Računalni kriminalitet

Bečarević, Dino

Sveučilište Josipa Jurja Strossmayera u Osijeku
Filozofski fakultet
Preddiplomski studij informatologije

Dino Bečarević

Računalni kriminalitet

Završni rad

Mentor: izv. prof. dr. sc. Gordana Dukić
Sumentor: dr. sc. Anita Papić

Osijek, 2016

Sveučilište J.J. Strossmayera u Osijeku

Filozofski fakultet Osijek

Odsjek za informacijske znanosti

Preddiplomski studij informatologije

Dino Bečarević

Računalni kriminalitet

Završni rad

Društvene znanosti, informacijske i komunikacijske znanosti, informacijski sustavi i informatologija

Mentor: izv. prof. dr. sc. Gordana Dukić

Sumentor: dr. sc. Anita Papić

Osijek, 2016

Sažetak

Cilj ovog rada je opisati računalni kriminalitet unutar informacijskih sustava te objasniti na koji način računalni kriminalitet utječe na informacijske sustave. Informacijski su sustavi složeni i zahtijevaju mnogo ulaganja kako bi bili sigurni pa je potrebno znati kako se ovi sustavi izgrađuju i razvijaju. Računalni kriminalitet samo je jedna od stvari koje mogu ozbiljno narušiti rad informacijskih sustava i time ograničiti njihovo djelovanje i postizanje zadanih ciljeva. Kriminalitet koji se provodi uz pomoć računalne tehnologije predstavlja potencijalnu opasnost ne samo za pojedince, već za i velike organizacije koje rukovode velikim projektima od kojih su neki i od međunarodne važnosti. Zato je potrebno znati na koji se način izvršavaju napadi putem računalnih tehnologija te osvijestiti društvo i pojedince o opasnim posljedicama. Mnogo je vrsta računalnog kriminaliteta i stoga je potrebno na vrijeme uočiti nepravilnosti u radu računalnog sustava da bi se na vrijeme otkrili potencijalni počinitelji. Tome služe znanja digitalne forenzike, koja se bavi i računalnim kriminalitetom.

Ključne riječi: digitalna forenzika, informacijski sustavi, računalni kriminalitet, zlouporaba računalne tehnologije

Sadržaj

1. UVOD

Razvoj brojnih tehnologija, kako telekomunikacijskih tako i elektroničkih, ukazuje na njihov važan položaj u čovjekovu životu, iako to nije uvijek bilo očito. Naravno da su upravo te tehnologije odgovorne za veliki dio današnjeg načina života – privatnog i poslovnog – i teško je zamisliv bez velike količine informacijskih i telekomunikacijskih tehnologija izumljenih u proteklih 30-ak godina. Informacijski sustavi razvili su se ponajviše u tom razdoblju, pa danas imamo velik broj raznorodnih tehnologija koje nam omogućuju stvari poput pohrane podataka, olakšavanje učenja u sustavima obrazovanja i slično.

S obzirom na postojanost stope kriminaliteta u svijetu, ne začuđuje činjenica da se veliki dio tog kriminaliteta modernizirao te iskorištava računalnu tehnologiju kao sredstvo kojim se pojedinci, ali i čitave organizacije, služe iskorištavajući druge pojedince ili organizacije. S obzirom na globalnu raširenost računalne tehnologije, mogućnosti za napad su gotovo neograničene. Najčešće se koriste razni programi koji se ubacuju u sustave kako bi onemogućili njihov rad ili pak donijeli neku financijsku dobit. O kojem god načinu napada da je riječ, potrebno je imati na umu potencijalnu opasnost koju oni predstavljaju te posljedice koje su neizbježne ukoliko do napada dođe. U poglavlju o zlouporabi računalnih tehnologija pobliže su opisane pojedine vrste napada i njihov utjecaj na informacijske sustave.

Poznata je i činjenica da se napadi ponekad pretvaraju u čitave kibernetičke ratove velikih razmjera, a kojima na meti nisu samo velike i vrijedne organizacije, već i nedužni pojedinci koji se slučajno zateknu na krivome mjestu u krivo vrijeme. Kibernetički ratovi utječu na cijelo društvo oštećujući ga na mnogim područjima, a najviše po pitanju ekonomije što je pobliže opisano u trećem poglavlju.

Na samome kraju rada osvrnut ćemo se na digitalnu forenziku, koja pokušava stati na kraj računalnom kriminalitetu proučavajući digitalne dokaze ne bi li se počiniteljima ušlo u trag. Grane digitalne forenzike i njihove uloge u zaštiti od računalnog kriminaliteta pobliže su opisane u posljednjem poglavlju rada.

S obzirom da računalni kriminalitet vrlo često napada velike informacijske sustave, u prvome se poglavlju opisuju informacijski sustavi, njihovi dijelovi, kao i mogući pristupi u radu s njima i proučavanju njihovog rada.

2. INFORMACIJSKI SUSTAVI

Pojam sustava podrazumijeva međusobnu interakciju dvaju ili više elemenata s ciljem ostvarivanja neke jednostavne ili složene funkcije.[1] Sustavi mogu imati različite uloge i zadatke ovisno o potrebama određene organizacije ili pojedinaca koji se njima koriste. U ovome radu riječ je o informacijskom sustavu, a popis i opis njegovih sastavnih dijelova, čemu služi jedan takav sustav te koji su ciljevi njegovog korištenja, teme su koje su pobliže opisane u nastavku rada.

2.1. Informacijski sustavi kao pojam

Informacijski sustav je veoma složen pojam. To je sustav sastavljen od ljudi i računala koja procesiraju, obrađuju, a ujedno i interpretiraju neku informaciju. Taj se izraz također nekad koristi i u užem smislu, kako bi se opisao softver koji se koristi pri upravljanju bazama podataka ili pak u onom najužem smislu, kako bi se opisao obični računalni sustav. Informacijski sustav postoji i kao akademski pojam te se u tom smislu odnosi na akademsko polje proučavanja, odnosno proučavanje mreža hardvera i softvera koje ljudi i organizacije koriste kako bi prikupili, pročistili, obradili, stvorili i diseminirali informacije.

