke vlade za provjeru odgovornosti (Government Accountability Office - GAO) predstavlja model, koji uključuje faze: sprječavanja, otkrivanja, istrage i procesuiranja kompjuterskog kriminala (Sl.1.). [3]




Slika 1. Model za suzbijanje cyber kriminala

Informacija je imovinu koja, kao i druga važna poslovna imovina, ima vrijednost za organizaciju te stoga treba biti odgovarajuće zaštićena. [4] Gubitak povjerljivosti, cjelovitosti, dostupnosti, autentičnosti, pouzdanosti i mogućnosti revizije informacija i usluga može imati negativan utjecaj na organizacije. Stoga, postoji kritična potreba za zaštitu informacija i upravljanje sigurnošću IT sistema unutar organizacije. Osim značajne koristi, svaka nova tehnologija donosi i nove izazove za zaštitu informacija. Zahtjev za zaštitu informacija je osobito važan u današnjim okruženjima, s obzirom da su mnoge organizacije iznutra i izvana povezane mrežama IT sistema. [5]

Informacijska sigurnost se ostvaruje provođenjem odgovarajućeg skupa kontrola, koje mogu biti politike, prakse, procedure, organizacione strukture i softverske funkcije. Te kontrole trebaju biti uspostavljene kako bi se osiguralo da su sigurnosni ciljevi organizacije postignuti. [6]

No, ni jedna politika informacijske sigurnosti ili mjera zaštite ne može jamčiti potpunu zaštitu informacija, informacijskih sistema, usluga ili mreža. Nakon što se provedu mjere zaštite, preostale slabosti će vjerojatno i dalje ostati. One mogu učiniti informacijsku sigurnost neučinkovitom, a time i incidente informacijske sigurnosti mogućim, uz potencijalne izravne i neizravne negativne utjecaje na organizacijsko poslovanje. Osim toga, nove prethodno nepoznate prijetnje će se pojaviti. Nedovoljna priprema organizacije da se nosi s takvim incidentima će učiniti bilo koji stvarni odgovor manje djelotvornim, i potencijalno povećati stepen mogućih štetnih utjecaja na poslovanje. Stoga je neophodno za bilo koju organizaciju, koja se ozbiljno odnosi prema informacijskoj sigurnosti, da ima strukturiran i planiran pristup za [7]:

- otkrivanje, izvještavanje i procjenu incidenata informacijske sigurnosti;
- reagiranje na incidente informacijske sigurnosti, uključujući i aktiviranje odgovarajućih mjera zaštite radi sprječavanja i umanjivanja, kao i povrata od, negativnih utjecaja (na primjer, u podršci i planiranju kontinuiteta poslovanja);
- učenje iz incidenata informacijske sigurnosti, ustanovljavanje preventivne zaštite, i, tijekom vremena, činjenja poboljšanja cjelokupnog pristupa upravljanju incidentima informacijske sigurnosti.

## IV. SPECIFIČNOSTI ORGANIZACIJSKIH OKRUŽENJA

U mnogim jurisdikcijama često je nejasno organizacijama koje uvjete i ograničenja zakon postavlja na prikupljanje i očuvanje potencijalnih digitalnih dokaza. Često je također nejasno kako se odgovornost dijeli između agencija za provedbu zakona i organizacija pogođenih kriminalnim aktivnostima koje su ostavile digitalne tragove. [8]

Može se reći da organizacije moraju preuzeti veću odgovornost u cyber svijetu nego što trenutačno čine u fizičkom svijetu. Razlog tome je kompleksnost okruženja, a time i kompleksnost istraživanja zločina u ovom okruženju. Agencije za provedbu zakona trebaju potporu u dobivanju uvida u pogođene sisteme. Osim toga, agencije za provedbu zakona mogu samo prikupljati dokaze post mortem, te stoga ovise o činjenici da su organizacije pogođene kriminalnom radnjom skupljale i sačuvale potencijalne digitalne dokaza na način koji jamči da su oni autentični, tačni i potpuni. [9]

Prva obaveza organizacije je da opstane kako bi mogla nastaviti služiti svojim kupcima i klijentima, nastaviti podmirivati svoje obveze prema dužnicima, bankama, zaposlenicima, široj javnosti i državi. Osim toga, od komercijalnih organizacija se očekuje da generiraju dobit za dioničare.

