Svetislav Lutovac*
Julijana Račić**

UDK 343.533::004
004.738.5.056.53

DOI: 10.5937/MegRev2104281L
Stručni članak
Primljen 12.04.2021.
Odobren 15.09.2021.

KOMPJUTERSKI KRIMINAL KAO SAVREMENI OBLIK KRIMINALITETA***

Apstrakt: *Razvoj tehnologije znatno je doprineo poboljšanju komunikacije, načinu poslovanja čovečanstva, proteku i dostupnosti informacija putem interneta, ali takođe, on za sobom povlači negativne posledice u vidu zloupotreba izvršenjem krivičnih dela iz oblasti bezbednosti računarskih programa. Borba protiv istog je jako teška, a razlog za to je konstantan napredak, odnosno modifikacija ovog oblika kriminaliteta, pri čemu je neophodno menjanje postojeće zakonske regulative, ostvarivanje međunarodne saradnje, ulaganje novčanih sredstava u opremu pogodnu za adekvatno reagovanje protiv kompjuterskog kriminaliteta. U ovom radu, akcenat se stavlja na sam pojam kompjuterskog kriminaliteta, međunarodnu i domaću zakonsku regulativu, oblike u kojima se najčešće manifestuje.*

Ključne reči: *tehnologija, kompjuterski kriminalitet.*

* Docent, Pravni fakultet, Megatrend univerzitet, Beograd; slutovac@megatrend.edu.rs

** Saradnik u nastavi, Pravni fakultet, Megatrend univerzitet, Beograd; jracic@megatrend.edu.rs

*** Rad je rezultat projekta Pravnog fakulteta FPPNT – Pravo i nove tehnologije

1. Uvod

Protekom vremena, razvojem društva, razmenom ideja, iskustava i novih saznanja došlo je do univerzalnog geopolitičkog procesa u formi globalizacije koji se nametnuo uspostavljanjem jednostavnije, savremenije, brže i praktičnije komunikacije, razmene informacija, usluga, roba, otvorenosti granica, kretanja ljudi koja je nametnula savremenije standarde i principe ekspanzivnih procesa. Globalizacija sa sobom donosi mnoge prednosti, ali i mnoge negativne posledice koje se odražavaju na celokupno društvo.

Naša zatečenost razvojem tehnologije usled brzine kojom se procesi na svetskoj sceni odigravaju, stvaraju dezorentaciju i nedoumice u kojima smo najčešće zbunjeni i zarobljeni. Neophodnost kompjuterizacije i interneta u poslovanju, poboljšala je uslove komunikacije, ali je sa druge strane omogućila i stvorila prostor za mnoge zloupotrebe kojima se nanosi ogromna materijalna šteta zbog pribavljanja protivpravne imovinske koristi. Dijapazon zloupotreba kompjuterskog, odnosno visokotehnološkog kriminala svrstan je u podvrstu imovinskog, kao i privrednog kriminaliteta.

Jedna od odlika visokotehnološkog kriminala ogleda se u brzom i lakom profitiranju, bez ulaganja ogromnih novčanih sredstava prilikom pripremanja i vršenja krivičnih dela. Ono što karakteriše ovu vrstu kriminaliteta je delovanje kako pojedinaca tako i organizovanih kriminalnih grupa u zavisnosti od njihovog pravca delovanja. Organizovane kriminalne grupe imaju strogu hijerarhiju, strukturu kao i način podele poslova među članovima, u zavisnosti od nivoa stručnosti za obavljanje određene vrste poslova.

Takođe, mnogi autori zastupaju stav da kompjuterski kriminalitet spada u podvrstu kriminaliteta belog okovratnika, prilikom kojeg zaposleni zloupotrebljava svoj prestižni status u društvu radi pribavljanja lične imovinske koristi ili koristi za kriminalnu grupu.