Cilj je svakog informacijskog sustava biti ispomoć i podrška pri raznim operacijama, upravljanju i donošenju odluka. U širem smislu, termin se ne koristi isključivo kako bi opisao informacijsko-komunikacijsku tehnologiju (IKT) koju neka pojedina organizacija koristi, već i način na koji ljudi vrše interakciju s tom tehnologijom u sklopu posla koji obavljaju. Kao takav, informacijski sustav povezuje podatkovne sustave s jedne strane te sustave obavljanja neke aktivnosti s druge. Moglo bi se reći i da je informacijski sustav zapravo jedan oblik komunikacijskog sustava ili pak da je to svojevrstan poluformalni jezik koji podržava ljudski princip donošenja odluka i poduzimanja nekih radnji.[2]

Važnost promatranja razvoja informacijskih sustava može se lako vidjeti iz činjenice da su brojni stari sustavi spašeni kako bi se sačuvao integritet podataka koji su u njima bili sačuvani,

[1] Usp. Uvodni pojmovi. // Poslovni informacijski sustavi / uredili Željko Panian i Katarina Ćurko. Zagreb: Elementi, 2010. Str. 1. URL: https://element.hr/artikli/file/1387 (2016-08-26).
[2] Isto, str. 2-3.

da se ne bi ništa u procesu prebacivanja izgubilo, ali i da bi se sačuvao kontekst situacije. Postoji pet dijelova koji moraju biti prisutni kako bi računalni informacijski sustav mogao funkcionirati:

- Hardver (eng. *Hardware*) – strojevi. Pri pojmu hardver misli se prvenstveno na CPU (eng. *central processing unit*) te sve komponente koje ga podržavaju. To su ulazni i izlazni uređaji, uređaji za pohranu te uređaji za komunikaciju.
- Softver (eng. *Software*) – računalni programi. Računalni programi zapravo su skup pravila koji hardver koristi kako bi uopće mogao funkcionirati. Oni upravljaju hardverskim komponentama i upućuju ga da radi ono što bi trebao i kako bi trebao.
- Podaci (eng. *Data*) – „činjenice" koje programi koriste kako bi proizveli korisnu informaciju.
- Upute – instrukcije kako rukovati sustavom i što mu zadati.
- Ljudski resursi – kako bi bilo koji sustav funkcionirao, treba ljude koji će ga pokretati i njime upravljati.[3]

2.2. Informacijski sustavi kao akademska disciplina

Znanstvena i akademska disciplina o informacijskim sustavima obuhvaća niz tema od kojih neke uključuju analizu tih sustava i njihov dizajn, umrežavanje računala, informacijsku sigurnost, upravljanje bazama podataka te sustave podrške pri donošenju odluka. Neke od disciplina posvećenih informacijskim sustavima su:[4]

- Informacijski menadžment bavi se praktičnim, ali i teorijskim problemima skupljanja i analiziranja informacija unutar područja u kojima se posao odvija.
- Komunikacije i mreže bave se telekomunikacijskim tehnologijama.
- Računalni informacijski sustavi (eng. CIS) polje je koje proučava računala i algoritamske procese, njihove principe, softverski i hardverski dizajn te njihov utjecaj na korisnike i društvo kojima je to izvorno i namijenjeno. S obzirom na velik i dugotrajan utjecaj koji

[3] Isto, str. 3-4.
[4] Rainer, R; Cegielski, C. Introduction to Information System: Support and Transforming Business. Hershey: John Wiley and Sons, 2012. Str. 14.

informacijski sustavi imaju u poslovnom i akademskom svijetu te svakodnevnom životu, nije nam teško ni pretpostaviti da će se ova grana još i više razvijati.

3. RAČUNALNI KRIMINALITET

Računalni kriminalitet (eng. *Cybercrime*) izraz je koji se u današnje vrijeme često spominje. Ova vrsta kriminaliteta može se opisati kao bilo koji kriminalitet koji uključuje neko računalo i mrežu. To je prilično oskudan opis, iako je u načelu točan. Bilo koji kriminalni čin koji je na neki način povezan s računalom, ili je barem izveden uz pomoć informacijsko-komunikacijske tehnologije, može se smatrati računalnim kriminalitetom, bez obzira na opseg samog čina. To može biti bilo koji čin u opsegu od običnog napada na nečije osobno računalo, pa sve do ogromnih hakiranja glavnih računala velikih svjetskih banaka. Računalo u takvom napadu može biti samo sredstvo napada, ali može biti i meta napada. Haldera i Jaishanakara računalni kriminalitet opisuju kao „kriminalno djelo počinjeno protiv pojedinca ili skupine pojedinaca s kriminalnom namjerom namjerne povrede reputacije pojedinca ili uzrokovanja fizičke ili mentalne boli na direktan ili indirektan način, koristeći telekomunikacijsku tehnologiju.“[5] Pojedini takvi kriminalni činovi mogu ugrožavati bilo što, počevši od financijskog stanja neke osobe ukoliko se radi o običnoj krađi ili pak može ugroziti i nacionalnu sigurnost. Pojedini činovi računalnog kriminaliteta neki su od najvećih problema današnjice, a najbolji primjeri su dječja pornografija, napadi na privatnost i krađe povjerljivih informacija. U računalni su kriminal uključeni bilo koji počinitelji, neovisno o njihovom statusu, položaju ili radnom mjestu, a radnje u koje su uključeni mogu biti špijunaža, krađa financijskih sredstava i ostali zločini počinjeni prema inozemstvu. Posebna vrsta računalnog kriminaliteta u koji su uključene i druge države te interesi istih zove se kibernetičko ratovanje (eng. *Cyberwarfare*). Taj pojam podrazumijeva računalni kriminal velikih razmjera i dugog trajanja, a uključuje sudionike s obje strane. Zlouporaba računala i kibernetičko ratovanje pobliže su prikazani u sljedećim poglavljima.

3.1. Zlouporaba računalnih tehnologija

[5] Halder, D.; Jaishankar, K. Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Pennsylvania: IGI Global, 2011., str 16.

Računalni virusi štetni su programi koji, jednom kada se pokrene njihovo izvođenje, napadaju računalo umetanjem svoje kopije u određene dijelove softvera (npr. računalne programe, podatke, baze podataka te odabrane sektore tvrdog diska), na taj ih način inficirajući. Jednostavnije rečeno, virus je „program ili kod koji se sam replicira u drugim datotekama s kojima dolazi u kontakt“[6] te se sastoji od dvaju dijelova: „samokopirajućeg koda koji omogućava razmnožavanje virusa“[7] i „korisne informacije koja može biti bezopasna i opasna.“[8]

Njihova je uloga da izvedu nekakav tip štetne radnje na računalu koje napadnu, kao što su krađa podataka, zauzimanje memorije ili vremena procesora, upropaštavanje podataka čineći ih neupotrebljivima i slično. Iako je većini virusa cilj zapravo onemogućiti ili znatno oslabiti korisniku korištenje njegovog računala, temeljno je obilježje virusa to da su to računalni programi koji se instaliraju na računalo bez pristanka vlasnika i ondje se umnažaju. Neki od najpoznatijih računalnih virusa su crv, trojanski konj, *backdoor*, *dialer* i s*pyware*.[9]

