УНИВЕРЗИТЕТ У НИШУ
ПРАВНИ ФАКУЛТЕТ

Компјутерски криминалитет

(мастер рад)

Ментор
Проф. др Дарко Димовски

Студент
Драгана Стојковић
Бр. индекса: М018/24-УП

Ниш, 2026. године

САДРЖАЈ

УВОД 1
I ТЕОРИЈСКО-КРИМИНОЛОШКИ ОСНОВИ КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА 5
1.1. Појам компјутерског криминалитета 5
1.1.1. Дефиниција компјутерског криминалитета 5
1.1.2. Правна природа и место компјутерског криминалитета у систему криминалитета 6
1.2. Историјски развој компјутерског криминалитета 7
1.3. Основне карактеристике компјутерског криминалитета 10
1.4. Класификација компјутерског криминалитета 12
II ЕТИОЛОШКЕ И ФЕНОМЕНОЛОШКЕ КАРАКТЕРИСТИКЕ КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА 13
2.1. Узроци компјутерског криминалитета 13
2.2. Циљеви и мотиви извршилаца 15
2.3. Начини извршења и злоупотреба информационих технологија 16
2.4. Последице компјутерског криминалитета 19
2.5. Врсте и типологија извршилаца 20
2.5.1. Аматери 20
2.5.2. Професионални криминалци 21
2.5.3. Хакери 22
III НОРМАТИВНИ ОКВИР 23
3.1. Међународна регулатива 23
3.1.1. Конвенција Савета Европе о сајбер криминалу 23
3.1.2. Допунски протоколи уз Конвенцију Савета Европе о сајбер криминалу . 24
3.2. Република Србија 24
3.2.1. Кривични законик 24
3.2.2. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала 25
3.2.3. Остали прописи 27
IV ОБЛИЦИ КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА 29
4.1. Компјутерска (рачунарска) крађа 29
4.1.1. Крађа идентитета 30
4.1.2. Крађа података 32
4.1.3. Крађа лозинки, кодова и идентификационих бројева 33
4.1.4. Савремени облици компјутерске крађе (фишинг, злоупотребе система и др.) 34
4.2. Компјутерска (рачунарска) превара 36
4.2.1. Нигеријска превара 37
4.2.2. Преваре ауторитета 38
4.2.3. Спам преваре 39
4.2.4. Преваре са наградама 40
4.2.5. Преваре са злонамерним апликацијама 40
4.2.6. Преваре из области електронског банкарства 41
4.3. Компјутерска (рачунарска) саботажа 42
4.4. Компјутерски (рачунарски) тероризам 44
4.5. Компјутерска (рачунарска) порнографија 44
4.6. Дипфејк 46
V ПРЕВЕНЦИЈА И СУЗБИЈАЊЕ КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА 47

5.1. Друштвена контрола 47
5.2. Улога институција 49
5.3. Међународна сарадња 51
ЗАКЉУЧАК 52
СПИСАК КОРИШЋЕНЕ ЛИТЕРАТУРЕ 54
СПИСАК ИСТРАЖИВАЧКЕ ГРАЂЕ 55
РЕЗИМЕ 59
SUMMARY 61
БИОГРАФИЈА 63

УВОД

Савремено друштво обележено је интензивним развојем информационо-комуникационих технологија (скр. ИКТ), које су у значајној мери измениле начин функционисања државних институција, привредних субјеката и свакодневног живота појединаца. Дигитализација је омогућила бржи проток информација, развој електронске трговине, електронске управе и нових облика комуникације, чиме су рачунарски системи и интернет постали неизоставан део савременог друштва. Истовремено, технолошки напредак створио је и нове могућности за вршење различитих противправних радњи, које се све чешће реализују у дигиталном окружењу и уз употребу савремених технолошких средстава.

У условима све веће зависности друштва од информационих система, појављује се компјутерски криминалитет као специфичан облик криминалитета који обухвата кривична дела усмерена против рачунарских система, података и мрежа, као и кривична дела која се врше употребом информационих технологија као средства извршења. [1] За разлику од традиционалних облика криминалитета, компјутерски криминалитет карактеришу висока техничка софистицираност, транснационални карактер, могућност анонимног деловања и велика брзина извршења.[2] Управо наведене особености отежавају откривање извршилаца, прикупљање доказа и ефикасно кривично гоњење, због чега ова појава представља један од најзначајнијих безбедносних и правних изазова савременог доба.

Развој интернета, дигиталних платформи, технологије „рачунарства у облаку“[3] и система заснованих на вештачкој интелигенцији (енгл. *artificial intelligence - AI*), допринео је појави нових и све сложенијих облика компјутерског криминалитета. Данас се међу најзаступљенијим облицима јављају неовлашћени приступ рачунарским системима, крађа и злоупотреба података, компјутерске преваре, фишинг напади (енгл. *phishing*), [4] малвери (енгл. *malware*), [5] рансомвер напади (енгл. *ransomware*), [6]

---

[1] Д. Димовски, Компјутерски криминалитет, *Зборник радова Правног факултета у Нишу*, бр. 55, 2010, стр. 197.

[2] Ј. Матијашевић, С. Игњатијевић, Компјутерски криминалитет у правној теорији, појам, карактеристике, последице, *INFOTEH-JAHORINA* Vol. 9, Ref. E-VI-8, p. 852-856, March 2010, стр. 853.

[3] Рачунарство у облаку (енгл. *cloud computing*) представља модел који корисницима омогућава приступ дељеним рачунарским ресурсима (попут простора за складиштење података, сервера или апликација) путем интернета. S. Susnjara, I. Smalley, „What Is Cloud Computing?”, IBM Think. Преузето: 27.6.2026. https://www.ibm.com/think/topics/cloud-computing

[4] Фишинг (енгл. *phishing*) је врста сајбер напада која користи лажне имејлове, СМС поруке, телефонске позиве или веб-странице како би се људи преварили да поделе осетљиве податке, преузму злонамерни софтвер или се изложили сајбер криминалу. Ови напади су облик социјалног инжењеринга јер користе људску грешку, лажне приче и тактике притиска како би манипулисали жртвама. Према подацима из

злоупотреба дигиталних идентитета, као и различити облици незаконитог садржаја на интернету. Посебан изазов представљају савремене технологије засноване на вештачкој интелигенцији, које поред бројних друштвених користи могу бити злоупотребљене за вршење кривичних дела, што потврђује све чешћа употреба дипфејк (енгл. d*eepfake)* технологије[7] у сврху превара, уцена и манипулације информацијама.

Последице компјутерског криминалитета не огледају се искључиво у материјалној штети коју трпе физичка и правна лица. Оне могу обухватити нарушавање приватности, повреду права на заштиту података о личности, угрожавање безбедности информационих система, нарушавање пословног угледа привредних субјеката, али и угрожавање критичне инфраструктуре и националне безбедности.[8] Због тога су државе широм света последњих деценија посветиле посебну пажњу развоју нормативних и институционалних механизама за превенцију, откривање и сузбијање овог облика криминалитета.

У Републици Србији нормативни оквир за борбу против компјутерског криминалитета чине, пре свега, *Кривични законик* [9] и *Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала*,[10] уз примену бројних међународних инструмената, међу којима посебно место заузима *Конвенција Савета Европе о сајбер криминалу* (енгл. *Convention on Cybercrime*), позната као *Будимпештанска конвенција*,[11] која је код нас ратификована 2009. године.[12]

IBM извештаја, фишинг је најчешћи узрок пробијања података, чини 15% свих инцидената и просечно кошта организације 4,88 милиона долара. Више о томе доступно на: M. Kosinski, „What Is Phishing?," IBM Think. Преузето: 2.7.2026. https://www.ibm.com/think/topics/phishing

[5] Малвер (енгл. *malware*, од *malicious software* - злонамерни софтвер) јесте заједнички назив за сваки програм или код који је намерно креиран да оштети рачунарски систем, украде податке или нанесе штету кориснику. Више о томе доступно на: „What Is Malware?," IBM Think. Преузето: 27.6.2026. https://www.ibm.com/think/topics/malware

[6] Рансомвер (енгл. *ransomware* - откупни софтвер) је врста злонамерног програма који закључава податке или рачунарски систем корисника, а за њихово откључавање захтева исплату откупнине. Више о томе доступно на: M. Kosinski, S. Susnjara, M. Goodwin, „What Is Ransomware?", IBM Think. Преузето: 27.6.2026. https://www.ibm.com/think/topics/ransomware

[7] Дипфејк (енгл. *deepfake,* од *deep (learning)* - дубоко (учење) и *fake*-лажно*)* је технологија заснована на вештачкој интелигенцији која омогућава генерисање хиперреалистичног, али потпуно лажног видео или аудио садржаја, најчешће са циљем манипулације, преваре или ширења дезинформација. Више о томе доступно на: „What Is a Deepfake?," Proofpoint. Преузето: 27.6.2026. https://www.proofpoint.com/us/threat-reference/deepfake

[8] Б. Бановић, Обезбеђење доказа у криминалистичкој обради кривичних дела привредног криминалитета, *Безбедност*, бр. 1, вол. 45, Београд, 2003, стр. 121-124.

[9] Кривични законик, *Сл. гласник РС*, бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019.

[10] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, *Сл. гласник РС*, бр. 61/2005, 104/2009, 10/2023, 10/2023 - др. закон и 9/2026.

[11] ETS No. 185, *Convention on Cybercrime*, Budapest, 23 November 2001.

[12] Наш законодавац користи термин „високотехнолошки криминал" па је тако закон којим је Конвенција ратификована назван Закон о потврђивању Конвенције о високотехнолошком криминалу, *Сл. гласник РС*

Развој домаћег законодавства у овој области прати међународне тенденције и потребу за усклађивањем са европским стандардима, али савремени облици криминалитета непрестано постављају нове изазове пред законодавца и надлежне институције.

Мотив за избор ове теме произлази из чињенице да компјутерски криминалитет представља један од најбрже растућих облика савременог криминалитета, чији интензитет и сложеност прате динамичан развој информационо-комуникационих технологија. Учесталост сајбер напада на државне органе, привредне субјекте и грађане, као и појава нових облика злоупотребе вештачке интелигенције, указују на потребу сталног преиспитивања постојећих кривичноправних механизама и њихове прилагођености савременим технолошким изазовима.

Предмет овог рада јесте анализа компјутерског криминалитета као савременог облика сајбер криминала, са посебним освртом на његов појам, карактеристике, узроке, облике испољавања и последице, као и на правни оквир којим је регулисан у Републици Србији и међународном праву. Истраживање је усмерено на сагледавање криминолошких и кривичноправних аспеката ове појаве, а посебна пажња посвећена је анализи најзначајнијих појавних облика компјутерског криминалитета и процени ефикасности постојећих механизама њиховог спречавања и сузбијања

Циљ рада је да се кроз анализу релевантне научне литературе, позитивноправних прописа и доступне праксе надлежних органа утврде основне карактеристике компјутерског криминалитета, његови најзначајнији појавни облици и специфичности у односу на традиционалне облике криминалитета, као и да се процени адекватност постојећег нормативног и институционалног оквира за његово сузбијање. Посебна пажња биће посвећена идентификацији савремених изазова које доноси развој нових технологија и могућностима унапређења система заштите у овој области.

Практични значај рада огледа се у могућности да резултати истраживања послуже као основ за унапређење законодавних решења, развој превентивних

- *Међународни уговори*, бр. 19/2009. Међутим, мишљења смо да је адекватнији изворни термин „сајбер криминал“, те ће исти бити коришћен у раду, с обзиром на то да савремена међународноправна пракса и научна литература користе управо овај термин. Такође, овај израз истиче суштину самих кривичних дела која се врше у виртуелном простору (сајбер простору), при чему су рачунарски системи, мреже и подаци истовремено и средство и објекат напада. Насупрот томе, израз „високотехнолошки криминал” наглашава техничку софистицираност алата која в пракси често изостаје, будући да се многа дела сајбер криминалитета, попут фишинга, врше уз минимално техничко знање, али искључиво унутар дигиталне инфраструктуре. У терминолошком смислу, у раду се термини „компјутерски криминалитет“ и „сајбер криминалитет“ користе као сродни, али се претежно користи термин „компјутерски криминалитет“ због назива рада.

механизама, као и јачање капацитета надлежних институција за откривање, доказивање и сузбијање компјутерског криминалитета.

Полазна хипотеза овог рада јесте да постојећи нормативни оквир Републике Србије у великој мери прати међународне стандарде у области борбе против компјутерског криминалитета, али да брз развој дигиталних технологија захтева континуирано унапређивање законодавства, институционалних капацитета и превентивних механизама.

Посебне хипотезе су:

1) да компјутерски криминалитет због своје транснационалности, техничке сложености и високог степена анонимности представља специфичан облик криминалитета који захтева посебне облике кривичноправне заштите;

2) да су међународна сарадња и хармонизација националних законодавстава неопходни предуслови ефикасног сузбијања компјутерског криминалитета;

3) да превенција, едукација корисника и развој информационе безбедности имају једнако значајну улогу као и репресивне мере кривичног права.

Приликом израде рада примењени су нормативни, историјски, компаративноправни, аналитички и аксиолошки метод. Поред тога, коришћен је и емпиријски приступ кроз анализу релевантне судске праксе, статистичких података, извештаја надлежних институција и доступних примера из праксе. Комбиновањем наведених метода обезбеђено је свеобухватно сагледавање криминолошких, кривичноправних и практичних аспеката компјутерског криминалитета.

Рад је конципиран у пет међусобно повезаних тематских целина које прате логичан ток истраживања, од теоријског одређења појма и карактеристика компјутерског криминалитета, преко анализе његових узрока, облика испољавања и нормативног оквира, до разматрања превентивних механизама и закључних запажања.

I ТЕОРИЈСКО-КРИМИНОЛОШКИ ОСНОВИ КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА

1.1. Појам компјутерског криминалитета

1.1.1. Дефиниција компјутерског криминалитета

Развој ИКТ довео је до значајних промена у начину функционисања савременог друштва. Рачунарски системи, интернет и дигиталне платформе постали су незаменљиви у области комуникације, пословања, образовања и управљања информацијама. Међутим, паралелно са развојем технологије појавили су се и нови облици злоупотреба који се реализују управо у дигиталном окружењу. Ове злоупотребе временом су прерасле у посебан облик криминалитета који се у правној и криминолошкој теорији означава као компјутерски криминалитет (енгл. *cyber crime)*.[13]

Компјутерски криминалитет, као најновији облик криминалитета, представља један од најдинамичнијих облика савременог криминалитета, јер је тесно повезан са развојем технологије и дигиталних система.[14] За разлику од традиционалних облика криминалитета, код овог облика кривичних дела рачунар може бити средство извршења кривичног дела (помоћу компјутера врши се реализација недозвољене радње), али и објекат напада.[15]

Са ширењем интернета и глобалних рачунарских мрежа компјутерски криминалитет добија и изражен транснационални карактер. Кривична дела се често врше са територије једне државе, док се штетне последице јављају у другој, што значајно отежава откривање и кривично гоњење учинилаца.[16] Управо због тога, компјутерски криминалитет има бројне специфичности које се огледају у начину извршења, доказивању и откривању учинилаца, а питање компјутерског криминалитета постало је значајна тема савременог правна.

У литератури не постоји јединствена дефиниција компјутерског криминалитета, али се у основи овај појам односи на противправне радње које се врше употребом рачунара, рачунарских система или рачунарских мрежа. На пример, према дефиницији коју даје Симоновић, „компјутерски криминалитет представља друштвеноопасну појаву за чије се остварење учинилац користи знањима компјутерске технологије, тако

[13] В. Николић Ристановић, С. Константиновић Вилић, *Криминологија*, Београд, 2018, стр. 174.
[14] Ђ. Ђорђевић, *Кривично право - посебни део*, Београд, 2011, стр. 177.
[15] Д. Димовски, *op. cit.*, стр. 197-198.
[16] З. Грујић, Компјутерски криминалитет: специфичности и савремени изазови, *Зборник радова Правног факултета у Нишу*, број 80, 2018, стр. 374.

што се компјутерски систем схваћен у најширем смислу (хардвер, софтвер, њихово јединство; један компјутер или мрежа компјутера), користи као средство или као објекат криминалног напада или једно и друго.“[17]

Према ширем схватању, компјутерски криминалитет обухвата сва кривична дела код којих се рачунар или информациони систем користи као средство за извршење противправних радњи. У ужем смислу, под компјутерским криминалитетом подразумевају се кривична дела која су директно усмерена против рачунарских система, рачунарских мрежа или рачунарских података.[18]

Анализом постојећих дефиниција компјутерског криминалитета уочавају се заједничке одреднице које обухватају:

1) кривичноправни аспект - друштвено опасне радње предвиђене законом;

2) *modus operandi* - употребу рачунара као кључног инструмента извршења;

3) објекат напада - интегритет података и информационих мрежа;

4) субјективни елемент - користољубље или намеру наношења штете другим субјектима.[19]

1.1.2. Правна природа и место компјутерског криминалитета у систему криминалитета

У правној теорији не постоји ни јединствено становиште о месту и природи компјутерског криминалитета у оквиру општег система криминалитета.[20] Поједини аутори полазе од становишта да се компјутерски криминалитет може посматрати као део имовинског криминалитета, имајући у виду да су прве злоупотребе рачунарских система биле усмерене пре свега на стицање противправне имовинске користи.[21] Ови облици криминалног понашања често се доводе у везу са криминалитетом „белог оковратника“, односно са привредним криминалитетом у ширем смислу.[22]

С друге стране, у савременој литератури све је присутније становиште да компјутерски криминалитет представља посебан облик криминалитета који захтева специфичан приступ у проучавању и правном регулисању. Разлог за то лежи у

[17] Б. Симоновић, *Криминалистика*, Крагујевац, 2004. година, стр. 665. Наведено према: Д. Димовски, *op. cit.*, стр. 197.
[18] В. Николић Ристановић, С. Константиновић Вилић, *op. cit.,* стр. 174.
[19] *ibid.*
[20] З. Грујић, *op. cit.,* стр. 330.
[21] В. Ђурђић, Д. Јовашевић, *Кривично право - посебни део*, Београд, 2010, стр. 176.
[22] M. Yar, *Cybercrime and society*, London, 2006, p. 9.

