Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

CYBER KRIMINAL KAO MODERNA SIGURNOSNA PRIJETNJA U BOSNI I HERCEGOVINI

CYBERCRIME AS A MODERN SECURITY THREAT IN BOSNIA AND HERZEGOVINA

Pregledni naučni rad

Amina SMAILHODŽIĆ[88]

SAŽETAK

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Razvojem informacijske tehnologije cyber kriminal egzistira kao netrpeljiv vid kršenja zakona i zloupotreba. Posjeduje specifične karakteristike koje ga izdvajaju od drugih kriminalnih delikata i pri tome predstavlja oblik kriminala koji nema granice i kao takvog ga je teško otkriti. Posljedice nastale cyber kriminalom su velike kako za pojedince, tako i za državu. Cyber kriminal je poprimio globalno obilježje i širokim razmjerama uništava poslovne sisteme stvarajući enormne finansijske troškove. Cyber kriminal ocrtava kriminalnu djelatnost počinjenu upotrebom računara, mreža i računarskih sistema. Veliki broj incidenata uzrokovanih cyber kriminalom odnosi se na bankarske prevare i na zloupotrebu identiteta na društvenim mrežama.

Ciljevi rada (naučni i/ili društveni): Tema ovog rada se obrađuje sa naučnog i društvenog aspekta. Trebaju se objasniti činjenice koje se odnose na problem cyber kriminala u Bosni i Hercegovini. Naučni cilj istraživanja treba da iskaže odgovarajući nivo naučnog saznanja o cyber kriminalu u Bosni i Hercegovini. Društveni cilj istraživanja odnosi se na informisanje o cyber kriminalu kao modernoj sigurnosnoj prijetnji u Bosni i Hercegovini, odnosno da se građani Bosne i Hercegovine, a i šire upoznaju sa karakteristikama i prisutnostima cyber kriminala u Bosni i Hercegovini.

Metodologija/Dizajn: U ovom istraživanju se analizira cyber kriminal kao moderna sigurnosna prijetnja u Bosni i Hercegovini. Paradigma kojoj istraživanje pripada jeste pozitivizam. Primjenom analize sadržaja dokumenata izvršen je pregled dostupne literature o cyber kriminalu. U istraživanju je zastupljena i hipotetičko-deduktivna metoda, induktivna, metoda analize, sinteze, metoda apstrakcije, metoda deskripcije i statistička metoda.

Ograničenja istraživanja/rada: Cyber kriminal je kompleksan i prekriva različite kriminalne djelatnosti u koje su uključeni napadi na računare, kompjuterske sisteme i podatke. Istraživanje će se usredočiti na prostor Bosne i Hercegovine.

Rezultati/Nalazi: Rezultati istraživanja trebaju opravdati naučni i društveni značaj istraživanja. Rezultatima naučnog istraživanja iskazana je ozbiljnost posljedica koje cyber kriminal proizvodi. Na internetu se svakodnevno ugrožava sigurnost putem društvenih mreža, web sajtova, kao i elektronske trgovine.

[88] Amina Smailhodžić, MA, Fakultet za kriminalistiku, kriminologiju i sigurnosne studije Univerziteta u Sarajevu, magistar sigurnosnih studija, aminasmailhodzic@fkn.unsa.ba

Generalni zaključak: Cyber kriminal označava negativnu društvenu pojavu savremenog doba. Istraživanje cyber kriminala u Bosni i Hercegovini treba se analizirati u kontinuitetu. Cyber kriminal nije nacionalno, geografsko i vremensko ograničen. Zbog dinamičnog razvoja informacijskih tehnologija neophodno je stalno posmatranje promjena koje se odigravaju da bi se uspješno suprotstavilo izazovima cyber kriminala. Prevencija se treba ogledati na preduzimanju djelatnosti da bi se otklonili propusti koji su naklonjeni zloupotrebi računarskih podataka i sistema. Prevencija podrazumijeva i preduzimanje aktivnosti i pripremanje plana osoblja koje radi na sistemu tehnologije kako bi se spriječio neovlašten pristup sistemu. Uspješno suprotstavljanje cyber kriminalu je moguće ukoliko se uključi cijela međunarodna zajednica.
Opravdanost istraživanja/rada: Rezultati istraživanja cyber kriminala kao moderne sigurnosne prijetnje u Bosni i Hercegovini trebaju opravdati naučni i društveni značaj. Naučna i društvena opravdanost ogleda se u povećanju naučnih saznanja iz oblasti cyber kriminala. Istraživanje je naučno opravdano, jer nas upućuje u problem, a ukoliko dobro poznajemo problem na putu smo da ga riješimo ili bar smanjimo posljedice uzrokovane cyber kriminalom. Naučna opravdanost ide u pravcu i heurističkog i verifikatornog rezultata. Pružanje doprinosa koji je heuristički kroz proučavanje cyber kriminala u Bosni i Hercegovini od velike je važnosti za cjelokupnu državu. Kada je u pitanju verifikacijski rezultat, u pravcu verifikacije se ide jer se istraživanje svodi na potvrdu teze da u Bosni i Hercegovini postoji cyber kriminal. Tendencija razvoja cyber kriminala predstavlja veliki problem koji kod većine građana stvara osjećaj nesigurnosti i zabrinutosti.

Ključne riječi
cyber kriminal, sigurnost, društvene mreže, elektronska trgovina

ABSTRACT
Reason for writing and research problem (s): By developing information technology, cybercrime exists as an intolerable aspect of violation of law and abuse. It has specific characteristics that distinguish it from other criminal delinquencies and is a form of crime that has no boundaries and as such is difficult to detect. The consequences of cybercrime are great for individuals as well as for the state. Cybercrime has taken a global dimension and broadly destroys business systems by creating enormous financial costs. Cybercrime illustrates the criminal activity committed by using computers, networks and computer systems. A large number of cybercrime incidents are related to bank fraud and the abuse of identity on social networks.
Aims of the paper (scientific and/or social): The theme of this paper is being studied from a scientific and social point of view. The facts related to the cybercrime problem in Bosnia and Herzegovina need to be explained. The scientific aim of the research should show the appropriate level of scientific knowledge about cybercrime in Bosnia and Herzegovina. The Social Objective of Research relates to information on cybercrime as a modern security threat in Bosnia and Herzegovina, respectively that citizens of Bosnia and Herzegovina, and beyond, are introduced to the characteristics and the presence of cybercrime in Bosnia and Herzegovina.
Methodology/Design: This research analyzes cybercrime as a modern security threat in Bosnia and Herzegovina. The paradigm to which research belongs is positivism. By using the method of analyzing the content of documents, a review of accessible cybercrime literature was performed. The hypothetical-deductive method, the inductive, the analysis method, the synthesis, the abstraction method, the descriptive method and the statistical method are represented in the research.

Research/Paper limitation: Cybercrime is complex and covers various criminal activities that involve attacks on computers, computer systems, and data. The research will be centered on the territory of Bosnia and Herzegovina.
Results/Findings: Research results should justify the scientific and social significance of research. The results of scientific research have shown the seriousness of the cybercrime consequences. The Internet is endangered on a daily basis through social networks, web sites, and e-commerce.
General Conclusion: Cybercrime means a negative social phenomenon of the contemporary age. Cybercrime research in Bosnia and Herzegovina needs to be analyzed in continuity. Cybercrime is not national, geographic, and time constrained. Due to the dynamic development of information technology, it is imperative to constantly observe the changes that are taking place in order to successfully counter the challenges of cybercrime. Prevention should be reflected in the take-up of activities in order to overcome the failures of abusing computer data and systems. Prevention also implies undertaking activities and preparing staff plans for the technology system to prevent unauthorized access to the system. Successful cybercrime is possible if the entire international community is involved.
Research/Paper Validity: Cybercrime findings as modern security threats in Bosnia and Herzegovina should justify scientific and social significance. Scientific and social justification is reflected in the increase of scientific knowledge in the field of cybercrime. The research is scientifically justified because it points to the problem, and if we know the problem in the way we are to solve it or at least reduce the consequences of cybercrime. Scientific justification goes in the direction of heuristic and verifiable results. Providing a heuristic contribution through cybercrime research in Bosnia and Herzegovina is of great importance to the entire country. When it comes to the verification result, the verification is going because the research is lowered to confirm the thesis that cybercrime exists in Bosnia and Herzegovina. The tendency to develop cybercrime is a major problem that creates a sense of insecurity and concern for most citizens.

Keywords
cyber crime, security, social networks, electronic commerce

1. UVOD

Najpotpunija definicija cyber kriminala data je u dokumentu „Kriminal vezan za kompjutersku mrežu“ (Report of Committee II, Workshop on crimes related to the computer-network) sa Desetog Kongresa Ujedinjenih nacija, posvećenog prevenciji kriminala i tretmanu počinilaca koji je održan u Beču od 10 do 17. aprila 2000. godine (Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, Wienna, 10-17 April 2000. godine). Radna grupa eksperata u sadržaju izvještaja pod cyber kriminalom podrazumjeva „kriminal koji se odnosi na bilo koji oblik kriminala koji se može izvršavati sa kompjuterskim sistemom i mrežama, u kompjuterskim sistemima i mrežama ili protiv kompjuterskih sistema i mreža (Porobić i Bajraktarević, 2012, str. 15)“.

Na Desetom kongresu UN o sprečavanju zločina i postupanju sa prestupnicima, koji je održan 2000. godine zaključeno je da se cyber kriminal pojavljuje u užem i širem smislu. U užem smislu cyber kriminal se može posmatrati kao protivpravno ponašanje koje je potaknuto na elektronsko obavljanje sigurnosti računarskih sistema, kao i podataka koji se obrađuju, dok cyber kriminal u širem smislu se posmatra kao protivpravno ponašanje koje je povezano za mrežu i računarski sistem, a obuhvata i protivpravno davanje i dijeljenje informacija preko mreže i računarskih sistema. Cyber kriminal predstavlja oblik kriminala gdje se kao sredstvo izvršenja kriminalnog djela javljaju računarske mreže. Ovaj vid kriminalnog ponašanja većinom vrše pojedinci, dok nije rijetkost da su i same kriminalne organizacije uključene u ovaj vid kriminala, koji za posljedicu ima neovlašten pristup informacijama sa stepenom povjerljivosti, ali i njihovo objavljivanje. Cyber kriminalom mijenjaju se računarski podaci. Cyber kriminal sadrži široki spektar protivpravnih djelatnosti kako neovlašteni pristup računarskoj mreži tako i maloljetničkoj pornografiji, zloupotrebi platnih kartica, ali isto tako i krivičnim djelima koja ugrožavaju sigurnost internet korisnika.