Ljudi koji se bave izradom i dizajnom računalnih virusa imaju veoma veliko i opsežno znanje o slabostima sustava kojeg napadaju. Često se među napadačima nalaze nezadovoljni zaposlenici koji žele svojem poslodavcu poslati nekakvu poruku ili ukazati na slabost informacijskog sustava tvrtke. Računalni virusi prvenstveno su pisani kako bi zaobišli što je moguće više zaštitnog softvera (kao što su npr. antivirusi) te za operacijske sustave koji se najviše koriste (npr. Microsoftovi Windowsi) zato što su korisnici tih sustava najranjiviji. Operacijski sustavi kao što je primjerice Linux su mnogo manje ranjivi zbog veoma drugačijih aplikacija koje njegovi korisnici koriste te zbog toga što je prosječni korisnik Linuxa i sličnih *open source* operacijskih sustava obično netko tko se bavi programiranjem ili sličnim aktivnostima te kao takav posjeduje znatno veće znanje od prosječnih korisnika Microsoftovih Windowsa, koji nisu na toj razini znanja o računalnim tehnologijama.

Denial of service ili takozvano „uskraćivanje usluge“ (u nastavku rada DoS), označava vrstu napada na informacijski ili računalni sustav, čiji je cilj jednostavno uskratiti normalno funkcioniranje tog servera ili računala onim korisnicima kojima je taj server namijenjen.[10] Sredstva kojima se postiže DoS napad, njegovi motivi te mete napada mogu biti različiti. Razlikujemo dvije vrste DoS napada: DoS (napadi koje izvodi pojedinac) te DdoS (napadi koje

[6] Računalni virusi. URL: http://svijet-informatike.weebly.com/ra269unalni-virusi.html (2016-06-29)
[7] Isto.
[8] Isto.
[9] Popić, A. *Najčešće vrste računalnih virusa*. 2012. URL: http://digitalnasigurnost.com/najcesce-vrste-racunalnih-virusa/ (2016-08-28).
[10] Napadi uskraćivanjem usluge. Naconalni CERT, str. 3. URL: http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2011-01-321.pdf (2016-08-27)

izvodi dvije ili više osoba te njihovih računala), a koji se mogu odvijati preko mreže (uspjeh napada ne ovisi o kvaliteti softvera), iskorištavanjem sigurnosne ranjivosti softvera (uspjeh napada ovisi o kvaliteti softvera) te fizičkim uništavanjem infrastrukture.[11]

DoS napadi jako su česti u poslovnom svijetu, a žrtve su uglavnom računalni sustavi i serveri koji pripadaju bankama, serveri zaduženi za obradu podataka kreditnih kartica, imenski serveri i sl. Također su veoma česti u *online gaming* svijetu. Mnogo konkurentskih tvrtki koje se bave izradom primjerice MMORPG-ova, znaju biti iza DoS napada na servere tvrtki proizvođača drugih igara kako bi konkurente prikazali u lošem svjetlu. To za cilj ima izazivanje ljutnje igrača i drugih korisnika, a sve zato da bi napustili proizvod napadnute tvrtke. Takvi napadi često koriste metodu preplavljivanja servera mnogim lažnim zahtjevima za komunikaciju (eng. *external communication request*) kako bi server bio manje-više beskoristan pravom korisniku zbog velike količine takvih lažnih korisnika na serveru. Napad također može funkcionirati tako da jednostavno opetovano ruši sustav ili briše i mijenja podatke potrebne za funkcioniranje tog servera. Simptomi prepoznavanja DoS napada su uglavnom veoma spor mrežni sustav, nemogućnost pristupa određenoj mrežnoj stranici ili nemogućnost pristupa bilo kojoj mrežnoj stranici, velika količina nepoželjne elektroničke pošte (tzv. *e-mail* bombe), prekidi veze s internetom i sl. Jedna od specifičnosti DoS napada je i to da napadač ne mora biti vješt pa čak ni posjedovati neka posebna tehnička znanja, već je bitno da ima velik broj računala s kojih može pokrenuti napad i time oštetiti čak i neke od najvećih računalnih mreža.[12]

Malware je pojam koji uključuje bilo koji softver koji se koristi s namjerom da omete normalan rad računala, izvuče osjetljive informacije ili na bilo koji način dobije pristup osobnom računalnom sustavu. Funkcija *malwarea* varira, ali s obzirom da taj pojam zapravo označava bilo koji program specifično stvoren s lošom namjerom, može biti korišten za špijunažu, sabotažu ili iznudu novca, te je u tom slučaju veoma težak za detektiranje. Velika većina *malwarea* zapravo funkcionira na način da preuzima oblik nekog programa ili sadržaja koji izgleda dobroćudno i zanimljivo, a nerijetko se dogodi da su uključeni u softver koji zapravo nije štetan sam po sebi, ali prilikom pokretanja *malware* se aktivira.

[11] Isto.
[12] Isto, str. 5.

Autori Bača i Ćosić[13] u svome radu navode koje su to osnovne osobine *malwarea* u današnje vrijeme:

- Modularnost – u isto vrijeme omogućava širenje programa internetom i onemogućava potencijalne programe za borbu protiv *malwarea*.
- Prodornost i razornost – preuzimanje potpune dominacije i inicijative nad zaraženim sustavom.
- Financije – često se žrtve financijski eksploatiraju te se programiranje *malwarea* smatra unosnim poslom.
- Uključenje na zahtjev– za potpuni učinak počinitelji unajmljuju tzv. zombi servere koji zatim izvršavaju DdoS napade.
- Homogenost – dominaciju nad tržištem ima Microsoft.
- Kontaminacija – započinje u istom trenutku u kojem *malware* inficira željeni sustav.
- Konkurentnost – u borbi protiv *malwarea* često se koriste drugi *malware*.
- Neprimjetnost – često se širi zavaravanjem.