Moguće je očekivati značajan konflikt između potrebe za organizacijskim kontinuitetom poslovanja i zahtjeva za pouzdanim prikupljanjem dokaza sa samih uređaja koji održavaju organizacije operativnim.

Osim ako organizacija nije razvila detaljni planirani odgovor na tipične rizik scenarije, mnogo potencijalnih dokaza nikada neće biti prikupljeno ili će postati bezvrijedni kao rezultat onečišćenja. Osim toga, tijekom istrage, organizacija će biti stalno suočena s dilemom: izgubiti poslovne prilike prilikom isključenja bitnih sistema, tako da dokazi mogu biti ispravno očuvani, ili imati potencijalne gubitke, jer dokazi nisu mogli biti proizvedeni. [10]

Iako su pojedinosti prikupljanja i analiziranja digitalnih dokazi u značajnoj mjeri pitanje implementacije tehničkih vještina, uspjeh u tome uvelike ovisi o nivou pažljivog pred-planiranja. Usred incidenta mogu postojati situacije u kojima će biti bitno donijeti važne odluke u vezi pravilnog očuvanja dokaza ili kontinuiteta poslovanja, naprimjer potreba za isključivanjem centralnog računarskog servisa na određeno vrijeme. To su odluke koje treba donijeti glavna uprava, a ne računarski tehničari ili hitno-angažirani vanjski savjetnik. [10]

## V. NEPRIJAVLJIVANJE UPADA U SISTEME

Rezultati istraživanja provedenog od strane Američkog ministarstva pravosuđa, pokazuju da mnoge organizacije nevoljko izvješćuju o provalama u svoje sisteme. Razlozi za neprijavljivanje upada uključuju sljedeće:

- Organizacija na koju je izvršen napad ne zna koju agenciju za provođenje zakona treba pozvati.
- Ukoliko organizacija na koju je izvršene napad prijavi napad nadležnom tijelu, agencija za provedbu zakona neće djelovati. Umjesto toga, informacija o upadu će postati javna, što će utjecati nepopravljivo na povjerenje ulagača i usmjeriti potencijalne kupce da izabor konkurencije koja nije izvijestila o upadima u svoj sistem.
- Ukoliko agencije za provedbu zakona djeluju nakon podnošenja izvještaja o upadu i provedu istragu, napadača neće moći pronaći. U tom procesu, međutim, organizacija će izgubiti kontrolu nad tijekom istrage. Osoblje agencije za provedbu zakona će izuzeti ključne podatake, a možda i cijele računare, oštetiti opremu i datoteke, kompromitovati privatne informacije koje pripadaju kupcima i partnerima, te ozbiljno ugroziti normalno poslovanje organizacije. Samo će konkurencija imati koristi od napuštanja kupaca i pada vrijednosti dionica.
- Čak i ukoliko agencije za provedbu zakona pronađu napadača, on će vjerojatno biti maloljetnik, ili biti u stranoj zemlji, ili oboje, a tužitelj će odbiti ili se neće moći nastaviti sa slučajem.
- Ako napadač nije maloljetnik, tužitelj će zaključiti da je iznos štete koju je napadač napravio premali da bi opravdao gonjenje.
- Ukoliko agencije za provedbu zakona uspješno procesuiraju napadača, on će dobiti uvjetnu kaznu ili neznatnu zatvorsku kaznu, koju će iskoristiti za postizanje hakerske slave i unosnog posla u oblasti sigurnosti mreža.
- Neki menadžeri informacijske sigurnosti ne žele izvijestiti o upadima, čak ni svojim nadređenim. Zbog same činjenica o upadu u sistem, IS menadžeri strahuju, da će kod uprave biti stvoreno mišljenje da on/ona nije ispravno osigurao sistem. [11]