Reč je o kriminalitetu transnacionalnog tipa, sa sve većim intenzitetom, koji se veoma teško otkriva zbog lakog uništavanja dokaza, posebno usled otežanosti identifikacije mesta i vremena izvršenja tih i takvih nezakonitih radnji. Ono što je bitno za njegovo otkrivanje je poseban pristup istražnih organa, njihova stručnost i multidisciplinarni aspekt predvidivosti krivičnih dela kojim se on može ostvariti. Pored izuzetnih specijalističkih znanja istražnih organa, neophodna je međunarodna saradnja i povezanost istih u prevenciji ove izuzetno specifične kriminalne aktivnosti.

Vršenje krivičnih dela iz ove oblasti povlači za sobom ostvarivanje dva cilja, a to su sticanje protivpravne imovinske koristi, kao i ostvarivanje osećaja "zadovoljstva" putem upada u obezbeđeni računarski sistem, kako bi se bitni podaci mogli plasirati u javnosti.

2. Pojam kompjuterskog kriminala

Kompjuterski kriminalitet je jako teško definisati zbog njegove fenomenološke raznovrsnosti, kao što je slučaj i sa organizovanim kriminalom, terorizmom i slično, iz razloga što predstavlja noviji oblik kriminalnog delovanja koji se protekom vremena sve više usavršava, odnosno razvijaju se razne nove metode u delovanju i načinu ponašanja (modus operandi).

„Kompjuterski kriminalitet predstavlja oblik kriminalnog ponašanja, kod koga se korišćenje kompjuterske tehnologije i informatičkih sistema ispoljava kao način izvršenja krivičnog dela, ili se kompjuter upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka u krivičnopravnom smislu relevantna posledica."[1]

Prema Ignjatoviću, razlikujemo dve definicije:

- šira, po kojoj u ovu kategoriju spada bilo koje krivično delo povezano sa upotrebom ili funkcionisanjem računara, i
- uža, po kojoj je kompjuterski kriminalitet poseban vid inkriminisanih ponašanja kod kojih se računarski sistem (shvaćen kao jedinstvo fizičkih jedinica – hardvera – i programa – softvera) pojavljuje ili kao sredstvo izvršenja ili kao objekat krivičnog dela, ukoliko se delo na drugi način ili prema drugom objektu ne bi uopšte moglo izvršiti ili bi ono imalo bitno drugačije karakteristike.[2]

Kompjuterski kriminalitet obuhvata kriminalitet vezan za kompjuterske mreže (Internet ili cyber kriminalitet) gde se kompjuterske mreže koriste:

- Kao cilj napada (napadaju se servisi, funkcije i sadržaji koji se nalaze na mreži);
- Kao sredstvo ili alat (online prodaja seksualnih usluga, ljudskih organa, žena i dece za prostituciju, proizvodnja i distribucija nedozvoljenih štetnih sadržaja, kao što su dečja pornografija, pedofilija, verske sekte, rasističke, nacističke i slične ideje i sl.)
- Kao okruženje u kome se napadi realizuju (korišćenje mreže za prikrivanje kriminalnih radnji).[3]

---

1 Lilić Stevan, Prlja Dragan (2011), *Pravna informatika veština*, Pravni fakultet Univerziteta u Beogradu, Beograd, str. 104.

2 Ignjatović Djordje (2016): *Kriminologija*, Pravni fakultet Univerziteta u Beogradu, Beograd, str. 122.

3 Vesna Nikolić-Ristanovič, Slobodanka Konstantinović-Vilić (2018): *Kriminologija,* Izdavačko-grafičko preduzeće "Prometej", Beograd, str. 177.