чињеници да се ова врста криминалитета одвија у оквиру информационо-комуникационих технологија, што условљава специфичне начине извршења, откривања и доказивања кривичних дела.[23]

Према нашем мишљењу, прихватљивије је схватање према којем компјутерски криминалитет представља посебан облик савременог криминалитета. Наиме, иако су његови почетни облици били претежно усмерени на стицање противправне имовинске користи, развој ИКТ-а довео је до појаве бројних нових облика противправног понашања који превазилазе оквире класичног имовинског криминалитета. Поред угрожавања имовинских интереса, компјутерски криминалитет данас обухвата и нападе на поверљивост, интегритет и доступност рачунарских система и података, злоупотребу података о личности, сајбер шпијунажу, сајбер тероризам и друге облике угрожавања безбедности дигиталног простора. Стога се његова правна природа не може свести искључиво на једну традиционалну категорију криминалитета. Напротив, специфичност заштићених правних добара, начин извршења, транснационални карактер и сложеност откривања и доказивања оправдавају становиште да компјутерски криминалитет представља самосталну категорију криминалитета која захтева посебан кривичноправни и криминолошки приступ.

Свакако, посматрање компјутерског криминалитета као самосталне категорије не искључује могућност његовог прожимања са другим облицима криминалитета. У пракси се често јављају ситуације у којима су елементи имовинског, привредног или организованог криминалитета присутни истовремено са злоупотребом информационо-комуникационих технологија.

1.2. Историјски развој компјутерског криминалитета

Компјутерски криминалитет почиње да се развија упоредо са развојем рачунарске технологије. Први рачунар, под називом ENIAC, настао је за време Другог светског рата (тачније 1944. године) и коришћен је за потребе рата. Оно што је за данашње стандарде непојмљиво јесте његова цена која је износила 400.000 америчких долара у то време.[24]

[23] З. Грујић, *op. cit.,* стр. 330-331.
[24] Д. Димовски, *op. cit.*, стр. 196.

Како су се друштво и култура развијали, тако се мењао и списак кажњивих дела. Криминалитет није статична појава већ се константно мења и прилагођава времену,[25] па тако први облици злоупотребе рачунарских система јављају се још шездесетих и седамдесетих година двадесетог века, када су рачунари почели да се користе у пословним системима и државним институцијама. У том периоду злоупотребе су углавном биле ограничене на неовлашћени приступ системима или манипулацију подацима.[26]

Први забележени случај компјутерског криминалитета датира из 1958. године, док је прво кривично гоњење на федералном нивоу у Сједињеним Америчким Државама забележено 1966. године, када је извршена измена банкарских записа у Минеаполису.[27] У Европи се као један од првих случајева наводи софтверска крађа у Финској 1968. године.[28] Током шездесетих година XX века почињу да се бележе и први облици компјутерских манипулација, саботажа и шпијунаже, као и случајеви неовлашћеног приступа рачунарским системима. У почетним фазама развоја, хакери су често били мотивисани радозналошћу и жељом да разумеју функционисање рачунарских система, што је у одређеној мери допринело и њиховом технолошком унапређењу.

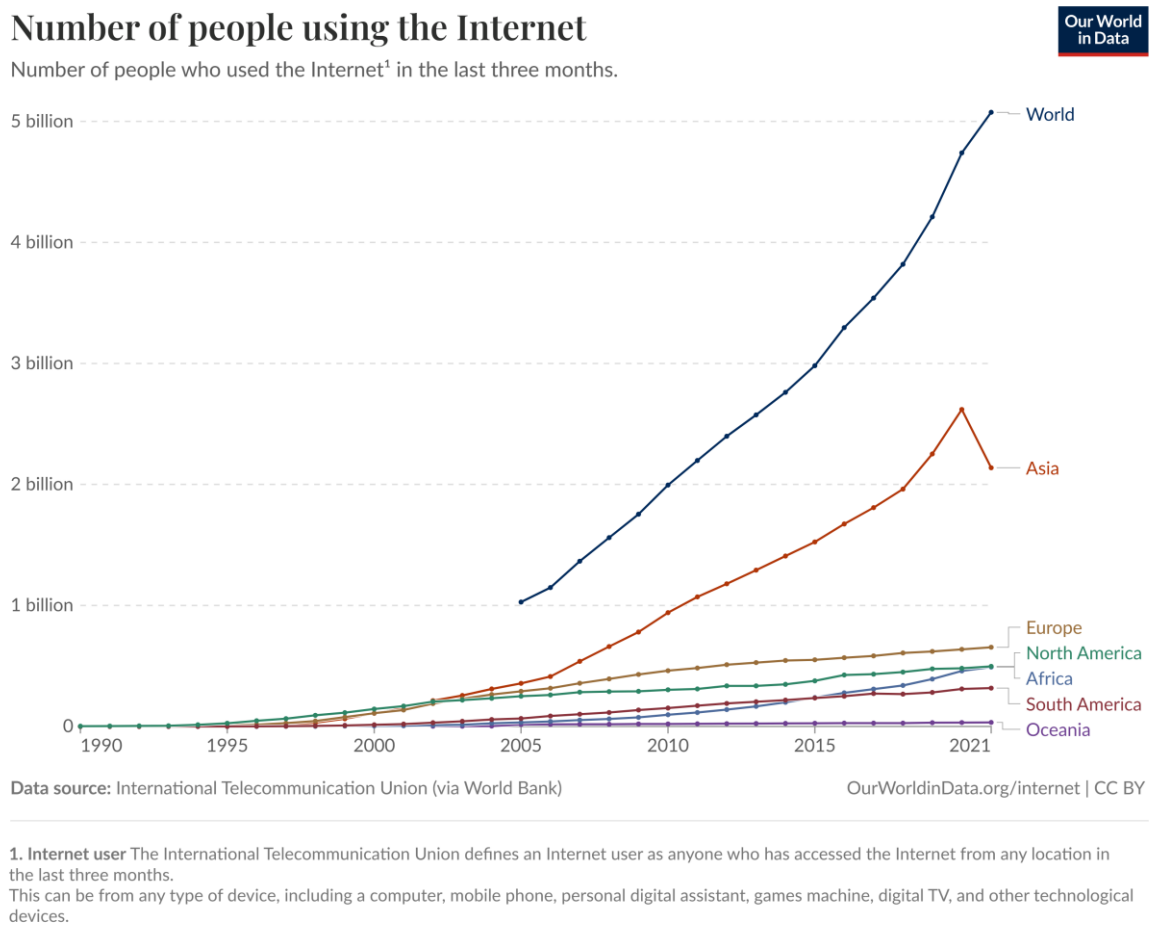
Озбиљнији приступ проучавању компјутерског криминалитета појављује се седамдесетих година XX века, када се ова врста криминала углавном односила на преваре у телекомуникацијама и злоупотребе у преносу електронских средстава. Са развојем информационих технологија и ширењем употребе персоналних рачунара и интернета, компјутерски криминалитет добија нове облике и значајно се шири. Развој глобалних рачунарских мрежа омогућио је појаву сложенијих облика криминалних активности, као што су ширење малвера, DDoS напади,[29] крађа података и повреде ауторских права.[30]

---

[25] С. Константиновић Вилић, В. Николић Ристановић, М. Костић, *Криминологија*, Београд, 2010, стр. 23.
[26] Д. Мирковић, *Криминолошки аспект компјутерског криминалитета (мастер рад)*, Правни факултет Универзитета у Нишу, Ниш, 2016, стр. 8. Преузето: 5.3.2026. године. https://www.prafak.ni.ac.rs/files/master-radovi/dragan-mirkovic.pdf
[27] *ibid.*
[28] *ibid.*
[29] DDoS (енгл. *Distributed Denial of Service* - дистрибуирано ускраћивање услуге) је напредни облик DoS (енгл. *Denial of Service*) напада, код којег се преоптерећење сервера или мреже врши симултано са великог броја географски дисперзованих рачунара, чиме се веб-страница или сервис потпуно онемогућава за легитимне кориснике. Више о томе доступно на: J. Holdsworth, M. Kosinski, „What Is a Distributed Denial-of-Service (DDoS) Attack?," IBM Think. Преузето: 27.6.2026. https://www.ibm.com/think/topics/ddos
[30] Д. Мирковић, *op. cit.*, стр. 9.

У савременим условима свеопште дигитализације, компјутерски криминалитет постаје све присутнији и сложенији, а његовим извршењем све чешће се баве и организоване криминалне групе. Поред економске користи, интернет и рачунарске мреже све више користе и терористичке организације за комуникацију, регрутовање присталица и ширење пропаганде, што указује на растући безбедносни значај борбе против ове врсте криминалитета.[31]

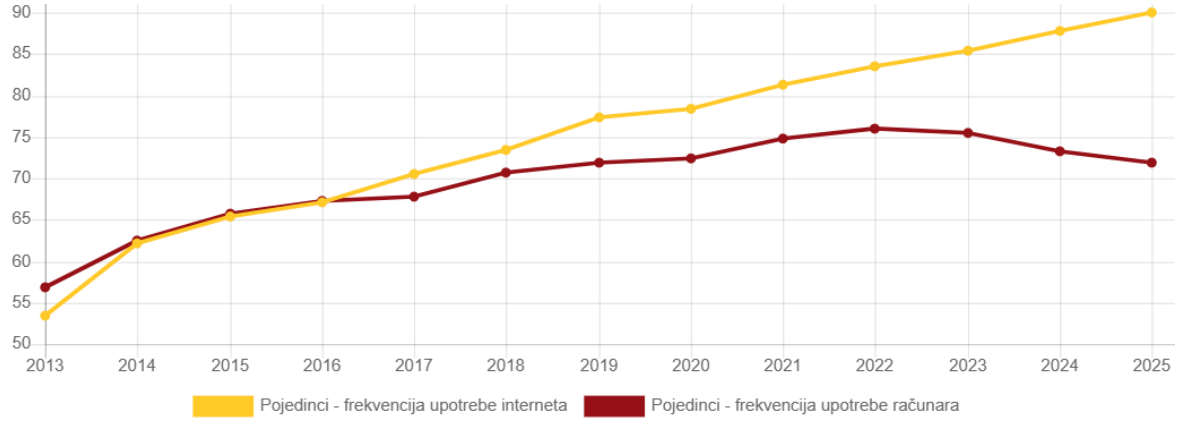
Због брзог технолошког напретка, компјутерски криминалитет се континуирано развија и прилагођава новим технолошким могућностима, што доводи до тога да државе настоје да кроз законодавство и институционалне механизме обезбеде ефикасну заштиту информационих система и података, као и адекватне механизме за откривање и кажњавање учинилаца ових кривичних дела.



1. Слика 1. Раст корисника интернета у свету у периоду 1991-2021.[32]

[31] *ibid.*, стр. 10-11.

[32] Our World in Data, Number of Internet users. Преузето: 11.7.2026. https://ourworldindata.org/grapher/number-of-internet-users



2. Слика 2. Фреквенција употребе рачунара и интернета у Републици Србији (без података за АП КиМ) у периоду 2013-2025.[33]

Посматрано историјски, развој компјутерског криминалитета одражава развој информационих технологија. Од првих злоупотреба великих рачунарских система педесетих и шездесетих година XX века, преко ширења интернета и електронске трговине, па све до савремених злоупотреба вештачке интелигенције и криптовалута, овај облик криминалитета пролази кроз континуирану трансформацију и постаје све сложенији безбедносни и правни изазов.

1.3. Основне карактеристике компјутерског криминалитета

Компјутерски криминалитет поседује одређене специфичне карактеристике које га разликују од традиционалних облика криминалитета. Ове карактеристике проистичу, пре свега, из технолошке природе информационо-комуникационих система и њихове све шире примене у савременом друштву. Разумевање ових елемената је од кључног значаја за ефикасно кривично гоњење, превенцију и правну заштиту жртава ових дела.

Једна од основних карактеристика компјутерског криминалитета јесте његова изразита динамичност, која је условљена брзим развојем информационих технологија и њиховом свакодневном применом. Са развојем компјутерских система и дигиталних мрежа, појављују се нови облици криминалних активности, док се истовремено и традиционална кривична дела могу извршавати на знатно сложенији и опаснији начин.[34]

Посебну карактеристику компјутерског криминалитета представља смањен значај просторних и временских оквира. Наиме, захваљујући интернету и рачунарским

[33] Републички завод за статистику, Употреба информационо-комуникационих технологија. Преузето: 11.7.2026. https://www.stat.gov.rs/sr-Latn/oblasti/upotreba-ikt/upotreba-ikt-pojedinci
[34] Д. Димовски, *op. cit.*, стр. 206-207.

мрежама, извршилац може са било ког места у свету, у било ком тренутку, извршити напад на рачунарски систем који се налази на потпуно другој локацији. Поред тога, рачунарски системи омогућавају изузетно брзо извршење криминалних активности, што додатно отежава њихово откривање и спречавање.[35]

Највећи део кривичних дела која припадају компјутерском криминалитету извршава се у виртуелном простору (енгл. *cyberspace*),[36] који, према одређеним ауторима, представља пети елемент савременог друштва.[37] У правној доктрини је развијена тзв. *теорија транзиције простора* (енгл. *Space Transition Theory*) која се користи за објашњење деловања појединаца у виртуелном простору.[38] Према овој савременој криминолошкој теорији, коју је развио Џаишанкар (Karuppannan Jaishankar), људи се понашају потпуно другачије када прелазе из физичког простора у сајбер простор, што ствара специфичне услове за појаву и ширење компјутерског криминалитета.[39]

У непосредној вези са наведеним налази се и још једна значајна карактеристика - постојање тзв. „тамне бројке“ компјутерског криминалитета. Реч је о великом броју кривичних дела која остају непријављена или неоткривена. Према појединим проценама, проценат неоткривених случајева компјутерског криминалитета може се кретати између 90% и 99%, што указује на значајне потешкоће у његовом откривању и процесуирању.[40]

За извршење ових кривичних дела често је потребан одређени ниво техничког знања и информатичке писмености. Међутим, са ширењем дигиталних технологија и повећањем компјутерске писмености становништва, повећава се и број потенцијалних извршилаца ових кривичних дела.[41]

На крају, значајан проблем у борби против компјутерског криминалитета представља и доказивање ових кривичних дела у кривичном поступку. Извршиоци често не остављају материјалне трагове, док се дигитални докази могу налазити на различитим локацијама, па чак и у различитим државама. Поред тога, велика количина

---

[35] *ibid.*
[36] З. Грујић, *op. cit.*, стр. 330-331.
[37] T. H. Winkler, F. Schreier, B. Weekes, Cyber Security: The Road Ahead, *Geneva Centre for Security Sector Governance (DCAF)*, 01-2015, p. 14. Преузето: 27.2.2026. https://connect.liblynx.com/wayf/69b34570978e8bfeb6ab08fed80290c4
[38] K. Jaishankar, Establishing a Theory of Cyber Crimes, *International Journal of Cyber Criminology*, Vol 1, Issue 2, July 2007, p. 7. Преузето: 27.2.2026. https://www.researchgate.net/publication/268032777_Establishing_a_Theory_of_Cyber_Crimes
[39] *ibid.*
[40] Д. Димовски, *op. cit.*, стр. 207.
[41] *ibid.*

података у рачунарским системима и висок степен анонимности који интернет пружа корисницима додатно отежавају идентификацију и процесуирање учинилаца.[42]

На основу изложеног може се закључити да су основне карактеристике компјутерског криминалитета: динамичност, транснационални карактер, висок степен анонимности, постојање велике тамне бројке, техничка софистицираност начина извршења и сложеност откривања и доказивања ових кривичних дела.

1.4. Класификација компјутерског криминалитета

У правној и криминолошкој литератури не постоји јединствена класификација компјутерског криминалитета. Разлог томе лежи у чињеници да је реч о изузетно динамичној појави која се непрестано развија упоредо са развојем ИКТ.

Најопштија подела разликује компјутерски криминалитет у ужем и ширем смислу. Ова подела прихваћена је и у оквиру Десетог конгреса Уједињених нација за превенцију криминалитета и поступање са преступницима.[43] Према овом схватању, компјутерски криминалитет у ужем смислу обухвата противправна понашања усмерена непосредно против рачунарских система, мрежа и података који се у њима обрађују, док компјутерски криминалитет у ширем смислу обухвата сва кривична дела код којих се рачунарски систем или мрежа користе као средство извршења или као окружење у коме се противправна радња реализује.[44]

У оквиру компјутерског криминалитета у ужем смислу најчешће се издвајају неовлашћени приступ рачунарским системима (хаковање), оштећење или уништење рачунарских података и програма, рачунарска саботажа, неовлашћено пресретање комуникација и рачунарска шпијунажа.[45] Насупрот томе, компјутерски криминалитет у ширем смислу обухвата различите облике компјутерских превара, фалсификовања, крађа, злоупотреба система електронског плаћања, повреде права интелектуалне својине, као и ширење незаконитих садржаја путем интернета.[46]

Значајну класификацију садржи и Конвенција Савета Европе о сајбер криминалу, која групише кривична дела у четири основне категорије. Прву групу чине кривична

---

[42] *ibid.*
[43] Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, *Background paper for the workshop on crimes related to the computer network: Crime-fighting on the Ne*t, 2000. Преузето: 3.6.2026. https://www.un.org/events/10thcongress/2088h.htm
[44] *ibid.*
[45] Ј. Матијашевић, С. Игњатијевић, *op. cit.*, стр. 854.
[46] *ibid.*

дела против поверљивости, интегритета и доступности рачунарских података и система, као што су незаконит приступ, незаконито пресретање, ометање података и ометање функционисања система. Другу групу чине кривична дела повезана са рачунарима, пре свега компјутерске преваре и компјутерска фалсификовања. Трећу групу чине кривична дела у вези са садржајем, међу којима посебно место заузима дечја порнографија. Четврта група обухвата повреде ауторских и сродних права извршене употребом информационих технологија.[47]

У домаћој криминолошкој литератури посебно је значајна класификација према којој се компјутерски криминалитет може поделити на: неовлашћено коришћење рачунара, манипулације рачунарима, рачунарску шпијунажу и рачунарску саботажу. Ова подела је довољно широка да обухвати већину савремених облика компјутерског криминалитета, укључујући компјутерске крађе, преваре, фалсификовања, нарушавање приватности, хаковање, софтверску пиратерију, као и израду и ширење злонамерних програма.[48]

Према циљу који се настоји постићи, компјутерски криминалитет може се поделити и на политички и економски. Политички облици обухватају рачунарску шпијунажу, сајбер тероризам, сајбер саботаже и различите облике сајбер ратовања. Економски компјутерски криминалитет усмерен је на стицање противправне имовинске користи и обухвата компјутерске преваре, крађе података, злоупотребе платних система, индустријску шпијунажу, софтверску пиратерију и друге облике незаконитог пословања у дигиталном окружењу.[49]

Без обзира на различите критеријуме класификације, може се закључити да је компјутерски криминалитет изузетно хетерогена појава која обухвата велики број различитих облика противправног понашања. Управо због његове разноврсности и сталне еволуције није могуће успоставити јединствену и коначну класификацију, већ се постојеће поделе посматрају као средство за лакше разумевање његових појавних облика и механизама испољавања.

