ОРИГИНАЛНИ НАУЧНИ РАД
doi:10.5937/zrpfni1880325G

Др Здравко Грујић,*
Доцент Правног факултета,
Универзитет у Приштини са привременим седиштем у Косовској Митровици

UDK: 343.533
Рад примљен: 30.09.2018.
Рад прихваћен: 23.10.2018.

*КОМПЈУТЕРСКИ КРИМИНАЛИТЕТ: СПЕЦИФИЧНОСТИ И САВРЕМЕНИ ИЗАЗОВИ***

Апстракт*: Криминалитет је патолошка друштвена појава, универзалног карактера. Без обзира на степен развоја и облик уређења социјалне заједнице криминалитет карактерише свеприсутност. Посматрано кроз призму историјског развоја људске цивилизације, временом се мењају појавни облици, феноменолошка обележја, обим и структура криминалитета. Процеси инкриминализације и декриминализације су динамичког карактера и нису искључиво везани за временску димензију - зависе и од степена развоја, традиције и културе, економског уређења, правног и политичког система појединих држава.*

Карактеристика постмодерног друштва у којем живимо је појава новог облика криминалног понашања - компјутерског криминалитета. Као "нужна консеквенца" дигиталног доба и примене информационих технологија у свим аспектима друштвеног живота, компјутерски криминалитет чине сви нови облици криминалног понашања који представљају последицу злоупотреба масовне употребе и коришћења нових технологија (компјутера, компјутерских система, информационо-комуникационих уређаја и технологија и глобалне мреже - Интернета), али и традиционална кривична дела која су извршена коришћењем компјутера као средства или објекта.

Нове инкриминације у кривичном законодавству Републике Србије које пружају заштиту безбедности рачунарских података представљају само део феномена компјутерског криминалитета, имајући у виду чињеницу да компјутери представљају потенцијално средство

* zdravko.grujic@pr.ac.rs

** Рад је саопштен на међународној научној конференцији „Право пред изазовима савременог доба“, која је одржана 13. и 14. априла 2018. године на Правном факултету Универзитета у Нишу.

извршења и других кривичних дела. Иако се, према типологији заступљеној у литератури, компјутерски криминалитет најчешће изучава као део имовинског криминалитета, његову специфичност и самосталност потврђује чињеница да у овај облик, поред кривичних дела имовинског карактера, спадају и дела која традиционално чине део општег, политичког, привредног или насилничког криминалитета.

Рад је посвећен анализи феномена компјутерског криминалитета и његовим специфичностима, као и изазовима на које, динамичан развој појавних облика, брисање просторних и временских граница приликом извршења, специфичан профил учинилаца, отежано пријављивање, откривање и доказивање, висока тамна бројка и масовна изложеност виктимизацији, савремено друштво мора да понуди и предложи адекватне одговоре.

***Кључне речи**: компјутерски криминалитет, безбедност рачунарских података, злоупотреба информационо-комуникационих технологија, Интернет.*

1. Уводна излагања

Криминалитет представља патолошку друштвену појаву и универзалног је карактера. Наиме, још у најстаријим историјским изворима сусрећемо се са описима разних понашања која су нарушавала основне вредности на којима је почивала људска заједница (Игњатовић, 2018: 11), а која су била предмет санкционисања. Са развојем друштва и културе мењао се број и садржај кажњивих понашања, јер криминалитет није статичан и фиксно одређен(феномен) већ се стално мења (Константиновић-Вилић, Николић-Ристановић, Костић, 2010: 23).

Промене се односе како на нове појавне облике, тако и на феноменолошка обележја, обим, структуру, стопу, етиологију криминалитета, начин друштвене реакције и систем кажњавања. Осим појаве нових облика кажњивих понашања, динамика криминалитета подразумева и изузимање одређених до тада санкционисаних понашања из надлежности кривичноправног система. Процеси уношења нових кажњивих понашања у кривично законодавство (инкриминализација) и изузимања одређених од тада санкционисаних радњи (декриминализација) су динамичког карактера и нису искључиво везани за временску или просторну димензију – детерминисани су степеном развоја друштва, традицијом и културом, економским, правним и политичким системом и уређењем. Криминалитет

представља реалност и богатих и сиромашних друштава, има различит обим, појавне облике и манифестације, али је у свим срединама фактор дестабилизације, кочница за економски, социјални и сваки други просперитет (Радуловић, 1999: 13).

Легитимност кривичноправне заштите подразумева да кривичноправна репресија и кривично право у целини морају у суштинском смислу бити оправдани и нужни. У том смислу, заштита човека и других основних друштвених вредности представља основ и границе за одређивање кривичних дела, прописивање кривичних санкција и њихову примену, а кривично право треба да буде *ultima ratio* у сузбијању друштвено опасних понашања (Стојановић, 2016: 40). Ипак, у последње време, многа кривична законодавства, нарочито кривично законодавство Републике Србије, карактерише супротан принцип –константно некритичко проширивање система инкриминација, тзв. кривичноправни експанзионизам. Уз потпуно оправдане критике експанзионизма кривичног права, у литератури се не негира потреба уношења нових инкриминација из одређених области друштвеног живота којима је кривичноправна заштита нужна и оправдана. Другим речима, критика кривичноправног експанзионизма не значи да је свака нова инкриминација неприхватљива – *ius criminale semper refomandum est*, што значи да се и врсте и обим инкриминисаних понашања мењају (Стојановић, 2010: 42).

Масовно коришћење компјутера, компјутерских система и мрежа, као и примена информационих технологија у свим аспектима савременог живота, поред неспорних предности, показала је и негативне последице кроз различите облике злоупотреба технологије и угрожавања права корисника. Рачунари и информациона технологија постали или средство за лакше или ефикасније вршење одређених кривичних дела, или су сами постали објект напада. Имајући у виду њихов значај у савременим друштвима, указала се потреба и за њиховом кривичноправном заштитом (Стојановић, 2016: 906).