3. Zakonska regulativa

Na međunarodnom planu, neophodno je postići saradnju kako bismo se ovom problemu kompjuterskog kriminaliteta suprotstavili na adekvatan način. Vremenom su propisane i ratifikovane određene konvencije. Hronološki posmatrano, prvi dokument na području Evrope, koji se odnosi na ovu problematiku, donet 17. maja 1991. godine, jeste direktiva Saveta Evropske zajednice o pravnoj zaštiti kompjuterskih programa. Države članice Evropske zajednice bile su obavezane na njenu primenu od 1. januara 1993. godine. Zatim, doneta je Konvencija o visokotehnološkom kriminalu, potvrđena 23. novembra 2001. godine u Budimpešti, koju je Republika Srbija ratifikovala 19. marta 2009. godine. U preambuli iste naglašeno je da države članice Saveta Evrope, kao i druge države potpisnice imaju cilj sprovođenja zajedničke politike u borbi protiv ovog globalnog problema. Prvo poglavlje konvencije odnosi se na definisanje osnovnih termina. Drugo poglavlje govori o merama koje je potrebno preduzeti na nacionalnom nivou. Treće poglavlje odnosi se na međunarodnu saradnju. Poslednjim, četvrtim poglavljem, određene su završne odredbe navedene konvencije. Takođe, Republika Srbija ratifikovala je 2009. godine dodatni protokol uz Konvenciju o visokotehnološkom kriminalu koji se odnosi na inkriminaciju krivičnih dela protiv rasizma i ksenofobije učinjenih putem računarskih sistema, koji je sačinjen 28. januara 2003. godine u Strazburu. Pored navedene konvencije i dopunskog protokola, doneti su sledeći akti:

- Konvencija Saveta Evrope o zaštiti dece od seksualnog iskorišćavanja i seksualnog zlostavljanja (tzv. Lanzarot konvencija – Savet Evrope 2007. godine, stupila na snagu 2010. godine i ratifikovana iste godine od strane Republike Srbije);
- Odluka Saveta Evropske unije o suzbijanju dečije pornografije na internetu 2000/375/JHA;
- Direktiva Evropskog parlamenta o borbi protiv seksualne zloupotrebe, seksualne eksploatacije i dečije pornografije 2011/92EU;
- Direktiva 2013/40/EU Evropskog parlamenta i Saveta EU o napadima na informacione sisteme i zameni Okvirne odluke Saveta 2005/222/JHA;
- Bezbednosna agenda Evropske unije za period od 2015. do 2020. godine;
- Strategija sajber bezbednosti Evropske unije iz 2013. godine – „Otvoren, bezbedan i zaštićen sajber prostor", i
- IOCTA (Internet organised crime threat assessment 2017) – Procena pretnje od Internet organizovanog kriminala.[4]

Republika Srbija se ovom obliku kriminaliteta suprotstavlja primenom sledećih zakona:

- Krivičnim zakonikom;
- Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, i

[4] Strategija za borbu protiv visokotehnološkog kriminala za period od 2019-2023. godine, str. 6

- Zakonom o krivičnom postupku;
- Zakon o elektronskim komunikacijama;
- Zakon o informacionoj bezbednosti;
- Zakon o organizaciji i nadležnosti državnih organa u suzbijanju organizovanog kriminala, terorizma i korupcije, i
- Zakon o sprečavanju pranja novca i finansiranja terorizma.

Krivični zakonik u svojoj XXVII glavi propisuje sledeća krivična dela protiv bezbednosti računarskih podataka:
- Oštećenje računarskih podataka i programa (član 298);
- Računarska sabotaža (član 299);
- Pribavljanje i unošenje računarskih virusa (član 300);
- Računarska prevara (član 301);
- Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka (član 302);
- Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (član 303);
- Neovlašćeno korišćenje računara ili računarske mreže (član 304), i
- Pribavljanje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka (član 304a).[5]

Objekt zaštite navedenih krivičnih dela je bezbednost računarskih programa. Kada su u pitanju krivične sankcije, propisana je primena kazne zatvora ili novčane kazne u zavisnosti od težine učinjenog dela.

Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala uređuje se obrazovanje, organizacija, nadležnost i ovlašćenja posebnih organizacionih jedinica državnih organa radi otkrivanja, krivičnog gonjenja i suđenja za krivična dela određena istim.[6]

Nadležne institucije u borbi protiv visokotehnološkog kriminaliteta u Republici Srbiji su:
- Posebno tužilaštvo za visokotehnološki kriminal;
- Služba za borbu protiv organizovanog kriminala, i
- Odeljenje za visokotehnološki kriminal.

Takođe, Vlada Republike Srbije donela je Strategiju za borbu protiv visokotehnološkog kriminala za vremenski period od 2019. do 2023. godine.

[5] Krivični zakonik ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019)

[6] Zakon o organizaciji nadležnih državnih organa za borbu protiv visokotehnološkog kriminala ("Sl. glasnik RS", br. 61/2005 i 104/2009)

4. Pojavni oblici kompjuterskog kriminaliteta

Bavljenje kompjuterskim (sajber) kriminalom odlikuje jedna jako bitna karakteristika – anonimnost. Ista se postiže korišćenjem VPN-a (engl. Virtual Private Network - Virtuelna privatna mreža) putem interneta, pri čemu se IP adresa računara koji se koristi neće videti, već će se zapravo videti IP adresa VPN-a koji se koristi. U pojedinim državama je njegova upotreba izričito zabranjena, a krivična sankcija koja se primenjuje u slučaju kršenja ove norme jeste novčana kazna, konkretno, u Evropi reč je o Rusiji i Belorusiji.

Krađe putem interneta predstavljaju najučestaliji, odnosno najčešći vid zloupotreba korišćenjem računara. Ovaj oblik kompjuterskog kriminaliteta manifestuje se putem krađa samih računara, podataka prodiranjem u računarski sistem, mejl adresa i lozinki, identiteta, pinova kreditnih kartica, pri čemu se ukradeni podaci pojavljuju na tržištu kako bi se ostvarila protivpravna imovinska korist, takođe time se ugrožava bezbednost i privatnost trećih lica. Kako bismo se obezbedili na adekvatan način, neophodno je preduzeti određene preventivne mere kako ne bi došlo do viktimizacije. Preciznije, voditi računa gde, kako i na koji način ostavljamo lične podatke, verifikovati sve mreže koje koristimo za komunikaciju i slično. Amerika godišnje trpi jako velike novčane gubitke baš iz ovog razloga i velike količine novca dolaze u Evropu. Podneblje je takvo, da njeni žitelji u ogromnom broju slučajeva za kupovinu koriste online transakcije. Te transakcije se "presreću" pristupom hakera mejl adresi naručioca robe, pri čemu se transakcija obustavlja, a dobija se lojaliti kartica u vrednosti novčanog iznosa poručene robe, pri čemu se ista krade sa mejla i stavlja na tržište u pola cene. Napomenuta krađa identiteta ostvaruje se prisvajanjem tuđeg identiteta, zarad prevare ili izvršenja nekog drugog krivičnog dela.

Kompjuterske prevare, među kojima je najpoznatija "Nigerijska prevara", manifestuju se potražnjom da se određena svota novca uplati zarad obavljanja poslovne obaveze pri čijoj bi se zagarantovanoj uspešnosti isplatila veća novčana suma od uložene. Primer za to jesu spam mejlovi (neželjena elektronska pošta) sadržine da je neophodno obratiti se kontaktu navedenom u istom, kako bismo nasledili imovinu preminulog rođaka.

Kompjutersko falsifikovanje ispoljava se u najvećem procentu falsifikovanjem ličnih dokumenata i novca. Nije retka pojava falsifikovanja papira za prenos nepokretnosti, hartija od vrednosti, platnih kartica, trenutno aktuelnih Covid propusnica, PCR rezultata testova i slično.

Zlonamerni softveri koriste se kako bi se pomoću virusa, trojanaca, crva ili nekog drugog programa preuzeli lični podaci.