II ЕТИОЛОШКЕ И ФЕНОМЕНОЛОШКЕ КАРАКТЕРИСТИКЕ КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА

2.1. Узроци компјутерског криминалитета

[47] ETS No. 185, *Convention on Cybercrime*, Budapest, 23 November 2001, ch. II, art. 2-10.
[48] М. Видојковић, *Компјутерски криминалитет (мастер рад)*, Правни факултет Универзитета у Нишу, Ниш, 2024, стр. 47. Преузето: 20.6.2026. https://www.prafak.ni.ac.rs/files/master-radovi/milos-vidojkovic.pdf
[49] Ј. Матијашевић, Светлана Игњатијевић, *op. cit.*, стр. 855.

Компјутерски криминалитет, као и други облици криминалног понашања, настаје као резултат деловања више различитих фактора. Ови фактори могу бити условљени друштвеним околностима, али и личним карактеристикама појединаца који приступају извршењу ових кривичних дела. У том смислу, узроци компјутерског криминалитета најчешће се посматрају кроз социо-економске, политичке и психолошке факторе.

Социо-економски и политички фактори односе се на шири друштвени контекст у коме појединци живе и делују. Одређени друштвени услови могу подстаћи појединце да прибегну незаконитим активностима у дигиталном окружењу, било из економских мотива, било као израз незадовољства постојећим друштвеним поретком. Међу најзначајнијим факторима који се у литератури издвајају налазе се сиромаштво, осећај неприпадања друштву, политичко незадовољство, неефикасно функционисање друштвених институција, као и појаве корупције и злоупотребе власти.[50] Ови фактори могу утицати на формирање ставова који подстичу појединце да кроз различите облике компјутерског криминалитета покушају да остваре личну корист или изразе протест према постојећем систему.

Ипак, истраживања показују да извршиоци ових кривичних дела не припадају увек друштвено маргинализованим групама. Напротив, међу њима се често налазе и високообразовани појединци, укључујући инжењере, програмере и друге стручњаке из области информационих технологија.[51] Ова чињеница указује на то да економски и социјални фактори сами по себи нису довољни за објашњење појаве компјутерског криминалитета.

Поред друштвених услова, значајну улогу имају и психолошки фактори који се односе на личност потенцијалних извршилаца. Међутим, важно је нагласити да извршиоци компјутерских кривичних дела не морају бити особе са психичким поремећајима. Према појединим истраживањима, многи појединци који се баве овим обликом криминалитета имају уобичајене психолошке карактеристике, али их на извршење кривичних дела могу подстаћи осећаји неправде, понижења или незадовољства. Поред тога, негативна животна искуства, породични проблеми или

[50] М. Васић, *Компјутерски тероризам (мастер рад)*, Правни факултет Универзитета у Нишу, Ниш, 2018, стр. 17. Доступно на: https://www.prafak.ni.ac.rs/files/master-radovi/11.-ZMR-Milos-Vasic.pdf, 6.3.2026. године

[51] J. Post, E. Sprinzak, L. Denny, *The terrorist in their own words, Interviews with 35 incarcerated Middle Easter Terrorist, Terrorism and Political Violence*, 2003, p. 171-184. Преузето: 3.3.2026. https://www.tandfonline.com/doi/abs/10.1080/09546550312331293007

друштвена изолација могу утицати на формирање девијантних ставова и понашања.[52] Развој савремених информационих технологија омогућио је да се поједини облици компјутерског криминалитета извршавају уз минималан ризик непосредног контакта са жртвом. Управо одсуство директног контакта са оштећеним код појединих извршилаца смањује осећај моралне одговорности и олакшава доношење одлуке о извршењу кривичног дела.

Такође, поред наведених општих друштвених и психолошких фактора, на развој компјутерског криминалитета значајно утичу и специфичности дигиталног окружења. Висок степен анонимности на интернету, могућност прикривања идентитета коришћењем различитих техничких средстава, као и релативно низак ризик непосредног откривања учинилаца, стварају повољне услове за вршење ових кривичних дела. Све већа зависност појединаца, привредних субјеката и државних институција од информационих система повећава број потенцијалних мета напада, док доступност специјализованих софтверских алата омогућава и лицима са ограниченим техничким знањем да учествују у појединим облицима компјутерског криминалитета.[53]

Дакле, сагледавање узрока компјутерског криминалитета захтева мултидисциплинарни приступ, који обухвата правне, социолошке и психолошке аспекте. Разумевање ових узрока представља важан предуслов за креирање ефикасних механизама превенције и сузбијања компјутерског криминалитета у савременом дигиталном друштву.

2.2. Циљеви и мотиви извршилаца

Мотиви извршилаца компјутерског криминалитета представљају један од кључних криминолошких аспеката за разумевање ове појаве. За разлику од традиционалног криминалитета, где су мотиви најчешће усмерени на стицање материјалне користи, код компјутерског криминалитета мотиви могу бити веома различити и често су условљени специфичностима дигиталног окружења.[54]

Најчешћи мотив представља стицање противправне имовинске користи.[55] Финансијски мотивисани извршиоци настоје да путем неовлашћеног приступа информационим системима прибаве новац, податке од економске вредности или друге

[52] М. Васић, *op. cit.,* стр. 17.
[53] З. Грујић, *op. cit.,* стр. 335-336.
[54] В. Николић Ристановић, С. Константиновић Вилић, *op. cit.,* стр. 175.
[55] *ibid.*

облике материјалне користи. У ову категорију спадају различити облици компјутерских превара, злоупотребе платних картица, крађе идентитета, рансомвер напади и други облици дигиталног криминала чији је основни циљ економска добит.

Поред финансијских мотива, значајно место заузимају и мотиви који проистичу из радозналости, жеље за доказивањем и интелектуалног изазова. У савременим условима све су присутнији и идеолошки и политички мотиви - тзв. *хактивисти* користе информационе технологије ради промовисања политичких, друштвених или идеолошких циљева. Њихове активности могу бити усмерене на објављивање поверљивих података, онемогућавање рада одређених интернет страница или организовање масовних дигиталних протеста.[56]

Посебну категорију чине мотиви повезани са индустријском, војном и политичком шпијунажом. У овим случајевима циљ није непосредна материјална корист већ прибављање поверљивих пословних, војних или политичких информација које могу обезбедити конкурентску или стратешку предност.[57]

Коначно, најопаснији облик мотивације представљају терористички мотиви. Терористичке организације све чешће користе информационе технологије за ширење пропаганде, регрутовање нових чланова, координацију активности и нападе на критичну инфраструктуру, што компјутерском криминалитету даје нову безбедносну димензију.

На основу наведеног може се закључити да мотиви извршилаца компјутерског криминалитета постају све сложенији и разноврснији. Док је некада доминирао мотив стицања имовинске користи, данас су све присутнији политички, идеолошки и геополитички мотиви, што овом облику криминалитета даје и значајну безбедносну димензију.

2.3. Начини извршења и злоупотреба информационих технологија

Начини извршења компјутерских кривичних дела условљени су технолошким карактеристикама информационих система и специфичностима дигиталног окружења. Савремени извршиоци компјутерских кривичних дела располажу широким спектром

[56] Fortinet, Hacktivism-A Cyberattack? Meaning, Types, And More. Преузето: 20.6.2026. https://www.fortinet.com/resources/cyberglossary/what-is-hacktivism

[57] Д. Тепавац, *Заштита пословних информација у функцији националне безбедности (докторска дисертација)*, Факултет безбедности Универзитета у Београду, Београд, 2018, стр. 154-163. Преузето: 20.6.2026. https://fb.bg.ac.rs/download/RepozitorijumDisertacija/2018-05-21%20Tepavac%20Dejan/Disertacija.pdf

техничких метода и алата, чија се употреба непрестано усавршава и прилагођава новим технолошким условима.

Међу најзаступљенијим начинима извршења издваја се фишинг, који представља облик дигиталне преваре заснован на обмани корисника. Такође, врло често се користе и злонамерни софтвери, где спадају рачунарски вируси, тројански коњи (енгл. *trojan horse*), шпијунски софтвер (енгл. *spyware*) и рансомвер напади, црви, DDoS напади, хаковање (енгл. *hacking*) и слично.[58]

1. Табела 1. Број инцидената по врстама у Републици Србији у 2025. години[59]

Група инцидената	Врста инцидента	Број инцидената
Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер)	Вирус	9.191
	Црв	499
	Рансомвер	48
	Тројанац	13.153
	Шпијунски софтвер	6.390
	Руткит	14
Неовлашћено прикупљање података	Скенирање портова	328.913.543
	Пресретање података између рачунара и сервера	33
	Социјални инжењеринг	2.784
	Компромитовање или цурење података	2.834
Превара	Фишинг	232.883
	Неовлашћено коришћење ресурса	15
Покушај упада у ИКТ систем	Покушај искоришћавања рањивости система	903.392
	Покушај откривања креденцијала	6.180.960
Упад у ИКТ систем	Откривање или	10

[58] Преузето: 27.6.2026. file:///C:/Users/PC/Downloads/vrste-sajber-napada.pdf

[59] Наведено према: Национални ЦЕРТ Републике Србије, *Извештај о статистичким подацима о свим инцидентима у ИКТ системима од посебног значаја у 2025. години*, 2026, стр. 11-12. Преузето: 11.7.2026. https://www.cert.rs/files/shares/Izve%C5%A1taj%20o%20statisti%C4%8Dkim%20podacima%202025.pdf

	неовлашћено коришћење привилегованих налога	
	Откривање или неовлашћено коришћење непривилегованих налога	79
	Неовлашћени приступ апликацији	9
	Мрежа заражених уређаја	412
Недоступност или ограничена доступност ИКТ система	Напад са циљем онемогућавања или ометања функционисања ИКТ система	48
	Дистрибуирани напад са циљем онемогућавања или ометања функционисања ИКТ система	3.537
	Саботажа	0
	Прекид у функционисању система или дела система	1.897
Угрожавање безбедности података	Неовлашћен приступ подацима	5
	Неовлашћена измена или брисање података	5
	Криптографски напад	0
Оперативни инциденти	Отказивање хардверских компоненти	3.686
	Проблеми у раду са софтверским компонентама	5.731
Инциденти физичкотехничке безбедности	Крађа хардверских компоненти	90
	Пожар	5
	Поплава	4
Остали инциденти	Инциденти који не спадају	21.351

	у наведене категорије	
	УКУПНО:	**336.303.148**

2.4. Последице компјутерског криминалитета

Последице компјутерског криминалитета могу бити вишеструке и испољавају се како у материјалном, тако и у нематеријалном облику. Најчешће се огледају у настанку имовинске штете, али њихов значај превазилази искључиво финансијске губитке. Злоупотреба рачунарских система може довести и до губитка поверења у сигурност и поузданост информација које се добијају из информационих система. Овакве ситуације могу негативно утицати на пословни углед привредних и других субјеката, довести до нарушавања пословних односа, као и изазвати страх од нових злоупотреба у функционисању рачунарских система.[60]

Штете настале извршењем кривичних дела у области компјутерског криминалитета често су веома велике и тешко мерљиве. Поред директних финансијских губитака који настају када учинилац прибави противправну имовинску корист или проузрокује материјалну штету, могу се јавити и нематеријалне последице. Оне се најчешће испољавају кроз неовлашћено откривање пословних тајни, нарушавање угледа организација или појединаца (тзв. репутациона штета), повреду ауторских и других права интелектуалне својине, као и друге облике повреде личних и професионалних интереса. У пракси су честе и комбиноване последице, када истовремено долази до материјалне и нематеријалне штете.[61]

Истраживања су још током осамдесетих година у Сједињеним Америчким Државама показала да финансијска штета настала услед компјутерског криминалитета достиже између 100 и 300 милиона долара годишње, док је просечна штета по појединачном случају износила око 430.000 долара. Са даљим развојем информационих технологија и ширењем интернета, обим и последице овог облика криминалитета значајно су се повећали.[62]

Посебан проблем у сагледавању стварних размера штете представља чињеница да многе компаније не пријављују случајеве злоупотребе рачунарских система. Разлог за такво поступање најчешће лежи у страху од нарушавања пословног угледа, негативног утицаја на пословне партнере и запослене, као и у процени да судски

[60] Б. Бановић, *op. cit.,* стр. 121-124.
[61] Ј. Матијашевић, С. Игњатијевић, *op. cit.,*стр. 854.
[62] *ibid.*

поступак може бити дуготрајан и финансијски захтеван, уз неизвесну могућност повраћаја украдених средстава. Због тога стварни обим последица компјутерског криминалитета често остаје недовољно видљив у званичним статистичким подацима.[63]

2.5. Врсте и типологија извршилаца

Савремени развој информационо-комуникационих технологија, масовна употреба дигиталних уређаја и доступност интернета значајно су проширили круг потенцијалних учинилаца, тако да је број потенцијалних извршилаца данас практично пропорционалан броју корисника информационих система.

Типичан профил извршиоца високотехнолошког криминала одступа од традиционалних криминолошких образаца. Најчешће је реч о мушкарцима млађе доби (18-30 година), високог интелектуалног капацитета и стручног образовања, који се одликују социјалном интегрисаношћу и непостојањем криминалне прошлости. [64] Парадоксално, често заузимају радна места која су испод њихових квалификација, иако поседују супериорна техничка знања. У погледу мотивације, разликује се категорија усмерена на стицање имовинске користи и категорија хакера вођених нефинансијским побудама. Прва група се даље градира према степену стручности и организације на аматере и професионалце, који могу деловати индивидуално или у оквиру сложених криминалних структура.[65]

2.5.1. Аматери

Аматери представљају најбројнију и најхетерогенију категорију извршилаца компјутерског криминалитета. Реч је о лицима која имају легално занимање, али повремено извршавају компјутерска кривична дела, при чему криминалне активности не представљају њихово основно занимање.[66]

У литератури се у оквиру ове групе издвајају три категорије аматера:

1) слаби и подложни појединци,
2) фрустрирани појединци

[63] *ibid.*
[64] В. Николић Ристановић, С. Константиновић Вилић, *op. cit.,* стр. 175.
[65] *ibid.*
[66] Д. Димовски, *op. cit.*, стр. 208.

3) лица код којих различити облици зависности, попут коцкања, алкохолизма или наркоманије, представљају мотив за вршење компјутерског криминалитета.[67]

Слаби и подложни појединци најчешће користе прилику да изврше кривично дело услед недовољно развијених механизама контроле, док фрустрирани и разочарани појединци своје незадовољство окружењем или животним околностима испољавају кроз незаконите активности у дигиталном окружењу.[68]

Иако ова категорија по правилу не припада организованом криминалу и најчешће не остварује значајну противправну имовинску корист, њихове активности могу проузроковати озбиљне последице.

2.5.2. Професионални криминалци

Професионални криминалци представљају најопаснију категорију извршилаца компјутерског криминалитета. За разлику од аматера, код њих је вршење криминалних активности основно занимање, а развој ИКТ омогућио је проширење традиционалних облика криминалног деловања на дигитално окружење.[69] Карактеришу их висок степен стручности, богато искуство, способност прилагођавања технолошким променама и употреба напредних метода прикривања трагова.

Према степену организације, професионални криминалци могу се поделити на:

1) индивидуалне криминалце,
2) организоване групе,
3) криминалне организације.[70]

Индивидуални криминалци најчешће делују самостално и повремено сарађују са другим лицима ради извршења појединачног кривичног дела, без развијене дугорочне стратегије.[71]

Организоване групе окупљају лица повезана заједничким криминалним интересима, што им омогућава већи криминални потенцијал и сложеније облике деловања.[72]

[67] *ibid.*
[68] *ibid.*
[69] *ibid.*
[70] *ibid.*
[71] *ibid.*, 209.
[72] *ibid.*

Криминалне организације представљају највиши степен организованости и одликују се чврстом хијерархијом, дисциплином, поделом улога, лојалношћу чланова и дугорочним планирањем криминалних активности.[73]

Развој информационих технологија омогућио је настанак виртуелних „сајбер“ криминалних група које делују на легалном и илегалном дигиталном тржишту и извршавају различите облике интернет превара, укључујући лажне интернет аукције, преваре у електронском плаћању, инвестиционе преваре, злоупотребе игара на срећу и друге облике дигиталних финансијских злоупотреба. [74] Због транснационалног карактера њиховог деловања, употребе криптовалута, анонимних комуникационих мрежа и савремених метода прикривања идентитета, ова категорија представља један од највећих безбедносних изазова савременог доба.

2.5.3. Хакери

Хакери представљају специфичну категорију извршилаца компјутерског криминалитета коју карактерише висок степен техничке стручности и способност неовлашћеног приступа информационим системима. Они су лица која, користећи своја рачунарска знања, продиру у туђе рачунарске системе, при чему мотиви њиховог поступања могу бити веома различити.[75]

У ранијој литератури истицано је да хакери нису нужно злонамерни и да им је основни мотив доказивање сопствених способности и савладавање техничких изазова.[76] Међутим, развој ИКТ значајно је променио природу хакерских активности, тако да је од некадашњег истраживања и унапређења информационих система хаковање све више постало средство вршења различитих облика компјутерског криминалитета.

Према намени и мотивима деловања, у литератури се разликују:

1) хакери креативци,
2) хакери деструктивци,
3) хакери криминалци.[77]

Креативци хаковање схватају као интелектуални изазов, средство усавршавања или истраживања без намере да нанесу штету. [78] Деструктивци неовлашћеним

[73] *ibid.*
[74] С.Константиновић Вилић, В. Николић Ристановић, М. Костић, *op. cit.*, стр. 184.
[75] З. Грујић, *op. cit.,* стр. 337.
[76] Д. Димовски, *op. cit.*, стр. 210.
[77] З. Грујић, *op. cit.,* стр. 337.
[78] *ibid.*

приступом настоје да испоље агресивност и фрустрацију уништавањем или изменом података и система.[79] Најзад, криминални хакери своја техничка знања користе ради стицања противправне имовинске користи, крађе података, уцене, индустријске шпијунаже или других облика противправне користи.[80]

У савременој међународној литератури најчешће се користи и класификација на:

1) *white hat* хакере,
2) *black hat* хакере,
3) *grey hat* хакере.[81]

White hat хакери делују уз овлашћење власника система и тестирају његову безбедност ради отклањања рањивости. Насупрот њима, *black hat* хакери неовлашћено приступају системима ради прибављања противправне користи или наношења штете и њихове активности представљају предмет кривичноправне заштите. Између ове две категорије налазе се *grey hat* хакери, који без овлашћења откривају безбедносне пропусте, али по правилу немају намеру да нанесу штету.[82]

III НОРМАТИВНИ ОКВИР

3.1. Међународна регулатива

3.1.1. Конвенција Савета Европе о сајбер криминалу

Конвенција Савета Европе о сајбер криминалу, о којој је било речи и у претходним деловима рада, представља најзначајнији међународни документ у области борбе против високотехнолошког криминалитета. Ова конвенција је први мултилатерални уговор који свеобухватно регулише инкриминацију кривичних дела у области сајбер простора, процесне механизме за њихово откривање и доказивање, као и међународну сарадњу у кривичним стварима.