Током протекле две деценије, интернет и сајбер простор (*cyberspace*)[1], у ширем смислу, имају огроман утицај на све делове и начин функционисања савременог друштва. Свакодневни живот, остваривање фундаменталних права, друштвене интеракције и економија зависе од беспрекорног функционисања информационих и комуникационих технологија.[2]

1 Сајбер простор представља "пети елемент" постмодерног друштва (Schreier, Weekes, Winkle, 2015: 14).

2 Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *Cybersecurity Strategy of the European*

Експанзија информационе технологије и аутоматизација пословних активности и процеса у свим сферама друштвеног живота представљају феномен данашњице који је савременом друштву донео безброј погодности али је створио и низ проблема и ризика, како за појединца или групе, тако и за друштво. Растућа зависност од информационе технологије условила је настајање бројних зона осетљивости са потенцијално врло озбиљним консеквенцама - савремено друштво излаже се новом ризику: осетљивости (рањивости)у информатичкој ери (Петровић, 2004: 11).

Вршење традиционалних кривичних дела коришћењем компјутера, компјутерских система и мрежа, тј. злоупотребом информационо-комуникационих средстава и технологија, и процес инкриминисања потенцијалних злоупотреба у сфери примене компјутерауказали су на потребу систематског проучавања ових инкриминација као предмета посебне врсте криминалног понашања - компјутерског криминалитета (cybercrime).

Иако су у раној фази развоја компјутери били неподобни за веће злоупотребе јер је њихово коришћење подразумевало специјалну едукацију корисника и масовност коришћења (Алексић, Шкулић, 2007: 385), рапидан пораст производње и употребе компјутера и других информационо-комуникационих средстава и технологија у овом миленијуму, развој, ширење и приступ интернету, као и поједностављено коришћење великог броја компјутерских програма потврђују постојање потенцијалне опасности од ширења различитих облика компјутерског криминалитета. То га, уједно, чини "најопаснијим" савременим обликом криминалног понашања (Бејатовић, 2012: 18), који са собом носи специфичне безбедносне изазове и ризике.[3] Информациона безбедност, стога, представља саставни део свеукупне безбедности у савременом друштву и у функцији је остваривања, поштовања и заштите права, слобода и интереса грађана, економског система и државе у целини.

Иако је, према времену настанка, компјутерски криминалитет "најновији" облик криминалног понашања (Ђорђевић, 2011: 177) активности на плану успостављања механизама кривичноправне заштите у циљу откривања, спречавања и сузбијања овог облика криминалитета одвијају се и на националном и на међународном нивоу.

Union: An Open, Safe and Secure Cyberspace. Brussels:https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf, (27.08.2018.)

3 Вид. Стратегија развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године "Службени гласник Републике Србије" број 53/2017.

Тако је у Републици Србији је изменама и допунама Кривичног закона из 2003. године[4] уведен низ инкриминација које чине део компјутерског криминалитета.[5] Важећи Кривични законик Републике Србије из 2006. године[6] садржи посебну главу кривичних дела против безбедности рачунарских података који садржи следеће инкриминације: оштећење рачунарски података и програма (чл. 298. КЗ), рачунарска саботажа (чл. 299. КЗ), прављење и уношење рачунарских вируса (чл. 300. КЗ), рачунарска превара (чл. 301. КЗ), неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (чл. 302. КЗ), спречавање и ограничавање приступа јавној рачунарској мрежи (чл. 303. КЗ), неовлашћено коришћење рачунара или рачунарске мреже (чл. 304. КЗ) и прављење, набављање, давање другом средстава за извршење кривичних дела против безбедности рачунарских података (чл. 304а КЗ). Увођењем ових инкриминација штити се коришћење информационе технологије у дозвољене сврхе, односно пружа се заштита самом функционисању информационе технологије. И овде, као и у другим областима, кривично право је супсидијарног карактера, док су по значају и ефикасности на првом месту различите технопревентивне мере које се развијају у оквиру саме информационе технологије (Стојановић, 2016: 906).

Усвајањем посебног Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала[7] утврђена је надлежност државних органа за откривање и сузбијање идругих кривичних дела која према начину извршења, употребљеном средству или објекту могу сматрати делима компјутерског криминалитета. У питању су, према систематици из Кривичног законика, кривична дела против интелектуалне својине, кривична дела против имовине, кривична дела

4 Закон о изменама и допунама Кривичног закона Републике Србије "Службени гласник Републике Србије" број 67/2003.

5 Ове године након усвајања најзначајнијег европског правног извора у овој области – Конвенције против компјутерског криминалитета Савета Европе (Будимпештанска конвенција). Convention on Cybercrime, Council of Europe, ETC No. 185, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561. Додатни протокол усвојен је 2003. године: Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systemsCouncil of Europe Treaty No. 189, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189; приступ 1. август 2018. године. Вид. Закон о потврђивању Конвенције о високотехнолошком криминалитету "Службени гласник Републике Србије – Међународни уговори" број 19/2009.

6 "Службени гласник Републике Србије"број85/2005, 88/2005 – испр., 107/2005 – испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 и 94/2016.

7 "Службени гласник Републике Србије"број61/2005 и 104/2009.

против привреде и кривична дела против правног саобраћаја, *код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци* (као и њихови производи у материјалном или електронском облику), али и кривична дела против слобода и права човека и грађанина, кривична дела против полне слободе, кривична дела против јавног реда и мира, кривична дела против уставног уређења и безбедности Републике Србије *која се због начина извршења или употребљених средстава могу сматрати кривичним делима високотехнолошкогкриминалитета*.

Утврђивањем стварне надлежности државних органа за ова кривична дела заокружен је систем инкриминација које се, подпрописаним условима, могу проучавати као садржај компјутерског криминалитета.