Iako vlasnici mreža imaju obavezu osigurati svoje sisteme, a agencije za provedbu zakona imaju obavezu istražiti i progoniti počinitelje kaznenih dijela kada je to potrebno, jedni bez drugih ne mogu učinkovito funkcionirati. Mrežni operatori trebaju vidjeti agencije za provedbu zakona kao nužan dio sistema zaštite, a agencije za provedbu zakona moraju biti u mogućnosti računati na suradnju žrtava u ispunjavanju svoje obaveze. [11]

## VI. NEDOSTATAK SVIJESTI O ZNAČAJU INFORMACIJSKE SIGURNOSTI

Nepostojanje, nedostatna ili neadekvatna primjena sigurnosnih mjera najčešći je razlog ugrožavanja sigurnosti. [1]

Glavni izazov u ublažavanju problema cyber kriminala je poboljšanje prakse informacijske sigurnosti od strane organizacija i pojedinačnih korisnika Interneta. Podizanje svijesti o cyber kriminalu i potrebi zaštite informacija i sistema je ključna aktivnost u rješavanju problema cyber kriminala.

Bez adekvatne informacijske sigurnosti, kritični sistemi i osjetljivi podaci su podložniji krivično kažnjivim pristupima, krađi, modifikaciji i uništenju. GAO revizija je pokazala da čak ni američke federalne agencije adekvatno ne štitite informacijske sisteme koje Vlada koristi za pružanje usluga svojim klijentima. [3]

Verizon studija ukazuje da su u 87% slučajeva, istraživači bili u mogućnosti zaključiti da su se povrede sigurnosti mogle izbjeći da su postojale razumne sigurnosne kontrole na licu mjesta u trenutku incidenta. Verizon studija nastala je na bazi više od 500 forenzičkih angažmana tijekom četverogodišnjeg razdoblja. [12]

## VII. PROCEDURA REAGOVANJA NA INCIDENT CYBER KRIMINALA

Ako odgovorne osobe u organizaciji ocijene da postoji sumnja da je incident informacijske sigurnosti uzrokovan izvršenjem krivičnog djela imaju pravo o toj sumnji obavijestiti ovlaštenu službenu osobu ili Tužitelja. Ako je prijava podnesena ovlaštenoj službenoj osobi oni će tu prijavu primiti i odmah je dostaviti Tužitelju. [13]

Tužitelj naređuje sprovođenje istrage ako postoje osnovi sumnje da je izvršeno krivično djelo. Tužitelj neće narediti sprovođenje istrage ako je iz prijave i pratećih spisa očigledno

da prijavljeno djelo nije krivično djelo ili ako postoje druge okolnosti koje isključuju krivično gonjenje.

U toku sprovođenja istrage Tužitelj može poduzeti sve istražne radnje, uključujući vršenje uviđaja i rekonstrukcije, naređivanje potrebnih vjestačenja i dr.

Tužitelj će naredbom obustaviti istragu ukoliko se ustanovi da nema dovoljno dokaza da je osumnjičeni učinio krivično djelo.

Kad u toku istrage Tužitelj nađe da postoji dovoljno dokaza iz kojih proizlazi osnovana sumnja da je osumnjičeni učinio krivično djelo, pripremit će i uputiti optužnicu sudiji za prethodno saslušanje.

Prilikom potvrđivanja optužnice, sudija za prethodno saslušanje proučava svaku tačku optužnice i materijale koje mu je dostavio Tužitelj kako bi utvrdio postojanje osnovane sumnje. Pošto se potvrde pojedine ili sve tačke optužnice, osumnjičeni dobija status optuženog. [13]

## VIII. ZAKONSKA PRIHVATLJIVOST DOKAZA

Pitanje zakonske prihvatljivosti se odnosi na to da li će sud prihvatiti dokaz (u ovom slučaju digitalni zapis). Neki dokazi mogu biti primljeni u sudu (tj. pravno dopušteni), ali advokat suprotne strane može postaviti upitnim njihovu dokaznu težinu. Stoga bi bilo važno dokazati da je [14]:

- zapis tačan, tj. da je cjelovit i nepromijenjen prikaz podataka;
- zapis autentičan, odnosno da je ono što pokazuje da jest;
- zapisi nitko nije neovlašteno mijenjao;
- zapis je pohranjen u sistemu koji je bio siguran tijekom cijelog životnog vijeka zapisa.