U današnjem svijetu sve više se koristi pojam „cyber“, a da u stvari i ne znamo šta on znači. Pojam „cyber“ prvo se pojavio u vojnoj terminologiji, u smislu predviđanja budućih oblika ratovanja. „Cyberwar“ predstavlja ratovanje znanjem, odnosno informacijama. Radi se o ratu visoke tehnologije, koji se odnosi na prikupljanje povjerljivih informacija (Gligorević, 2014, str. 164). Cyber rat predstavlja događaj koji se dešava u cyber prostoru i ima elemente konvencionalnog rata. Pojedini teoretičari smatraju da je operacija Orchard, koju je Izrael iskoristio aktivacijom komponenti ugrađenih u informacioni sistem kako sirijski radari ne bi bili u mogućnosti da uoče izraelske zrakoplove na sirijskoj teritoriji predstavljala cyber rat. Zagovornici povećanih proračunskih izdvajanja za osposobljavanje američke vojske za vođenje operacija u cyber-prostoru nerijetko pokušavaju uvjeriti javnost da je cyber-rat već otpočeo i pritom se koriste metaforom „cyber Pearl Harbor”. No, dok o tome tko je, kada, gdje i kako izveo stvarni napad na Pearl Harbor nema nikakve dvojbe, kao ni o trenutnim i dugoročnim posljedicama koje je taj napad imao na odvijanje i ishod 2. svjetskog rata, o tome tko je i kada izveo „cyber Pearl Harbor”, kao i o tome je li se to uopće dogodilo, suglasnosti nema. Uvjerljivost te metafore, koja je u opticaj stavljena 1990-ih, bitno je umanjena terorističkim napadima na New York i Pentagon 11. rujna 2001. Te napade svi su vidjeli i broj njihovih žrtava mjeri se tisućama. Vidljivih razornih posljedica i ljudskih žrtava cyber-napada nema i stoga je javnost teško uvjeriti da je cyber-rat već otpočeo (Kovačević, 2013, str. 92). Riječ kibernetika, engl. Cybernetics nema isto značenje kao riječ cyber. Cyber u riječniku stranih riječi označava osnovnu materiju koja je povezana za svijet imaginarne stvarnosti nastalu preko kompjutera. Kibernetika se može definisati kao “sustavno proučavanje komunikacije i upravljanja u organizacijama svih vrsta“ (Deutsch, 1966, str. 76).

Veoma težak put predstavlja ulazak u trag kriminalnim počiniteljima koji koriste specifičan način, kao i sredstvo za izvršenje krivičnog djela cyber kriminala pomoću računara. Na tom putu je zaista potrebno uložiti mnogo zalaganja. Kriminalni počinitelji su osobe koje su veoma dobro upoznate sa savremenom tehnologijom. Kriminalni počinitelji cyber

kriminala sa predumišljajem nastoje drugima nanijeti štetu i ostvariti sebi ili drugima imovinsku ili neimovinsku korist. Lica koja se bave ovim nelegalnim radnjama su, uglavnom, studenti, informatički stručnjaci, bivši inspektori kriminalističkih službi i brojni drugi koji dobro poznaju savremenu tehnologiju (Gligorević, 2014, str. 166). Cyber kriminal predstavlja visokotehnološki kriminal i počinioci ovog vida kriminala su veoma obrazovana lica. Kriminalna lica koriste svoja stručna znanja kako bi ostvarili svoje motive. Najčešće se kao motiv ističe novac, odnosno sticanje imovinske koristi. Pojam cyber kriminal se može definisati kao oblik kriminalnog ponašanja za čije izvršenje se koristi računarska oprema. Lica koja obavljaju takve kriminalne radnje su cyber kriminalci. Uglavnom su to muškarci između 19 i 30 godina starosti. Postoji veoma mali broj žena koje se bave ovim nedozvoljenim radnjama, ali se one uglavnom pojavljuju kao saučesnici (Mesarović, 2006). Cyber kriminal čini lice koje nezakonito uđe u tuđu bazu informacija i obavlja unošenje, izmjenu, sakrivanje, kopiranje, upotrebu, objavu, onemogućavanje upotrebe programa korisnika i unošenje nekog podatka ili virusa. Pojam „haker" ima više značenja: novajlija, početnik u igri golfa koji raskopava teren; kopač rovova ili taksista; kreativni programer ili onaj koji neovlašćeno ulazi u tuđi kompjuterski sistem. Dodatne karakteristike hakera jesu: dominiraju pripadnici muškog pola; ekstremno su bistri, skloni istraživačkom i logičkom razmišljanju i uvijek takmičarski raspoloženi; sa svakom uspješnom realizacijom na tastaturi oni vide sebe kao afirmisane autoritete nad računarom i nad bilo kim ko je povezan sa njim, što im daje osjećaj snage i kontrole; teže da se informatičkim proizvodima bave površno; imaju malo respekta prema onima koji ne znaju ništa o njihovoj omiljenoj temi – kompjuteru (Krstić, 2009).

I najmanji propust cyber kriminalcu pruža pogodak za lakšu zloupotrebu povjerljivih informacija." Sajber kriminal kao savremena prijetnja doživljava svoju ekspanziju, a kao vrste ove prijetnje u literaturi se uglavnom navode: državno-sponzorisani sajber napadi; ideološki i politički ekstremizam; organizovani sajber kriminal i sajber kriminal na nivou pojedinaca (Cornish, Hughes, Livingstone, 2009). Tradicionalne kriminalne grupe i organizacije modernizuju se korišćenjem ICT, a *cyber prostor* postaje sredina u kojoj deluju i koja im istovremeno služi kao skrovište (Porobić, i Bajraktarević, 2012, str. 13). Kibernetski prostor određujuće je obilježje suvremenog života i ključno područje svjetskog gospodarstva (Vuković, 2012). U listopadu 2006. Združeni stožer oružanih snaga SAD-a definirao je kibernetski prostor kao „područje koje karakterizira upotreba elektroničkog i elektromagnetskog dijapazona za pohranjivanje, modificiranje i razmjenjivanje podataka putem mrežnih sustava i povezanih fizičkih infrastruktura" (Wynne, 2006).

Kod sajber kriminala cilj napada su servisi, funkcije i sadržaji koji se nalaze na kompjuterskoj mreži. Reč je o krađi podataka ili identiteta, uništavanju ili oštećenju delova ili celih mreža i kompjuterskih sistema. Cilj počinilaca je mreža u koju se ubacuju virusi, obaraju sajtovi, upadaju hakeri i vrši „odbijanje usluga". Kada je reč o alatu, sredstvima koje moderni kriminalci koriste, važno je naglasiti da oni ne „prljaju" ruke koristeći mrežu u činjenju dela. Nekada ova upotreba mreže predstavlja potpuno novi alat, dok se u drugim prilikama toliko usavršava da ju je teško i prepoznati (Radnović, Ilić, i Radović, 2012, str. 131).

Kako bi se prikrile nedozvoljene radnje kompjuterska mreža predstavlja idealno oruđe za izvođenje napada poput trgovine ljudima, trgovine drogom, dječije pornografije, pedofilije i sl. Većinom počinitelji u obavljanju krivičnog djela cyber kriminala vrše DOS napade, odnosno napade na kompjuterski servis kako bi korisnicima bilo onemogućeno korištenje i ubacuju štetni softver. Trojanski konj, računarski crv, špijunski softver, oglašivački softver, keylogger, računarski virus, lažni antivirusni programi predstavljaju samo neke od štetnih programa kako bi se preuzela kontrola nad korisnikovim računarom.

Trojanski konj sposoban je obavljati razne radnje kao što su krađa brojeva sa platne kartice, zloupotreba lozinki i ostale informacije koje se zatim šalju drugom licu. Trojanski konj većinom se koristi da bi se preuzela datoteka ili nekoliko njih, a odmah nakon preuzimanja se instalira zlonamjerni softver na zaraženom računaru. Napadač može samostalno izgraditi ili kupiti od drugog napadača Trojanskog konja. Naročito su opasni bankarski Trojanski konji, koji imaju za cilj udar na bankarske sisteme i berze dionica kojima je Internet oslonac. Glavna funkcija bankarskih Trojanskih konja je zloupotreba korisnikovih ličnih podataka, preuzimanje kontrole nad računarom u potpunosti ili djelimično i krađa brojeva platnih kartica i PIN-ova. Trojanski konji su specifični jer se dijele u nekoliko porodica i različiti su po oruđu koje koriste za izvođenje napada i djelovanju zaraženog korisnika. Računarski crv označava zlonamjernu vrstu programa koja se rasprostire mrežom i obično se rasprostiru putem elektronske pošte. Špijunski softver predstavlja zlonamjerni program koji prikuplja podatke o korisnikovom korištenju računara i na osnovu toga preuzima kontrolu nad računarom. Oglašivački softver predstavlja softver koji korisniku pokazuje oglase i u vremenu kada uopšte nije povezan sa internetom.

Keylogger predstavlja zlonamjerni špijunski program čija je osnovna svrha praćenje unosa korisnika putem tastature. Programi praćenja se odlažu na poseban računar, koji napadač koristi. Osim toga, keylogger na klik miša korisnika može da uzima snimak sa ekrana i na osnovu toga se vidi program koji korisnik koristi i šta pretražuje na internetu. Keylogger se pojavljuje kao aparat koji se ugrađuje u pojedine dijelove računara i kao oruđe u formi programskih paketa. Računarski virus predstavlja program kojim se zaraze programi i datoteke, dok lažni antivirusni programi imaju namjeru da navedu korisnika na kupovinu simulacijom pretraživanja korisnikovog računara. Kao mogući ciljevi cyber kriminala mogu se navesti napad na hardver, napad na softver, napad na programe kako bi se uništila, prisvojila ili nanijela šteta kompjuterskom sistemu i kako bi se neovlašteno koristila informaciona sredstva. Veoma su česte prevare putem e:mail adresa, plaćanje preko interneta, prevare platnim karticama, lažni identitet. Osnovni oblici falsifikovanja i zloupotreba platnih kartica jesu:

1. Zloupotreba ukradenih ili izgubljenih kartica;
2. Zloupotreba neuručenih platnih kartica;
3. Neovlašćena upotreba tuđe platne kartice;
4. Pravljenje i korišćenje lažnih platnih kartica;
5. Pribavljanje podataka za pravljenje lažne platne kartice (Radnović, Ilić, i Radović, 2012. str. 137).