2. Специфичности компјутерског криминалитета и савремени изазови

2.1. Појам компјутерског криминалитета

У литератури не постоји јединствена и општеприхваћена дефиниција компјутерског криминалитета. Постоје различити приступи и схватања која полазе од тога да је компјутерски криминалитет део имовинског криминалитета (имајући у виду да су прве злоупотребе компјутерских система биле усмерене на прибављање противправне имовинске користи (Ђурђевић, Јовашевић, 2010: 176), односно део криминалитета "белог оковратника", део привредног криминалитета (у ширем смислу), посебан облик криминалитета који захтева специфичан приступ приликом проучавања, чак и схватање да се уместо проучавања као јединственог феномена исти може посматрати путем појединачних незаконитих активности чија је заједничка карактеристика улога информационо-комуникационих технологија приликом извршења кривичних дела (Yar, 2006: 9).

Неспорно је да компјутерски криминалитет у савременом друштву представља аутохтони облик криминалног понашања, имајући у виду бројне карактеристике које га разликују од осталих типова криминалног понашања, због чега је и неопходан специфичан приступ приликом његовог истраживања и проучавања. Изучавање феномена компјутерског криминалитета у оквирима нпр. имовинског или привредног криминалитета представља анахрони приступ. Вршење компјутерских кривичних дела не мора да значи и постојање намере учиниоца да прибави противправну имовинску корист или причини штету другом

јер се коришћењем и злоупотребом информационо-комуникационе технологије могу вршити разноврсна кривична дела која се традиционално сматрају делима општег, политичког, насилничког или неког другог типа криминалитета.

У домаћој литератури се указује да је проблем дефинисања компјутерског криминалитета отежан јер представља релативно нови облик криминалног понашања који се још није у потпуности издиференцирао у односу на друге облике, испољава велику феноменолошку разноврсност и постоје отежавајући фактори у дефинисању уколико се одређивање појма ослања на позитивну кривичноправну легислативу. Свеобухватна дефиниција мора се заснивати на три основна елемента: начину извршења, средству извршења и последици криминалног деловања. Стога се компјутерски криминалитет дефинише као облик криминалног понашања код кога се коришћење компјутерске технологије и информатичких система испољава као начин извршења кривичног дела или се компјутер употребљава као средство или циљ извршења, чиме се остварује нека у кривичноправном смислу релевантна последица (Алексић, Шкулић, 2007: 385).

Покушај да се дескриптивним приступом који "покрива кључне начине коришћења рачунара и све познате облике компјутерског криминалитета" дефинише компјутерски криминалитет полази од става да се под овим обликом криминалитета подразумевају недозвољене активности у којим је рачунар објект или "субјект" дела, а којима је циљ: уништење, оштећење или отуђење рачунарског система или његових компоненти; уништење, оштећење, отуђење и неовлашћена измена, објављивање или коришћење софтверских и програмских производа; уништење, оштећење, отуђење и неовлашћена измена, објављивање или коришћење података; извршавање кривичних дела; неовлашћено коришћење рачунарских ресурса и нарушавање и пробијање система заштите (Петровић, 2004: 61,62).

Потпуно прихватљиви начини дефинисања компјутерског криминалитета заступљени у нашој доктрини полазе од ширег контекста незаконитих понашања која чине садржај овог феномена, средства и циља кажњивих радњи, односно ужег, који полази од понашања забрањених кривичноправним нормама, компјутеру као јединственом систему хардвера и софтвера, начину и средству извршења и карактеристикама извршеног кривичног дела. Према првој дефиницији, компјутерски криминалитет чинесва делинквентна понашања у којима се уређаји за електронску обраду података користе као средство за постизање кажњивих радњи или као директан циљ кажњиве радње" (Бошковић, 1995: 164; Константиновић-Вилић, Николић-Ристановић, Костић, 2010:

181). Према ужој и прецизнијој дефиницији, компјутерски криминалитет представља посебан вид инкриминисаних понашања код којих се рачунарски систем (схваћен као јединство физичких јединица - хардвера - и програма - софтвера) појављује или као средство извршења или као објекат кривичног дела, уколико се дело на други начин или према другом објекту не би уопште могло извршити или би оно имало битно другачије карактеристике" (Игњатовић, 1991: 142).

Легислативно одређивање појма компјутерског криминалитета у нашем законодавству утврђено је чланом 2. став 1. Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала према којем овај облик криминалитета представља вршење кривичних дела код којих се као објекат или средство извршења јављају компјутери, компјутерски системи, компјутерске мреже, компјутерски подаци, као и њихови производи у материјалном или електронском облику (док је значење ових термина дефинисано у чл. 112. Кривичног законика).

2.2. Транснационални карактер компјутерског криминалитета

2.2.1. Просторна димензија

Специфичност компјутерског криминалитета представља недостатак уобичајене кривичноправне просторне димензије вршења радње и наступања последице кривичног дела, имајући у виду да се највећи број ових дела извршава увиртуелном (сајбер) простору. Учинилац и жртва кривичног дела могу у тренутку извршења дела бити у најудаљенијим државама, различитим континентима или временским зонама, правним системима и националним јурисдикцијама, али уколико су путем компјутера или других информационо-комуникационих уређаја повезани на глобалну мрежу (интернет) и "налазе се" у сајбер простору између њих не постоји просторна, ни временска граница (димензија). Понашање у "новом простору" и вршење кривичних дела у литератури се објашњава "теоријом транзиције простора" (Jaishankar, 2007: 7).

2.2.2. Активности на међународном плану и најважнији међународни документи

Ова чињеница је кључна за разумевање транснационалног карактераовог облика криминалитета (Schreier, Weekes, Winkle, 2015: 20)[8]и, уједно, потребе за афирмацијом заједничких активности држава и међународних

8 Односно, еволутивном облику транснационалног криминалитета. https://www.unodc.org/unodc/en/cybercrime/index.html (22.08.2018.).