Посебан значај Конвенције огледа се и у успостављању процесних механизама прилагођених специфичностима дигиталних доказа, укључујући убрзано обезбеђење и чување компјутерских података, налоге за достављање података, претрес рачунарских система и пресретање комуникација.[83] Такође, Конвенција предвиђа успостављање

[79] *ibid.*
[80] *ibid.*
[81] Више о томе: М. Будимлић, П. Пухарић, *Компјутерски криминалитет - криминолошки, кривичноправни и сигурносни аспект*, Сарајево, Факултет за криминалистику, криминологију и сигурносне студије, 2009, стр. 33-38. Наведено према: Д. Мирковић, *op. cit.*, стр. 78-79.
[82] *ibid.*
[83] ETS No. 185, *Convention on Cybercrime*, Budapest, 23 November 2001, ch. II, art. 14-22.

мреже контакт тачака доступних 24 часа дневно, 7 дана у недељи, ради пружања непосредне помоћи у истрагама са прекограничним елементом.[84]

3.1.2. Допунски протоколи уз Конвенцију Савета Европе о сајбер криминалу

Први Допунски протокол уз Конвенцију Савета Европе о сајбер криминалу усвојен је 28. јануара 2003. године у Стразбуру[85] и односи се на инкриминацију дела расизма и ксенофобије извршених путем рачунарских система. Његов значај се огледа у проширивању правног оквира за регулисање незаконитих активности у сајбер простору.

Други Допунски протокол уз Конвенцију Савета Европе о сајбер криминалу усвојен је 12. маја 2022. године у Стразбуру [86] и односи се на прекогранично прикупљање електронских доказа и значајно убрзање међународне сарадње у кривичним истрагама.

3.2. Република Србија

3.2.1. Кривични законик

Компјутерски криминалитет, због своје специфичности, сложености и сталног развоја, захтева адекватан и свеобухватан правни оквир који омогућава ефикасно откривање, процесуирање и санкционисање кривичних дела из ове области. У Републици Србији законска регулатива која уређује ову проблематику обухвата више прописа чија је примена усмерена на заштиту информационих система, рачунарских података, као и права појединаца и правних лица. Поред националног законодавства, Србија активно учествује и у међународним иницијативама усмереним на борбу против високотехнолошког криминалитета.

Основни правни акт којим се уређује кривичноправна заштита у овој области јесте *Кривични законик* (скр. КЗ). Кривични законик у посебном делу, у глави двадесет седмој, прописује кривична дела против безбедности рачунарских података. У оквиру ове групе кривичних дела предвиђена су следећа дела:

---

[84] ETS No. 185, *Convention on Cybercrime*, Budapest, 23 November 2001, ch. III, art. 35.
[85] ETS No. 189, *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, Strasbourg, 28.1.2003, доступно на: https://rm.coe.int/168008160f
[86] CETS No. 224, *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, Strasbourg, 12.5.2022, доступно на: https://rm.coe.int/1680a49dab

1) Оштећење рачунарских података и програма;[87]
2) Рачунарска саботажа;[88]
3) Прављење и уношење рачунарских вируса;[89]
4) Рачунарска превара;[90]
5) Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података;[91]
6) Спречавање и органичавање приступа јавној рачунарској мрежи;[92]
7) Неовлашћено коришћење рачунара или рачунарске мреже;[93]
8) Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података.[94]

Наведене одредбе обухватају различите облике злоупотребе рачунарских система, као што су неовлашћени приступ информационим системима, уништавање или измена података, компјутерске преваре, као и друге активности које могу угрозити безбедност дигиталних система и информација.

Поред посебних кривичних дела из ове области, Кривични законик садржи и општа правила о кривичној одговорности, санкцијама и казненој политици која се примењују на учиниоце ових кривичних дела. Ове одредбе омогућавају санкционисање радњи које могу угрозити стабилност и безбедност информационих система, укључујући и оне случајеве који имају транснационални карактер. На тај начин КЗ представља основни нормативни оквир за утврђивање кривичне одговорности и поступање надлежних органа у борби против различитих облика компјутерског криминалитета.

3.2.2. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала

Поред Кривичног законика, значајан правни акт у области борбе против компјутерског криминалитета у Републици Србији представља *Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала*. Овим

[87] Кривични законик, чл. 298.
[88] Кривични законик, чл. 299.
[89] Кривични законик, чл. 300.
[90] Кривични законик, чл. 301.
[91] Кривични законик, чл. 302.
[92] Кривични законик, чл. 303.
[93] Кривични законик, чл. 304.
[94] Кривични законик, чл. 304а.

законом уређују се образовање, организација, надлежност и овлашћења посебних организационих јединица државних органа које су надлежне за откривање, кривично гоњење и суђење за кривична дела из области високотехнолошког криминала (скр. ВТК).[95]

Према одредбама овог закона, високотехнолошки криминал обухвата кривична дела код којих се као средство или објекат извршења појављују рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци и њихови производи у материјалном или електронском облику. У ову категорију посебно спадају рачунарски програми и друга ауторска дела која се могу користити у електронском облику.[96]

Закон се примењује у поступцима откривања, кривичног гоњења и суђења за више категорија кривичних дела. Пре свега, он се односи на кривична дела против безбедности рачунарских података прописана Кривичним закоником.[97] Поред тога, закон се примењује и на одређена кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, уколико су она извршена употребом рачунара, рачунарских система или мрежа, односно ако је настала материјална штета значајне вредности.[98] Такође, поједина кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и уставног уређења могу се сматрати делима високотехнолошког криминала ако су извршена употребом информационо-комуникационих технологија.[99]

Овим законом предвиђено је и формирање посебних организационих јединица надлежних за поступање у овим предметима. За кривично гоњење кривичних дела високотехнолошког криминала надлежно је Више јавно тужилаштво у Београду, у оквиру којег је образовано Посебно одељење за борбу против високотехнолошког криминала.[100] Ово одељење има надлежност за поступање на територији целе Републике Србије.

[95] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, чл. 1.
[96] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, чл. 2, ст. 1-2.
[97] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, чл. 3, ст. 1, тач. 1.
[98] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, чл. 3, ст. 1, тач. 2.
[99] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, чл. 3, ст. 1, тач. 3.
[100] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, чл. 4, ст. 1-2.

У оквиру Министарства унутрашњих послова образована је Служба за борбу против високотехнолошког криминала, чији је задатак откривање и прикупљање доказа у вези са кривичним делима из ове области. Ова служба поступа по захтевима надлежног тужилаштва и спроводи истражне радње у складу са законом.[101]

Што се тиче судске надлежности, за суђење у првом степену у предметима високотехнолошког криминала надлежан је Виши суд у Београду, у оквиру којег је формирано посебно одељење за поступање у овим предметима. За одлучивање у другом степену надлежан је Апелациони суд у Београду.[102]

Увођењем специјализованих тужилачких, полицијских и судских јединица омогућено је ефикасније откривање и процесуирање кривичних дела из области високотехнолошког криминала. Специјализација кадрова, као и поседовање посебних знања из области информационих технологија, представљају важан предуслов за успешну борбу против овог сложеног облика криминалитета.

3.2.3. Остали прописи

Поред Кривичног законика и Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала, значајну улогу у борби против компјутерског криминалитета имају и други прописи који уређују поједине аспекте кривичног поступка, заштите малолетника и интелектуалне својине.

Посебан значај има *Законик о кривичном поступку* (скр. ЗКП),[103] који садржи процесноправне одредбе које се односе на откривање учинилаца кривичних дела, прикупљање доказа и вођење кривичног поступка. У поступцима који се односе на компјутерски криминалитет примењују се општа правила кривичног поступка, јер не постоји посебна кривичнопроцесна форма за ова кривична дела. Иако ЗКП не дефинише посебно појам електронског доказа, електронски записи и рачунарски подаци могу се користити као доказна средства, при чему се на њих примењују иста процесна правила као и на друге материјалне доказе. ЗКП такође предвиђа могућност претресања рачунарских уређаја и опреме на којој се чувају електронски подаци,

[101] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, чл. 9, ст. 1-2.
[102] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, чл. 10, ст. 1-2.
[103] Законик о кривичном поступку, *Сл. гласник РС*, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 - одлука УС и 62/2021 - одлука УС

привремено одузимање таквих уређаја, као и примену посебних доказних радњи, попут тајног надзора комуникација и рачунарског претраживања података.[104]

Значајну улогу има и *Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима*,[105] познат као „Маријин закон“.[106] Овај закон прописује посебне мере које се примењују према лицима осуђеним за кривична дела против полне слободе извршена према малолетним лицима, као и вођење посебне евиденције о тим лицима.[107] Његов циљ је спречавање сексуалне делинквенције над малолетницима.[108] Закон се примењује и на одређена кривична дела која се могу извршити употребом рачунара и интернета, као што су приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетних лица за порнографију, као и искоришћавање рачунарске мреже или других техничких средстава ради извршења кривичних дела против полне слободе.[109] Посебне мере које се могу изрећи учиниоцима након издржане казне затвора обухватају обавезно јављање полицији, забрану посећивања места на којима се окупљају малолетници, обавезно похађање саветовалишта, као и обавезу обавештавања надлежних органа о промени пребивалишта, радног места или путовању у иностранство.[110]

У оквиру нормативног оквира значајан је и *Закон о ауторском и сродним правима,*[111] који уређује заштиту ауторских дела, укључујући и рачунарске програме. Овим законом рачунарски програми се признају као ауторска дела, чиме се обезбеђује њихова правна заштита.[112] Закон такође предвиђа одређена права лица које је законито прибавило рачунарски програм, као што су право да програм користи у складу са

---

[104] Законик о кривичном поступку, чл. 178-180.
[105] Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима, *Сл. гласник РС,* бр. 32/2013.
[106] Закон је назван по Марији Јовановић (2002-2010), жртви сексуалног деликта са смртним исходом који је извршио раније осуђивани педофил. Нацрт закона поднео је отац настрадале девојчице, Слободан Јовановић, са циљем да се пооштри надзор над починиоцима најтежих кривичних дела против полне слободе над малолетницима. Наведено према: А. Николић, *Дечја порнографија као облик компјутерског криминалитета (мастер рад)*, Правни факултет Универзитета у Нишу, Ниш, 2024, стр. 35. Преузето: 9.3.2026. године https://www.prafak.ni.ac.rs/files/master-radovi/12-ZMR_AleksandraNikolic_M015_22_UP.pdf
[107] Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима, чл. 1.
[108] Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима, чл. 2.
[109] Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима, чл. 3.
[110] Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима, чл. 7.
[111] Закон о ауторском и сродним правима, *Сл. гласник РС,* бр. 104/2009, 99/2011, 119/2012, 29/2016 - одлука УС и 66/2019
[112] Закон о ауторском и сродним правима, чл. 2, ст. 1, тач. 1.

његовом наменом, да отклања грешке у програму и изврши неопходне измене, као и да направи резервну копију програма. Поред тога, законом су прописане санкције за недозвољено коришћење, умножавање или стављање у промет рачунарских програма и других ауторских дела.[113]

Поред наведеног, значај има и *Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине*,[114] који уређује овлашћења државних органа у циљу спречавања повреда права интелектуалне својине. Закон се примењује на производњу, промет и употребу робе и услуга којима се повређују ова права, укључујући и пиратске примерке ауторских дела и рачунарских програма.[115] Овим законом предвиђена је одговорност правних лица и одговорних лица у правном лицу за привредне преступе који се односе на неовлашћену производњу, увоз, извоз или стављање у промет производа којима се повређују права интелектуалне својине.[116]

Наведени прописи, заједно са кривичноправним нормама, чине важан део правног оквира који омогућава ефикасније откривање, процесуирање и спречавање компјутерског криминалитета у Републици Србији.

IV ОБЛИЦИ КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА

4.1. Компјутерска (рачунарска) крађа

Компјутерске крађе представљају чест облик компјутерског криминалитета и најчешће су усмерене на прибављање података који имају економску или личну вредност.[117] Међутим, сам појам компјутерске крађе није једноставно дефинисати, имајући у виду специфичност објекта заштите и начин извршења овог кривичног дела.

Полазећи од општег појма крађе, као кривичног дела против имовине које подразумева одузимање туђе покретне ствари у намери прибављања противправне имовинске користи,[118] намеће се питање да ли и у којој мери дигитални подаци могу бити обухваћени овим појмом. Компјутерска крађа јесте један од појавних облика компјутерског криминалитета, али као такав није појмовно одређен и прецизно дефинисан. Управо због чињенице да се као објекат присвајања могу јавити како

[113] Закон о ауторском и сродним правима, чл. 215-217.
[114] Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине, *Сл. гласник РС,* бр. 46/2006, 104/2009 - др. закони и 129/2021
[115] Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине, чл. 2, ст. 1.
[116] Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине, чл. 39-40.
[117] В. Николић Ристановић, С. Константиновић Вилић, *op. cit.,* стр. 175.
[118] Кривични законик, чл. 203. ст. 1.

материјалне ствари (рачунари и опрема), тако и нематеријална добра (подаци, датотеке, приступни кодови), њено прецизно нормативно одређење је отежано.[119]

У том смислу, основно обележје овог дела је противправно одузимање туђе покретне ствари (било да је реч о стварима у физичком облику или подацима и датотекама у преносивом облику),[120] што указује на потребу ширег тумачења појма „ствари“ у дигиталном окружењу. Савремена теорија и пракса све више прихватају став да и подаци могу бити предмет противправног присвајања, нарочито када имају економску вредност.

Поред класичне крађе рачунарске опреме, компјутерска крађа обухвата и читав спектар различитих појавних облика. Појам компјутерске крађе, поред крађе која се изводи тако што се отуђују рачунари и рачунарска опрема, подразумева и крађу идентитета, крађу рачунарских података, крађу кодова, лозинки, идентификационих бројева, као и разноврсне робе.[121] Развој интернета и мрежног окружења додатно је проширио могућности за извршење ових дела, омогућавајући неовлашћен приступ великим количинама података.

Посебно је значајно истаћи да мрежно окружење и интернет пружају велике могућности за крађу пословних и других тајни, софтвера и ауторских дела, али и за крађу личних података и њихову злоупотребу ради стицања имовинске користи, што компјутерску крађу чини изузетно опасном и друштвено штетном појавом.[122] У пракси се све чешће јављају случајеви масовних крађа података, који се даље користе за финансијске злоупотребе, продају на црном тржишту или уцену.

Имајући у виду наведено, може се закључити да компјутерска крађа представља сложен и динамичан појам, чији садржај обухвата различите облике противправног присвајања у дигиталном окружењу, што захтева флексибилан и свеобухватан правни приступ у њеном дефинисању и сузбијању.

4.1.1. Крађа идентитета

[119] С. Петровић, *Компјутерски криминал*, Министарство унутрашњих послова Републике Србије-Уредништво часописа „Безбедност" и „Полицајац", Београд, 2000, стр. 118.
[120] *ibid.*
[121] А. Трифуновић, *Компјутерска крађа (мастер рад),* Правни факултет Универзитета у Нишу, Ниш, 2019, стр. 8. Преузето: 7.3.2026. https://www.prafak.ni.ac.rs/files/master-radovi/5.-ZMR_AleksandraTrifunovic_M007_20_UP.pdf
[122] А. Ђукић, Крађа идентитета - облици, карактеристике и распрострањеност, *Војно дело,* бр. 3, вол. 69, 2017, стр. 100. (стр. 99-118)

Крађа идентитета се сматра једним од најопаснијих облика компјутерских крађа, јер доводи до нарушавања интегритета комерцијалних трансакција и угрожава приватност појединаца.[123]

Овај облик криминалитета подразумева неовлашћено коришћење личних података, као што су име, адреса, бројеви личних докумената или банковни подаци, ради остваривања материјалне користи или извршења других кривичних дела.

У теорији постоји више различитих дефиниција крађе идентитета (енгл. *identity theft*), као једног од облика компјутерске крађе. Према дефиницији коју даје Петровић, „крађа идентитета је форма криминала у којој неко користи туђи идентитет ради извршења криминалне радње".[124] Ђукић прецизније одређује овај облик компјутерског криминалитета и истиче да крађа идентитета представља посебан вид компјутерске крађе који подразумева нелегално прибављање поверљивих личних података једног или више лица и њихово коришћење ради извршења нових кривичних дела, при чему се оно врши без знања и пристанка жртве, уз присвајање њеног имена и других идентификационих обележја.[125]

Постоји разлика између крађе идентитета у ширем смислу и крађе идентитета у ужем смислу. Наиме, у ширем смислу, крађа идентитета обухвата различите моделе злоупотребе података о личности, укључујући њихову продају, уступање трећим лицима и коришћење за извршење других кривичних дела, а у ужем смислу обухвата само нелегално прибављање података.[126]

Начини извршења крађе идентитета су бројни и разноврсни. Најчешће методе укључују фишинг нападе, коришћење злонамерног софтвера, лажне интернет странице и технике социјалног инжењеринга. Мета напада су најчешће идентификациони подаци (ЈМБГ, број личне карте, подаци о банковним рачунима), као и корисничка имена и лозинке. Мотиви извршилаца најчешће су стицање материјалне користи, прикривање сопственог идентитета или припрема за извршење других кривичних дела.[127]

О значају и распрострањености ових метода сведоче бројни познати случајеви у пракси. На пример, у оквиру глобалних инцидената, истиче се случај *Equifax* из 2017. године, у коме су компромитовани лични подаци скоро 150 милиона лица, што је

[123] *ibid.*
[124] С. Петровић, *Компјутерски криминал*, Војноиздавачи завод, Београд, 2004, стр. 133.
[125] А. Ђукић, *op. cit.*, стр. 101.
[126] А. Трифуновић, *op. cit.,* стр. 10.
[127] *ibid.*

довело до масовних злоупотреба идентитета.[128] У Републици Србији постоји велики број случајева крађе идентитета, попут случаја *Asomacum*[129] за који је постојало велико интересовање и изазвао је бројне полемике у јавности.

Последице крађе идентитета могу бити вишеструке и крећу се од директне материјалне штете до нарушавања угледа жртве и дуготрајних проблема у доказивању сопственог идентитета. Овај облик криминалитета представља посебно озбиљан изазов у савременом дигиталном друштву, имајући у виду масовну употребу интернета и све већу количину личних података који се размењују у електронском облику.