Visokotehnološki kriminal obuhvata sledeće oblike:

- Slučajnu upotrebu informacionog sistema u slučajevima kršenja poslovne i bezbednosne politike firme ili preduzimanju koraka protivno bezbednosnoj politici firme i time izlaganje sistema i podataka firme sajber napadima;

- Klasične oblike kriminala koji uključuju primenu računara ili drugih IT komunikacionih ili evidencionih sredstava kao podršku nelegalim aktivnostima;
- onlajn prevare kao što su fišing napadi, spufing, spiming, forming ili drugim oblicima dela kojima se pokušavaju prevariti lica s ciljem ostvarivanja protivpravne imovinske koristi;
- Hakerisanje, krekovanje šifara, nedozvoljeni upad u računar s svrhom krađe ili nezakonitog uvida u šifre administratorskih i drugih naloga ili s ciljem upada u računare ili informacione sisteme kako bi se vršili drugi nezakoniti akti oflajn ili onlajn; ti oblici imaju veoma značajnu perspektivu u okvirima organizovanih kriminalnih grupa;
- Pribavljanje malicioznih i distribuiranje drugih računarskih programa ili kodova, koji u sebi sadrže aktivnosti stvaranja, kopiranja i/ili ispuštanja zloćudnih programa (na primer, destruktivne ili ometajuće viruse, trojance, crve, advertajzing programe – advere, ili špijunske programe – spajvere). Piraterija (digitalna) muzike, video-zapisa (filmova);
- Sajber uznemiravanja, uznemiravanja, pretnje, intenciona izlaganja poruzi, iznude uključujući i sajber zlostavljanja;
- Onlajn proganjanja i uhođenja, kao i druga dela sajber seksualne konotacije, uključujući slanje fotografija ili tekstualnih poruka seksualne prirode, sadržajem koji promoviše seksualni turizam, ili zloupotrebu interneta u omogućavanju trgovine ljudima u seksualne ili druge svrhe, naročito u okvirima socijalnih mreža;
- Akademske prevare i naučno nedolično ponašanje studenata, nastavnog osoblja u plagiranju (preuzimanje zasluga za pisane ideje drugih lica ili druge materije), varanje na pismenim ispitima, ili lažna i fingirana istraživanja, rezultate istih ili metode;
- Organizovani kriminal koji podrazumeva zloupotrebu interneta etnički vezanih i organizovanih bandi u omogućavanju kombinovanih ilegalnih i legalnih aktivnosti kao na primer kupoprodaju ljudskih bića, njihovo krijumčarenje, ali i drugih nelegalnih roba – oružja i narkotika;
- Špijunske aktivnosti država ili slobodnjaka koji uključuju i korporativnu špijunažu vezanu za zabranjenu upotrebu špijunskih programa kao i kiloger programa u cilju otkrivanja podataka koji se imaju ukrasti ili iskoristiti u vršenju daljih kriminalnih aktivnosti;
- Kiberterorizam izvršen od strane osoba koje nameravaju da stvore „socijalne, religiozne ili političke ciljeve nanošenjem straha i panike putem oštećivanja ili ometanja kritičkih informacionih struktura“.[7]

[7] Bošković Goran (2011): *Organizovani kriminal,* Kriminalističko-policijska akademija, Beograd, str. 107-108.

Većina oblika visokotehnološkog kriminala realizuje se različitim vrstama sajber napada, koje ćemo ukratko opisati.