организација (глобалног, регионалног или локалног карактера) у супротстављању и сузбијању компјутерског криминалитета. У том контексту, важну околност представља усвајање и примена међународних докумената (стандарда) неопходних за усаглашавање кривичноправних и других механизама заштите од овог облика криминалитета. Велики број међународних аката у овој области - резолуција, конвенција и препорука, као и имплементација њихових одредаба у национална законодавства, представља предуслов уједначавања нормативног оквира и успостављања заједничких систематских активности у борби против компјутерског криминалитета.

С обзиром на карактер овог рада, у кратким цртама ћемо указати на најзначајније акте настале у оквирима организације Уједињених нација, Савета Европе и Европске Уније, не умањујући улогу, значај и активности Интерпола, Еуропола (Европског центра за супротстављање компјутерском криминалитету -European Cybercrime Centre), Канцеларије УН за контролу наркотика и превенцију криминалитета (UNODC), Организације америчких држава (OAM), Међународне телекомуникационе уније (ITU), Европске агенције за безбедност мрежа и информационих система(ENISA) и других организација.

На VIII Конгресу УН о превенцији криминалитета и поступању са преступницима 1990. године усвојена је Резолуција о компјутерском криминалитету, која се сматра значајним актом УН у овој области.[9] Генерална скупштина УН је 2000. године усвојила Резолуцију о борби против злоупотребе информационих технологија,[10] која је ревидирана 2001. године, а наредне, 2002. године у посебној резолуцији државе су позване да приликом својих активности уваже резултате рада Комисије за превенцију криминалитета и кривично правосуђе. Економско-социјални савет УН је 2007. године усвојио резолуцију (2007/20) у којој се указује на пораст стопа транснационалног криминалитета и употребе информационо-комуникационих технологија у извршењу кривичних дела. Значајна је и резолуција Генералне скупштине УН из 2010. године (A/RES/65/230) због формирања међувладине експертске групе која би се бавила питањима заштите од компјутерског криминалитета, у складу са ставовима из Салвадорске декларације усвојене на XII Конгресу УН за превенцију криминалитета и кривично правосуђе.

9 https://digitallibrary.un.org/record/1296532/files/a-conf-144-28-rev-1-e.pdf (21.08.18.)

10 UN A/RES/55/63 Resolution on combating the criminal misuse of information technologies,http://repository.un.org/handle/11176/152207 (21.08.18.)

Савет Европеје организација која је на овом пољу усвојила бројне и значајне акте, међу којима посебну важност у овом пољу имају Препорука о пиратерији у области ауторских и сродних права (Recommendation No. R (88) 2) из 1988. године, Препорука о криминалитету повезаном са компјутерима (Recommendation No. R (89) 9) из 1989. године којом се позивају државе чланице да размотре инкриминисање и питање потребе кажњавања за компјутерска кривична дела, утврђујући при том смернице законодавцима које се односе на начин дефинисања кривичних дела компјутерског криминалитета. Од посебне важности су Конвенција о заштити појединаца у вези са аутоматском обрадом личних података из 1981. године,[11] Конвенција о заштити деце од сексуалне експлоатације и сексуалног злостављања,[12] Конвенција о спречавању тероризма,[13] а нарочито Конвенција о компјутерском криминалитету (Будимпештанска конвенција) из 2001. године[14] и њен додатни протокол који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко компјутерских система.[15]

У оквирима ЕУ усвојен је већи број аката који се односе на борбу против компјутерских кривичних дела, међу којима је од посебног значаја неколико докумената: Оквирна одлука о борби против превара и фалсификовања безготовинским средствима плаћања из 2001. године (Framework Decision combating fraud and counterfeiting of non-cash means of payment), дефинише незаконита понашања које државе чланице морају инкриминисати као компјутерска кривична дела; Директива о електронској приватности (Directive 2009/136/EC)из 2002. године се односи на сигурност услуга и поверљивости података о корисницима коју морају обезбедити пружаоци услуга електронских комуникација; Директива о борби против сексуалне експлоатације деце на интернету и дечије порнографије из 2009. године (Directive 2011/92/EU), као и Директива о нападима на информационе системе из 2013. године (A Directive on attacks against information systems).[16]

11 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (21.08.2018.)

12 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201(21.08.2018.)

13 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196(21.08.2018.)

14 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (21.08.2018.)

15 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189 (21.08.2018.)

16 https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en (21.08.2018.)

2.3. Етиолошки аспект компјутерског криминалитета (специфичност криминогених фактора)

У криминолошкој литератури се појам криминогени фактори употребљава са циљем да се помоћу њега истакну елементи који у погледу криминалитета имају првенствено етиолошки значај. Појму криминогени фактор се придаје значење које обухвата све везе које се на било који начин успостављају између криминалитета као индивидуалне или масовне појаве и разних околности објективног и субјективног карактера (Милутиновић, 1990: 300).

Питање етиологије компјутерског криминалитета је веома сложено, недовољно теоретски приказано и емпиријски истражено. Несумњиво је да велики број емпиријски потврђених криминогених фактора који утичу на појаву криминалитета уопште утичу и на овог облика криминалитета, као и да постоје специфични фактори који утичу на криминогенезу компјутерског криминалитета.

У литератури се истиче да се криминогени фактори компјутерског криминалитета могу поделити у две групе: криминогене факторе (у ширем смислу) који погодују, односно подстичу настајање, ширење и интензитет ове врсте криминалитета и оне (у ужем смислу) који непосредно утичу на извршиоца компјутерског криминалног дела. У ширем смислу, криминогене факторе који подстичу овај облик криминалитета спадају: технолошки развој, преузимање функција, концентрација података, нови амбијент деловања, нове вредности, нове форме старих вредности, нове временске границе, нове просторне границе, богатство избора, нове криминалне методе и технике, стабилност ризика, неосетљивост на величину, паралелне акције, инжењерско планирање, повећање моћи појединца, ширење информатичке писмености, глорификација компјутерских криминалаца, информатичка етика, законска регулатива и заштита. У ужем смислу, криминогени фактори који утичу на извршиоце компјутерских кривичних дела су мотив (финансијски разлози, економска конкуренција, милосрђе, технички синдром, феномен ситуације, лични став, лош пример, емотивни разлози, ментални проблеми, карактерне црте, идеологија, политика и етички кодекс), спремност и могућност (Петровић, 2004: 63-128).