Spyware je vrsta *malwarea* koji je, primjerice, ugrađen u programe koje službeno diseminiraju određene tvrtke. Na prvi pogled djeluje veoma atraktivno ili korisno, ali prilikom instalacije tog softvera, instalira se i *spyware* čija je svrha izvlačenje povjerljivih ili čak banalnih informacija s računala koje je inficirano. *Malware* softver može se odstraniti određenim metodama kao što su antivirusni softveri, čistači registra, i sl.[14]

Cyberstalking je korištenje informacijsko-računalne tehnologije u svrhu uhođenja, maltretiranja te praćenja neke osobe, grupe ili organizacije. Jako je često popraćen i uhođenjem u pravom životu te uključuje mnoge akcije čiji je krajnji cilj dominacija nad osobom ili grupom, prijetnje i generalno pružanje osjećaja nesigurnosti. Ova vrsta napada često se svodi na iznude, lažne optužbe, degradaciju, sramoćenje, vandalizam i slično. Baš kao i uhođenje u stvarnom životu, kriminalno je djelo. Sam *cyberstalking*, iako ilegalan i klasificiran kao kriminalno djelo,

[13] Usp. Bača, M.; Ćosić, J. *Prevencija računalnog kriminaliteta*. // Policija i sigurnost, vol. 22, br. 1 (2013.), str. 152-153. URL: http://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=155396 (2015-06-01).
[14] Usp. Hu, Q.; Dinev, T. *Is Spyware an Internet Nuisance or Public Menace?* // Communications of the ACM, vol. 48, br. 9 (2005.), New York, str. 61-65. URL: http://beta.orionsshoulders.com/Resources/articles/26_22317_%20().pdf (2015-03-06).

sastoji se od niza akcija koje same po sebi ne moraju biti ilegalne te se smatra da ga je obično počinila strane osoba koja poznaje žrtvu, a vjerojatno s njom ima nekakav odnos.[15] Profesor Lamber Royakkers definira *cyberstalking* kao „oblik mentalnog napada u kojemu napadač konstantno i bez pristanka žrtve, provaljuje u život žrtve s kojom nema (ili više nema) odnos.“[16] S obzirom da se *cyberstalking* svakako smatra kriminalnim djelom, postoje razne legislative koje se bave ovom problematikom, a koje uglavnom variraju od države do države. Ali takvi su napadi nova pojava te se zakoni pojedinih država još nisu uskladili u vezi kazni za slučaj da je počinitelj utvrđen. Ukoliko je čin usmjeren na slavnu osobu, zatvorska kazne je također jedna od mogućnih sankcija. Najčešće zakonske legislative su one koje brane osobe mlađe od 18 godina.

Phishing je jedan od najpopularnijih oblika računalnog kriminaliteta koji koristi računala kao sredstvo napada, a prvi je puta opisan 1987. godine.[17] Veoma je raširen i teško ga je otkriti onima koji nemaju dovoljno znanja o informacijskim tehnologijama što ga ujedno čini i vrlo popularnom vrstom napada. *Phishing* uključuje bilo koji pokušaj izvlačenja povjerljivih informacija iz osobe, kao što su podaci za prijavu na nekoj platformi, podaci o kreditnoj kartici, bankovni računi, itd.[18] Ono što *phishing* razlikuje od drugih pokušaja prevare je način na koji funkcionira – prikriva se kao stranica kojoj se može vjerovati te se zapravo svodi na to da osobe svoje podatke daju same, svojom voljom i pristankom. *Phishing* se najčešće provodi pomoću nepoželjne elektroničke pošte, ali i lančanim porukama ili u sustavima za trenutnu razmjenu poruka (eng. *Instant messaging*). Uglavnom vodi na stranicu koja nije službena, već ju je prevarant sam izradio te poslao poruku u kojoj je poveznica na njegovu stranicu. Ta je stranica spojena s bazom podataka koja pamti sve što je netko unio u nju, a onog trenutka kada žrtva stisne tipku za potvrdu unosa informacija, te se informacije šalju vlasniku stranice, najčešće u obliku izvješća spremljenih u jednostavnim formatima. Posljedice *phishinga* su teške, a ono što ga čini devastirajuće štetnim i čestim je činjenica da ga je jednostavno provoditi. Bilo tko bi ovog trenutka u tražilicu na Youtubeu mogao upisati pretragu „how to make a phishing site“[19] i dobio bi više stotina relevantnih rezultata o tome kako izraditi jednu takvu stranicu te kako namjestiti i poslati elektroničku koji izgleda dovoljno pouzdano da bi osoba, koja se ne razumije u informacijske tehnologije, bez straha kliknula na tu stranicu te samim time ugrozila svoje podatke. Mnoge legislative jednostavno nemaju dovoljnu zakonsku podlogu za djelovanje protiv

[15] Usp. Bača, M.; Ćosić, J., Nav. dj., str. 154-155.
[16] O'Reilly, C. American Diplomat Accused for Cyberstalking. URL: http://www.explorersweb.com/pdf/Cyberstalking.pdf (2016-08-31)

[17] Bača, M.; Ćosić, J., Nav. dj., str. 155.
[18] Isto.
[19] Youtube. URL: https://www.youtube.com/results?search_query=how+to+make+a+phishing+site (2015-05-30)

ove vrste zlouporabe iz razloga što ova tehnika koristi pretežno legalna sredstva kako bi počinila ilegalno djelo.[20] Ono po čemu se *phishing* stranica može efikasno razlikovati od legitimne je pečat autentičnosti, vidljiv po ikonici malog zlatnog lokota u lijevom dijelu adresnog polja internetskog pretraživača. Također, bliži pogled na sam URL stranice može isto mnogo reći, jer stranice vezane za, primjerice, Paypal, uvijek imaju svoj standardni URL te neku ekstenziju nakon toga, umjesto nekih izvrnutih verzija tog URL-a.[21]

Spam je također jedan od najčešćih oblika računalnog kriminaliteta, ali se on razlikuje od ostalih po tome što pretežno nikada sam po sebi ne uzrokuje štetu, već je u najgorem slučaju iznimno iritantan i disruptivan. *Spam* je varijanta DdoS napada koji se odnosi na veliku količinu elektroničke pošte istog sadržaja poslane u paketima na različite adrese s ciljem da onemoguće rad napadnutih računala.[22] *Spam* sam po sebi neće uzrokovati rušenje servera ili neki drugi oblik štete, ali bi mogao veoma jednostavno preplaviti server elektroničke pošte te ispuniti dozvoljeni kapacitet pretinca za primljenu poštu tako da primatelj više ne može dobiti korisne poruke (metoda prilično disruptivna u velikim tvrtkama koje komuniciraju preko velikih informacijskih sustava). Također može voditi na razne *phishing* mrežne stranice ili stranice na kojima će se posjetitelju računalo iznimno jednostavno inficirati raznim *malware* programima. *Spam* nerijetko ima i neke priloge uz pisani sadržaj, ali se pisani sadržaj veoma često (ako ne i uvijek) sastoji od nepovezanih i loše sastavljenih rečenica te, u najširem smislu, sadržaja koji uopće ne djeluje vjerodostojno. Posljednja je mogućnost zapravo rezultat toga da je generator *spama* zapravo *bot*, odnosno računalni program stvoren isključivo u svrhu obavljanja jedne zadaće koju nadgleda osoba koja ga je napravila. *Spammeri* adrese elektroničke pošte skupljaju iz raznih prostora za trenutnu komunikaciju, s mrežnih stranica, od virusa koji skupljaju adrese s računala koja inficiraju, pomoću raznih *newsletter* popisa i sl.[23]