Informacijska sigurnost je ključna kada se raspravlja o pitanjima pravne prihvatljivosti. Glavna rasprava na ovu temu će vjerojatno biti u vezi autentičnosti pohranjenih informacija. Kada su elektroničke informacije snimljene na sistem za pohranu, da li je proces bio siguran? Da li je li prava informacija uhvaćena, i da li je bila potpuna i tačna? Tijekom skladištenja, da li je informacija promijenjena na bilo koji način, bilo slučajno ili zlonamjerno? Prilikom davanja odgovora na ova pitanja, provedba i praćenje informacijske sigurnosti je ključna u demonstriranju autentičnosti. [15]

Pitanje nezakonitog dokaza se rješava neovisno od njegove kvalitete istine. Dokaz može biti zabranjen bez obzira na njegovu autentičnost, relevantnost i pouzdanost. Postoje razlike u klasificiranju nezakonitih dokaza, ovisno o njihovim autorima, ali najčešće pitanje nezakonitih dokaza se može svrstati u tri osnovne kategorije i to [16]:

- dokazi pribavljeni povredom određenih ljudskih prava;
- dokazi koji su u ZKP-u predviđeni da se ne smiju uporabiti kod donošenja sudbene odluke u kaznenom postupku;
- dokazi pribavljeni na način koji je sam za sebe zakonit, ali se za te dokaze saznalo iz nekog izvora dokaza pribavljenog na nezakonit način - tzv. „plodovi otrovne voćke“.

Organizacija treba voditi računa da potencijalni digitalni dokazi koje prikuplja nisu pribavljeni povredama ljudskih prava i sloboda propisanih ustavom i međunarodnim ugovorima koje je Bosna i Hercegovina ratifikovala, s obzirom da prema Zakonu o krivičnom postupku sud ne može zasnovati svoju odluku na takvoj vrsti dokaza. Ovo pitanje je naročito značajno za elektroničke zapise dobivene nadzorom uposlenika na radnom mjestu.

Treba uvijek imati na umu da radnici imaju pravo na određeni stepen privatnosti na radnom mjestu, ali to pravo mora biti uravnoteženo s pravom poslodavca da kontrolira funkcioniranja svog poslovanja i da se zaštiti od aktivnosti radnika koje mogu naškoditi legitimnim interesima poslodavca. [17] Da bi se elektroničko praćenje aktivnosti uposlenika moglo smatrati dopuštenim i opravdanim neophodno je, između ostalog, pridržavanje osnovnih načela zakonite obrade ličnih podataka izvedenih iz EU Direktive 95/46/EC i Zakona o zaštiti ličnih podataka Bosne i Hercegovine. [18] [19].

S obzirom na visoku stopu nelegalnog softvera instaliranog na računarima u Bosni i Hercegovini, potrebno je voditi računa da se potencijalni digitalni dokazi ne prikupljaju nelegalnim softverskim alatima.

Zabilježeno je nekoliko slučajeva forenzičkih istraga, u SAD i drugim zemljama, u kojima su forenzičari koristili piratske kopije forenzičkih softvera. To je imalo za posljedicu da je odbrana, opravdano, postavila upitnim autentičnost i pouzdanost dokaza i forenzičara.