У домаћој литератури је представљена и подела на егзогене и ендогене факторе компјутерског криминалитета. Егзогене криминогене факторе представљају брзина развоја информационе технологије, број корисника, информатичка неписменост, несналажење и неприлагођавање новонасталим технолошким променама, непостојање свести о безбедносним ризицима

коришћења интернета, анонимност (псеудоанонимност) корисника, несклад између нормативног и реалног, неадекватна техничка опремљеност и недовољно познавање начина функционисања уређаја, заштита информационих система, кадровски и материјални проблеми органа надлежних за спречавање овог облика криминалитета и недостатак едукације о безбедности на интернету. Ендогени фактори представљени су ефектом *on line* дезинхибиције (која се манифестује у шест тачака: дисоцијативна анонимност, невидљивост, асинхроност, дисоцијативна имагинација, солипсистичка интројекција и минимизирање ауторитета), али је указано и на жељу за злостављањем и успостављањем моћи над другим, синдром зависности од интернета и недостатком самоконтроле као унутрашњим факторима који доводе до појаве компјутерског криминалитета. (Вилић, 2016: 240-244).

2.4. Профил извршилаца кривичних дела компјутерског криминалитета

Први облици злоупотреба компјутера и компјутерских система повезани су са извршиоцима који су поседовали посебна знања и вештине за коришћење система због чега се овај облик криминалитета сматрао делом криминалитета "белог оковратника". Пар деценија након појаве првих злоупотреба компјутерских система карактерише масовна производња, коришћење, симплификована употреба великог броја информационо-комуникационих уређаја, повезаност путем глобалне мреже, "настањеност" у сајбер простору и доступност најразличитијих информација и података који могу бити средство или објект инкриминисаних понашања. То, уједно, значи да је број потенцијалних извршилаца пропорционалан броју корисника информационих система, чиме се усложњава проблем њихове типологије. С обзиром на број појавних облика и феноменолошке карактеристике компјутерског криминалитета, али и мотиве извршења кривичних дела не може се говорити о јединственом профилу извршиоца. Може се извршити систематизација извршилаца у три основне групе: аматери, професионални извршиоци и хакери (Димовски, 2010: 208).

Групи аматера припадају појединци који најчешће имају легално занимање али из различитих разлога се повремено упуштају у криминалну активност. Њихова структура није монолитна, из ње је могуће издвојити карактеристичне узроке: слаби и подложни појединци (пружена им је могућност да нешто украду или проневере једноставно због тога што су инструменти контроле недовољни и неефикасни; у питању су слабе личности или слабих инструмената контроле); људи са пороком и

фрустрирани појединци - незадовољни, разочарани, огорчени (Петровић, 2004: 333, 334).

Професионални криминалци су особе који је једно од главних занимања бављење криминалом. У овом послу имају богато искуство и знање, због чега представљају значајну друштвену опасност а карактерише их и велика адаптивност на нове ситуације, пре свега оне које настају као последица технолошког развоја. У организационом смислу, професионални криминалци наступају појединачно, у групама или организацијама, а сваки од ових облика има специфичне карактеристике. Криминалци индивидуалци наступају самостално и независно у реализацији својих циљева, у неким ситуацијама могу сарађивати са другима, углавном повремено и ради реализације конкретног криминалног дела, немају дугорочну стратегију и разрађену тактику због чега им је потенцијал за вршење кривичних дела релативно ограничен. Организоване групе представљају скупове појединаца са заједничким интересима и деловањем, потенцијал за вршење кривичних дела им је знатно већи у односу на индивидуалног криминалца. Криминалне организације представљају највиши структурални облик криминалне активности које карактерише чврстина организације, хијерархијски односи строга дисциплина, послушност и лична лојалност, уз изграђену дугорочну стратегију и детаљно разрађену тактику (Петровић, 2004: 335, 336).

Хакери представљају специфичну групу интернет или сајбер криминалаца чија основна активност подразумева противправни упад у компјутерске системе или мреже, док свака даља зависи од намере хаковањакомјутерског система, односно специфичног профила хакера. Иако је крајем шездесетих и седамдесетих година XX века појам хакер подразумевао особу (”компјутерску мудрицу”) која поседује знања о компјутерима и има вештине и жељу за истраживањем и унапређивањем компјутерских система, деценију касније, активности које су до тада имале најчешће случајни или добронамерни карактер, хаковање (хакинг) битно мења своју садржину, актере, циљеве и последице и постаје претња сваком компјутерском систему, појединцима, организацијама, али и државама (Вилић, 2016: 103). У односу на намере извршења противправног упада у компјутерске системе, хакери се могу класификовати на креативце (који хаковање схватају као истраживање, стручно усавршавање, интелектуални изазов, забаву, самодоказивање, без икаквих злих намера и негативних последица илегалних активности), деструктивце (којима хаковање представља могућност за испољавање сопствене фрустрације и агресивности, чија је активност вандалистичка и своди се на безразложно уништавање и модификацију нападнутих система) и криминалце (чији

је основни мотив да своја знања из области компјутерских технологија користе за остваривање противправне имовинске користи) (Петровић, 2004: 348-350).[17]

2.5. Пријављивање, пресуђивање и тамна бројка компјутерског криминалитета

У литератури је заступљено мишљење да данас компјутерски криминалитет представља "најопаснији" облик криминалног понашања имајући у виду потенцијалне последице криминалне активности у сајбер простору по појединце, организације (локалног, регионалног и глобалног карактера), привредне субјекте и корпорације, државне огране, економске, монетарне и фискалне системе, али и правне системе у целини. Потецијална угроженост и вулнерабилностна глобалној мрежи и сајбер простору већ дуго није на нивоу националног, него наднационалног проблема. Безбедност информационо-комуникационих система и технологија представља основ заштите функционисања држава и заштите права свих грађана, али и она представља феномен ширег, глобалног, карактера.