Jedan od načina borbe protiv *spama* je metoda reputacije koja se bazira na listama. Te liste mogu biti bijele (liste servera od povjerenja), sive (privremeno odbijaju poruke elektroničke pošte pošiljatelja kojeg ne preoznaju) i crne (sadrži IP adrese već poznatih spamera).[24]

[20] Usp. Bača, M., Ćosić; J. Nav. dj., str. 155-156.
[21] Usp. PHISHING („pecanje podataka“ putem e-pošte). URL: http://www.sigurnostnainternetu.hr/index.php/vrste-prijevara/phishing (2015-06-01).
[22] Usp. Bača, M..; Ćosić, J. Nav. dj., str. 151-152.
[23] Usp. O spamu. URL: http://www.cert.hr/spam (2016-08-30).
[24] Usp. Bača, M.; Čosić, J.; Nav. dj., str. 151-152.

3.2. Kibernetičko ratovanje

Kibernetičko ratovanje (eng. *Cyberwarfare*) koncept je začet u službi vojske SAD-a te se zapravo odnosi na korištenje, manipulaciju i upravljanje informacijsko-komunikacijskom tehnologijom u svrhu dobivanja prednosti nad konkurencijom.[25] Ono može uključivati skupljanje taktičkih informacija, potvrda točnosti vlastitih informacija, širenje propagande ili dezinformacija u svrhu manipuliranja i sl.[26] Učinci koji se najčešće postižu su uglavnom demoralizacija protivnika, manipulacija, prikazivanje protivničke strane kao manje kvalitetne, pa je samim time kibernetičko ratovanje jako često poistovjećeno s psihološkim ratovanjem. „Cilj napada u kibernetičkom ratu može biti širenje štetnih virusa, izazivanje pada mrežnih sistema, uništavanje podataka, prikupljanje obavještajnih podataka i širenje dezinformacija, kao i ometanje zapovijedanja, nadzora, veza, prijenosa podataka, navigacije, logističke podrške i operacija.“[27] S obzirom da su informacijsko komunikacijske tehnologije u današnje vrijeme ključan dio gotovo svake ljudske djelatnosti, postoji poveći rizik da ih se napadne i uvuče u kibernetičko ratovanje. Civilne tehnologije mogu također biti meta kibernetičkih napada, koji mogu biti inicirani kroz civilna računala ili mrežne stranice. S obzirom na to da je kontrolirati kompletnu civilnu infrastrukturu gotovo nemoguće, podloga za poticanje kibernetičkog ratovanja je gotovo čitavo vrijeme postavljena. Naposljetku, toliko velik stupanj integracije informacijsko-komunikacijske tehnologije predstavlja veliku odgovornost prema određenom pojedincu ili skupini jer je tehnologija mnogo i dostupne su velikom krugu ljudi. S obzirom na to koliko je napada izvedeno s računalnih sustava ljudi koji za to zapravo nisu bili krivi, već su iskorišteni, kibernetičko ratovanje je veoma teško za regulirati ili mu odrediti uzročnika.

3.3. Posljedice računalnog kriminala

[25] Usp. Popić, A. Cyberkriminal načela i djelovanje. 2012. URL: http://digitalnasigurnost.com/cyber-kriminal-nacela-djelovanje/ (2016-08-27).
[26] Usp. Vacca, John R. Computer and Information Security: Handbook. Waltham: Morgan Kaufmann Publishers, 2012. Str. 976. URL: https://books.google.hr/books?id=zb916YOr16wC&printsec=frontcover&hl=hr&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false (2015-06-02).

[27] Popić, A. Nav. dj.

Računalni kriminalitet odgovoran je za milijarde dolara štete godišnje. Procjenjuje se da svake godine uspori veliki dio proizvodnje i globalnog ekonomskog razvoja samim time što postoji. Gotovo svaka tvrtka na svijetu ima problem s računalnim kriminalitetom, izravno ili neizravno. Godišnja procjena američke tvrtke McAfee, vodeće tvrtke u svijetu na području istrebljivanja računalnog kriminaliteta, izvještava o visini štete koju je svjetskome gospodarstvu prouzrokovao računalni kriminalitet 2015. godini – vrtoglavih 112 bilijuna američkih dolara.[28] Zbog samog postojanja računalnog kriminaliteta, baš kao i postojanja materijalnog kriminaliteta (onog u stvarnom životu), tvrtke i pojedinci prisiljeni su podizati digitalne zidove, svakoga i sve preispitivati, nikom ne vjerovati te koristiti veliku količinu zaštitnog softvera, kao i zaposliti velik broj stručnjaka sve u svrhu obrane od računalnog kriminaliteta od strane pojedinaca, neimenovane grupe ili pak konkurenata. Kazna predviđena za počinitelje računalnog kriminaliteta varira ovisno o veličini počinjenog zločina, ali može biti od obične novčane kazne pa sve do osam godina zatvora.[29]

Računalni kriminal neuhvatljiva je pojava te borba protiv njega nije jednostavna. Prvenstveno zato što se on odvija virtualnim putem te za sobom ne ostavlja neki materijalni, opipljiv dokaz. Međutim, računalo jako lako može postati dokazni materijal. Čuvanje starih datoteka ili pak elektroničkih poruka uvelike može pomoći istražiteljima. A čak i ako pojedino računalo nije bilo ono koje je korišteno za samu kriminalnu aktivnost, ono i dalje može sadržavati vrijedne informacije istražiteljima čuvajući *log* datoteke, koje bilježe određene aktivnosti, promet te komunikaciju između računala i udaljenog servera. U većini država su davatelji internet usluga dužni čuvati te *log* datoteke svojih korisnika, a nova direktiva iz Europske Unije također propisuje da bi sav promet elektroničke pošte trebalo čuvati minimalno 12 mjeseci.[30]