## IX. MEĐUNARODNA SURADNJA

Sve veći broj djela cyber kriminala ima međunarodnu dimenziju. Jedan od razloga iza ove pojave je činjenica da postoji vrlo malo potrebe za fizičkom prisutnosti počinitelja na mjestu gdje se usluga pruža. Kao rezultat toga, kriminalci uglavnom ne moraju biti prisutni na mjestu gdje se žrtva nalazi. Općenito govoreći, cyber kriminal istrage imaju potrebu za međunarodnom suradnjom. Jedan od ključnih zahtjeva istražitelja u prekograničnim istragama je neposredna žurna reakcija njihovih kolega u zemlji u kojoj se potencijalni počinitelj krivičnog djela nalazi. Pogotovo je značajno rješavanje pitanja tradicionalnih instrumenata uzajamne pomoći koji, u većini slučajeva, ne ispunjavaju zahtjeve u pogledu potrebne brzine istraga na Internetu. [20]

## X. SMJERNICE I PROCEDURE ZA PRIKUPLJANJE DIGITALNIH DOKAZA

Trenutno ne postoji globalno prihvaćen standard prikupljanja digitalnih dokaza. Policije nekih zemalja su razvile vlastite smjernice i procedure za prikupljanje i zaštitu digitalnih dokaza. Međutim, to stvara probleme u slučaju prekogranično počinjenih zločina, s obzirom da će digitalni forenzički dokazi prkupljeni u jednoj zemlji možda morati biti prezentirani u sudovima drugih zemalja. [21]

Još od vremena prve digitalna forenzička istraživanja radionice (Digital Forensic Research Workshop - DFRWS) u 2001. godini, potreba za standardnim okvirom digitalne forenzičke istrage je prepoznata i istaknuta, ali do danas je bilo malo napretka u razvoju općenito prihvaćene metodologije. Generalni okvir digitalne forenzičke istrage mora biti dovoljno fleksibilan kako bi podržao buduće tehnologije i različite vrste incidenata. [22]

Međunarodni standard ISO/IEC 27037 bi trebao dati smjernice za specifične aktivnosti rukovanja digitalnim dokazima, kao što su identifikacija, prikupljanje, stjecanje i očuvanje potencijalnih digitalnih dokaza. [23] Iako kompletan proces rukovanja digitalnim dokazima uključuje i druge korake (npr. prezentacija, odlaganje i sl.), opseg ovih smjernica odnosi se samo na početne procese rukovanja. [24]

## XI. ZAKLJUČAK

Budući da na sadašnjem stepenu razvoja nije moguće ostvariti apsolutnu sigurnost kompjuteriziranih i međusobno povezanih informacijskih sistema, bez obzira na poduzete fizičke, tehničke (hardverske i softverske) i druge mjere, nužno je uz postojeće mjere, metode i sredstva zaštite, osigurati efikasnu pravnu zaštitu koja će se provoditi u suradnji s nadležnim organizacijama i ustanovama drugih zemalja širom svijeta.

Na sadašnjem stepenu razvoja prvenstvo imaju tehnološke pretpostavke zaštite, njihova cjelovita i efikasna primjena, te njihovo permanentno preispitivanje. Pravna, a posebno kaznenopravna zaštita, najvažniju ulogu ima na području generalne prevencije, tj. od odvraćanja od činjenja takvih dijela.

Neprekidno osposobljavanje agencija za provođenje zakona, u smislu jačanja kadrovskih i tehničkih kapaciteta, neophodno je za efikasnu borbu protiv ove vrste kriminala.

Uz tehnološke i pravne pretpostavke za suzbijanje i zaštitu od cyber kriminala i drugih opasnosti koje prijete informacijskim sistemima potrebno je poduzeti i niz drugih aktivnosti, osobito na području etike i obrazovanja. U prvom redu je podizanje svijesti o opasnostima koje prijete i isticanju potrebe pažljivog i odgovornog korištenja informacijskih sistema.

## LITERATURA


[1] D. Dragičević, Kompjutorski kriminalitet i informacijski sustavi – 2. izmijenjeno i dopunjeno izdanje, Informatorov Biro Sustav, Zagreb, 2004.

[2] Federal Bureau of Investigation - Internet Crime Complaint Center, 2014 Internet Crime Report, 2015.

[3] United States Government Accountability Office (GAO), Public and Private Entities Face Challenges in Addressing Cyber Threats, Report to Congressional Requesters, 2007.

[4] ISO/IEC 27002:2013, Information technology -- Security techniques -- Code of practice for information security controls, International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC), 2013.

[5] ISO/IEC 13335-1:2004, Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management, International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC), 2004.