Полазећи од претходне констатације може се претпоставити овај облик криминалитета има све већу заступљеност у укупној стопи криминалитета, нарочито у делу који се односи на структуру пресуђеног криминалитета. Претпоставка је и да је велики број пријављених кривичних дела, имајући у виду број корисника компјутера и глобалне мреже, а отвара се и питање тамне бројке компјутерског криминалитета.

Међутим, анализа података о инкриминацијама које се односе само на безбедности рачунарских података (глава XXVII КЗ) у Републици Србији, у

17 Да би се разумеле активности хакера на мрежи навешћемо пример који се догодио у нашој земљи ове године. Наиме, у полицијској акцији у којој су учествовале полиције Холандије, Велике Британије, Хрватске, Канаде, Сад, Немачке, Шпаније, Хонгконга, Шкотске, Италије и Аустралије, полиција је на територији Републике Србије ухапсила М.Ј. (19) и Д.В (21) због сумње да су били администратори сервиса Webstresser који је сматран на највеће светско криминално тржиште за изнајмљивање тзв. DDoS напада, са више од 136.000 регистрованих корисника и више од четири милиона напада изведених до априла 2018. године на разне интернет домене из целог света. Напади су циљали критичне *on line* услуге које нуде банке, државне институције и полицијске снаге, као и индустрију игара на интернету. Нападачи су преко интернета управљали повезаним рачунарима са циљем да усмере огромну количину интернет саобраћаја на циљане web-локације и *on line* платформе. Са овим криминалним сервисом било који регистровани корисник са мало или нимало техничког знања могао би да плати одређену новчану накнаду, користећи системе плаћања путем интернета или криптовалута, и оствари циљани напад на жељени интернет портал или сервис. Извор: www.politika.rs (26.04.2018.)

периоду од 2007-2016 године, односно само дела феномена компјутерског криминалитета, не потврђују претходну претпоставку, напротив. Број пријављених кривичних дела, оптужених и осуђених лица не може се сматрати већим од симболичног.

Наиме, у посматраном десетогодишњем периоду поднето је укупно 202 кривичне пријаве за кривична дела против безбедности рачунарских података (Табела 1). Укупан број оптужених лица је 70, док је укупно осуђено 45 лица. Од тог броја изречена је 31 условна осуда, 3 новчане казне и 11 казни затвора (само три у трајању дужем од 2 године) (Грујић, Благић, 2018: 307-310).

Година	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**
Пријављена кр. дела(XXVII КЗ)	8	25	45	20	22	15	28
Оптужена лица	3	10	6	4	10	6	6
Осуђена лица	2	5	4	4	4	5	4
Осуђени на казну затвора	1	2	-	-	1	4	1

Година	**2014**	**2015**	**2016**	**Укупно**
Пријављена кр. дела(XXVII КЗ)	9	14	16	**202**
Оптужена лица	17	3	12	**70**
Осуђена лица	8	2	7	**45**
Осуђени на казну затвора	1	-	1	**11**

Табела 1. Кривична дела против безбедности рачунарских података (број пријава, оптужења, осуда, осуда на казну затвора)

Извор података: *Републички завод за статистику*

Овакав приступ указује на једну од две претпоставке: да нема значајнијег учешћа ове групе кривичних дела у укупној стопи криминалитета или да је велика тамна бројка криминалитета услед непријављивања дела од стране жртава, отежаног откривања, недовољне активности и оспособљености државних органа надлежних за откривање, доказивање, процесуирање и пресуђивање ове врсте криминалитета, и сл. Иако у домаћој литератури недостају емпиријска истраживања у овој области, мишљења смо да је, ипак, имајући у виду масовну изложеност виктимизацији корисника

компјутерских система и информационо-комуникационих мрежа, компјутерски криминалитет облик криминалног понашања којег карактерише највећа тамна бројка криминалитета. Једна од претпоставки која се наводи у литератури је да је однос откривених и неоткривених дела код активности хакера 1:10000 (Игњатовић, 2018: 56).

2.6. Масовна изложеност виктимизацији и угрожавање основних људских права

Специфичност феномена компјутерског криминалитета представља и масовна изложеност виктимизацији корисника компјутера, компјутерских мрежа, интернета као глобалне мреже и других информационо-комуникационих уређаја и система. Наиме, ни код једног од облика криминалног понашања степен виктимизираностии вулнерабилности није толико изражен као код компјутерског криминалитета.

Без обзира на системе заштите компјутерских система и мрежа, повезивање на глобалну мрежу отвара просторне и временске димензије између потенцијалног извршиоца и жртве компјутерског кривичног дела. Масовна производња различитих информационо-комуникационих уређаја и њихова доступност свим слојевима друштва у савременом свету, поједностављена употреба великог броја система и програма, приступ и коришћење Интернета као основ свакодневног функционисања појединца, друштва, економије, држава и глобалне заједнице, друштвене мреже као услов комуникативности, "настањеност" у сајбер простору, доступност информација, манипулација информацијама и садржајем,откривање или угроженост личних података, недостатак свести и знања о системима и потреби заштите, као и читав низ других околности указују да је сваки корисник компјутерских или информационо-комуникационих система потенцијална жртва кривичног дела компјутерског криминалитета.[18]

У погледу угрожености основних људских права важно је указати на појединачна права грађана загарантована међународним документима (и националним законодавствима савремених држава) која могу бити угрожена или повређена активностима које чине садржај феномена компјутерског криминалитета. Наиме, злоупотребе информационо-комуникационих система и компјутерске технологије могу да угрозе читав низ основних људских права, односно: право на слободу и људског

18 Студија о коришћењу информационо-комуникационих технологија у 2017. години у Републици Србији показала је да 68.1% домаћинстава поседује компјутер, од чега је 68% било повезано на интернет. http://publikacije.stat.gov.rs/G2017/PdfE/G20176006.pdf, (01.05.2018.).