4.1.2. Крађа података

Крађа података представља један од најзначајнијих облика компјутерске крађе, који је посебно добио на значају са развојем информационо-комуникационих технологија. Савремено дигитално окружење омогућило је масовно прикупљање, складиштење и размену података, што је истовремено отворило простор за њихову злоупотребу и нелегалну трговину.

Посебну вредност на „црном тржишту“ имају подаци који се односе на пословне тајне, будући да директно утичу на конкурентску позицију привредних субјеката. Трговина овим подацима одвија се путем различитих интернет сервиса, укључујући анонимне платформе, дискусионе групе и друге облике онлајн комуникације, који омогућавају прикривање идентитета учесника и отежавају откривање извршилаца.[130]

Кључну улогу у овом облику криминалитета има анонимност виртуелног простора, која смањује ризик од откривања и подстиче извршење ових дела. Поред тога, употреба криптографских метода и анонимних комуникационих алата додатно отежава праћење незаконитих активности.

Међу најпознатијим случајевима крађе података издвајају се случајеви попут *Yahoo* (2013-2014), где је извршена крађа података са преко 3 милијарде налога;[131] напада на Републички геодетски завод из 2022. године када је више од месец дана био

[128] Equifax Data Breach. Преузето: 1.4.2026. https://archive.epic.org/privacy/data-breach/equifax/
[129] Овај случај изазвао је велико интересовање јавности јер је суд утврдио да је украден идентитет Андреја Вучића и још неколико особа како би се основале фантомске фирме за прање новца. KRIK. Преузето: 7.3.2026. https://www.krik.rs/wp-content/uploads/2016/12/Slu%C4%8Daj-Asomakum-pred-Prekr%C5%A1ajnim-sudom.pdf
[130] А. Трифуновић, *op. cit.*, стр. 26.
[131] Huntress, Yahoo Data Breach. Преузето: 2.4.2026. https://www.huntress.com/threat-library/data-breach/yahoo-data-breach

онемогућен рад система и угрожена безбедност података[132]; напада на ЕПС из 2023. године, када је извршена компромитација система и потенцијална крађа интерних података;[133] као и најновији напади, попут Телекома (март 2026. године)[134] и једне приватне клинике.[135]

Иако крађа пословних тајни није нова појава, интернет и дигиталне технологије су значајно проширили њене размере и омогућили брзу и глобалну размену украдених података. У том контексту, заштита података, нарочито пословних тајни, постаје један од кључних изазова савременог правног и економског система.

4.1.3. Крађа лозинки, кодова и идентификационих бројева

Крађа лозинки, кодова и идентификационих бројева представља специфичан облик компјутерске крађе који се може упоредити са крађом кључева у физичком свету. Ови подаци функционишу као „логички кључеви“, који омогућавају приступ заштићеним системима, налозима и информацијама.[136]

Прибављањем ових података, учинилац стиче могућност неовлашћеног приступа различитим дигиталним ресурсима, што често представља увод у извршење других облика компјутерског криминалитета, као што су крађа идентитета или финансијске преваре.

Начини извршења овог облика крађе у великој мери се поклапају са методама које се користе код крађе идентитета, укључујући фишинг нападе, злонамерни софтвер и технике социјалног инжењеринга.[137] Поменути примери из домаће праксе јасно илуструју ову појаву; у случају хакерског напада на Републички геодетски завод 2022. године, нападачи су претходно пресрели и прибавили службене мејл акредитиве и

[132] BIRN, Hakeri imali pristup mejlovima zaposlenih u katastru Srbije, stručnjaci kažu da opasnost još nije prošla. Преузето: 2.4.2026. https://birn.rs/hakeri-imali-pristup-mejlovima-zaposlenih-u-katastru-srbije-strucnjaci-kazu-da-opasnost-jos-nije-prosla/

[133] Nova.rs, Objavljeno ko je izvršio hakerski napad na EPS — grupa preuzela sve podatke i preti da će ih objaviti u roku od 10 dana. Преузето: 2.4.2026. https://nova.rs/vesti/biznis/objavljeno-ko-je-izvrsio-hakerski-napad-na-eps-grupa-preuzela-sve-podatke-i-preti-da-ce-ih-objaviti-u-roku-od-10-dana/

[134] Mts.rs, Saopštenje Telekoma Srbija. Преузето: 2.4.2026. https://mts.rs/Privatni/Korisnicka-zona/Vesti/Servisne-informacije/a129765-Saopstenje-Telekoma-Srbija.html;
Danas, Podaci građana, bezbednost podataka, Telekom Srbija, hakerski napad, 600.000 korisnika. Преузето: 2.4.2026. https://www.danas.rs/vesti/ekonomija/podaci-gradjana-bezbednost-podataka-telekom-srbija-hakerski-napad-600-000-korisnika/

[135] Radio Slobodna Evropa, Srbija - hakerski napad, medicinski podaci. Преузето: 2.4.2026. https://www.slobodnaevropa.org/amp/srbija-hakerski-napad-medicinski-podaci/33723353.html

[136] С. Петровић, *Компјутерски криминал*, Министарство унутрашњих послова Републике Србије-Уредништво часописа „Безбедност" и „Полицајац", Београд, 2000, стр. 126.

[137] Računarski fakultet, Zlonamerni softver Alien predstavlja sve veću pretnju za korisnike mobilnog bankarstva. Преузето: 2.4.2026. https://raf.edu.rs/citaliste/clanci/svastara/zlonamerni-softver-alien-predstavlja-sve-vecu-pretnju-za-korisnike-mobilnog-bankarstva/

администраторске лозинке запослених, искористивши их као логичке кључеве за инфицирање целокупног мејл сервера државне институције. [138] Слично томе, безбедносни инциденти у ЕПС-у и Телеком Србији показали су да компромитација приступних кодова и корисничких лозинки омогућава извршиоцима неовлашћен улазак унутар дигиталне инфраструктуре, што је резултирало масовним секундарним последицама у виду изнуде и цурења комплетних база података грађана.[139] Исто тако, мотиви извршилаца најчешће су стицање материјалне користи или омогућавање даљих незаконитих активности.

Због своје улоге у омогућавању приступа осетљивим подацима и системима, овај облик компјутерске крађе има значајне безбедносне импликације и захтева посебну пажњу у оквиру система заштите информација.

4.1.4. Савремени облици компјутерске крађе (фишинг, злоупотребе система и др.)

Развој ИКТ условио је појаву нових, све софистицираних облика компјутерске крађе, који се разликују од традиционалних облика како по начину извршења, тако и по обиму и последицама. Савремени облици компјутерске крађе карактеришу се високим степеном техничке сложености, транснационалним карактером и тешкоћама у откривању и доказивању.

Један од најраспрострањенијих облика јесте фишинг.[140] Традиционални фишинг је заправо тзв. смишинг (енгл. *smishing*),[141] који се састоји у слању лажних СМС порука, врло често се јавља у пракси. На пример, грађани масовно добијају СМС поруке са лажним линком за исплату царине или трошкова доставе, које наводно шаље Пошта Србије. Када кликну, систем их води на лажну страницу која је дизајнирана тако да

[138] Преузето: 2.4.2026. https://birn.rs/hakeri-imali-pristup-mejlovima-zaposlenih-u-katastru-srbije-strucnjaci-kazu-da-opasnost-jos-nije-prosla/
[139] Преузето: 2.4.2026. https://www.danas.rs/vesti/ekonomija/podaci-gradjana-bezbednost-podataka-telekom-srbija-hakerski-napad-600-000-korisnika/komentari/
[140] Више о томе доступно на: E. Cahill, „What's the Difference Between Phishing, Smishing and Vishing?", Experian, 20.3.2022. Преузето: 27.7.2026. https://www.experian.com/blogs/ask-experian/phishing-smishing-vishing/
[141] Код смишинга (енгл. *smishing - SMS phishing*), нападачи користе текстуалну комуникацију, углавном путем лажних СМС порука или апликација за размену порука, лажно се представљајући као легитимне институције, банке или курирске службе. Напад се заснива на измишљеним причама које код жртве изазивају осећај хитности како би она отворила злонамерни линк, што нападачима омогућава крађу личних података, лозинки или неовлашћени приступ финансијским рачунима. Више о томе: M. Kosinski, „What is smishing (SMS phishing)?", IBM Think, 24.6.2024. Преузето: 26.6.2026. https://www.ibm.com/think/topics/smishing

заобиђе безбедносне протоколе банке.[142] Напади су се ослањали на масовно произведене, генеричке поруке дизајниране да преваре кориснике како би открили осетљиве информације. Такве поруке често показују препознатљиве недостатке, укључујући граматичке грешке или сумњиве линкове, што је омогућавало њихово релативно лако препознавање од стране корисника и система заштите.[143] Међутим, развој вештачке интелигенције омогућава креирање високо персонализованих, контекстуално релевантних и језички исправних порука у великом обиму, чиме се значајно смањује могућност њиховог откривања традиционалним методама.

Други врло чест облик фишинга јесте тзв. вишинг (енгл. *vishing*), тј. преваре путем телефонских позива или говорних порука .[144]

Заједнички циљ свих ових модалитета јесте да се корисници наведу на откривање поверљивих информација, као што су корисничка имена, лозинке, бројеви платних картица или други лични идентификациони подаци.[145]

Поред текстуалних порука, савремени нападачи користе и напредне технике као што су клонирање гласа, измена гласа у реалном времену и дипфејк (енг. *deepfake*) видео садржаји,[146] чиме се додатно повећава уверљивост преваре. Ове технологије омогућавају да се жртве доведу у заблуду чак и током телефонских или видео комуникација.[147]

Такође, значајно је повећан обим и брзина извршења напада. Док је раније било потребно значајно време за креирање појединачних фишинг порука, савремени језички модели могу генерисати велики број варијација у кратком временском периоду. Поред

---

[142] RTS, Pošte Srbije - prevara. Преузето: 2.4.2026. https://www.rts.rs/lat/vesti/drustvo/5351451/poste-srbije-prevara-.html

[143] Insajder, NBS upozorava: fišing i investiciona prevara - dva najčešća tipa SMS prevarnih šema. Преузето: 23.6.2026. https://insajder.net/prenosimo/nbs-upozorava-fising-i-investiciona-prevara-dva-najcesca-tipa-sms-prevarnih-sema

[144] Код вишинга (енгл. *vishing - voice phishing*), нападачи користе гласовну комуникацију, често путем аутоматизованих робо-позива, лажно се представљајући као агенти легитимних компанија. Поједини преваранти снимају глас жртве постављајући питања на која је највероватнији одговор „Да", како би тај звучни запис касније злоупотребили за ауторизацију нелегалних финансијских трансакција преко телефона. Више о томе доступно на: E. Cahill, „What's the Difference Between Phishing, Smishing and Vishing?", Experian, 20.3.2022. Преузето: 27.7.2026. https://www.experian.com/blogs/ask-experian/phishing-smishing-vishing/

[145] *ibid.*

[146] Појава лажних видео снимака на друштвеним мрежама у којима познати лекари или политичари у Србији „рекламирају" сумњиве лекове или инвестиционе платформе. Nova.rs, Poplava lažnih reklama na društvenim mrežama u kojima se promovišu suplementi - zloupotrebljen lik Danice Grujičić, Branimira Nestorovića, Tatjane Vojtehovski. Преузето: 2.4.2026. https://nova.rs/vesti/hronika/poplava-laznih-reklama-na-drustvenim-mrezama-u-kojima-se-promovisu-suplementi-zloupotrebljen-lik-danice-grujicic-branimira-nestorovica-tatjane-vojtehovski-foto/

[147] T. Nakovski, N. Blazheska Tabakovska, M. Bogdanoska Jovanovska, AI-Driven Phishing Attacks: Emerging Threats and Security Strategies, *Serbian Journal of Engineering Management Special Edition*, 2026, p. 21.

тога, употреба података из реалног окружења, као што су актуелне вести, пословни догађаји и лични подаци корисника, омогућава креирање изузетно уверљивих и циљаних напада.

Овакви трендови представљају озбиљан изазов за постојеће механизме сајбер безбедности и указују на потребу за развојем нових, напреднијих система за детекцију и превенцију, а основ успеха фишинг напада лежи у злоупотреби поверења и недовољне информисаности корисника.

Поред фишинга, значајан облик представљају и злоупотребе рачунарских система, које обухватају неовлашћен приступ системима, искоришћавање безбедносних пропуста и незаконито преузимање контроле над информационим ресурсима. Ове активности често укључују употребу злонамерног софтвера.[148]

Посебан вид савремених облика компјутерске крађе представљају напади засновани на социјалном инжењерингу, који се не ослањају искључиво на техничке рањивости, већ пре свега на психолошку манипулацију корисника. Учиниоци користе различите технике обмане како би навели жртву да добровољно открије осетљиве податке или омогући приступ систему.[149]

У пракси се све чешће јављају и комбиновани облици напада, у којима се истовремено користе различите методе, као што су фишинг поруке у комбинацији са злонамерним софтвером. Ови облици напада могу довести до масовних злоупотреба података, финансијских губитака и нарушавања безбедности информационих система.

Имајући у виду наведено, може се закључити да савремени облици компјутерске крађе представљају динамичну и стално еволуирајућу категорију криминалитета, која захтева континуирано унапређење правних и техничких механизама заштите, као и подизање свести корисника о ризицима у дигиталном окружењу.

4.2. Компјутерска (рачунарска) превара

Компјутерска превара представља један од најраспрострањенијих облика компјутерског криминалитета. Она подразумева манипулисање рачунарским системом, било изменом софтвера, било злоупотребом хардвера, са циљем прибављања противправне имовинске користи или наношења штете другом лицу.[150] До преваре може доћи уношењем нетачних података у рачунарски систем, пропуштањем уношења

[148] А. Трифуновић, *op. cit.,* стр. 20.
[149] А.Ђукић, *op. cit.*, стр. 106.
[150] В. Николић Ристановић, С. Константиновић Вилић, *op. cit.,* стр. 175.

тачних података или на други начин злоупотребом рачунара у сврху обмане. У пракси се јавља велики број различитих облика ових превара - од једноставних и грубих до веома сложених, које извршиоци реализују уз висок степен техничке стручности.[151]

Код компјутерских превара заблуда се не односи на човека, већ на рачунарски систем, у који се уносе нетачни подаци, пропушта уношење тачних података или се рачунар користи на други начин како би се остварила противправна имовинска корист.[152] Ово потврђује и судска пракса, па се тако у Пресуди Врховног суда, Кзз 779/23 од 19.9.2023. године истиче да кривично дело рачунарска превара представља посебан облик преваре, али се од кривичног дела превара разликује пре свега с обзиром на то да у овом случају нема довођења или одржавања у заблуди неког лица, па се зато случајеви компјутерске преваре не могу подвести под опште кривично дело преваре.[153]

Компјутерска превара представља озбиљан проблем савременог друштва и може се извршити различитим техникама, као што су манипулација подацима у рачунарским системима, злоупотреба електронских система плаћања или неовлашћени приступ финансијским информацијама.[154] Последице оваквих радњи могу бити значајне и укључују финансијске губитке, нарушавање приватности и губитак поверења у електронске системе.[155] Овај облик криминалитета привлачи значајну пажњу јавности, али га је често тешко открити и доказати, јер се извршава сложеним техничким методама.[156]

4.2.1. Нигеријска превара

Нигеријска превара (енгл. *Nigerian scam* или *419 fraud*) представља један од најпознатијих облика интернет превара. Назив потиче од одредбе Кривичног законика Нигерије којом су инкриминисане овакве преварне активности, иако се данас овај модел користи широм света.[157] Суштина преваре огледа се у томе што учинилац контактира потенцијалну жртву електронском поштом, путем друштвених мрежа или апликација за комуникацију, лажно се представљајући као лице које располаже великом сумом новца, наследством или вредном имовином, уз обећање да ће део тог

[151] *ibid.*
[152] Д. Димовски, *op. cit.*, стр. 205.
[153] Пресуда Врховног суда, Кзз 779/23 од 19.9.2023. године. Propisi.net. Преузето: 7.3.2026. https://pn2.propisi.net/Home/ShowDocument/?di=rp39580&dt=rp&dl=13804
[154] М. Зиројевић, З. Ивановић, *Сајбер законодавство Србије - други део*, Београд, 2025, стр. 163.
[155] М. Бошковић, *Криминологија*, Нови Сад, 2020, стр. 368.
[156] Д. Димовски, *op. cit.*, стр. 205.
[157] Х. Стевић, *Компјутерска превара (мастер рад)*, Правни факултет Универзитета у Нишу, Ниш, 2020, стр. 27-32. Преузето: 15.5.2026. https://www.prafak.ni.ac.rs/files/master-radovi/9_ZMR_Hristina_Stevic.pdf

новца припасти примаоцу поруке уколико претходно уплати одређени износ ради наводних административних трошкова, пореза или банкарских провизија.[158]

Ова врста преваре заснива се на злоупотреби поверења и психолошкој манипулацији жртвом, док се ИКТ користе као средство масовног ширења лажних порука. Иако су појединачни новчани износи које жртве уплаћују често релативно мали, велики број оштећених лица омогућава извршиоцима стицање значајне противправне имовинске користи.[159]

Савремени облици нигеријске преваре прилагођени су дигиталном окружењу, па се поруке често персонализују, користе се украдени идентитети, фотографије и лажни документи, чиме се повећава вероватноћа да ће жртва поверовати у истинитост понуде.[160]

Према нашем мишљењу, специфичност нигеријске преваре огледа се у чињеници да успех извршења не зависи првенствено од техничке сложености напада, већ од способности учиниоца да применом метода социјалног инжењеринга стекне поверење оштећеног. У савременом дигиталном окружењу, где су лични подаци великог броја корисника јавно доступни, а комуникација се одвија претежно електронским путем, овакав облик преваре постаје све убедљивији и друштвено опаснији. Због тога је, поред кривичноправне заштите, неопходно континуирано подизање свести корисника о техникама манипулације које преваранти користе приликом успостављања контакта са потенцијалним жртвама.

4.2.2. Преваре ауторитета

Преваре ауторитета заснивају се на злоупотреби поверења које грађани имају према државним органима, банкама, полицији, пореским управама или другим институцијама.[161] Извршиоци се представљају као службена лица или представници познатих организација и на тај начин наводе жртву да добровољно достави поверљиве податке, лозинке, бројеве платних картица или да изврши уплату одређеног новчаног износа.[162]

---

[158] *ibid.*
[159] *ibid.*
[160] *ibid.*
[161] Министарство унутрашњих послова Републике Србије, званична интернет презентација. Преузето: 12.6.2026. https://www.mup.gov.rs/
[162] Х. Стевић, *op. cit.*, стр. 33.