S obzirom na današnji razvoj tehnologije i interneta, hakersko je znanje dostupnije nego ikad. Prije dvadesetak godina hakeri su morali imati pristup snažnim serverima, posjedovati veliko znanje kako bi uopće mogli upravljati tim serverom, mnogo novca itd. Danas su hakeri odlučili podijeliti to znanje s mlađim naraštajima, što znači da su te informacije dostupne i ostalima, pa tako i policiji i istražiteljima. Nažalost, neke usluge zamišljene da pomognu ljudima

[28] Usp. McAfee Labs 2016 Threats Predictions, str. 14. URL: http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf (2016-08-28).
[29] Usp. Kazneni zakon Republike Hrvatske (Narodne novine, br. 125/11, 144/12, 56/15, 61/15), glava dvadeset peta. URL: http://www.zakon.hr/z/98/Kazneni-zakon (2016-08-29).
[30] Usp. Zakon o elektroničkim medijima Republike Hrvatske (Narodne novine, br. 73/08, 90/11, 133/12, 80/13, 71/14), čl. 109., st. 3. URL: http://www.zakon.hr/z/182/Zakon-o-elektroni%C4%8Dkim-komunikacijama (2015-05-30).

kibernetički kriminalci besramno iskorištavaju. Najreprezentativniji primjer za to je novi način na koji funkcionira elektronička pošta. *Software-as-a-service* (SaaS) je softverski model licenciranja po kojem pristup softveru funkcionira na pretplatničkoj bazi. Upravo zbog toga se ovaj model još zove i *on demand software*. Uporabom SaaS-a, računalni bi kriminalci mogli platiti korištenje mrežnog servera da mogu započeti *spam* kampanju. S obzirom da ta mrežna domena nije u njihovom vlasništvu, prijave nisu korisne kao što bi bile korisne da se radi o nečijoj privatnoj adresi. Anonimnost koju ovaj sustav pruža je nešto što kibernetički kriminalci uvelike koriste kao prednost te besramno iskorištavaju uslugu prvotno nastalu u svrhu pomaganja ljudima.[31]

Što se tiče Republike Hrvatske, računalni kriminalitet je potpuno nova pojava u zakonodavstvu. Iako hrvatsko zakonodavstvo razlikuje računalne pojmove i poznaje terminologiju srodnu toj temi te konstantno uvodi nova kaznena djela vezana uz računala, za sada je taj zakon iznimno teško provesti u djelo zbog ograničenih sredstava te iznimno teške dokazivosti s obzirom da se zločin nije dogodio fizički. Kazne koje su propisane hrvatskim zakonima u skladu su sa svakim drugim kriminalnim činom, odnosno u skladu s kaznenim zakonom Republike Hrvatske, ukoliko se počinitelju djelo uspije dokazati.[32]

3.4. Digitalna forenzika

Digitalna forenzika posebna je grana forenzičke znanosti koja obuhvaća oporavak i istragu materijala pronađenog u digitalnim uređajima, te je često usko vezana uz računalni kriminal.[33] Izvorno se sam termin digitalna forenzika koristio kao sinonim za računalnu forenziku, ili drugim riječima, smatralo ih se istoznačnima.[34] Međutim, pojam se raširio i danas se smatra da digitalna forenzika obuhvaća istragu svih uređaja koji su sposobni pohranjivati

[31] Usp. Umawing, J. Thousands of Hacked Sites Lead to Offer of Famous Spy Software. URL: https://blog.malwarebytes.com/cybercrime/2015/09/thousands-of-hacked-sites-lead-to-offer-of-famous-spy-software/ (2016-08-26).
[32] Usp. Vojković, G. Štambuk-Sunjić, M. Konvencija o kibernetičkom kriminalu i kaznenom zakonu Republike Hrvatske. Split: Pravni Fakultet, 2006., str. 7. URL: http://www.pravst.unist.hr/dokumenti/zbornik/200681/zb200601_123-136.pdf (2016-08-28).
[33] Usp. Reith, M. Carr; C., Gunsch, G. *An examination of digital forensic models*. // International Journal of Digital Evidence, vol. 1, br. 3 (2002.), str. 1-2. URL: http://digital4nzics.com/Student%20Library/An%20Examination%20of%20Digital%20Forensic%20Models.pdf (2015-06-01).

[34] Usp. Yasinsac, A.; Erbacher, R.; Marks, D. *Computer forensics education*. // IEEE Security & Privacy. URL: http://www.pmsommer.com/CSDS_Paper.pdf (2015-06-02).

digitalne podatke. Ova se vrsta forenzike može koristiti za detekciju konkretnog dokaza nekog zločina, kao trag koji vodi do određenog sumnjivca, za potvrđivanje alibija, određivanje nečije namjere ili pak vjerodostojnosti dokumenata. Početkom razvoja digitalne foreznike smatra se početak 80-ih godina 20. stoljeća, kada su se pojavila prva računalna kriminalna djela u pravom smislu. Prijelazom u 90-e godine počinju se formirati prave agencije i grupe u svrhu borbe protiv računalnog kriminala.

Digitalni dokaz[35] objekt je koji se pred zakonskim tijelom može jednako upotrijebiti te spada pod iste pravne točke kao i bilo koji drugi oblik dokaznog materijala. Digitalni dokaz je obično proizvod rada digitalne forenzike. Međutim, zakoni koji se bave digitalnim dokazom obično imaju dvije stvari na koje moraju paziti: autentičnost i integritet. Integritet je važan jer dokazuje da sam čin dolaženja do tog dokaza i uzimanje istog nisu taj dokaz ni na koji način izmijenili. Autentičnost se odnosi na sposobnost potvrđivanja vjerodostojnosti informacije. U slučaju da je dokazni materijal fotografija, ona mora biti autentična kako bi sačuvala integritet, a to znači da mora biti neizmijenjeni prikaz onoga što je fotografirano. S obzirom da digitalni dokaz ima mogućnost izmjene i namještanja, jako je teško uvjeriti pravnu stranu da je digitalni dokaz zapravo relevantan i da ga se može koristiti u redovnom sudskom postupku. No, stručnjaci su iznijeli argumente da mnogi digitalni dokazi sadržavaju određene digitalne potpise, vodene žigove i druge oblike zaštite, kako bi se uvjerili da nitko ne narušava integritet digitalnog dokaza.[36]

Digitalna forenzika obuhvaća nekoliko grana, a te se grane odnose na vrstu uređaja i princip na koji određeni sustav funkcionira.