достојанство (злоупотребе технологија кроз електронско надзирање корисника, коришћење личних података и идентификационих докумената корисникаод стране владиних тела и агенција), право на заштиту од дискриминације (сајбер расизам, "компјутерска зависност"), право на слободу мишљења и изражавања (надзор над базама података, надзирање информационо-комуникационих уређаја, напад на оперативни систем или уређаје, забрана приступа одређеним on line садржајима), право на личну безбедност и забрана нехуманих облика кажњавања (електронски надзор, имплантирање електронских чипова у тело, биометријска идентификација), право на правично суђење и угрожавање претпоставке невиности (откривање лозинки и криптованих шифри корисника, коришћење електронских доказа на суду, преправљање електронских доказаи ограничавање приступа одређеним интернет садржајима), право на имовину и интелектуалну својину (дигитална пиратерија, компјутерска хаковања, електронска шпијунажа), право на приватност (електронско надзирање, надзор над базама података, електронска трговања, нежељене понуде за пласман производа), право на живот (сајбер тероризам и смртна казна за кривична дела компјутерског криминалитета), право кандидовања на изборима и право гласања (*on line* индоктринација, дигитални монополи, напад на приватност корисника, надзор над електронским системом гласања, електронско надзирање) (Smith, 2007: 170, 171).

3. Закључна разматрања

Компјутерски криминалитет представља најновији облик криминалног понашања који је настао као последица злоупотреба компјутера, компјутерских система и мрежа и других информационо-комуникационих уређаја, али и противправних активности у сајбер (виртуелном) простору. Иако се у основним типологијама криминалитета проучавао у оквирима имовинског, криминалитета "белог оковратника" или привредног криминалитета, различитост појавних манифестација, инкриминисање компјутерских кривичних дела и одређивање "традиционалних" кривичних дела која према начину или средству извршења могу бити сматрана делом овог облика криминалитета, систематско и научно проучавање овог феномена захтев приступ компјутерском криминалитету као посебном, аутохтоном, облику криминалног понашања. У раду смо покушали да укажемо на најважније специфичности овог облика криминалитета, које уједно представљају изазове савременог друштва на плану његовог спречавања и сузбијања.

Основна специфичност је појмовно дефинисање компјутерског криминалитета јер се кроз њега одређује и садржај самог феномена. Иако у литератури, најзначајним међународним и националним изворима права не постоји јединствена дефиниција компјутерског криминалитета, представили смо оне које сматрамо значајним и одредили се према онима које сматрамо потпуно прихватљивим. Транснационални карактер компјутерског криминалитета приказали смо кроз указивање на недостатак класичне просторне димензије вршења радње и наступања последице, као и на брисање временских граница између извршиоца и жртве компјутерских кривичних дела. Имајући у виду транснационални карактер, приказали смо најзначајније међународне акте у овој области и указали на потребу заједничких активности на међународном плану. Посебности компјутерског криминалитета представљају и криминогени фактори, ендогени и егзогени, поред емпиријски потврђених који утичу на криминогенезу криминалитета уопште. Профилисање извршиоца кривичних дела компјутерског криминалитета је од посебне важности за разумевање феномена овог облика криминалитета, али и за планирање и активности на његовом сузбијању и спречавању. Незнатан број пријављених кривичних дела компјутерског криминалитета, више него симболичан број оптужених и осуђених лица у Републици Србији представљају индикаторе за другачију активност органа формалне социјалне контроле и потврђују претпоставку о великој тамној бројци компјутерског криминалитета. Масовна изложеност виктимизацији и вулнерабилност корисника компјутерских система и мрежа, "настањеност" у сајбер простору потврђују мишљење да компјутерски криминалитет представља "најопаснији" облик криминалног понашања у савременом свету.

Представљене специфичности и савремени изазови које условљава развој компјутерског криминалитета, свакако, захтевају посебан приступ њиховом проучавању. Емпиријска истраживања свих наведених, али и других специфичности овог облика криминалитета, предуслов су за разумевање и објашњење овог феномена, али и за планирање активности усмерених на спречавању и сузбијањукомпјутерског криминалитета.

Литература/References

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Council of Europe Treaty No. 189, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189;

A/RES/55/63 UN Resolution on combating the criminal misuse of information technologies,http://repository.un.org/handle/11176/152207 (21.08.18.)

Алексић, Живојин; Шкулић Милан; (2007). *Криминалистика.* Београд: Службени гласник;

Бејатовић, Станко; (2012). Високотехнолошки криминал и кривичноправни инструменти супростављања. *Сузбијање криминала и европске интеграције, с освртом на високотехнолошки криминал.* Бања Лука: Висока школа унутрашњих послова;

Бошковић, Мило; (1995). *Криминологија и социјална патологија*. Нови Сад: Матица Српска;

Вилић, Вида; (2016). *Повреда права на приватност злоупотребном друштвених мрежа као облик компјутерског криминалитета.* Докторска дисертација. Ниш;

Grujić, Zdravko; Blagić Dragan; (2018).Incriminationsagainstsecurityagainstsecurityofcomputer data – Effectivenessofcriminaljusticemechanismdirected on cybercrime. Internationalscientificconference"ArchibaldReissDays" ThematicConferenceProceeddingsofInternationalSignificance, Tom I. Belgrade: AcademyofCriminalisticand Police Studies;