Veliki broj djela cyber kriminala posjeduje međunarodnu dimenziju. Počinitelji cyber kriminala ne moraju biti prisutni na određenom mjestu gdje je prisutna žrtva, a u skladu sa time istrage cyber kriminala zahtijevaju međunarodnu saradnju. „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“ (Hamidović, Hamidović, i Zajmović, 2016, str. 561).

2. CYBER SIGURNOST

Cyber sigurnost je upala u žarište zainteresovanosti usljed raširenog korištenja interneta. Cyber kriminal orijentisan je protiv sigurnosti informacionog sistema kako bi kriminalno lice pribavilo sebi korist a istovremeno nanijelo štetu drugome. Cyber sigurnost treba se odnositi na zaštitu od zloupotrebe informacionog sistema. Neke od mjera tehničke zaštite predstavljaju lozinke, identifikatori korisnika i slično. Kako bi korisnici stekli povjerenje u korištenje informacione tehnologije potrebno je da informacioni sistemi pruže sigurnost korištenja informacione tehnologije. Mnoge osobe strahuju da njihovi podaci ne budu predmet zloupotrebe. Neprikladno primjenjivanje mjera sigurnosti predstavlja razlog za ugrožavanje sigurnosti. Neizostavno je da organizacija koja ima ozbiljan pristup za informacijsku sigurnost da:

1. posjeduje razvijeni plan za otkrivanje, izvještaj i procjenu nastalu incidentima,
2. odgovori nastalim incidentima obuhvatajući određene mjere zaštite kako bi se spriječili i smanjili negativni uticaji,
3. nauči iz nastalih incidenata i u budućnosti unaprijedi sistem manipulisanja incidenata.

S obzirom na to da je internet poslednjih godina doživeo ekspanziju omogućujući brzu komunikaciju među korisnicima na udaljenim destinacijama, stvorila se potreba da se znatno ozbiljnije pristupi problemu bezbednosti na internetu (Milašinović, Mijalković i Amidžić, 201. str. 31). Za suprotstavljanje cyber kriminalu neophodno je usvajanje adekvatne zakonske regulative u području materijalnog i procesnog prava i adekvatno primjenjivanje tih normi. Kompjuterska mreža služi kao dokaz u postupku dokazivanja cyber kriminala. U suprotstavljanju cyber kriminalu postoji nekoliko mehanizama da bi se objasnile i opisale faze kojima se djeluje na suzbijanje cyber kriminala.

U Bosni i Hercegovini ne postoje odgovarajući mehanizmi za suprotstavljanje cyber kriminalu. Nedostatak novca za ulaganje u sigurnosne sisteme predstavlja ogroman problem kada je u pitanju odgovarajuća i uspješna borba protiv cyber kriminala u Bosni i Hercegovini. Suprotstavljanje cyber kriminalu predstavlja neizostavan dio Strategije Bosne i Hercegovine za prevenciju i borbu protiv terorizma od 2010.-2013. godine, gdje

je zabilježeno da nema pouzdanih pokazatelja u kom obimu i u kolikoj mjeri je ova moderna sigurnosna prijetnja zastupljena u Bosni i Hercegovini. Na nivou entiteta u Bosni i Hercegovini zakonski su regulisana djela protiv sistema mreže elektronske obrade podataka, dok je na državnom nivou nedozvoljeno korištenje autorskih prava usko vezano za kompjuterski kriminal. U krivičnom zakonu Federacije Bosne i Hercegovine nalaze se krivična djela protiv sustava elektronske obrade podataka.

Član 393. (Oštećenje računalnih podataka i programa)

(1) Ko ošteti, izmijeni, izbriše, uništi ili na drugi način učini neupotrebljivim ili nepristupačnim tuđe računalne podatke ili računalne programe, kaznit će se novčanom kaznom ili kaznom zatvora do jedne godine.

(2) Ko unatoč zaštitnim mjerama neovlašćeno pristupi računalnim podacima ili programima ili neovlašćeno presreće njihov prijenos, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(3) Kaznom iz stava 2. ovog člana kaznit će se ko onemogući ili oteža rad ili korišćenje računalnog sustava, računalnih podataka ili programa ili računalnu komunikaciju.

(4) Ako je krivično djelo iz st. od 1. do 3. ovog člana učinjeno u odnosu na računalni sustav, podatak ili program organa vlasti, javne službe, javne ustanove ili privrednog društva od posebnog javnog interesa, ili je prouzrokovana znatna šteta, kaznit će se kaznom zatvora od tri mjeseca do pet godina.

(5) Ko neovlašćeno izrađuje, nabavlja, prodaje, posjeduje ili čini drugom dostupne posebne naprave, sredstva, računalne programe ili računalne podatke stvorene ili prilagođene radi učinjenja krivičnog djela iz st. od 1. do 3. ovog člana, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(6) Posebne naprave, sredstva, računalni programi ili podaci stvoreni, korišćeni ili prilagođeni radi učinjenja krivičnih djela, kojima je krivično djelo iz st. od 1. do 3. ovog člana učinjeno, oduzet će se.

Član 394. (Računalno krivotvorenje)

(1) Ko neovlašćeno izradi, unese, izmijeni, izbriše ili učini neupotrebljivim računalne podatke ili programe koji imaju vrijednost za pravne odnose, s ciljem da se upotrijebe kao pravi ili sam upotrijebi takve podatke ili programe, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(2) Ako je krivično djelo iz stava 1. ovog člana učinjeno u odnosu na računalne podatke ili programe organa javne službe, javne ustanove ili privrednog društva od posebnog

javnog interesa, ili je prouzrokovana znatna šteta, kaznit će se kaznom zatvora od tri mjeseca do pet godina.

(3) Ko neovlašćeno izrađuje, nabavlja, prodaje, posjeduje ili čini drugom pristupačnim posebne naprave, sredstva, računalne programe ili računalne podatke stvorene ili prilagođene radi učinjenja krivičnog djela iz st. 1. i 2. ovog člana, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(4) Posebne naprave, sredstva, računalni programi ili podaci stvoreni, korišćeni ili prilagođeni radi učinjenja krivičnih djela kojima je učinjeno krivično djelo iz stava 1. ili 2. ovog člana, oduzet će se.

Član 395. (Računalna prijevara)

(1) Ko neovlašćeno unese, ošteti, izmijeni ili prikrije računalni podatak ili program ili na drugi način utiče na ishod elektronske obrade podataka s ciljem da sebi ili drugom pribavi protupravnu imovinsku korist i time drugom prouzrokuje imovinsku štetu, kaznit će se kaznom zatvora od šest mjeseci do pet godina.

(2) Ako je krivičnim djelom iz stava 1. ovog člana pribavljena imovinska korist koja prelazi 10.000 KM, učinitelj će se kazniti kaznom zatvora od dvije do deset godina.

(3) Ako je krivičnim djelom iz stava 1. ovog člana pribavljena imovinska korist koja prelazi 50.000 KM, učinitelj će se kazniti kaznom zatvora od dvije do dvanaest godina.

(4) Ko krivično djelo iz stava 1. ovog člana učini samo s ciljem da drugog ošteti, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

Član 396. (Ometanje rada sustava i mreže elektronske obrade podataka)

Ko neovlašćenim pristupom u sustav ili mrežu elektronske obrade podataka izazove zastoj ili poremeti rad tog sustava ili mreže, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

Član 397. (Neovlašćeni pristup zaštićenom sustavu i mreži elektronske obrade podataka)

(1) Ko se neovlašćeno uključi u sustav ili mrežu elektronske obrade podataka kršenjem mjera zaštite, kaznit će se novčanom kaznom ili kaznom zatvora do jedne godine.

(2) Ko upotrijebi podatak dobijen na način iz stava 1. ovog člana, kaznit će se kaznom zatvora do tri godine.

(3) Ako su krivičnim djelom iz stava 2. ovog člana prouzrokovane drugom teške posljedice, učinitelj će se kazniti kaznom zatvora od šest mjeseci do pet godina.

Član 398. (Računalna sabotaža)

Ko unese, izmijeni, izbriše ili prikrije računalni podatak ili program ili se na drugi način umiješa u računalni sustav, ili uništi ili ošteti naprave za elektronsku obradu podataka s ciljem da onemogući ili znatno omete postupak elektronske obrade podataka značajnim organima vlasti, javnim službama, javnim ustanovama, trgovačkim društvima ili drugim pravnim osobama od posebnog javnog interesa, pa time prouzrokuje štetu u iznosu većem od 500.00 KM, kaznit će se kaznom zatvora od jedne do osam godina.[89]

U Krivičnom zakonu Republike Srpske, u glavi HHIVa (Krivična djela protiv bezbjednosti računarskih podataka) implementirana je Međunarodna konvencija o suzbijanju kompjuterskog kriminaliteta, koja je razrađena kroz sedam članova: • oštećenje računarskih podataka i programa, • računarska sabotaža, • izrada i unošenje računarskih virusa, • računarska prevara, • neovlašćeni pristup zaštićenom računaru, računarskoj mreži, telekomunikacionoj mreži i elektronskoj obradi podataka, • sprečavanje i ograničavanje pristupa javnoj računarskoj mreži, • neovlašćeno korišćenje računara ili računarske mreže (Vasić, Šarić i Jovanić, 2012, str. 183).

U krivičnom zakonu Republike Srpske, glava XXXIV, navedena su krivična djela protiv bezbjednosti kompjuterskih podataka:

Član 407. (Oštećenje kompjuterskih podataka i programa)

(1) Ko neovlašteno izbriše, izmijeni, ošteti, prikrije ili na drugi način učini neupotrebljivim kompjuterski podatak ili program, kazniće se novčanom kaznom ili kaznom zatvora 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 kaznom zatvora od šest mjeseci do tri godine.

(3) Ako je djelom iz stava 1. ovog člana prouzrokovana šteta u iznosu koji prelazi 50.000 KM, učinilac će se kazniti kaznom zatvora od jedne do pet godina.

---

[89] *Krivični zakon Federacije Bosne i Hercegovine*. Glava XXXII. Krivična djela protiv sustava elektronske obrade podataka, Službene novine Federacije BiH, br. 36/2003, 21/2004-ispr., 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 i 75/2017

(4) Uređaji i sredstva kojima je izvršeno krivično djelo iz st. 1. i 2. ovog člana oduzeće se.