- Socijalni inženjering obuhvata prevaru žrtve s ciljem ostvarivanja profita ili zabave. Socijalni inženjering predstavlja sredstvo kojim lice vara druga lica koristeći različite smicalice kako bi ih primorao da nešto učine, a obično se te aktivnosti ostvaruju odlaskom na neki inficirani sajt. Ta tehnika zasniva se na ometanju pažnje (ili obmanjivanju na različite načine) određenog lica, s ciljem prikupljanja informacija, koje ono, inače, ne bi odalo, a kako bi se ti podaci kasnije zloupotrebili (radi odavanja korisničkih imena, lozinki ili, npr., podataka o platnim karticama).
- Lažno predstavljanje (spoofing) predstavlja krađu usluga od autorizovanih legitimnih korisnika, preko njihovog identifikacionog korisničkog imena i šifre. Izuzetno je značajna situacija u kojoj se na harderskim forumima tako pribavljeni podaci o ličnosti prodaju na virtuelnom kriminalnom tržištu.
- Eksploatacija softverskih rupa ili rupa u operativnim sistemima realizuje se tako što učinioci pretražuju sisteme aktivne na mreži kako bi pronašli one koji su s postojećim slabim tačkama. Posebno je interesantno angažovanje, na različite načine (prinudom, korupcijom, zloupotrebom zavisnosti od nekih oblika narkotika i sl.) IT stručnjaka za masovno pronalaženje takvih manjkavosti od strane kriminalnih organizacija.
- Tranzitni bezbednosni eksploatatori koriste sigurnosne veze između domaćina i mreža. To se ostvaruje putem klijent – server sigurnosnih protokola, između dva mrežna domaćina, tokom određene vrste kontakta i transmisije, kada postoji uzajamno poverenje. Upravo okolnost postojanja poverenja koriste hakeri za različite zloupotrebe.
- Napadi podataka odnose se na programiranje skripti ili šablona, pri čemu postoji opasnost proturanja zlćudnih kodova u sisteme. Te skripte mogu raditi kroz servere, ali i kroz korisnički računar, te tako mogu dozvoliti zlonamernima da upadnu u računar ili ubace zlćudne kodove u sistem.
- Korišćenje slabosti infrastrukture najčešće se odnosi na mrežne slabosti koje postoje u komunikacionim protokolima. Mnogi hakeri svoju stručnost koriste u zloupotrebi pronalaženja rupa u mrežnim komunikacijama, i to kao vrata za ulazak u sisteme svojih žrtava.
- Odbijanje pružanja usluga (denial of service) se sastoji od akata koji dovode do sprečavanja korišćenja sistema u planiranom kapacitetu kroz opterećivanje servera saobraćajem. Žrtvin server na taj način biva bombardovan preuzetim i posednutim IP adresama. Posebno je interesantno organizovanje i iskorišćavanje velikog broja računara u botnetovima, i posebno angažovanje organizovanih kriminalnih grupa u njihovom kreiranju i zloupotrebi u izvršenju klasičnih oblika kriminala kao što su iznude i ucene.
- Aktivno prisluškivanje se dešava u toku transmisije – poruke se presreću dok se šalju. Tom prilikom mogu se desiti dve stvari. Prvo, presretnuti podaci

mogu biti kompromitovani uništenjem podataka u paket (izmena izvora, ili destinacije IP adrese ili izmenom broja sekvenci paketa). Drugo, mogu se kopirati kako bi se kasnije koristili. [8]