Računalna forenzika je grana digitalne forenzike koja se odnosi na računala i objekte za digitalnu pohranu podataka kao što su kućna osobna računala, ugrađeni računalni sustavi (sustavi s rudimentarnim napajanjem i unutarnjom memorijom), te uređaje sa statičnom memorijom (USB stickovi i sl.). Njezin je cilj istražiti digitalne podatke na forenzički način s ciljem identifikacije, očuvanja, spašavanja podataka te kasnijeg prezentiranja tih činjenica do kojih se došlo istraživanjem. Računalna forenzika se koristi u velikom broju slučajeva te je u današnje vrijeme široko prihvaćena kao veoma pouzdana, posebice u Europi i SAD-u. Ova se grana

[35] Usp. Reith, M.; Carr, C.; Gunsch, G.; Nav. dj., str. 2.
[36] Isto, str. 2-4.

forenzike može se baviti datotekama zapisa (kao što je povijest pregledavanja interneta), ali i konkretnim podacima na tvrdom disku.[37]

Forenzika mobilnih uređaja je grana digitalne forenzike koja se odnosi na povrat i istraživanje podataka na mobilnim uređajima pod forenzičkim uvjetima. Kada spominjemo forenziku mobilnih uređaja vjerojatno većina odmah pomisli na mobilne telefone. Iako je ova grana forenzike dosta povezana s mobilnim telefonima, oni nisu jedini uređaji koji spadaju u ovu granu. Može se odnositi na bilo koje druge digitalne uređaje koji imaju unutarnju memoriju i sposobnost telekomunikacije, a to uključuje razne GPS-ove te čak i tablete. Ova je grana digitalne forenzike među najmlađima, nastala je tek ranih 2000-ih godina. Za razliku od računala, mobilni uređaji imaju ugrađen komunikacijski sustav te samim time i unutarnji mehanizam pohrane podataka (kod računala je to komad hardvera – tvrdi disk, koji se može zamijeniti bez posljedica za računalo). Kod forenzike mobilnih uređaja najvažniji su podaci o pozivima i porukama te sam povrat obrisanih podataka ne igra toliku ulogu. Također je važno spomenuti da GPS uređaji pokazuju lokaciju te su zbog toga beskonačno važni u privođenju kriminalaca.[38]

Mrežna forenzika grana je digitalne forenzike koja se bavi nadziranjem i analizom računalnog mrežnog prometa u svrhu skupljanja informacija, legalnog dokaza ili detekciju uljeza.[39] Ono što ovu granu digitalne forenzike čini posebnom u odnosu na prethodne dvije je to što se mrežna forenzika uglavnom nosi s nestabilnim i dinamičnim informacijama koje su podložne konstantnim promjenama. Iz toga proizlazi da istraga mrežne forenzike mora biti proaktivna i pratiti sve promjene koje se zbivaju u području njezina proučavanja. Ona uključuje praćenje i promatranje mreže za bilo kakvim neuobičajenim prometom te pokušava otkriti uljeze koji pristupaju mreži. Mrežna forenzika uključuje lokalnu mrežu (LAN) i internet (WAN). Promet na mreži se obično pohranjuje u paketima koji se kasnije mogu filtrirati i posebno analizirati. S obzirom na ranije spomenutu dinamičnu prirodu informacija na mreži te manjak *log* datoteka, ova se grana digitalne forenzike često smatra najizazovnijom. Postoje dva principa unutar mrežne forenzike, a to su[40]:

---

[37] Usp. Guidelines on Digital Forensic Procedures for OLAF Staff. URL: https://ec.europa.eu/anti-fraud/sites/antifraud/files/guidelines_en.pdf (2016-08-26).
[38] Usp. Vacca, John R.; Nav. dj., str. 285-298, 323-341.
[39] Palmer, G. A Road Map for Digital Forensic Research. // First Digital Forensic Research Workshop, Utica, New York, str. 27-28. URL: https://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf (2015-05-30).
[40] Garfinkel, S. Network Forensics: Tapping the Internet, 2002. URL: http://archive.oreilly.com/pub/a/network/2002/04/26/nettap.html (2015-06-02).

- *Catch-it-as-you-can* – princip po kojem se svi paketi koji prolaze kroz određenu točku prometa bilježe u memoriji, a u isto vrijeme odvija se analiza tih podataka. Ovaj pristup zahtijeva veliku količinu prostora u memoriji.

- *Stop, look and listen* – princip po kojem je svaki paket analiziran u najosnovnijem obliku u memoriji, a samo je određena najvažnija informacija pohranjena u memoriji za kasniju analizu. Ovaj pristup zahtijeva brži procesor kako bi mogao pratiti frekvenciju dolazećeg prometa.

Forenzika baza podataka grana je digitalne forenzike koja se bavi proučavanjem baza podataka i njihovih pripadajućih metapodataka. Ova je grana digitalne forenzike dosta slična računalnoj forenzici, jer uključuje normalni forenzički proces te ga može primijeniti na tablice u bazi podataka, kao i uključene metapodatke. Ova se grana uglavnom odnosi na praćenje izmjena u bazi te interakcija pojedinih korisnika s bazom podataka. Najčešća primjena forenzike baza podataka je kod detekcije pronevjere novca unutar neke tvrtke, jer može otkriti kako su se podaci u tablici određene baze mijenjali, kao i koji zadaci su bazi podataka uopće zadani. Mnogi softverski alati mogu se koristiti kako bi se upravljalo podacima i analiziralo ih, a mnogi od tih alata omogućuju i pohranu podataka o bazi u zasebnu datoteku. Međutim, mnogi alati za upravljanje bazama podataka nisu pouzdani niti dovoljno precizni da bi se koristili kao sredstvo forenzičkog istraživanja te također postoji samo mali broj radova na tu temu.[41]

4. ZAKLJUČAK

Informacijski su sustavi izum koji se, ukoliko je dobro upotrijebljen, može iskoristiti na razne dobre načine u svrhu unaprjeđivanja znanja, učenja na daljinu ili olakšavanja samog procesa učenja i pamćenja. Sami informacijski sustavi zamišljeni su kako bi ih ljudi vidjeli u pozitivnom svjetlu te kako bi ih koristili u svrhu olakšavanja nekih procesa. Ipak, nemaju svi ljudi dobre namjere i neki od njih su pojedinci koji su posvetili život iskorištavanju tih sustava za svoje osobne ciljeve, a počesto i na nelegalne načine.

[41] Usp. Olivier, M. S.; *On Metadata Context in Database Forensics* // Digital Investigation. The Internationa Journal of Digital Forensics & Incident Response, vol. 5, br. 3-4 (2009.), str. 115-213. URL: http://ccf.cs.uml.edu/forensicspapers/On%20metadata%20context%20in%20Database%20Forensics.pdf (2016-08-28).