Član 408. (Kompjuterska sabotaža)

Ko unese, uništi, izbriše, izmijeni, ošteti, prikrije ili na drugi način učini neupotrebljivim kompjuterski podatak ili program ili uništi ili ošteti kompjuter 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 republičke organe, javne službe, ustanove, privredna društva ili druge subjekte, kazniće se kaznom zatvora od šest mjeseci do pet godina.

Član 409. (Izrada i unošenje kompjuterskih virusa)

(1) Ko napravi računarski virus u namjeri njegovog unošenja u tuđi kompjuter ili kompjutersku ili telekomunikacionu mrežu, kazniće se novčanom kaznom ili kaznom zatvora do šest mjeseci.

(2) Ko unese računarski virus u tuđi kompjuter ili kompjutersku mrežu i time prouzrokuje štetu, kazniće se novčanom kaznom ili kaznom zatvora do dvije godine.

(3) Uređaj i sredstva kojima je izvršeno krivično djelo iz st. 1. i 2. ovog člana oduzeće se.

Član 410. (Kompjuterska 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 kaznom zatvora 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 kaznom zatvora 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 kaznom zatvora od dvije do deset godina.

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

Član 411. (Neovlašteni pristup zaštićenom kompjuteru, kompjuterskoj mreži, telekomunikacionoj mreži i elektronskoj obradi podataka)

(1) Ko se, kršeći mjere zaštite, neovlašteno uključi u kompjuter ili kompjutersku mrežu ili neovlašteno pristupi elektronskoj obradi podataka, kazniće se novčanom kaznom ili kaznom zatvora do šest mjeseci.

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

(4) Kaznom iz stava 1. ovog člana kazniće se i ko izradi, pribavi, proda ili da na korištenje uputstvo ili sredstvo koje je namijenjeno za ulaženje u kompjuterski sistem.

Član 412. (Sprečavanje i ograničavanje pristupa javnoj kompjuterskoj mreži)

(1) Ko neovlašteno sprečava ili ometa pristup javnoj kompjuterskoj mreži, kazniće se novčanom kaznom ili kaznom zatvora do jedne godine.

(2) Ako djelo iz stava 1. ovog člana učini službeno lice u vršenju službe, kazniće se novčanom kaznom ili kaznom zatvora do tri godine.

Član 413. (Neovlašteno korištenje kompjutera ili kompjuterske mreže)

(1) Ko neovlašteno koristi kompjuterske usluge ili kompjutersku mrežu u namjeri da sebi ili drugom pribavi protivpravnu imovinsku korist, kazniće se novčanom kaznom ili kaznom zatvora do šest mjeseci.

(2) Gonjenje za djelo iz stava 1. ovog člana preduzima se po prijedlogu.[90]

U krivičnom zakonu Brčko distrikta Bosne i Hercegovine, glava XXXII, nalaze se krivična djela protiv sistema elektronske obrade podataka. Prema članu 387. krivičnog zakona Brčko distrikta Bosne i Hercegovine (***Oštećenje računarskih podataka i programa)***:

(1) Ko ošteti, izmijeni, izbriše, uništi ili na drugi način učini neupotrebljivim ili nepristupačnim tuđe računarske podatke ili računarske programe, kaznit će se novčanom kaznom ili kaznom zatvora do jedne godine.

[90] *Krivični zakon Republike Srpske*. Glava XXXIV. Krivična djela protiv bezbjednosti kompjuterskih podataka. Službeni glasnik Republike Srpske broj: 64/17 i 104/2018-odluka US

(2) Ko unatoč zaštitnim mjerama neovlašteno pristupi računarskim podacima ili programima ili neovlašteno presreće njihov prenos, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine. Kaznom iz stava 2. ovoga člana kaznit će se ko onemogući ili oteža rad ili korištenje računarskog sistema, računarskih podataka ili programa ili računarsku komunikaciju.

(3) Ako je krivično djelo iz stavova od 1. do 3. ovoga člana počinjeno u odnosu na računarski sistem, podatak ili program tijela vlasti, javne službe, javne ustanove ili trgovačkog društva od posebnog javnog interesa, ili je prouzrokovana znatna šteta, kaznit će se kaznom zatvora od tri mjeseca do pet godina.

(4) Ko neovlašteno izrađuje, nabavlja, prodaje, posjeduje ili čini drugome dostupne posebne sprave, sredstva, računarske programe ili računarske podatke stvorene ili prilagođene radi počinjenja krivičnog djela iz stavova od 1. do 3. ovoga člana, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(5) Posebne sprave, sredstva, računarski programi ili podaci stvoreni, korišteni ili prilagođeni radi počinjenja krivičnih djela, kojima je krivično djelo iz stavova od 1. do 3. ovoga člana počinjeno, oduzet će se.

Član 388. (Računarsko krivotvorenje)

(1) Ko neovlašteno izradi, unese, izmijeni, izbriše ili učini neupotrebljivim računarske podatke ili programe koji imaju vrijednost za pravna lica, s ciljem da se upotrijebe kao pravi ili sam upotrijebi takve podatke ili programe, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(2) Ako je krivično djelo iz stava 1. ovoga člana počinjeno u odnosu na računarske podatke ili programe tijela, javne službe, javne ustanove ili trgovačkog društva od posebnog javnog interesa, ili je prouzrokovana znatna šteta, kaznit će se kaznom zatvora od tri mjeseca do pet godina.

(3) Ko neovlašteno izrađuje, nabavlja, prodaje, posjeduje ili čini drugome pristupačnim posebne sprave, sredstva, računarske programe ili računarske podatke stvorene ili prilagođene radi počinjenja krivičnog djela iz stavova 1. i 2. ovoga člana, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(4) Posebne sprave, sredstva, računarski programi ili podaci stvoreni, korišteni ili prilagođeni radi počinjenja krivičnih djela, kojima je počinjeno krivično djelo iz stavova 1. ili 2. ovoga člana, oduzet će se.

Član 389. (Računarska prevara)

(1) Ko neovlašteno unese, ošteti, izmijeni ili prikrije računarski podatak ili program ili na drugi način utiče na ishod elektroničke obrade podataka s ciljem da sebi ili drugome pribavi protivpravnu imovinsku korist i time drugome prouzrokuje imovinsku štetu, kaznit će se kaznom zatvora od šest mjeseci do pet godina.

(2) Ako je krivičnim djelom iz stava 1. ovoga člana pribavljena imovinska korist koja prelazi 10.000 KM, počinilac će se kazniti kaznom zatvora od dvije do deset godina.

(3) Ako je krivičnim djelom iz stava 1. ovoga člana pribavljena imovinska korist koja prelazi 50.000 KM, počinilac će se kazniti kaznom zatvora od dvije do dvanaest godina.

(4) Ko krivično djelo iz stava 1. ovoga člana počini samo s ciljem da drugoga ošteti, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

Član 390. (Ometanje rada sistema i mreže elektroničke obrade podataka)

Ko neovlaštenim pristupom u sistem ili mrežu elektroničke obrade podataka izazove zastoj ili poremeti rad toga sistema ili mreže, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

Član 391. (Neovlašteni pristup zaštićenome sistemu i mreži elektroničke obrade podataka)

(1) Ko se neovlašteno uključi u sistem ili mrežu elektroničke obrade podataka kršenjem mjera zaštite, kaznit će se novčanom kaznom ili kaznom zatvora do jedne godine.

(2) Ko upotrijebi podatak dobijen na način iz stava 1. ovoga člana, kaznit će se kaznom zatvora do tri godine.

(3) Ako su krivičnim djelom iz stava 2. ovoga člana prouzrokovane drugome teške posljedice, počinilac će se kazniti kaznom zatvora od šest mjeseci do pet godina.

Član 392. (Računarska sabotaža)

Ko unese, izmijeni, izbriše ili prikrije računarski podatak ili program ili se na drugi način umiješa u računarski sistem, ili uništi ili ošteti sprave za elektronsku obradu podataka s ciljem da onemogući ili znatno omete postupak elektronske obrade podataka značajnih organima vlasti, javnim službama, javnim ustanovama, trgovačkim društvima ili drugim pravnim licima od posebnog javnog interesa, kaznit će se kaznom zatvora od jedne do osam godina.[91]

Uspješno suprotstavljanje cyber kriminalu zahtijeva znatno ozbiljniji pristup i zaštitu korisnika interneta, između ostalog i stalno praćenje, upotrebom moderne sigurnosne opreme za suprotstavljanje cyber kriminala i proširivanje znanja o cyber kriminalu. Za uspješno reagovanje na cyber kriminal potrebno je preduzeti mjere prevencije da bi se suzbio ovaj vid kriminala kao i povećala svijest o opasnosti koji cyber kriminal sa sobom pruža. Za uspješnu borbu neophodna je također međunarodna saradnja državnih organa koji imaju zadatak otkrivanja i progona izvršilaca krivičnog djela cyber kriminala. Krivično pravo predstavlja neizostavni element u borbi kriminala. Pravovremeno usvajanje zakonskih propisa da bi se obezbijedio mehanizam za obračun sa cyber kriminalom, kao i uspješna upotreba takvih propisa trebaju predstavljati zakonsku podlogu izgradnje kriminalne politike kada su u pitanju represivne mjere. Moguće je otkriti računar na koji program šalje prikupljene podatke obavljanjem dinamičke analize upotrebom programa za analizu ponašanja nedobronamjernih programa i simulacijom nedobronamjernih programa u kontrolisanom okruženju. Podaci dobiveni na takav način mogu se iskoristiti za automatsko otkrivanje računara za odlaganje podataka koje je prikupio program za praćenje unosa znakova s tastature. Upotreba ove tehnike vrlo je uspješna (Porobić, i Bajraktarević, 2012, str. 112).

Prvi potpuni dokument koji se odnosi na probleme cyber kriminala jeste Konvencija o kibernetičkom kriminalu Vijeća Europe, koja je potpisana 23. novembra 2001. godine, a stupila na snagu 1. jula 2004. godine. Konvencija o kibernetičkom kriminalu Vijeća Europe ima formu međunarodnog ugovora. Konvenciju je potpisalo tridesetosam zemalja, dok je Bosna i Hercegovina istu ratifikovala 25. marta 2006. godine. Odredbe Konvencije nisu direktno primjenjive. „Brza zaštita pohranjenih kompjuterskih podataka (član 16.) je mjera koju članice konvencije trebaju propisati kako bi omogućile svojim organima da izdaju naredbe ili na neki drugi način nametnu brzu (hitnu) zaštitu elektronskih podataka koji su pohranjeni u kompjuterskom sistemu“ (Selimović, 2015, str. 74).