Успех ових превара у великој мери зависи од психолошког ефекта ауторитета, односно уверења жртве да поступа по налогу овлашћеног органа. Због тога извршиоци често користе формалан језик, службене логотипе и друге елементе који повећавају уверљивост преваре.[163]

Мишљења смо да посебна опасност превара ауторитета произлази из чињенице да се оне заснивају на злоупотреби институционалног поверења, које представља један од темеља правног поретка и сигурности правног промета. Развој дигиталних технологија омогућио је извршиоцима да веома верно имитирају комуникацију државних органа, банака и других институција, коришћењем лажних интернет страница, електронских адреса, логотипа и бројева телефона. Због тога грађани често не могу лако да уоче разлику између легитимне и лажне комуникације, што овом облику компјутерске преваре даје изразиту друштвену опасност. Ефикасна превенција ових превара подразумева не само кривичноправну заштиту, већ и континуирано информисање грађана о начинима на које надлежне институције остварују службену комуникацију са корисницима.

4.2.3. Спам преваре

Спам преваре (енгл. *spam scams*) представљају облик компјутерске преваре који се заснива на масовном слању нежељених електронских порука великом броју корисника интернета.[164] Основни циљ оваквих порука јесте да примаоца наведу да отвори злонамерни линк, преузме заражени прилог или достави личне и финансијске податке.[165]

Иако већина прималаца препозна овакве поруке као нежељене, довољно је да мали број корисника реагује како би превара била финансијски исплатива. Поред директне имовинске штете, спам поруке представљају значајан механизам ширења злонамерног софтвера, фишинг напада и различитих облика крађе идентитета.

Развој аутоматизованих система за масовно слање електронске поште омогућио је извршиоцима да уз минималне трошкове истовремено контактирају милионе потенцијалних жртава, што овај облик преваре чини једним од најраспрострањенијих у сајбер простору.[166]

---

[163] *ibid.*
[164] *ibid.,* 36.
[165] *ibid.*
[166] *ibid.*

За разлику од већине других облика компјутерских превара, код спам превара извршиоци рачунају на статистички ефекат масовности. Слањем великог броја идентичних порука значајно се повећава вероватноћа да ће одређени број корисника поступити по упутствима из поруке, без обзира на то што већина прималаца препознаје превару. Из тог разлога, овај модел представља један од најекономичнијих начина извршења компјутерских превара, а његова распрострањеност указује да технолошки развој истовремено повећава и могућности за злоупотребу електронских комуникација.

4.2.4. Преваре са наградама

Код превара са наградама учиниоци обавештавају жртву да је наводно освојила вредну награду, новац, аутомобил или путовање, иако претходно није учествовала ни у каквој наградној игри. Да би награда наводно могла бити исплаћена, од оштећеног се захтева плаћање пореза, административних трошкова, поштарине или других накнада, након чега учинилац прекида сваку комуникацију.[167]

Ова врста преваре заснива се на стварању осећаја хитности и узбуђења код жртве, чиме се смањује могућност рационалне процене истинитости понуде. У савременим условима овакве преваре најчешће се реализују путем електронске поште, СМС порука и друштвених мрежа.

Специфичност превара са наградама огледа се у томе што њихов успех почива на искоришћавању људске склоности ка брзој и неочекиваној материјалној добити. Из тог разлога, извршиоци најчешће настоје да код жртве створе уверење да је реч о јединственој прилици која захтева хитну реакцију, чиме се умањује могућност критичког преиспитивања истинитости примљене поруке. У савременом дигиталном окружењу, овакве преваре додатно добијају на уверљивости захваљујући могућности злоупотребе визуелног идентитета познатих компанија и институција, што њихово благовремено препознавање чини знатно тежим.

4.2.5. Преваре са злонамерним апликацијама

Преваре са злонамерним апликацијама заснивају се на дистрибуцији програма који се представљају као легитимне мобилне или рачунарске апликације, а у стварности садрже злонамерни код. Инсталирањем таквих програма корисник несвесно омогућава приступ својим личним подацима, лозинкама, банкарским информацијама или другим

[167] *ibid.,* 42-43.

осетљивим садржајима који се налазе на уређају.[168] Злонамерне апликације могу бити представљене као програми за убрзавање рада телефона, антивирусни софтвер, игре или апликације за комуникацију. Након инсталације оне могу преузимати податке, снимати активности корисника, пресретати комуникацију или омогућити удаљену контролу уређаја.[169]

Посебну опасност представља чињеница да се овакве апликације често пласирају преко незваничних продавница апликација или путем линкова који се достављају електронском поштом и друштвеним мрежама, што значајно повећава број потенцијалних жртава.

Може се закључити да преваре са злонамерним апликацијама представљају један од најопаснијих облика компјутерских превара, јер жртва често није ни свесна да је компромитовала сопствени уређај. За разлику од појединих других облика интернет превара, код којих је неопходно активно поступање оштећеног, овде је довољна једна непромишљена инсталација апликације како би нападач стекао дуготрајан приступ осетљивим подацима. Због тога је, поред примене техничких мера заштите, од посебног значаја едукација корисника о преузимању апликација искључиво из проверених извора и пажљивој провери дозвола које се одобравају приликом инсталације.

4.2.6. Преваре из области електронског банкарства

Развој електронског банкарства значајно је унапредио брзину и доступност финансијских услуга, али је истовремено створио нове могућности за извршење различитих облика компјутерских превара. Преварама из области електронског банкарства сматрају се све противправне активности усмерене на неовлашћено прибављање новчаних средстава или осетљивих банкарских података злоупотребом електронских платних система, интернет банкарства и мобилних банкарских апликација.

Најчешћи облици ових превара подразумевају крађу корисничких имена и лозинки за приступ електронском банкарству, неовлашћено преузимање контроле над корисничким налогом, злоупотребу платних картица, пресретање једнократних

[168] *ibid.,* 45.
[169] *ibid.,* 45-47.

сигурносних кодова, као и навођење корисника да добровољно доставе своје банкарске податке путем лажних интернет страница, електронске поште или СМС порука.[170]

Извршиоци често комбинују различите технике социјалног инжењеринга са техничким средствима, настојећи да стекну поверење корисника и наведу их да сами открију поверљиве податке или одобре неовлашћене трансакције.[171]

Посебну опасност представљају злонамерни програми (банкарски тројанци) који се инсталирају на рачунар или мобилни уређај корисника, омогућавајући учиниоцима пресретање података за аутентификацију, праћење активности корисника и неовлашћено располагање средствима са банковних рачуна.[172]

Може се закључити да преваре из области електронског банкарства представљају један од најдинамичнијих и најопаснијих облика компјутерских превара, јер су непосредно усмерене на финансијску имовину грађана и привредних субјеката. Њихова специфичност огледа се у томе што се успех преваре најчешће заснива на комбинацији техничких средстава и психолошке манипулације корисником, због чега ни најсавременији системи заштите не могу обезбедити потпуну сигурност без одговарајућег нивоа дигиталне писмености корисника. Управо из тог разлога, поред континуираног унапређења безбедносних механизама електронског банкарства, неопходно је и стално информисање грађана о најчешћим облицима превара и начинима њиховог препознавања.

4.3. Компјутерска (рачунарска) саботажа

Сам појам саботаже (фран. *sabotage*) означава намерно и противправно кварење или уништавање одређених добара ради наношења штете и изазивања поремећаја у функционисању система.[173] Компјутерска саботажа представља криминалну активност усмерену на ометање или уништавање функционисања рачунарских система. У контексту информационих технологија, рачунарска саботажа подразумева намерно уништавање или оштећење рачунарских система, података или програма са циљем да се онемогући или значајно отежа њихово функционисање.

---

[170] NBS. Преузето: 27.6.2026. https://nbs.rs/sr/scripts/showcontent/index.html?id=19190, https://www.nbs.rs/sr/scripts/showcontent/index.html?id=21393, https://nbs.rs/sr/scripts/showcontent/index.html?id=19190

[171] Х. Стевић, *op. cit.*, стр. 49.

[172] *ibid.*

[173] Vokabular.org. Преузето: 8.3.2026. https://www.vokabular.org/?search=sabota%C5%BEa&lang=sr-lat#google_vignette

У праву Републике Србије рачунарска саботажа инкриминисана је чланом 299. Кривичног законика. Према законској дефиницији, ово кривично дело постоји када учинилац *унесе, уништи, избрише, измени, оштети, прикрије или на други начин учини неупотребљивим рачунарски податак или програм, или уништи односно оштети рачунар или други уређај за електронску обраду и пренос података, са намером да онемогући или знатно омете поступак електронске обраде и преноса података који су од значаја за државне органе, јавне службе, установе, предузећа или друге субјекте. За ово кривично дело прописана је казна затвора од шест месеци до пет година*.[174]

Из законског описа произлази да се рачунарска саботажа може испољити у два основна облика. Први облик односи се на незаконите радње усмерене на рачунарске податке или програме, као што су њихово брисање, измена, оштећење или прикривање.[175] Други облик обухвата уништење или оштећење рачунара или других уређаја за електронску обраду података, чиме се директно угрожава функционисање информационог система.[176]

Она се може поделити на физичку и логичку саботажу. Физичка саботажа подразумева физичко оштећење или уништење рачунара и других уређаја за обраду података, док логичка саботажа обухвата брисање, модификовање или спречавање коришћења информација које се налазе у меморији рачунарских система.[177]

Компјутерска саботажа обухвата различите активности као што су брисање важних информација, измена података или програма, као и упади у рачунарски систем ради ометања његовог нормалног функционисања.[178]

У пракси се рачунарска саботажа често извршава употребом различитих злонамерних софтвера, као што су вируси, „тројански коњи“, рачунарски црви и друге врсте штетних програма који могу довести до оштећења података или ометања рада система.[179] Ови програми омогућавају учиниоцу да на даљину измени или уништи податке, блокира приступ систему или изазове поремећаје у раду информационе инфраструктуре.

Посебна карактеристика овог кривичног дела јесте постојање намере да се онемогући или значајно омете поступак електронске обраде и преноса података. Због

[174] Кривични законик, чл. 299.
[175] З. Стојановић, О. Перић, *Кривично право – посебни део*, Београд, 2009, стр. 253–254.
[176] *ibid.*
[177] Д. Димовски, *op. cit.*, стр. 206.
[178] М. Зиројевић, З. Ивановић, *op.cit*, стр. 163.
[179] Ж. Миладиновић Богавац, Рачунарска саботажа, *FBIM Transactions,* бр. 1, 2019, стр. 3. Преузето: 8.3.2026. https://www.meste.org/fbim/fbim_srpski/FBIM_najava/XIV_Miladinovic.pdf

тога се рачунарска саботажа може извршити искључиво са директним умишљајем, јер је управо намера кључни субјективни елемент овог кривичног дела.[180] Дело се не може извршити нечињењем већ само чињењем, тј. активним поступањем.[181]

4.4. Компјутерски (рачунарски) тероризам

Компјутерски тероризам (енгл. *cyberterrorism*)[182] представља посебно опасан облик савременог криминалитета и најчешће се дефинише као акт уништавања или ометања компјутерског система са циљем дестабилизације једне државе или вршења притиска на њену владу.[183] Међутим, постоје и друге дефиниције компјутерског тероризма.[184]

У литератури се компјутерски тероризам најчешће класификује кроз три вида деловања на системе. Физички напади подразумевају директно уништавање хардвера конвенционалним средствима, попут експлозива. Синтатички напади усмерени су на измену унутрашње логике софтвера (нпр. путем вируса) како би се изазвали застоји или систем учинио непоузданим. На крају, семантички напади злоупотребљавају поверење корисника тако што прикривено мењају улазне или излазне податке, чиме се генеришу грешке у раду без знања оператера.[185]

4.5. Компјутерска (рачунарска) порнографија

Компјутерска порнографија обухвата производњу, поседовање, дистрибуцију или приказивање порнографског материјала путем рачунара и интернета. Посебно тежак облик овог криминалитета односи се на дечију порнографију, која подразумева искоришћавање малолетних лица у порнографске сврхе или дистрибуцију таквих садржаја путем интернета. Савремене информационе технологије омогућиле су брзу и масовну дистрибуцију оваквог материјала, што представља озбиљан изазов за кривичноправну заштиту малолетника.[186]

---

[180] *ibid.*
[181] Пресуда Основног суда у Врању, К. бр. 3881/10 од 7.3.2011. године и Пресуда Апелационог суда у Нишу, 7Кж. 1. бр. 2607/11 од 31.8.2012. године. Propisi.net. Преузето: 8.3.2026. https://pn2.propisi.net/Home/ShowDocument/?di=rp39580&dt=rp&dl=13804
[182] B. Collin, The Future of Cyberterrorism, *Crime and Justice International*, Volume 13, Issue 2, 1997, p. 15-17.
[183] Д. Димовски, *op. cit.*, стр. 206.
[184] Више о томе: М. Васић, *op. cit.*, стр. 21-22.
[185] Д. Димовски, *op. cit.*, стр. 206.
[186] М. Зиројевић, З. Ивановић, *op.cit*, стр. 36-38.

На жалост, случајеви дечје порнографије су скоро свакодневни. Практични примери указују на то да објављивање фотографија малолетне деце на друштвеним мрежама може послужити као окидач за сексуално узнемиравање. Забележен је инцидент у којем је мајци из Крагујевца непознати починилац упућивао непримерне захтеве након што је јавно поделила слику бебе са летовања. Овај пример потврђује тезу да предатори користе јавно доступне информације како би ступили у контакт са потенцијалним жртвама или њиховим законским заступницима. [187]

Нарочито забрињавају случајеви у којима се као починиоци појављују родитељи, чиме се из корена руши претпоставка о породици као сигурном окружењу. Драстичан пример забележен је 2020. године у околини Панчева, где је отац извршио кривично дело обљубе над својом малолетном ћерком. Овај случај пратила је и додатна дигитална виктимизација: починилац је неовлашћено снимао и фотографисао чин, а затим путем више лажних профила на друштвеним мрежама дистрибуирао експлицитан садржај својим контактима. Овакво поступање указује на спрегу директног физичког насиља и злоупотребе информационих технологија у сврху даље експлоатације жртве.[188]

Такође, не сме се занемарити ни постојање тзв. „осветничке порнографије“, тј. дељење експлицитних фотографија или снимака бивших партнера без њиховог пристанка, најчешће из разлога освете према бившем партнеру.

Према нашем мишљењу, компјутерска порнографија представља један од друштвено најопаснијих облика компјутерског криминалитета, јер поред повреде полне слободе и достојанства жртве омогућава брзо и неконтролисано ширење незаконитог садржаја у дигиталном окружењу. Посебну тежину овим кривичним делима даје чињеница да се једном објављен порнографски материјал тешко може у потпуности уклонити са интернета, што последице виктимизације чини дуготрајним, а често и трајним. Управо због тога, ефикасна борба против овог облика криминалитета захтева истовремено деловање кривичноправних механизама, техничких мера за уклањање незаконитог садржаја и континуиране едукације деце, родитеља и других корисника интернета.

---

[187] Blic, Roditelji, oprez - dovoljno je da jednom objavite sliku vašeg golišavog deteta. Преузето: 8.3.2026. https://www.blic.rs/vesti/drustvo/roditelji-oprez-dovoljno-je-da-jednom-objavite-sliku-vaseg-golisavog-deteta-i-da-tako/2xmbqgw, наведено према: Александра Николић, *op. cit.*, стр. 40.

[188] Blic, Obljubio ćerku i sve snimio - otac monstrum iz sela kod Pančeva. Преузето: 11.3.2026. https://www.blic.rs/vesti/hronika/obljubio-cerku-i-sve-snimio-otac-monstrum-iz-sela-kod-panceva-devojcicine-gole/eflfn2k, наведено према: *ibid.*, стр. 42.

4.6. Дипфејк

Термин дипфејк (енгл. *deepfake*) настао је на платформи *Reddit* крајем 2017. године. Корисник под псеудонимом „*u/deepfakes*" објавио је тада монтиран експлицитни снимак познате глумице, што је довело до оснивања наменске заједнице „*r/deepfakes*".[189] Сама реч представља кованицу енглеских појмова „*deep*" (који се односи на дубоко учење напредних система вештачке интелигенције) и „*fake*" (лажно). Овај израз обухвата све облике дигитално изманипулисаних аудио-визуелних записа - од сензационалистичких лажних вести и изјава политичара у сврхе пропаганде или сатире, до емитовања исказа наводних жртава измишљених злочина (енгл. *deep true crime*).[190]

Дипфејк технологија представља један од најсавременијих начина злоупотребе вештачке интелигенције у оквиру компјутерског криминалитета. Њеном применом могу се креирати веома уверљиви фото, аудио и видео записи који не одговарају стварности, али код просечног корисника остављају утисак аутентичности.[191] Поред угрожавања права личности, ова технологија све чешће се користи и као средство за извршење других кривичних дела, попут компјутерских превара, изнуда, крађе идентитета и манипулације јавним мњењем. Посебан ризик представља могућност да се дипфејк садржај искористи за имитирање гласа или лика одређене особе ради прибављања противправне имовинске користи или изазивања штетних последица по оштећеног.

Дипфејк технологија представља значајан изазов за савремено кривично право, јер традиционални механизми доказивања све теже могу да разликују аутентичан од вештачки генерисаног садржаја. Истовремено, брзина развоја система заснованих на вештачкој интелигенцији превазилази динамику законодавних измена, због чега се у пракси јављају бројне недоумице у погледу правне квалификације појединих радњи и одговорности учинилаца.

Наведене опасности нису више само теоријске природе, већ су потврђене и у савременој пракси. Тако је почетком 2024. године у Хонг Конгу забележен случај у

---

[189] A. Pechenik Gieseke, "The New Weapon of Choice": Law's Current Inability to Properly Address Deepfake Pornography, *Vanderbilt Law Review*, vol. 73, iss. 5, 2020, p. 1484–1485. Преузето: 10.3.2026. https://scholarship.law.vanderbilt.edu/vlr/vol73/iss5/4/

[190] Н. Мрвић Петровић, Кривичноправни приступ регулисању дигиталне порнографије настале употребом вештачке интелигенције (non-consesual deepfake porn), *Безбедност*, бр. 2/2024, Београд, стр. 6.

[191] М. Момчиловић, *Видео снимци генерисани уз помоћ вештачке интелигенције (дипфејк) као облик сајбер криминалитета (мастер рад),* Правни факултет Универзитета у Нишу, Ниш, 2024, стр. 22. Преузето: 11.3.2026. https://www.prafak.ni.ac.rs/files/master-radovi/13-ZMR_MilicaMomcilovic_M033_23_UP.pdf

којем су извршиоци употребом дипфејк видео-конференције успешно имитирали главног финансијског директора једне мултинационалне компаније, услед чега је запослени извршио трансфер од приближно 23 милиона евра на рачуне превараната.[192] Сличан случај забележен је и у Великој Британији, где је синтетички генерисан глас руководиоца искоришћен за навођење запосленог да изврши неовлашћено плаћање значајног новчаног износа.[193] Ови примери указују на то да дипфејк технологија више није средство искључиво за ширење дезинформација, већ се све чешће користи и као инструмент извршења сложених компјутерских превара и финансијског криминалитета.