[6] ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems – Requirements, International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC), 2013.

[7] ISO/IEC 27035:2011, Information technology -- Security techniques -- Information security incident management, International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC), 2011.

[8] P. Sommer, „The future for the policing of cybercrime“ Computer Fraud & Security, Issue 1, January 2004, pp 8-12.

[9] J. Danielsson, T. Ingvar, „The need for a structured approach to digital forensic readiness - Digital forensic readiness and e-commerce“, IADIS Internacional Conference e-Commerce, 2004.

[10] The Information Assurance Advisory Council (IAAC), Directors' and Corporate Advisors' Guide to Digital Investigations and Evidence, 2009.

[11] R. P. Salgado, Working with Victims of Computer Network Hacks, USA Bulletin, U.S. Department of Justice, 2001.

[12] Verizon Business Risk Team, Data Breach Investigations Report, 2008.

[13] Zakon o krivičnom postupku Bosne i Hercegovine (Službeni glasnik Bosne i Hercegovine, br. 3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09, 72/13)

[14] A. Dazey, A. Grzybowski, „Electronic records and legal admissibility: explanatory guidance“, The University of Edinburgh, 2009.

[15] BIP 0008-1:2014, Evidential Weight and Legal Admissibility of Information Stored Electronically: Code of Practice for the Implementation of BS 10008, British Standards Institution, 2014

[16] V. Antonić, M. Šikman, D. Kulić, R. Peleš, Preduzimanje radnji dokazivanja u istrazi pod nadzorom tužioca i zakonitost pribavljenih dokaza, Projekat "Uspostava boljih mehanizama saradnje policije i tužilaštava u BiH", 2009.

[17] H. Hamidović, „Nadzor elektroničkih komunikacija na radnom mjestu“, Telekomunikacije, God.11, br. 35, Bosanskohercegovačko udruženje za telekomunikacije Sarajevo, 2012.

[18] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Official Journal L 281 , 23/11/1995 P. 0031 - 0050)

[19] Zakon o zaštiti ličnih podataka Bosne i Hercegovine (Službeni glasnik Bosne i Hercegovine br. 49/06, 76/11)

[20] International Telecommunication Union (ITU), Understanding Cybercrime: A Guide for Developing Countries, 2009.

[21] M. Meyers, M. Rogers, „Computer Forensics:The Need for Standardization and Certification“, International Journal of Digital Evidence, Fall 2004, Volume 3, Issue 2, 2004.

[22] B. Carrier D., E. Spafford H., „An Event-Based Digital Forensic Investigation Framework“, DFRWS 2004, Baltimore, MD, 2004.

[23] ISO/IEC 27037:2012, Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence, International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC), 2012.

[24] H. Hamidović, H. Salkić, "The basic steps of digital evidence handling process", International Journal of information and communication technologies, Number 4, FIT, University of Vitez and Tambov State University, 2016.

ABSTRACT

Despite all the benefits promulgated by information technology, their versatile use and general acceptance, there are also some negative consequences. In addition to new forms of crime, information technology has enabled traditional forms of crime to be carried out on a new, qualitatively and quantitatively different way. In the fight against cyber crime, there are various models that are used to describe the phases and procedures used. In this paper we present a general model, which includes phases: prevention, detection, investigation and prosecution of cyber crime. Furthermore, we present the major challenges facing the public and private entities in addressing cyber crime.

At the present stage of development priority is given to technological protection prerequisites, their full and effective implementation, and their continuous review. The legal, especially criminal law protection, the most important role has in the general prevention, ie. in deterrence from committing such criminal acts.

Continuous training of law enforcement agencies, in terms of strengthening the human and technical capacity, is necessary to effectively combat these crimes.

With the technological and legal requirements for prevention and protection from cyber crime and other threats to information systems it is necessary to take a number of other activities, particularly in the area of ethics and education. In the first place is to raise awareness about the dangers and emphasizing the need of careful and responsible use of information systems.

**FRAMEWORK FOR ADDRESSING CYBER CRIME**

Haris Hamidović, Amra Hamidović, Mahir Zajmović