Vijeće Europe je donijelo 28. januara 2003. godine Dodatni protokol uz Konvenciju o kibernetičkom kriminalu o kriminalizaciji akata rasizma i ksenofobije koje su počinjene

[91] *Krivični zakon Brčko distrikta Bosne i Hercegovine*. Glava XXXII. Službeni glasnik Brčko distrikta BiH br. 33/2013 - prečišćen tekst, 47/2014 - ispravka 26/2016, 13/2017 i 50/2018

pomoću pojedinih kompjuterskih sistema. Četiri skupine krivičnih djela Konvencija o kibernetičkom kriminalu Vijeća Europe je predvidjela, i to:

- krivična djela protiv povjerljivosti, integriteta i disponibilnosti kompjuterskih podataka i sistema (nedozvoljen pristup, nezakonito presretanje, povreda integriteta podataka, povreda integriteta sistema i zloupotreba uređaja),
- kompjuterska krivična djela (kompjutersko krivotvorenje, kompjuterska prevara, krivična djela u vezi sa sadržajem, krivična djela koja se odnose na dječiju pornografiju),
- krivična djela u vezi napada na intelektualnu svojinu i odnosna prava (krivična djela koja se odnose na kršenje autorskih i njima sličnih prava).

Analizom sadržaja odredbi državnih i nedržavnih zakona se može zaključiti da se obaveza preuzeta potpisom i ratifikacijom Konvencije u pogledu krivično materijalnog prava uglavnom ispoštovala i da su krivična djela predviđena odredbama Konvencije u modificiranoj formi i sadržaju ugrađena u nove glave i odredbe nedržavnih krivičnih zakona u Bosni i Hercegovini (Porobić, i Bajraktarević, 2012, str. 23). Na osnovu Konvencije o kibernetičkom kriminalu Vijeća Europe i Direktive Savjeta Europske Zajednice Bosna i Hercegovina je konstituisala pravnu regulativu koja se primjenjuje u području otkrivanja i sprečavanja cyber kriminala.

3. METODE ISTRAŽIVANJA

Metodom istraživanja dolazimo do naučnog saznanja. Disciplinarna prednost teme *Cyber kriminal kao moderna sigurnosna prijetnja u Bosni i Hercegovini* spada u područje metodologije društvenih nauka. Metodom analize sadržaja dokumenata analiziranjem sadržaja sa interneta, sadržaja iz knjiga, časopisa, prikupili su se različiti podaci informacijskog materijala. Glavni zadatak ovog rada je analiza dostupnih izvještaja o informaciji o stanju sigurnosti i izvodi na području Bosne i Hercegovine da bi se detaljnije upoznali sa stanjem cyber kriminala na području Bosne i Hercegovine. Istraživanje se bavi uporednim pokazateljima krivičnih djela u određenom vremenskom periodu.

Hipotetičko-deduktivna metoda se primjenjuje zbog toga što se predmet odnosi na društvenu stvarnost. Deskripcija se primjenjuje u početnoj fazi istraživanja i predstavlja postupak opisivanja činjenica o cyber kriminalu. Apstrakcijom se odvajaju nebitne, a ističu bitne osobine određene pojave istraživanja, u ovom istraživanju pojave cyber kriminala. U istraživanju je zastupljena i induktivna metoda, metoda analize, sinteze i statistička metoda.

Metodologija prikupljanja podataka bazirala se na kvalitativnom i kvantitativnom istraživanju. Kvalitativno istraživanje sastoji se u sekundarnoj analizi kvalitativnih podataka sadržanih u publikacijama o cyber kriminalu, dok se kao metod prikupljanja kvantitativnih podataka sproveo intervju. Osnovni cilj istraživanja jeste da se na osnovu

prikupljenih podataka dođe do saznanja o dinamici cyber kriminala. Namjera je da se u analizu uzmu predmeti koji se odnose na cyber kriminal u Bosni i Hercegovini i to za vremenski period od 01. 01. 2015. do 31. 12. 2018. godine. Uzorci koji će biti podvrgnuti analizi u ovom istraživačkom projektu jesu izvještaji grupe eksperata o cyber kriminalu u Bosni i Hercegovini u vremenskom periodu 01. 01. 2015.-31. 12. 2018. godine. Za potrebe ovog istraživanja konsultovali su se iskazi najcitiranijih eksperata u Bosni i Hercegovini, izneseni u dostupnoj literaturi. Na temelju navedenih podataka ne možemo reći da je uzorak reprezentativan. S obzirom na navedene podatke o krivičnim djelima protiv sistema elektronske obrade podataka za uzorak možemo reči da je ilustrativan. Uzorci koji su podvrgnuti analizi jesu godišnji izvještaji podataka Federalne uprave policije o stanju cyber kriminala, Ministarstva unutrašnjih poslova Republike Srpske i Ministarstva unutrašnjih poslova Brčko distrika Bosne i Hercegovine i informacije o stanju sigurnosti Bosne i Hercegovine, koja je sačinjena u okviru nadležnosti Ministarstva sigurnosti Bosne i Hercegovine na osnovu dostupnih podataka sigurnosnih agencija (Državne agencije za istrage i zaštitu, Granične policije BiH, Službe za poslove sa strancima, Obavještajno-sigurnosne agencije, entitetskih Ministarstava unutrašnjih poslova i Policije Brčko distrikta Bosne i Hercegovine).

Prostorno određenje cyber kriminala kao moderne sigurnosne prijetnje u Bosni i Hercegovini se odnosi na teritoriju Bosne i Hercegovine, odnosno na entitete Federaciju Bosne i Hercegovine i Republiku Srpsku i Brčko distrikt Bosne i Hercegovine. Osim ovog istraživanja napravljena je anketa na populaciji od šezdeset ispitanika starijih od 18 godina kako bismo spoznali da li su građani glavnog grada Bosne i Hercegovine bili ikada žrtve cyber kriminala, da li često mijenjaju svoje lozinke, da li imaju instaliran anti virus na svojim uređajima, obavljaju li kupovinu online i da li su korisnici internet bankarstva. Savremeni pojavni oblici kriminaliteta zahtijevaju novu metodiku otkrivanja krivičnih djela, koja podrazumijeva i pribavljanje dokaza u elektronskoj formi, odnosno elektronskih, softverskih ili kompjuterskih dokaza, kako ih nazivaju u teoriji i još uvijek nedovoljno izgrađenoj praksi (Pena, i Mitrović, 2012, str. 93). Cyber kriminal po osobinama veoma je sličan sa protivpravnim radnjama prevare i otuđivanja tuđe stvari.

4. REZULTATI

Prema Ministarstvu sigurnosti Bosne i Hercegovine djela koja se klasificiraju pod pojmom cyber kriminala su ometanje rada sistema i elektroničke obrade podataka, prevare na internetu, neovlašten pristup zaštićenom sistemu i mreži elektroničke obrade podataka, krivotvorenje kreditnih i ostalih kartica bezgotovinskog načina plaćanja, posjedovanje i distribucija dječije pornografije, kaznena djela u vezi sa zloupotrebama wireless mreža te društvenih mreža, kaznena djela povrede autorskih prava. Također, u Bosni i Hercegovini sve češća je pojava ekonomske špijunaže, širenja malware – a, neovlaštenog upada u zaštićene sisteme, krađe bankovnih kartica, a najčešča pojava je slučajeva koji se tiču internet prevare (Šakić, 2016, str. 1). Glavna hipoteza autora u istraživanju glasi: „*Cyber kriminal predstavlja modernu sigurnosnu prijetnju u Bosni i Hercegovini i izražen je u formi kriminala vezanog za kompjuterske mreže i upada u kompjuterski sistem.“* Pomoću

kompjuterske mreže napad se provodi na sadržaj i servis koji je na mreži sa ciljem zloupotrebe podataka, ali i uništenja mreže. Cyber kriminalci imaju cilj da navedu osobe da otkriju što više podataka o sebi kako bi ih zloupotrijebili za usluge bez korisnikovog znanja. Uništenje mreže može biti djelimično ili u cjelosti. Upad u kompjuterski sistem vrše hakeri služeći se internetom. Hakere motiviše finansijska dobit. Internet cyber kriminalcima olakšava krađu platnih kartica, krađu identiteta i obavljanje drugih nezakonitih radnji.

„Postoje mnogobrojni inkriminisani primjeri u praksi koji su se desili a da je prethodno slobodni prostor korištenja interneta i mogućnost korištenja lažnog identiteta pored nebrojeno provedenih sati za računarom, upravo psihički „okidač" da osoba nekome ili nečemu nanese neko zlo ili štetu. Često su prisutne ucjene i razne prijetnje objavljivanja kompromitujućih sadržaja neke osobe putem interneta ukoliko se ne plati određeni iznos novca ili se ne učini neka usluga itd. Pored ovakvih, postoje još i ekstremniji slučajevi. Naime, internet u današnje vrijeme služi kao veoma moćno sredstvo za teroriste, kao i za vršenje krivičnih djela, ali, isto tako, internet služi i kao sredstvo propagande, širenja nemoralnih sadržaja, raznih nacionalističkih, retrogradnih i drugih društveno i globalno neprihvatljivih ideja" (Blagojević i Guska, 2016, str. 18).

Internet omogućava anonimnost, kao i krađu identiteta, a što svakako utiče i na sadržaje na internetu. Naime, korisnici interneta u sajber-prostoru imaju vlastite identitete, koje je veoma teško „provaliti" i identifikovati sa društveno prihvatljivim i normiranim identitetom. Na taj način se ostvaruje i omogućava interakcija između svih korisnika, bez mogućnosti (ili je ta mogućnost izuzetno mala) otkrivanja identiteta druge strane, ali se stiče utisak da većina korisnika i ne želi da sazna pravi identitet druge osobe, naravno, sve dok nema štete od komunikacijskog odnosa koji postoji između navedenih korisnika interneta (Milašinović, Mijalković i Amidžić, 2012, str. 34). Na području Bosne i Hercegovine cyber kriminal postepeno dominira. BiH je 2006. godine raficirala Konvenciju o kibernetičkom kriminalu Vijeća Evrope iz 2001. godine. Odredbe Konvencije su uključene u entitetske zakone (poput odredbi o oštećenju računarskih podataka i programa; računarska sabotaža). Sadržajem odredaba državnog Zakona o krivičnom postupku i entitetskih zakona o krivičnom postupku nisu preuzeta krivično procesna rješenja sadržana u Konvenciji, što za posljedicu ima brojne dileme u provedbi krivičnih odredbi iz oblasti (Porobić i Bajraktarević 2012). Unutar Federalne uprave policije u okviru Sektora kriminalističke policije djeluje Odjel za borbu protiv organiziranog kriminala, u okviru kojeg rade istražitelji cyber kriminala, a koji postoji od 2008. godine, dok u Ministarstvu unutrašnjih poslova Republike Srpske postoji od 2010. godine. Policija Brčko distrikta Bosne i Hercegovine u sastavu Jedinice kriminalističke policije, u okviru odsjeka za Droge i organizovani kriminalitet i odsjeka za krim. obavještajnu podršku i terorizam, bavi se istragama koje su vezane za cyber kriminal. U posmatranom vremenskom periodu od 01. 01. 2015. do 31. 12. 2018. godine izvršena je analiza izvještaja podataka Federalne uprave policije o stanju cyber kriminala, Ministarstva unutrašnjih poslova Republike Srpske i Ministarstva unutrašnjih poslova Brčko distrika Bosne i Hercegovine i informacije o stanju sigurnosti u Bosni i Hercegovini.