Може се закључити да ће ефикасна борба против злоупотребе дипфејк технологије захтевати не само унапређење кривичноправне регулативе, већ и развој техничких механизама за откривање вештачки генерисаног садржаја, као и јачање дигиталне писмености грађана.

V ПРЕВЕНЦИЈА И СУЗБИЈАЊЕ КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА

5.1. Друштвена контрола

Превенција компјутерског криминалитета захтева свеобухватан, системски и мултидисциплинаран приступ који превазилази традиционалне оквире кривичноправног реаговања и обухвата координисано деловање на технолошком, правном, институционалном и ширем друштвеном нивоу. Ефикасна стратегија супротстављања овом облику криминалитета не подразумева само развој нормативног оквира и јачање капацитета органа формалне контроле, већ и континуирано унапређење безбедносне културе и свести грађана, запослених у јавном сектору и привредних субјеката о ризицима који произлазе из употребе дигиталних технологија. Савремени концепт сајбер безбедности више се не може посматрати као искључива надлежност специјализованих државних органа, већ као систем заједничке одговорности свих учесника дигиталног окружења.

Друштвена контрола компјутерског криминалитета заснива се на међусобном деловању формалних и неформалних механизама контроле. Формална друштвена

[192] Euronews Srbija, Deepfake tehnologija u službi bankarskih prevara - vaš novac je u opasnosti sedam dana u nedelji. Преузето: 5.7.2026. https://www.euronews.rs/biznis/biznis-vesti/120382/deepfake-tehnologija-u-sluzbi-bankarskih-prevara-vas-novac-je-u-opasnosti-sedam-dana-u-nedelji/vest

[193] Bitdefender, Deepfake Boss Scam: CEO Impersonation BEC. Преузето: 5.7.2026. https://www.bitdefender.com/en-us/blog/hotforsecurity/deepfake-boss-scam-ceo-impersonation-bec

контрола сајбер криминалитета остварује се кроз организовану и институционализовану активност државних органа, пре свега полиције, специјализованих организационих јединица за борбу против високотехнолошког криминалитета, јавног тужилаштва и судова.

Значајан међународни инструмент у овој области представља Будимпештанска конвенција, која успоставља стандарде за усклађивање националних законодавстава и механизме међународне сарадње у борби против компјутерског криминалитета.[194] У Републици Србији посебан значај има Посебно одељење за борбу против високотехнолошког криминала, које је образовано у оквру Вишег јавног тужилаштва у Београду. [195] Формални механизми контроле укључују примену кривичноправних норми, дигиталну форензику, прикупљање електронских доказа и међународну оперативну сарадњу, посебно имајући у виду чињеницу да компјутерски криминалитет има транснационални карактер.

Неформална друштвена контрола представља допунски механизам превенције који се остварује кроз деловање породице, образовног система, струковних организација, медија и организација цивилног друштва. За разлику од формалне контроле, која се заснива на правним санкцијама и институционалном реаговању, неформална контрола делује кроз развијање друштвених вредности, јачање одговорног понашања и усвајање правила безбедног коришћења дигиталних технологија.

Посебан аспект неформалне друштвене контроле представља индивидуална превенција сајбер криминалитета, која подразумева одговорно и безбедносно оријентисано понашање сваког појединачног корисника информационих технологија. Будући да су грађани и запослени у организацијама често прва линија одбране од дигиталних претњи, степен њихове информисаности и придржавања основних правила сајбер хигијене може значајно утицати на смањење ризика од настанка и последица сајбер напада. Превентивно деловање појединца обухвата примену техничких мера заштите, али и развијање свести о потенцијалним облицима злоупотребе у дигиталном окружењу.[196]

Једна од основних мера индивидуалне превенције јесте коришћење одговарајућих система техничке заштите, пре свега активираних заштитних зидова (енгл. *firewall*) и редовно ажурираних антивирусних програма. Одговорно понашање

[194] Више речи о овоме било је у поглављу 3.1. Међународна регулатива.
[195] Више речи о овоме било је у поглављу 3.2. Република Србија.
[196] Д. Мирковић, *op. cit.*, стр. 103/104.

корисника подразумева и примену адекватних правила приликом управљања приступним подацима. Коришћење сложених и јединствених лозинки, избегавање употребе личних података као елемената лозинке, периодична промена приступних података и примена вишефакторске аутентификације представљају основне мере заштите од неовлашћеног приступа налозима и информационим системима. Ове мере су нарочито значајне у пословном окружењу, где компромитовање једног корисничког налога може довести до угрожавања већег броја података и ресурса организације.[197]

Такође, важан елемент индивидуалне превенције представља редовно прављење резервних копија података, које омогућавају очување информација у случају њиховог случајног брисања, оштећења система или напада путем злонамерног софтвера, попут рансомвера.[198] У области компјутерског криминалитета овај вид контроле има посебан значај јер велики број инцидената настаје услед недовољне информисаности корисника, непажње или недостатка основних знања о дигиталним ризицима. Развијање дигиталне писмености и сајбер хигијене смањује број потенцијалних жртава и повећава отпорност друштва на различите облике дигиталних злоупотреба.[199]

Посебно место у систему неформалне превенције заузима образовање, јер дугорочна заштита дигиталног простора зависи од способности корисника да препознају и адекватно реагују на безбедносне претње. Савремени приступи превенцији сајбер криминалитета наглашавају значај континуираног развоја дигиталних компетенција, како код ученика и грађана, тако и код запослених у јавном и приватном сектору. Програми едукације, националне кампање подизања свести и специјализоване обуке имају за циљ трансформацију пасивних корисника информационих система у активне учеснике система сајбер безбедности. На тај начин друштво постаје отпорније на социјални инжењеринг, фишинг нападе, крађу идентитета и друге облике савременог сајбер криминалитета.

5.2. Улога институција

Ефикасно сузбијање компјутерског криминалитета кроз механизме формалне друштвене контроле заснива се на координисаном деловању специјализованих државних органа, чија је надлежност усмерена на откривање, процесуирање и спречавање кривичних дела у дигиталном окружењу. За разлику од традиционалних

[197] *ibid.*
[198] *ibid.*
[199] *ibid.*

облика криминалитета, компјутерски криминалитет карактеришу висока технолошка сложеност, могућност анонимности учинилаца, брзина извршења и често прекогранична природа последица, што захтева постојање специјализованих институционалних капацитета и континуирано прилагођавање механизама државног одговора.

Кључну улогу у систему сузбијања компјутерског криминалитета у Републици Србији имају већ поменуто Посебно одељење за борбу против високотехнолошког криминала, као део Вишег јавног тужилаштва у Београду, које приликом откривања дела из своје надлежности најближе сарађује са Службом за борбу против организованог криминала Министарства унутрашњих послова Републике Србије. Ови органи представљају централне носиоце формалне контроле у области откривања и процесуирања кривичних дела повезаних са употребом информационих технологија. Њихова активност обухвата откривање дигиталних трагова, обезбеђивање електронских доказа, идентификацију учинилаца и спровођење поступака у случајевима неовлашћеног приступа информационим системима, злоупотребе података, ширења злонамерних програма, интернет превара и других облика сајбер криминалитета.

Поред органа кривичног гоњења, значајну улогу у систему превенције и заштите информационих система имају институције надлежне за информациону безбедност. Национални ЦЕРТ, који функционише у оквиру Регулаторне агенције за електронске комуникације и поштанске услуге (РАТЕЛ), обавља послове превенције и координације активности у области заштите од безбедносних ризика у ИКТ системима од посебног значаја. Његова улога огледа се у праћењу инцидената, пружању упозорења и препорука за заштиту, као и сарадњи са другим субјектима у систему информационе безбедности.[200]

Ефикасност институционалног одговора на сајбер криминалитет у значајној мери зависи од техничке опремљености, развијених капацитета за дигиталну форензику и сталног усавршавања кадрова. Дигитални докази имају специфичну природу јер се могу лако изменити, избрисати или се могу налазити на инфраструктури која припада другим јурисдикцијама. Због тога је неопходно постојање одговарајућих процедура за њихово прикупљање, очување и анализу, како би се обезбедила њихова доказна вредност у кривичном поступку.

[200] Национални ЦЕРТ Републике Србије, званична интернет презентација. Преузето: 7.7.2026. https://www.cert.rs/rs

Институционална превенција компјутерског криминалитета не ограничава се само на репресивно деловање након извршења кривичног дела, већ подразумева и стратешке активности усмерене на управљање безбедносним ризицима, подизање нивоа заштите информационих система и развој безбедносне културе унутар јавног сектора и друштва у целини. Савремени приступ сајбер безбедности заснива се на концепту отпорности, према којем институције морају бити способне не само да реагују на нападе, већ и да их предвиде, спрече и ограниче њихове последице.

5.3. Међународна сарадња

Транснационални карактер сајбер криминалитета представља један од основних разлога због којих национални механизми борбе против ове појаве не могу бити у потпуности ефикасни без развијене међународне сарадње. Учиниоци сајбер кривичних дела често делују са територије једне државе, користе инфраструктуру која се налази у другој држави, док се последице њихових активности могу испољити на територији више различитих држава. Из тог разлога, откривање учинилаца, прикупљање електронских доказа и успешно вођење кривичних поступака често захтевају координацију више националних органа.

Основни међународноправни инструмент у области борбе против сајбер криминалитета представља поменута Будимпештанска конвенција. Поред Будимпештанске конвенције, значајну улогу у међународној борби против компјутерског криминалитета имају билатерални и мултилатерални споразуми о правној помоћи, као и оперативни механизми сарадње у оквиру међународних организација као што су Interpol[201] и Europol.[202] Ови облици сарадње омогућавају размену оперативних информација, координацију истрага, идентификацију учинилаца и заједничко реаговање у случајевима сложених сајбер напада и организованих облика дигиталног криминалитета.[5]

Даљи развој међународне сарадње подразумева континуирано усклађивање националних законодавстава, размену стручних знања, заједничке обуке и развој институционалних капацитета. С обзиром на динамичан развој технологије и појаву нових облика дигиталних злоупотреба, међународна координација представља

[201] Interpol, званична интернет презентација. Преузето: 7.7.2026. https://www.interpol.int/
[202] Europol, званична интернет презентација. Преузето: 7.7.2026. https://www.europol.europa.eu/

неопходан елемент савремене безбедносне архитектуре и један од основних предуслова ефикасног сузбијања сајбер криминалитета.

ЗАКЉУЧАК

Компјутерски криминалитет представља један од најзначајнијих изазова савременог друштва, чији развој непосредно прати динамичан напредак информационо-комуникационих технологија. За разлику од традиционалних облика криминалитета, ова врста криминалних активности одликује се специфичностима које произлазе из природе дигиталног окружења, пре свега могућношћу анонимног деловања, брзином извршења, тешкоћама у откривању учинилаца и прекограничним карактером последица.

У раду је анализиран појам и основне карактеристике компјутерског криминалитета, његови узроци, последице, као и најзначајнији облици испољавања. Анализа различитих облика испољавања компјутерског криминалитета показала је да развој дигиталних технологија истовремено ствара нове могућности за друштвени развој, али и нове ризике који захтевају адекватан правни и институционални одговор.

У погледу правног оквира, Република Србија је успоставила систем кривичноправне заштите који у значајној мери прати међународне стандарде, нарочито кроз усклађивање са Будимпештанском конвенцијом и развој посебних механизама за борбу против високотехнолошког криминала. Ипак, брз развој технологије и појава нових облика дигиталних злоупотреба указују на потребу континуираног прилагођавања законодавства и јачања институционалних капацитета.

Анализа институционалног одговора показала је да ефикасна борба против компјутерског криминалитета не може бити заснована искључиво на репресивном деловању државних органа. Неопходан је свеобухватан приступ који обухвата превенцију, развој безбедносне културе, подизање нивоа дигиталне писмености, унапређење техничких капацитета и јачање сарадње између државних органа, приватног сектора и међународних организација.

Посебан значај има међународна сарадња, јер природа сајбер простора превазилази границе националних правних система. Ефикасно откривање учинилаца и обезбеђивање електронских доказа често захтевају координисано деловање више држава, размену информација и примену заједничких стандарда.

На основу спроведене анализе може се закључити да је полазна хипотеза рада потврђена. Постојећи нормативни и институционални механизми Републике Србије представљају значајну основу за борбу против компјутерског криминалитета, али савремени технолошки развој захтева њихово непрекидно усавршавање. Будућа ефикасност система заштите зависиће од способности државе и друштва да истовремено развијају правне, техничке и превентивне механизме одговора.

Компјутерски криминалитет представља динамичну појаву која се стално мења, због чега борба против њега не може бити једнократан процес, већ трајан задатак усмерен ка очувању безбедности дигиталног окружења и заштити права грађана, привредних субјеката и државних институција.

СПИСАК КОРИШЋЕНЕ ЛИТЕРАТУРЕ

1. Бановић Божидар, *Обезбеђење доказа у криминалистичкој обради кривичних дела привредног криминалитета*, Безбедност, бр. 1, вол. 45, Београд, 2003.
2. Бошковић Мило, *Криминологија*, Нови Сад, 2020.
3. Будимлић Мухамед, Пухарић Предраг, *Компјутерски криминалитет - криминолошки, кривичноправни и сигурносни аспект*, Сарајево, Факултет за криминалистику, криминологију и сигурносне студије, 2009.
4. Collin Barry, The Future of Cyberterrorism, *Crime and Justice International*, Volume 13, Issue 2, 1997.
5. Димовски Дарко, Компјутерски криминалитет, *Зборник радова Правног факултета у Нишу*, бр. 55, 2010.
6. Ђорђевић Ђорђе, *Кривично право - посебни део*, Београд, 2011.
7. Ђукић Анђелија, Крађа идентитета - облици, карактеристике и распрострањеност, *Војно дело*, бр. 3, вол. 69, 2017.
8. Ђурђић, Војислав, Јовашевић, Драган, Кривично право - посебни део, Београд, 2010.
9. Gieseke Anne Pechenik, "The New Weapon of Choice": Law's Current Inability to Properly Address Deepfake Pornography, *Vanderbilt Law Review*, vol. 73, iss. 5, 2020.
10. Грујић Здравко, Компјутерски криминалитет: специфичности и савремени изазови, *Зборник радова Правног факултета у Нишу*, бр. 80, 2018.
11. Jaishankar Karuppannan, Establishing a Theory of Cyber Crimes, I*nternational Journal of Cyber Criminology*, Vol. 1, Issue 2, July 2007.
12. Константиновић Вилић Слободанка, Николић Ристановић Весна, Костић Миомира, *Криминологија*, Београд, 2010.
13. Миладиновић Богавац Живанка, Рачунарска саботажа, *FBIM Transactions*, бр. 1, 2019. Преузето: 8.3.2026. https://www.meste.org/fbim/fbim_srpski/FBIM_najava/XIV_Miladinovic.pdf
14. Мирковић Драган, *Криминолошки аспект компјутерског криминалитета (мастер рад)*, Правни факултет Универзитета у Нишу, Ниш, 2016. Преузето: 5.3.2026. https://www.prafak.ni.ac.rs/files/master-radovi/dragan-mirkovic.pdf
15. Момчиловић Милица, *Видео снимци генерисани уз помоћ вештачке интелигенције (дипфејк) као облик сајбер криминалитета (мастер рад)*, Правни факултет Универзитета у Нишу, Ниш, 2024. Преузето: 11.3.2026. https://www.prafak.ni.ac.rs/files/master-radovi/13-ZMR_MilicaMomcilovic_M033_23_UP.pdf
16. Мрвић Петровић Наташа, Кривичноправни приступ регулисању дигиталне порнографије настале употребом вештачке интелигенције (non-consensual deepfake porn), *Безбедност*, бр. 2/2024, Београд.
17. Nakovski, Toni, Blazheska Tabakovska, Natasha, Bogdanoska Jovanovska, Mimoza, AI-Driven Phishing Attacks: Emerging Threats and Security Strategies, *Serbian Journal of Engineering Management Special Edition*, 2026.
18. Николић Александра, *Дечја порнографија као облик компјутерског криминалитета (мастер рад)*, Правни факултет Универзитета у Нишу, Ниш, 2024. Преузето: 9.3.2026. https://www.prafak.ni.ac.rs/files/master-radovi/12-ZMR_AleksandraNikolic_M015_22_UP.pdf
19. Николић Ристановић Весна, Константиновић Вилић Слободанка, *Криминологија*, Београд, 2018.
20. Петровић Слободан, *Компјутерски криминал*, Војноиздавачки завод, Београд, 2004.

21. Петровић Слободан, *Компјутерски криминал*, Министарство унутрашњих послова Републике Србије - Уредништво часописа „Безбедност" и „Полицајац", Београд, 2000.
22. Post Jerrold, Sprinzak Ehud, Denny Laurita, The terrorist in their own words, Interviews with 35 incarcerated Middle Eastern Terrorist, *Terrorism and Political Violence*, 2003.
23. Симоновић Бранислав, *Криминалистика*, Крагујевац, 2004.
24. Стевић, Христина, *Компјутерска превара (мастер рад)*, Правни факултет Универзитета у Нишу, Ниш, 2020. Преузето: 15.5.2026. https://www.prafak.ni.ac.rs/files/master-radovi/9_ZMR_Hristina_Stevic.pdf
25. Стојановић Зоран, Перић Обрад, *Кривично право - посебни део*, Београд, 2009.
26. Тепавац Дејан, *Заштита пословних информација у функцији националне безбедности (докторска дисертација)*, Факултет безбедности Универзитета у Београду, Београд, 2018. Преузето: 20.6.2026. https://fb.bg.ac.rs/download/RepozitorijumDisertacija/2018-05-21%20Tepavac%20Dejan/Disertacija.pdf
27. Трифуновић Александра, *Компјутерска крађа (мастер рад),* Правни факултет Универзитета у Нишу, Ниш, 2019. Преузето: 7.3.2026. https://www.prafak.ni.ac.rs/files/master-radovi/5.-ZMR_AleksandraTrifunovic_M007_20_UP.pdf
28. Васић Милош, *Компјутерски тероризам (мастер рад)*, Правни факултет Универзитета у Нишу, Ниш, 2018. Преузето: 6.3.2026. https://www.prafak.ni.ac.rs/files/master-radovi/11.-ZMR-Milos-Vasic.pdf
29. Видојковић Милош, *Компјутерски криминалитет (мастер рад)*, Правни факултет Универзитета у Нишу, Ниш, 2024. Преузето: 20.6.2026. https://www.prafak.ni.ac.rs/files/master-radovi/milos-vidojkovic.pdf
30. Winkler Theodor H., Schreier Fred, Weekes Barbara, Cyber Security: The Road Ahead, *Geneva Centre for Security Sector Governance (DCAF)*, 01-2015.
31. Yar Majid, *Cybercrime and society*, London, 2006.
32. Зиројевић Мина, Ивановић, Звонимир, *Сајбер законодавство Србије - други део*, Београд, 2025.