5. Zaključak

Kompjuterski kriminal za sobom povlači enormne ekonomske – finansijske gubitke, kako za pojedinca, tako i za društvo u celini, narušava privatnost, nanosi materijalnu i nematerijalnu štetu specifičnim načinom delovanja kao i sredstvima za vršenje krivičnih dela. Protekom vremena, pored tradicionalnih oblika, javljaju se novi, modifikovaniji, složeniji oblici i forme, koji šire svoj geografski prostor delovanja, primenjuju se nove metode i tehnike paralelno sa tehnološkim razvojem i napretkom društva. Kako bismo u granicama normale suzbili ovaj globalni problem, odnosno smanjili postojeću tamnu brojku kriminaliteta, neophodno je reformisati postojeću zakonsku regulativu, oformiti specijalno edukovane istražne timove, osmisliti adekvatnu strategiju za borbu protiv istog, uspostaviti međunarodnu saradnju, razmeniti prikupljene informacije i dokaze, preciznije, poraditi na preventivnim merama i pooštriti krivične sankcije. To nije nimalo lak zadatak iz razloga što je gotovo nemoguće predvideti nove oblike ove vrste kriminaliteta, predvideti koji će to objekti biti budući predmet napada, predvideti buduću povezanost ovog oblika kriminaliteta sa ostalim oblicima, koje će se metode i tehnike koristiti prilikom vršenja inkriminisanih radnji i slično. Takođe, profil ličnosti samih učinilaca predstavlja dodatni problem s obzirom da ih odlikuje visok stepen inteligencije, savršeno poznavanje načina funkcionisanja računarskih programa. Posebno otežavajuća činjenica je da u velikom procentu slučajeva izvršioci ne ostavljaju dokaze prilikom vršenja krivičnog dela, pa je samim tim veoma teško njegovo otkrivanje i dokazivanje. Iznete činjenice ukazuju da je savremeno društvo prinuđeno stalno usavršavati mehanizme borbe protiv ovog oblika kriminaliteta, organizovano, kontinuirano, strategijski sa posebnim akcentom efikasnog procesuiranja koji bi obeshrabrio potencijalne izvršioce.

[8] Bošković Goran (2011): *Organizovani kriminal,* Kriminalističko-policijska akademija, Beograd, str. 111-112.

Literatura:

- Bošković, G. (2011): *Organizovani kriminal*, Kriminalističko-policijska akademija, Beograd;
- Ignjatović, Dj. (2016): *Kriminologija*, Pravni fakultet Univerziteta u Beogradu, Beograd;
- Ljiljić, S., Prlja, D. (2011): *Pravna informatika veština*, Pravni fakultet Univerziteta u Beogradu, Beograd;
- Nikolić-Ristanović, V., Konstantinović-Vilić S. (2018): *Kriminologija,* Izdavačko-grafičko preduzeće "Prometej", Beograd
- Stojanović, Z., Delić N. (2017): *Krivično pravo posebni deo*, Pravni fakultet Univerziteta u Beogradu, Beograd;
- Krivični zakonik ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019);
- Zakon o organizaciji nadležnih državnih organa za borbu protiv visokotehnološkog kriminala ("Sl. glasnik RS", br. 61/2005 i 104/2009);
- Strategija za borbu protiv visokotehnološkog kriminala za period od 2019-2023. godine;
- Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu;
- Zakon o potvrđivanju dodatnog protokola uz Konvenciju o visokotehnološkom kriminalu koji se odnosi na inkriminaciju dela rastističke i ksenofobične prirode preko računarskih programskih sistema;
- Direktiva Saveta Evropske zajednice o pravnoj zaštiti kompjuterskih programa;
- http://www.beograd.vtk.jt.rs/
- http://www.rjt.gov.rs/sr/organizacija/odeljenja/odeljenje-za-visokotehnolo%C5%A0ki-kriminal

Svetislav Lutovac
Julijana Račić

UDC 343.533::004
004.738.5.056.53

DOI: 10.5937/MegRev2104281L
Expert article
Received 12.04.2021.
Approved 15.09.2021.

COMPUTER CRIME AS A MODERN FORM OF CRIME

Abstract: *The development of technology has significantly contributed to the improvement of communication, the way of doing business of humanity, the flow and availability of information via the Internet, but it also entails negative consequences in the form of abuse by committing crimes in the field of computer security. The fight against it is very difficult, and the reason for that is the constant progress, ie modification of this form of crime, where it is necessary to change the existing legislation, achieve international cooperation, invest money in equipment suitable for adequate response to computer crime. In this paper, the emphasis is placed on the very concept of computer crime, international and domestic legislation, the forms in which it most often manifests itself.*

Keywords: *technology, computer crime.*