Najčešći oblici načina izvršenja krivičnog djela iz oblasti kompjuterskog kriminala su:

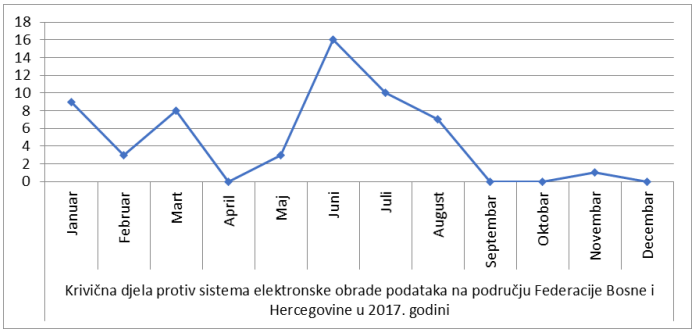
- neovlašteno dolaženje do pasvorda i korištenje istih bez dozvole stvarnih vlasnika a u cilju pribavljanja protivpravne materijalne koristi ili drugih benefita (zloupotreba informacija u cilju diskreditacije vlasnika ili sakrivanja stvarnog autora informacija preko drugih IP adresa...)
- neovlašteno sprečavanje ili ometanje pristupa javnoj mreži,
- izrada i unošenje računarskih virusa u namjeri njegovog unošenja u tuđi računar ili računarsku mrežu ili telekomunikacionu mrežu,
- unos netačnih ili propuštanje unosa tačnih podataka ili na drugi način uticanje na rezultat elektronske obrade i prenosa podataka u namjeri pribavljanja protivpravne imovinske koristi,
- zloupotreba audio-vizuelnih sadržaja.[92]

Najčešće prevare u svijetu, ali i u BiH su CEO (Chief Executive Officer) i BEC (Business E-mail Compromise) prevare. U CEO prevarama, napadač korištenjem autoriteta osobe u nekoj privrednoj organizaciji šalje podređenom instrukcije za plaćanje sa maila unaprijed kreiranog tako da se predstavlja kao autoritet pod oznakom hitnosti. Ovaj bez provjeravanja namjera svog nadređenog šalje novac na račun, većinom je to Velika Britanija. Iz Velike Britanije se redirektuje u Afriku, to je u skladu sa istragama, ne mora biti uvijek. I BEC prevare, to je najčešće i u BiH i u svijetu, kada napadač preuzima korištenje e-maila od privrednih subjekata u BiH, primjera, i u dijelu maila u forwarding stavlja svoj mail. Ovo je jedna tehnika, da napomenem. Čitavo vrijeme prati korespondenciju između privrednog subjekta iz BiH i njegovog dobavljača, recimo iz Njemačke, daću primjer. U jednom momentu kada dođe do plaćanja, avansnog ili nešto slično, šalje fakturu, odnosno mijenja dio fakture koji se odnosi na plaćanje. Predstavljaju se kao taj dobavljač, šalje žrtvi, žrtva uplaćuje novac i tek shvati, kada roba nije isporučena ili kada dobije žalbe svog dobavljača, da je prevarena". U BiH do sada najveća takva prevara iznosila je 900.000 konvertibilnih maraka (KM), a u Evropi oko 40 miliona eura. U takvim prevarama nije teško pratiti digitalne i tragove novca, ali je veoma teško kada su to napadači iz Afrike, što se u većini slučajeva i dešava... U BiH, uz CEO i BEC prevare, postoje i mnoge druge, kao što su prodaja robe nevjerovatnih svojstava, tačnije nepostojeće robe.[93]

Prema analitičkim pokazateljima Federalne uprave policije Bosne i Hercegovine najrasprostranjeniji slučajevi cyber kriminala na području Federacije Bosne i Hercegovine su: krađe novca posredstvom bankovnih kartica, sabotiranje poslovnih e-mail računa, kriptiranje informacijskih sistema korisnika, odnosno napadi koji se vrše putem malicioznih

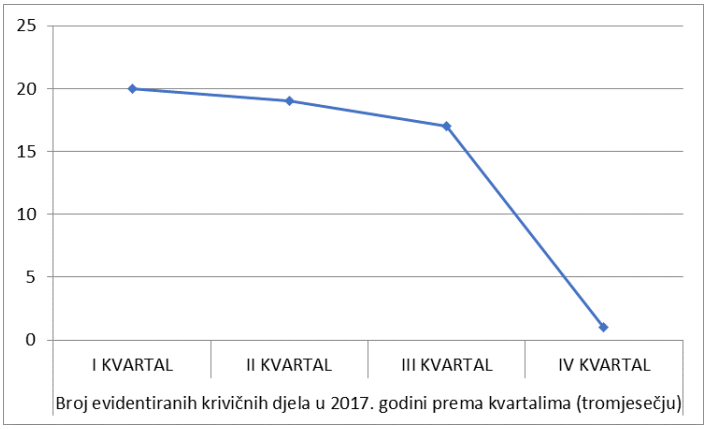
[92] Više pogledati: *Informacija o stanju sigurnosti u Bosni i Hercegovini u 2017. godini*. Bosna i Hercegovina, Ministarstvo sigurnosti. Januar-decembar 2017. Sarajevo, juni 2018.
[93] Više pogledati: Intervju na temu „Cyber kriminal sve češća pojava u BiH: Informisati se o opasnostima interneta" sa Saša Petrović, istražitelj za borbu protiv kompjuterskog kriminala u Federalnoj upravi policije (FUP).

programa na IT sistem. Prema podacima o stanju sigurnosti u Bosni i Hercegovini u 2015. godini na području Federacije Bosne i Hercegovine je izvršeno ukupno 18 krivičnih djela protiv sistema elektronske obrade podataka, a za ista krivična djela prijavljeno je samo 6 lica. Tokom 2016. godine broj krivičnih djela je naglo porastao na 26 krivičnih djela (računalna prijevara i neovlašćeni pristup zaštićenom sistemu i mreži elektronske obrade podataka) i prijavljeno je 16 lica, na osnovu čega možemo zaključiti da od ukupnog broja izvršenih krivičnih djela broj prijava opada. Kada je u pitanju broj otkrivenih djela protiv sistema elektronske obrade podataka u toku 2016. godine od ukupnog navedenog broja otkriveno je samo 18 krivičnih djela što znači da je kada je u pitanju ukupan broj otkriveno 69,23% krivičnih djela protiv sistema elektronske obrade podataka, dok se u toku 2017. godine bilježi znatan porast kako u povećanom broju krivičnog djela tako i u rasvijetljenosti 39 krivičnih djela, odnosno 68,42%.



Ilustracija 1

Ilustracija 1. pokazuje broj krivičnih djela izvršenih po mjesecima u toku 2017. godine. Uzimajući u obzir cijelu 2017. godinu na području Federacije Bosne i Hercegovine evidentirano je 57 krivičnih djela protiv sistema elektronske obrade podataka (računalna prijevara i neovlašćeni pristup zaštićenom sistemu i mreži elektronske obrade podataka), što znači da opšta sklonost ka krivičnim djelima protiv sistema elektronske obrade podataka za 2016/17. godinu iznosi 119, 23%.



Ilustracija 2.

U ilustraciji 2. su prikazana krivična djela protiv sistema elektronske obrade podataka raspoređena po kvartalima. Primjetno je opadanje broja krivičnih djela tokom IV kvartala. Na području Federacije Bosne i Hercegovine tokom 2018. godine evidentirano je 21 krivično djelo protiv sistema elektronske obrade podataka. Otkriveno je 14 krivičnih djela, što iznosi 66,67% od ukupnog broja krivičnih djela protiv sistema elektronske obrade podataka.

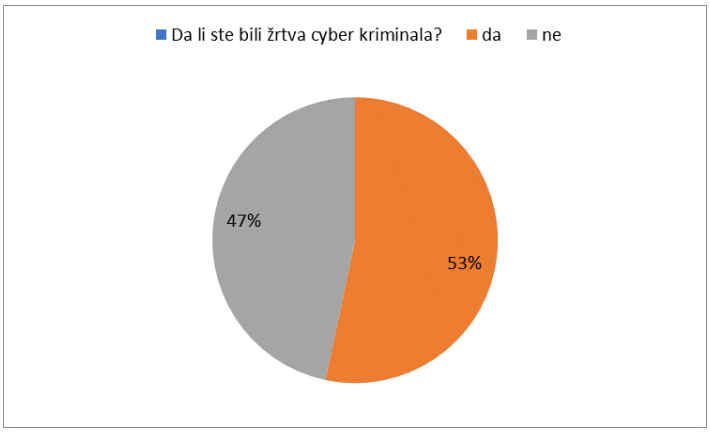
Prema dostupnim analitičkim pokazateljima Izvještaja o radu Ministarstva unutrašnjih poslova Republike Srpske najrasprostranjeniji slučajevi cyber kriminala na području Republike Srpske su: računarske prevare, izrađivanje i unošenje računalnih virusa, iskorištavanje djece i maloljetnika za pornografiju, neovlašten pristup zaštićenom računalu, računalnoj i telekomunikacijskoj mreži i elekronskoj obradi podataka, falfiskovanje kreditnih i kartica za bezgotovinsko plaćanje, kompjuterska sabotaža i oštećenje računarskih podataka i programa. Tokom 2015. godine na području Republike Srpske prijavljeno je 11 krivičnih djela cyber kriminala, dok je otkriveno svega 9 krivičnih djela cyber kriminala. Tokom 2016. godine zabilježeno je dvostruko više krivičnih djela cyber kriminala (izrada i unošenje računalnih virusa, računarske prevare, neovlašten pristup zaštićenom računalu, računalnoj i telekomunikacijskoj i elektronskoj obradi podataka, falsifikovanje kreditnih kartica i kartica za bezgotovinsko plaćanje, proizvodnja, posjedovanje i prikazivanje dječje pornografije, iskorištavanje djece i maloljetnih lica za pornografiju u odnosu na prethodnu godinu. Prijavljeno je 20 osoba što itekako predstavlja povećanje kriminala u odnosu na 2015. godinu. Tokom 2018. godine na području Republike Srpske je otkriveno 50 krivičnih djela iz oblasti cyber kriminala, što je za 19 krivičnih djela više u odnosu na 2017. godinu, gdje su dominirale računarske prevare, neovlašten pristup zaštićenom računaru, računalnoj i telekomunikacijskoj i elektronskoj obradi podataka, oštećenje računarskih podataka i programa i proizvodnja, posjedovanje i prikazivanje dječje pornografije.