СПИСАК ИСТРАЖИВАЧКЕ ГРАЂЕ

Домаћи прописи

1. Закон о ауторском и сродним правима, *Сл. гласник РС*, бр. 104/2009, 99/2011, 119/2012, 29/2016 - одлука УС и 66/2019;
2. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, Сл. гласник РС, бр. 61/2005, 104/2009, 10/2023, 10/2023 - др. закон и 9/2026;
3. Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима, *Сл. гласник РС*, бр. 32/2013;
4. Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине, *Сл. гласник РС*, бр. 46/2006, 104/2009 - др. закони и 129/2021;
5. Закон о потврђивању Конвенције о високотехнолошком криминалу, *Сл. гласник РС - Међународни уговори*, бр. 19/2009;
6. Законик о кривичном поступку, *Сл. гласник РС*, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 - одлука УС и 62/2021 - одлука УС;
7. Кривични законик, *Сл. гласник РС*, бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019.

Међународни документи

1. CETS No. 224, *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, Strasbourg, 12.5.2022.
2. ETS No. 185, *Convention on Cybercrime*, Budapest, 23 November 2001.
3. ETS No. 189, *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, Strasbourg, 28.1.2003.
4. Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, *Background paper for the workshop on crimes related to the computer network: Crime-fighting on the Net*, 2000. Доступно на: https://www.un.org/events/10thcongress/2088h.htm

Судска пракса

1. Апелациони суд у Нишу, 7Кж. 1. бр. 2607/11 од 31.8.2012. године
2. Врховни суд Србије, Кзз 779/23 од 19.9.2023. године
3. Основни суд у Врању, К. бр. 3881/10 од 7.3.2011. године

Извештаји

1. Национални ЦЕРТ Републике Србије, *Извештај о статистичким подацима о свим инцидентима у ИКТ системима од посебног значаја у 2025. години*, 2026. Преузето: 11.7.2026. https://www.cert.rs/files/shares/Izve%C5%A1taj%20o%20statisti%C4%8Dkim%20podacima%202025.pdf
2. Републички завод за статистику, Употреба информационо-комуникационих технологија. Преузето: 11.7.2026. https://www.stat.gov.rs/sr-Latn/oblasti/upotreba-ikt/upotreba-ikt-pojedinci

Остали електронски извори

1. BIRN, Hakeri imali pristup mejlovima zaposlenih u katastru Srbije, stručnjaci kažu da opasnost još nije prošla. Преузето: 2.4.2026. https://birn.rs/hakeri-imali-pristup-mejlovima-zaposlenih-u-katastru-srbije-strucnjaci-kazu-da-opasnost-jos-nije-prosla/
2. Bitdefender, Deepfake Boss Scam: CEO Impersonation BEC. Преузето: 5.7.2026. https://www.bitdefender.com/en-us/blog/hotforsecurity/deepfake-boss-scam-ceo-impersonation-bec
3. Blic, Obljubio ćerku i sve snimio - otac monstrum iz sela kod Pančeva. Преузето: 11.3.2026. https://www.blic.rs/vesti/hronika/obljubio-cerku-i-sve-snimio-otac-monstrum-iz-sela-kod-panceva-devojcicine-gole/eflfn2k
4. Blic, Roditelji, oprez - dovoljno je da jednom objavite sliku vašeg golišavog deteta. Преузето: 11.3.2026. https://www.blic.rs/vesti/drustvo/roditelji-oprez-dovoljno-je-da-jednom-objavite-sliku-vaseg-golisavog-deteta-i-da-tako/2xmbqgw
5. Cahill, Emily, „What's the Difference Between Phishing, Smishing and Vishing?", Experian, 20.3.2022. Преузето: 27.7.2026. https://www.experian.com/blogs/ask-experian/phishing-smishing-vishing/
6. Danas, Podaci građana, bezbednost podataka, Telekom Srbija, hakerski napad, 600.000 korisnika. Преузето: 2.4.2026. https://www.danas.rs/vesti/ekonomija/podaci-gradjana-bezbednost-podataka-telekom-srbija-hakerski-napad-600-000-korisnika/
7. Equifax Data Breach. Преузето: 1.4.2026. https://archive.epic.org/privacy/data-breach/equifax/
8. Euronews Srbija, Deepfake tehnologija u službi bankarskih prevara - vaš novac je u opasnosti sedam dana u nedelji. Преузето: 5.7.2026.

https://www.euronews.rs/biznis/biznis-vesti/120382/deepfake-tehnologija-u-sluzbi-bankarskih-prevara-vas-novac-je-u-opasnosti-sedam-dana-u-nedelji/vest
9. Europol, званична интернет презентација. Преузето: 7.7.2026. https://www.europol.europa.eu/
10. Fortinet, Hacktivism—A Cyberattack? Meaning, Types, And More. Преузето: 20.6.2026. https://www.fortinet.com/resources/cyberglossary/what-is-hacktivism
11. Holdsworth, Jim, Kosinski, Matthew, „What Is a Distributed Denial-of-Service (DDoS) Attack?", IBM Think. Преузето: 27.6.2026. https://www.ibm.com/think/topics/ddos
12. Huntress, Yahoo Data Breach. Преузето: 2.4.2026. https://www.huntress.com/threat-library/data-breach/yahoo-data-breach
13. IBM Think, „What Is Malware?". Преузето: 27.6.2026. https://www.ibm.com/think/topics/malware
14. Insajder, NBS upozorava: fišing i investiciona prevara - dva najčešća tipa SMS prevarnih šema. Преузето: 23.6.2026. https://insajder.net/prenosimo/nbs-upozorava-fising-i-investiciona-prevara-dva-najcesca-tipa-sms-prevarnih-sema
15. Interpol, званична интернет презентација. Преузето: 7.7.2026. https://www.interpol.int/
16. Kosinski, Matthew, „What Is Phishing?", IBM Think. Преузето: 2.7.2026. https://www.ibm.com/think/topics/phishing
17. Kosinski, Matthew, „What is smishing (SMS phishing)?", IBM Think, 24.6.2024. Преузето: 26.6.2026. https://www.ibm.com/think/topics/smishing
18. Kosinski, Matthew, Susnjara, Stephanie, Goodwin, Michael, „What Is Ransomware?", IBM Think. Преузето: 27.6.2026. https://www.ibm.com/think/topics/ransomware
19. KRIK. Преузето: 7.3.2026. https://www.krik.rs/wp-content/uploads/2016/12/Slu%C4%8Daj-Asomakum-pred-Prekr%C5%A1ajnim-sudom.pdf
20. Министарство унутрашњих послова Републике Србије, званична интернет презентација. Преузето: 12.6.2026. https://www.mup.gov.rs/
21. Mts.rs, Saopštenje Telekoma Srbija. Преузето: 2.4.2026. https://mts.rs/Privatni/Korisnicka-zona/Vesti/Servisne-informacije/a129765-Saopstenje-Telekoma-Srbija.html
22. Национални ЦЕРТ Републике Србије, званична интернет презентација. Преузето: 7.7.2026. https://www.cert.rs/rs
23. NBS. Преузето: 27.6.2026. https://nbs.rs/sr/scripts/showcontent/index.html?id=19190
24. NBS. Преузето: 27.6.2026. https://www.nbs.rs/sr/scripts/showcontent/index.html?id=21393
25. Nova.rs, Objavljeno ko je izvršio hakerski napad na EPS / grupa preuzela sve podatke i preti da će ih objaviti u roku od 10 dana. Преузето: 2.4.2026. https://nova.rs/vesti/biznis/objavljeno-ko-je-izvrsio-hakerski-napad-na-eps-grupa-preuzela-sve-podatke-i-preti-da-ce-ih-objaviti-u-roku-od-10-dana/
26. Nova.rs, Poplava lažnih reklama na društvenim mrežama u kojima se promovišu suplementi / zloupotrebljen lik Danice Grujičić, Branimira Nestorovića, Tatjane Vojtehovski. Преузето: 2.4.2026. https://nova.rs/vesti/hronika/poplava-laznih-reklama-na-drustvenim-mrezama-u-kojima-se-promovisu-suplementi-zloupotrebljen-lik-danice-grujicic-branimira-nestorovica-tatjane-vojtehovski-foto/
27. Our World in Data, Number of Internet users. Преузето: 11.7.2026. https://ourworldindata.org/grapher/number-of-internet-users
28. Proofpoint, „What Is a Deepfake?". Преузето: 27.6.2026. https://www.proofpoint.com/us/threat-reference/deepfake

29. Radio Slobodna Evropa, Srbija - hakerski napad, medicinski podaci. Преузето: 2.4.2026. https://www.slobodnaevropa.org/amp/srbija-hakerski-napad-medicinski-podaci/33723353.html
30. Računarski fakultet, Zlonamerni softver Alien predstavlja sve veću pretnju za korisnike mobilnog bankarstva. Преузето: 2.4.2026. https://raf.edu.rs/citaliste/clanci/svastara/zlonamerni-softver-alien-predstavlja-sve-vecu-pretnju-za-korisnike-mobilnog-bankarstva/
31. RTS, Pošte Srbije - prevara. Преузето: 2.4.2026. https://www.rts.rs/lat/vesti/drustvo/5351451/poste-srbije-prevara-.html
32. Susnjara, Stephanie, Smalley, Ian, „What Is Cloud Computing?", IBM Think. Преузето: 27.6.2026. https://www.ibm.com/think/topics/cloud-computing
33. Vokabular.org. Преузето: 8.3.2026. https://www.vokabular.org/?search=sabota%C5%BEa&lang=sr-lat;
34. Преузето: 27.6.2026. file:///C:/Users/PC/Downloads/vrste-sajber-napada.pdf

Компјутерски криминалитет

РЕЗИМЕ

Кључне речи: *компјутерски криминалитет, сајбер криминалитет, информационо-комуникационе технологије, Будимпештанска конвенција, кривичноправна заштита.*

Компјутерски криминалитет представља један од најзначајнијих и најбрже растућих облика савременог криминалитета, чији је развој непосредно повезан са интензивним напретком информационо-комуникационих технологија и све већом дигитализацијом савременог друштва. Развој интернета, електронског пословања, информационих система, рачунарства у облаку и технологија заснованих на вештачкој интелигенцији омогућио је значајан привредни и друштвени напредак, али је истовремено створио нове могућности за вршење различитих облика противправног понашања. Специфичности компјутерског криминалитета огледају се у високом степену анонимности учинилаца, великој брзини извршења, техничкој сложености откривања и доказивања, као и његовом израженом транснационалном карактеру, што овај облик криминалитета чини једним од највећих изазова савременог кривичног права и безбедности.

Предмет овог рада јесте анализа компјутерског криминалитета као савременог облика криминалитета, са посебним освртом на његов појам, карактеристике, узроке, облике испољавања, последице и механизме превенције и сузбијања. Циљ рада је да се, анализом релевантне научне литературе, позитивноправних прописа, међународних докумената и доступне праксе надлежних органа, сагледају основне карактеристике компјутерског криминалитета, процени адекватност постојећег нормативног и институционалног оквира Републике Србије и укаже на савремене изазове које доноси развој дигиталних технологија.

Приликом израде рада примењени су нормативни, историјски, компаративноправни, аналитички и аксиолошки метод, као и емпиријски приступ заснован на анализи судске праксе, статистичких података, извештаја надлежних институција и карактеристичних примера из праксе. Комбиновањем наведених метода омогућено је свеобухватно сагледавање криминолошких, кривичноправних и практичних аспеката компјутерског криминалитета.

У раду су анализирани појам и основне карактеристике компјутерског криминалитета, његов историјски развој, најзначајнији узроци и последице, као и

најчешћи облици испољавања, међу којима се издвајају компјутерске крађе, компјутерске преваре, компјутерска саботажа, компјутерски тероризам, злонамерни софтвер, фишинг напади, рансомвер напади и злоупотреба савремених технологија, укључујући и примену вештачке интелигенције и дипфејк технологије у криминалне сврхе. Посебна пажња посвећена је анализи кривичноправног оквира Републике Србије, улози институција надлежних за борбу против високотехнолошког криминала, значају превентивних мера и друштвене контроле, као и међународној сарадњи, са посебним освртом на примену Будимпештанске конвенције о високотехнолошком криминалу као најзначајнијег међународноправног инструмента у овој области.

Резултати истраживања потврђују полазну хипотезу рада да постојећи нормативни оквир Републике Србије у великој мери прати међународне стандарде у области борбе против компјутерског криминалитета, али да брз развој дигиталних технологија намеће потребу за његовим континуираним унапређивањем. Истовремено, потврђено је да транснационални карактер компјутерског криминалитета захтева ефикасну међународну сарадњу, хармонизацију националних законодавстава и континуирано јачање институционалних капацитета. Истраживање је такође показало да превенција, развој дигиталне писмености, едукација корисника и унапређење информационе безбедности имају једнако важну улогу као и кривичноправна репресија. Може се закључити да успешно сузбијање компјутерског криминалитета захтева свеобухватан приступ који обједињује нормативне, институционалне, техничке и превентивне механизме, како би се обезбедила ефикасна заштита информационих система, права грађана и безбедности савременог дигиталног друштва.

Cybercrime

SUMMARY

Key words: *cybercrime, information and communication technologies, Budapest Convention on Cybercrime, criminal law protection.*

Cybercrime represents one of the most significant and rapidly expanding forms of contemporary criminality, whose development is closely associated with the accelerated advancement of information and communication technologies and the digital transformation of modern society. The growth of the Internet, electronic commerce, information systems, cloud computing, and artificial intelligence-based technologies has contributed to substantial economic and social progress, while simultaneously creating new opportunities for various forms of unlawful conduct. The specific nature of cybercrime is reflected in the anonymity of offenders, the speed and global reach of criminal activities, the technical complexity of detection and evidence gathering, and its distinctly transnational character. These characteristics make cybercrime one of the most complex challenges faced by modern criminal justice systems and security structures.

This paper examines cybercrime as a contemporary form of criminal activity, with particular focus on its concept, characteristics, causes, manifestations, consequences, and mechanisms for prevention and suppression. The aim of the research is to analyse the essential features of cybercrime through the examination of relevant scientific literature, national legislation, international legal instruments, and the practice of competent authorities, while assessing the adequacy of the existing legal and institutional framework and identifying the challenges arising from the continuous development of digital technologies.

The research applies normative, historical, comparative legal, analytical, and axiological methods, together with an empirical approach based on the analysis of judicial practice, statistical data, reports of relevant institutions, and selected practical examples. The combination of these methods enables a comprehensive examination of the criminological, criminal law, and practical aspects of cybercrime.

The paper analyses the concept and fundamental characteristics of cybercrime, its historical development, major causes and consequences, as well as its most common forms, including computer fraud, computer sabotage, cyberterrorism, malware, phishing attacks, ransomware attacks, and the misuse of emerging technologies, particularly artificial intelligence and deepfake technology for criminal purposes. Special attention is devoted to the criminal law framework of the Republic of Serbia, the role of institutions responsible for

combating cybercrime, the importance of preventive measures and social control mechanisms, as well as international cooperation in this field. Particular emphasis is placed on the Budapest Convention on Cybercrime as the most important international legal instrument for establishing common standards and facilitating cooperation in combating cybercrime.

The research findings confirm the initial hypothesis that the legal framework of the Republic of Serbia largely follows international standards in the field of combating cybercrime; however, the rapid evolution of digital technologies requires continuous adaptation and improvement of existing legal and institutional mechanisms. Furthermore, the research demonstrates that the transnational nature of cybercrime necessitates effective international cooperation, harmonisation of national legislation, and the continuous strengthening of institutional capacities. The findings also indicate that preventive measures, the development of digital literacy, public awareness, user education, and the improvement of cybersecurity mechanisms are equally important as criminal law enforcement measures.

It may be concluded that effective combating of cybercrime requires a comprehensive approach combining legal, institutional, technical, and preventive mechanisms in order to ensure adequate protection of information systems and enhance the security of modern digital society.

БИОГРАФИЈА

Драгана Стојковић рођена је 12. фебруара 1995. године у Нишу, где је завршила Гимназију „9. мај“, спортско одељење.

Основне академске студије завршила је 2018. године на Факултету за правне и пословне студије „Др Лазар Вркатић“, у наставном центру Ниш, на студијском програму Безбедност и криминалистика, стекавши звање дипломираног менаџера безбедности. По окончању основних студија наставила је професионално усавршавање у области безбедности, где је успешно завршила обуку у Центру за основну полицијску обуку у Сремској Каменици. У жељи да настави са академским усавршавањем, 2024. године уписала је мастер академске студије права на студијском програму Унутрашњи послови, на Правном факултету Универзитета у Нишу.

Од октобра 2019. године запослена је у Министарству унутрашњих послова Републике Србије.

Поред професионалног ангажовања, скоро две деценије активно се бавила каратеом. Носилац је звања мајстора каратеа и некадашња репрезентативка Републике Србије. Током своје успешне спортске каријере освајала је медаље на државним, балканским и европским првенствима, а учествовала је и на светском првенству, остварујући запажене резултате.

ИЗЈАВА О ИСТОВЕТНОСТИ ШТАМПАНОГ И ЕЛЕКТРОНСКОГ ОБЛИКА МАСТЕР РАДА

Име и презиме аутора мастер рада: Драгана Стојковић

Наслов мастер рада: *Компјутерски криминалитет*

Ментор: Проф. др Дарко Димовски

Изјављујем да је електронски облик мастер рада у .pdf формату истоветан штампаном облику, који сам предала Правном факултету Универзитета у Нишу.

У Нишу, _____

Потпис аутора

_____

ИЗЈАВА О АУТОРСТВУ И ОДОБРАВАЊУ ОБЈАВЉИВАЊА МАСТЕР РАДА

Изјављујем да мастер рад, под насловом *Компјутерски криминалитет*, пријављен и одбрањен на Правном факултету Универзитета у Нишу:

- представља резултат сопственог истраживачког рада;
- није у целини, нити у деловима с моје стране пријављиван на одбрану на другим факултетима или универзитетима;
- не крши ауторска права или интелектуалну својину других лица.

Дозвољавам да се овај мастер рад чува у библиотеци и објави на сајту Правног факултета Универзитета у Нишу.

Аутор мастер рада:_____

У Нишу, _____

Потпис аутора

_____