Računalni je kriminal pojava koja, baš kao i stvarni kriminal, jako utječe na svakodnevni život i poslovanje. Rasprave o magnitudi štete koju računalni kriminalitet prouzrokuje te metodama borbe protiv njega mogu se voditi iz dana u dan, ali same rasprave ne donose rezultate. Najbolje što se može poduzeti je edukacija korisnika. Velike bi organizacije trebale uložiti mnogo sredstava u obranu od računalnog kriminaliteta, ali i na edukaciju svojih zaposlenika te uposliti više stručnjaka, koji bi prijetnje prepoznali i na vrijeme otklonili ukoliko je to moguće.

Mnogi bi stručnjaci rekli da je boriti se protiv računalnog kriminaliteta nalik borbi s vjetrenjačama. Protivnik je zapravo imaginaran i ne postoji, ali svi zapisi koji dokumentiraju godišnju štetu ipak kažu drugačije. Treba što više ulagati u znanost računalne forenzike, jer se ona za sada pokazala kao prilično učinkovita metoda borbe protiv računalnog kriminaliteta.

Možda će suzbijanje računalnog kriminaliteta uskoro postati mnogo lakše, navedene metode će možda postati mnogo pouzdanije, a otkrivanje počinitelja brže i učinkovitije. Žrtvom kriminala može postati bilo koja osoba bez obzira na društveni status, financijsku situaciju, vjeroispovijest ili koji god drugi društveni, odgojni ili biološki čimbenik, a bez metoda brzog otkrivanja i prevencije, šteta bi mogla imati puno veće razmjere nego što bismo ikada mogli zamisliti.

5. POPIS IZVORA I LITERATURE

1. Bača, M.; Ćosić, J. *Prevencija računalnog kriminaliteta*. // Policija i sigurnost, vol. 22, br. 1 (2013.). URL: http://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=155396 (2015-06-01)
2. Garfinkel, S. Network Forensics: Tapping the Internet, 2002. URL: http://archive.oreilly.com/pub/a/network/2002/04/26/nettap.html (2015-06-02)
3. Guidelines on Digital Forensic Procedures for OLAF Staff. URL: https://ec.europa.eu/anti-fraud/sites/antifraud/files/guidelines_en.pdf (2016-08-26)
4. Halder, D.; Jaishankar, K. Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Pennsylvania: IGI Global, 2011.
5. Hu, Q.; Dinev, T. *Is Spyware an Internet Nuisance or Public Menace?* // Communications of the ACM, vol. 48, br. 9 (2005.), New York, str. 61-65. URL: http://beta.orionsshoulders.com/Resources/articles/26_22317_%20().pdf (2015-06-03)
6. Kazneni zakon Republike Hrvatske (Narodne novine, br. 125/11, 144/12, 56/15, 61/15), glava dvadeset peta. URL: http://www.zakon.hr/z/98/Kazneni-zakon (2016-08-29)
7. McAfee Labs 2016 Threats Predictions. URL: http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf (2016-09-09)
8. Napadi uskraćivanjem usluge. Naconalni CERT. URL: http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2011-01-321.pdf (2016-08-27)
9. O spamu. URL: http://www.cert.hr/spam (2016-08-30)
10. Olivier, M. S.; *On Metadata Context in Database Forensics* // Digital Investigation. The Internationa Journal of Digital Forensics & Incident Response, vol. 5, br. 3-4 (2009.). URL: http://ccf.cs.uml.edu/forensicspapers/On%20metadata%20context%20in%20Database%20Forensics.pdf (2016-08-28).
11. O'Reilly, C. American Diplomat Accused for Cyberstalking. URL: http://www.explorersweb.com/pdf/Cyberstalking.pdf (2016-08-31)
12. Palmer, G. A Road Map for Digital Forensic Research. // First Digital Forensic Research Workshop, Utica, New York. URL: https://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf (2015-05-30).
13. PHISHING („pecanje podataka“ putem e-pošte). URL: http://www.sigurnostnainternetu.hr/index.php/vrste-prijevara/phishing (2015-06-01)

14. Popić, A. Cyberkriminal načela i djelovanje. 2012. URL: http://digitalnasigurnost.com/cyber-kriminal-nacela-djelovanje/ (2016-08-27)
15. Popić, A. *Najčešće vrste računalnih virusa*. 2012. URL: http://digitalnasigurnost.com/najcesce-vrste-racunalnih-virusa/ (2016-08-28)
16. Računalni virusi. URL: http://svijet-informatike.weebly.com/ra269unalni-virusi.html (2016-06-29)
17. Rainer, R; Cegielski, C. Introduction to Information System: Support and Transforming Business. Hershey: John Wiley and Sons, 2012.
18. Reith, M. Carr; C., Gunsch, G. *An examination of digital forensic models*. // International Journal of Digital Evidence, vol. 1, br. 3 (2002.). URL: http://digital4nzics.com/Student%20Library/An%20Examination%20of%20Digital%20Forensic%20Models.pdf (2015-06-01)
19. Umawing, J. Thousands of Hacked Sites Lead to Offer of Famous Spy Software. URL: https://blog.malwarebytes.com/cybercrime/2015/09/thousands-of-hacked-sites-lead-to-offer-of-famous-spy-software/ (2016-08-27)
20. Uvodni pojmovi. // Poslovni informacijski sustavi / uredili Željko Panian i Katarina Ćurko. Zagreb: Elementi, 2010. URL: https://element.hr/artikli/file/1387 (2016-08-26)
21. Vacca, John R. Computer and Information Security: Handbook. Waltham: Morgan Kaufmann Publishers, 2012. URL: https://books.google.hr/books?id=zb916YOr16wC&printsec=frontcover&hl=hr&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false (2015-06-02)
22. Vojković, G. Štambuk-Sunjić, M. Konvencija o kibernetičkom kriminalu i kaznenom zakonu Republike Hrvatske. Split: Pravni Fakultet, 2006.URL: http://www.pravst.unist.hr/dokumenti/zbornik/200681/zb200601_123-136.pdf (2016-08-28)
23. Yasinsac, A.; Erbacher, R.; Marks, D. *Computer forensics education*. // IEEE Security & Privacy. URL: http://www.pmsommer.com/CSDS_Paper.pdf (2015-06-02)
24. Youtube. URL: https://www.youtube.com/results?search_query=how+to+make+a+phishing+site (2015-05-30)
25. Zakon o elektroničkim medijima Republike Hrvatske (Narodne novine, br. 73/08, 90/11, 133/12, 80/13, 71/14), čl. 109., st. 3. URL: http://www.zakon.hr/z/182/Zakon-o-elektroni%C4%8Dkim-komunikacijama (2015-05-30)