Prema mišljenju eksperata iz oblasti cyber sigurnosti najrasprostranjeniji slučajevi cyber kriminala na području Brčko distrikta Bosne i Hercegovine su računarske prevare i oštećenja računarskih podataka i programa. Na području Brčko distrikta Bosne i Hercegovine prema informaciji o stanju sigurnosti u Bosni i Hercegovini tokom 2015. i 2016. godine nije bilo evidentiranih krivičnih djela protiv sistema elektronske obrade podataka, dok je u 2017. godini evidentirano jedno krivično djelo protiv sistema elektronske obrade podataka. Prema informaciji o stanju sigurnosti u Bosni i Hercegovini nije navedeno koje od navedenih krivičnih djela protiv sistema elektronske obrade podataka je evidentirano. Kada je u pitanju 2018. godina za sada nema dostupnih podataka koliki je tačan broj krivičnih djela protiv sistema elektronske obrade podataka na području Brčko distrikta Bosne i Hercegovine.

Pozitivna zakonska praksa u Bosni i Hercegovini suočava se sa izrazito kompliciranim vrstama krivičnih djela cyber kriminala. Cyber kriminal postaje najopasniji vid kriminala kako zbog veće prisustva u institucijama društva, tako i otežanog načina dokazivanja i otkrivanja. Vrste, kao i broj krivičnih djela cyber kriminala i finansijsku štetu koju uzrokuje cyber kriminal zaista je teško procijeniti. Narednih godina u Bosni i Hercegovini izvjesno je očekivati naglu ekspanziju krivičnih djela protiv sistema elektronske obrade podataka budući da informacijska tehnologija brzo napreduje.

Osim toga u istraživanju su zastupljeni i stavovi građana (N=60) na području Sarajeva tokom mjeseca juna 2019. godine. Istraživanje se svodi na glavni grad Bosne i Hercegovine[94]. S obzirom na provedenu anketu koja je obuhvatila Sarajevo, glavni grad Bosne i Hercegovine, koji ulazi u sastav Federacije Bosne i Hercegovine za navedeni uzorak ne može se reći da je reprezentativan, jer ne odražava stavove građana kroz osvrt na sve administrativne jedinice Bosne i Hercegovine U okviru empirijskog istraživanja koristila se i metoda analize sadržaja dokumenata i metoda ispitivanja. Pošto građani koriste internet svakodnevno za instrument istraživanja se sproveo intervju, kreiran za tu priliku. U ovom dijelu rada možemo saznati koliko je građana od ukupno šezdeset ispitanih lica na području glavnog grada Bosne i Hercegovine starijih od 18 godina bilo žrtva cyber kriminala, da li često mijenjaju svoje lozinke, imaju li instaliran antivirus na svojim uređajima, kupuju li online i da li koriste internet bankarstvo. Svi ispitanici koriste internet.

[94] Bosna i Hercegovina je država sastavljena iz dva entiteta: Federacije Bosne i Hercegovine i Republike Srpske i Distrikta Brčko. Glavni i najveći grad Bosne i Hercegovine je Sarajevo. Iako Sarajevo ulazi u sastav Federacije Bosne i Hercegovine, cilj ankete je bio spoznati stavove građana u glavnom gradu države Bosne i Hercegovine. Zbog toga je anketa provedena u Sarajevu.

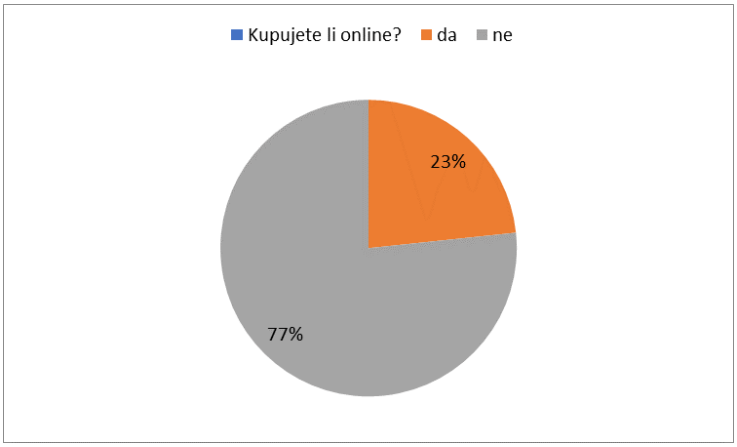


Ilustracija 3.

U ilustraciji 3. prikazano je da od ukupnog broja ispitanika (N=60) na području Sarajeva 53% ispitanika je bilo žrtva cyber kriminala, dok 47% ispitanika nije bilo žrtva krivičnog djela cyber kriminala. Od ukupnog broja ispitanika koji su bili žrtve cyber kriminala pet ispitanika je bilo žrtva računarskih virusa, dva ispitanika su bila žrtve krađe novca posredstvom bankovne kartice, dok je ostalim ispitanicima izvršen upad na korisnički profil na društvenoj mreži Facebook.

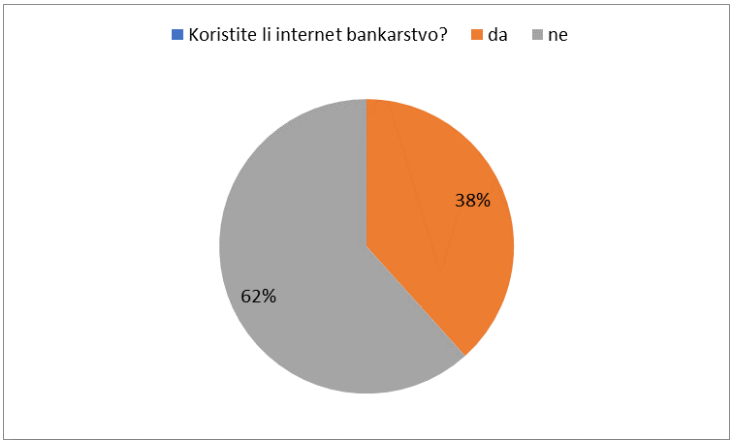
Ilustracija 4.

Ilustracija 4. pokazuje da od ukupnog broja ispitivanih lica, 70% građana na području glavnog grada Bosne i Hercegovine često mijenja svoje lozinke na korisničkim računima, dok 30% građana je odgovorilo da ne mijenja često svoje lozinke. Od ukupnog broja ispitanika na području glavnog grada Bosne i Hercegovine svi ispitanici imaju instaliran antivirus na svojim uređajima.



Ilustracija 5.

Ilustracija 5. pokazuje da 23% od ukupnog broja ispitanika kupuje online, dok 77% ispitanika ne kupuje online.



Ilustracija 6.

Ilustracija 6. pokazuje da 62 % ispitanika ne koristi internet bankarstvo, dok 38% ispitanika koristi usluge internet bankarstva. Na osnovu provedene ankete građani u glavnom gradu Bosne i Hercegovine su se susreli sa krađom novca posredstvom bankovnih kartica, računarskim virusima i upadima na korisnički profil na društvenoj mreži Facebook.

U vezi navedenog problema zaključujemo da su društvene mreže novo poprište cyber kriminala. Jednostavno trebamo biti oprezni koje stranice otvaramo. Većina stranica nas

potiče na davanje ličnih podataka, kao i za razmjenu informacija putem interneta. Lica sklona cyber kriminalu traže osobe koje otkrivaju previše ličnih informacija, koristeći manipulisanje da bi naveli osobu da prezentira svoje lične podatke, a potom ih nezakonito koriste bez znanja osobe koja otkrije svoje lične podatke. Pomoću kupovine online, kriminalna lica oglašavaju usluge koje ili nisu njihove ili ne postoje u stvarnosti kako bi uvjerili korisnika na direktno plaćanje na njihov račun. Neophodno je prije nego se odlučimo na kupovinu online istražiti poslodavce kako bismo sa sigurnošću mogli utvrditi njihovu pouzdanost. Ono što se dešava online ima uticaj i posljedice na stvarni, offline svijet-Internet jeste stvarni život. Upravo zbog toga, online napade treba shvatiti kao stvarne i obezbijediti adekvatnu zaštitu.[95] Čovjek igra značajnu ulogu kada je u pitanju cyber sigurnost. Internet predstavlja jednak prostor za sve korisnike tako da svi korisnici interneta kako građani, pravna lica tako i javni organi trebaju razviti osnovne uslove kako bi zaštitili svoje uređaje i sve informacije na njima i time djelovali nesmetano na internetu. Potrebno je pratiti tehnološki napredak iz oblasti cyber sigurnosti i modernizirati kako tehnologiju tako i sistem da bismo potisli moguće napade. Samo praćenje tehnologije neće dati odgovarajuće rezultate ukoliko se ne primjene od strane određenih stručnjaka koji svoje znanje paralelno usavršavaju sa principima svih novosti koji su izraženi u oblasti cyber sigurnosti. Za bezbjedno korištenje interneta i zaštitu na računaru neophodno je zaštiti e-mail od poruka koje su sumnjivog sadržaja, ne otvarati sumnjive e-mailove, napraviti sigurnosnu kopiju podataka, upotrebljavati kompleksne lozinke, koristiti programe koji su legalni, biti oprezan u korištenju javne WiFi mreže, računar ugasiti kada ga ne koristimo, upotrebljavati operativne sisteme koji su legalni, instalirati i ažurirati antivirusni program, držati anti virusni program uključen, skenirati vanjske uređaje koji se priključuju na računar, USB i sl.