Димовски, Дарко; (2010). Компјутерски криминалитет. *Зборник радова Правног факултета.* Ниш: Правни факултет;

Ђурђевић, Војислав; Јовашевић, Драган; (2010). *Кривично право – посебни део*, Београд: Номос;

Ђорђевић, Ђорђе; (2011). *Кривично право – посебни део.* Београд: Криминалистичко-полицијска академија;

Закон о изменама и допунамаКривичногзаконаРепубликеСрбије "Служб енигласникРепубликеСрбије" број 67/2003;

Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала "Службени гласник Републике Србије" број 61/2005 и 104/2009;

Закон о потврђивањуКонвенције о високотехнолошкомкриминалитету "СлужбенигласникРепубликеСрбије – Међународниуговори" број 19/2009;

Игњатовић, Ђорђе; (2018). *Криминологија*. Београд: Правни факултет – Центар за издаваштво и информисање;

Игњатовић, Ђорђе; (1991). Појмовно одређење компјутерског криминалитета. *Анали Правног факултета.* Београд: Правни факулет;

Jaishankar, Karuppannan; (2007). Establishing a TheoryofCyberCrimes. *InternationalJournalofCyberCriminology*, Vol. 1 (2).https://www.cybercrimejournal.com/ editorialijccvol1is2.htm (21.08.2018.);

Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Brussels:https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf, (27.08.2018.);

Константиновић-Вилић Слободанка; Николић-Ристановић Весна; Костић, Миомира. (2010). *Криминологија*. Београд: ИГП Прометеј;

Кривични законик Републике Србије "Службени гласник Републике Србије" број 85/2005, 88/2005-испр., 107/2005-испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 и 94/2016;

Милутиновић, Милан; (1990). *Криминологија.* Београд: Савремена администрација;

Петровић, Слободан; (2004). *Компјутерски криминал.* Београд: Војноиздавачки завод;

Радуловић, Љиљана; (1999). *Криминална политика (политика сузбијања криминалитета).* Београд: Центар за публикације Правног факултета;

Билтени 629, 613, 603, 588, 576, 558, 546, 529, 514, 502.Пунолетни учиниоци кривичних дела у Републици Србији. (2008-2017).Београд: Републички завод за статистику;

Smith, Russell; (2007). Crime Control in the Digital Age: An exploration of Human Rights Implications. *International Journal of Cyber Criminology.* Vol. 1 (2).http://www.cybercrimejournal.com/rusellijccvol1is2.htm, (21.08.2018.);

Стојановић, Зоран; (2016). *Коментар Кривичног законика.* Београд: Службени гласник;

Стојановић, Зоран; (2016). Кривичноправни експанзионизам и законодавство Србије, Тематска монографија: *Стање криминалитета у Србији и правна средства реаговања, IV део,* (прир. Игњатовић, Ђ.). Београд: Правни факултет;

Стратегија развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године "Службени гласник Републике Србије" број 53/2017;

Schreier, Fred; Weekes, Barbara; Winkle, H. Theodor (2015). *Cyber Security: The Road Ahead*. DCAF Horizon 2015 Working paper No. 4. Geneva: The Geneva Centre for the Democratic Control of Armed Forces.

https://digitallibrary.un.org/record/1296532/files/a-conf-144-28-rev-1-e.pdf (21.08.18.);

http://publikacije.stat.gov.rs/G2017/PdfE/G20176006.pdf, (01.05.2018.)

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (21.08.2018.);

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201(21.08.2018.);

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196(21.08.2018.);

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (21.08.2018.);

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189 (21.08.2018.);

https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en (21.08.2018.);

Convention on Cybercrime, Council of Europe, ETC No. 185, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561;

Yar, Majid; (2006). *Cybercrime and Society.* London, Thousand Ouks, New Delhi: Sage Publications;

Zdravko Grujić. LL.D.
Assistant Professor,
Faculty of Law, University of Priština (Head Office in Kosovska Mitrovica)

CYBERCRIME: SPECIFICITY AND CONTEMPORARY CHALLENGES

Summary

Crime is a pathological social phenomenon of a universal character. Regardless of the degree of development and the form of organization of social community, crime is omnipresent. Viewed through the prism of the historical development of human civilization, the phenomenological features, forms and structure of crime changed over time. In addition to the existing incriminations, new forms of crime appear; concurrently, crimes that have been incriminated for a certain period cease to be prohibited and/or sanctioned. These processes are dynamic and not exclusively related to the temporal dimension; they depend on the level of development, tradition and culture, economic, legal and political system of individual states.

The characteristic of the contemporary post-modern society is the emergence of a new form of criminality – cybercrime. As an inevitable consequence of the digital age and the application of information technologies in all aspects of social life, cybercrime entails new forms of criminal behavior resulting from the mass use and abuse of new technologies (computers, computer systems, electronic communication devices, the global network - Internet), as well as traditional offenses committed by using a computer.

The provision of new criminal offences envisaged to provide protection of computer data security are only a small part of efforts to counteract cyber crime, particularly given the fact that computers are a potential tool for the execution of other criminal offenses. According to typology provided in the criminal law literature, cybercrime is most often studied as part of crimes against property. However, in addition to property-related criminal offences, the distinctive features and autonomy of the committed crimes show that cybercrime includes criminal offences which are traditionally part of general, political, economic or violent crimes.

The paper provides analysis of the phenomenon of cybercrime and its specific features. The author discusses the challenges that have to be addressed by the modern society: the dynamic development of ample forms of cybercrime, the erosion of spatial and temporal boundaries in execution of these crimes, the specific profile of the perpetrators, the problems in detecting and proving these crimes, the high "dark figure" and the massive exposure to victimization. The contemporary society has to provide an adequate response to all these issues.

Keywords*: cybercrime, computer data security, abuse of information technology, Internet.*