5. RASPRAVA

Internet je postao sastavni dio svakodnevnice. Građani Bosne i Hercegovine svjedoci su da su svakodnevno prisutne prevare preko interneta. Internet se sve više koristi u poslovnoj sferi. Kako se povećava broj korisnika interneta tako se povećava i broj internet prevara. Prezentirani podaci o fenomenu cyber kriminala ukazuju da trebamo biti oprezniji kada koristimo internet jer veoma lako možemo postati žrtva cyber kriminala. Postoji značajna povezanost između cyber kriminala i kompjuterske mreže. Kompjuterske mreže koje su meta napada mogu se iskorištavati u različite svrhe. Postoji značajna povezanost između cyber kriminala i kompjuterskog sistema. Kompjuterski sistem predstavlja uređaj ili skup uređaja koji su međusobno povezani gdje jedan od njih ili nekoliko njih obavlja automatsku obradu podataka. Kod krivičnih

[95] Više pogledati: Lejla Gačanica i Marija Arnautović, *„Mehanizmi zaštite od online nasilja“*. Sarajevo: Mediacentar. 2018., str. 10

djela protiv sistema elektronske obrade podataka radnja izvršenja krivičnog djela sadržana je u neovlašćenom pristupu u tuđu kompjutersku bazu podataka.

Prezentirani statistički podaci vezani za izvještaj o evidentiranim krivičnim djelima protiv sistema elektronske obrade podataka na području Federacije Bosne i Hercegovine, Republike Srpske i Brčko distrikta Bosne i Hercegovine ne predstavljaju dovoljno tačan pokazatelj kojim se može predstaviti opseg cyber kriminala na području Federacije Bosne i Hercegovine, Republike Srpske i Brčko distrikta Bosne i Hercegovine. Prezentirani statistički podaci predstavljaju trenutne pokazatelje krivičnih djela protiv sistema elektronske obrade podataka na području Federacije Bosne i Hercegovine, Republike Srpske i Brčko distrikta u Bosni i Hercegovini. Rezultati provedenog istraživanja ukazuju da trend krivičnih djela protiv sistema elektronske obrade podataka u Bosni i Hercegovini varira. Na osnovu predstavljenog istraživanja možemo sa sigurnošću utvrditi da tokom određenog posmatranog vremenskog perioda u Bosni i Hercegovini cyber kriminal je najmanje izražen u Brčko distriktu Bosne i Hercegovine. Uporedo sa prezentiranim podacima o krivičnim djelima protiv sistema elektronske obrade podataka izneseni su stavovi građana na području glavnog grada Bosne i Hercegovine. Na osnovu iznesenih stavova uočavamo da su svi ispitanici svjesni opasnosti da veoma lako mogu postati meta nekog štetnog programa. Da bi izbjegli takav scenario svi ispitanici su instalirali antivirus na svojim uređajima.

Rezultat istraživanja treba proširiti naučno teorijsko saznanje o ovoj pojavi. U ovom istraživanju naučna opravdanost ide u pravcu i heurističkog i verifikatornog rezultata. Doprinos istraživanja je heuristički u dijelu opisivanja spoznaja provedenog istraživanja na području Bosne i Hercegovine. Kada je u pitanju verifikacijski rezultat istraživanja, u pravcu verifikacije se ide jer se istraživanje svodi na potvrdu teze da cyber kriminal predstavlja modernu sigurnosnu prijetnju u Bosni i Hercegovini i izražen je u formi kriminala vezanog za kompjuterske mreže i upada u kompjuterski sistem.

6. ZAKLJUČAK

Cyber kriminal kao fenomen modernog doba posebna je vrsta kriminala koja se ispoljava u različitim oblicima zloupotreba informacionih tehnologija. Nijedna osoba ne može garantovati da će njegovi/njeni podaci biti zaštićeni od zloupotrebe. Može se zaključiti da je internet proizveo ogromnu brojku sigurnosnih rizika kako zbog razvoja programa tako i različitih internet prevara. Posljedice koje nastaju zloupotrebom ličnih podataka internet korisnika su ogromne. Bosna i Hercegovina je država korisnica globalne mreže. Cyber kriminal uključuje krivična djela koja se izvršavaju kako protiv pojedinaca tako i protiv države kao organizovane društvene zajednice koja je uređena političkim sistemom.

Kako bi se ublažio problem fenomena modernog doba cyber kriminala neophodno je da se poboljša rad informacijske sigurnosti kako od organizacija tako i od lica koja koriste internet. Otkrivanje krivičnih djela protiv sistema elektronske obrade podataka postaje sve više složenije. Bosna i Hercegovina u pogledu nacionalne sigurnosti u cilju borbe protiv cyber kriminala treba da sprovodi mjere zaštite na operativnoj, državnoj, proizvodnoj, tehničkoj i organizacionoj razini. Osobitost cyber kriminala zahtijeva odgovarajući oblik edukacije operativnih lica koja koja su uključena u borbu protiv cyber kriminala. Zaštitne mjere ogledaju se u primjenjivanju najmodernijih sredstava kako bi se zaštitili podaci od zloupotrebe. Uspješno suprotstavljanje cyber kriminalu zahtijeva potpun krivičnoprocesni sistem otpora na cyber kriminal. Neophodno je razmjenjivanje informacija na međunarodnom nivou između organa za borbu protiv cyber kriminala. Brzo djelovanje po saznanju da je počinjeno krivično djelo od velike je važnosti za otkrivanje počinilaca i obezbjeđivanje dokaza. Neophodno je i da građani povećaju svijest o opasnostima koje cyber kriminal proizvodi kako bi zaštitili svoje lične podatke, što znači da su oprez i informiranost od krucijalnog značaja.

BIBLIOGRAFIJA

- Blagojević, G. i Guska, G. (2016). *Zavisnost od interneta-predrasude ili realnost*. Edukator Travnik: Univerzitet u Vitezu,12-20.
- Cornish, P., Hughes, R., Livingstone, D. (2009). *Cyberspace and the National Security of the United Kingdom – Threats and Responses*. London: Royal Institute of International Affairs.Chatham House Report
- Deutsch, Karl W. (1966). *The Nerves of Government: Moñels of Political Communication and Control*, 2nd ed.. New York
- Gačanica, L. i Arnautović, M. (2018). *Mehanizmi zaštite od online nasilja*. Sarajevo: Mediacentar
- Gligorević, R. (2014). *Cyber kriminal*. Digitalna ekonomija-Digital Economics, 163-174.
- Hamidović, H, Hamidović, A. i Zajmović, M. (2016). *Okvir za rješavanje problema cyber kriminala*. INFOTEH-JAHORINA, 557-562.
- Kovačević, B. (2013). *Cyberwar-Američka izlika za novi hladni rat?* Polemos, 91-110.
- Krstić, O. (2009). *Maloljetnička delinkvencija*. Banja Luka: Fakultet za bezbjednost i zaštitu
- Mesarović, S. (2006). *Motiv i profil izvršilaca*. Zbornik Ziteh '06. Beograd. IT veštak
- Milašinović, R, Mijalković, S. i Amidžić, G. (2012). *Bezbednost i internet*. Zbornik radova. Laktaši. Visoka škola unutrašnjih poslova, Bulevar Živojina Mišića 10A. Banja Luka, 31-42.
- Pena, U. i Mitrović, D. (2012). *Značaj digitalnih dokaza u krivičnom postupku*. Zbornik radova. Laktaši. Visoka škola unutrašnjih poslova, Bulevar Živojina Mišića 10A. Banja Luka, 93-108.
- Porobić, M. i Bajraktarević, M. (2012). *Cyber kriminal, pranje novca i finansijske istrage.* Sarajevo
- Radnović, B. Ilić, M. i Radović, N. (2012). *Ekonomski sajber kriminal u Srbiji-aspekt zaštite internet potrošača*. Zbornik radova. Laktaši. Visoka škola unutrašnjih poslova, Bulevar Živojina Mišića 10A. Banja Luka, 129-142.
- Selimović, M. (2015). *Implementacija procesnih odredbi Konvencije o kibernetičkom kriminalu u Zakonu o krivičnom postupku Federacije Bosne i Hercegovine*. Kriminalističke teme, str. 74, 71-83.
- Šakić, D. (2016). *Cyber kriminal*. Edukator. God 3. Br. 4. Travnik. Univerzitet Vitez.
- Vasić, G., Šarić, B. i Jovanić, V. (2012). *Kompjuterski kriminalitet*. Zbornik radova. Laktaši. Visoka škola unutrašnjih poslova, Bulevar Živojina Mišića 10A. Banja Luka, 181-192.
- Vuković, H. (2012). *Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj*. NATIONAL SECURITY AND THE FUTURE, 12-31.

Ostali korišteni izvori:

- Informacija o stanju sigurnosti u Bosni i Hercegovini u 2015. godini. (2016). Bosna i Hercegovina. Ministarstvo sigurnosti. Sarajevo
- Informacija o stanju sigurnosti u Bosni i Hercegovini u 2016. godini. (2017). Bosna i Hercegovina. Ministarstvo sigurnosti. Sarajevo
- Informacija o stanju sigurnosti u Bosni i Hercegovini u 2017. godini. (2018). Bosna i Hercegovina. Ministarstvo sigurnosti. Sarajevo
- Krivični zakon Brčko distrikta Bosne i Hercegovine. Glava XXXII. Službeni glasnik Brčko distrikta BiH br. 33/2013 - prečišćen tekst, 47/2014 - ispravka 26/2016, 13/2017 i 50/2018
- Krivični zakon Federacije Bosne i Hercegovine. Glava XXXII. Krivična djela protiv sustava elektronske obrade podataka, Službene novine Federacije BiH, br. 36/2003, 21/2004-ispr., 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 i 75/2017
- Krivični zakon Republike Srpske. Glava XXXIV. Krivična djela protiv bezbjednosti kompjuterskih podataka. Službeni glasnik Republike Srpske broj: 64/17 i 104/2018-odluka US

Internet izvori:

- Cyber kriminal sve češća pojava u BiH: Informisati se o opasnostima interneta. (2019). https://akos.ba › cyber-kriminal-sve-cesca-pojava-u-bih-informisati-se-o-o...
- Wynne, M.W. (2006). *Cyberspace as a Domain in Which the Air Force Flies and Fights*, govor s C4ISR Integration Conference. Dostupno na: https://www.af.mil›About Us › Speeches Archive
- https://www.msb.gov.ba
- https://www.mup.vladars.net
- https://www.fup.gov.ba
- https://www.policijabdbih.gov.ba