

**XIX међународни научни скуп „Правнички дани –
Проф. др Славко Царић”
„ПРАВО, НАУКА И ДРУШТВО – АКТУЕЛНА
ПИТАЊА И ПЕРСПЕКТИВЕ”**

**XIX International scientific meeting „Legal days –
Prof. Slavko Carić, PhD”
„LAW, SCIENCE AND SOCIETY – THE CURRENT
ISSUES AND PERSPECTIVES”**

Универзитет Привредна академија у Новом Саду
Правни факултет за привреду и правосуђе у Новом Саду
The University of Business Academy in Novi Sad
The Faculty of Law for Commerce and Judiciary in Novi Sad

Нови Сад, 23. септембар 2022.

Зборник радова са XIX међународног научног скупа

„Правнички дани – Проф. др Славко Царић“
„ПРАВО, НАУКА И ДРУШТВО – АКТУЕЛНА ПИТАЊА И ПЕРСПЕКТИВЕ“

23. септембар 2022. године у Новом Саду,
у организацији Универзитета Привредна академија у Новом Саду
Правни факултет за привреду и правосуђе у Новом Саду

Издавач:

Универзитет Привредна академија у Новом Саду
Правни факултет за привреду и правосуђе у Новом Саду
Гери Кароља бр. 1, телефон: 021/ 400 - 499
Web: www.pravni-fakultet.info

Рецензенти:

Др Мирко Кулић редовни професор	Др Гордана Бејатовић, ванредни професор
Др Милан Почуча редовни професор	Др Јелена Стојшић Дабетић, ванредни професор
Др Владимир Козар редовни професор	Др Сања Шкорић, ванредни професор
Др Милош Марковић редовни професор	Др Маријана Младенов, ванредни професор
Др Јелена Матијашевић редовни професор	Др Срђан Дамњановић ванредни професор
Др Предраг Мирковић ванредни професор	Др Марко Станковић, доцент
Др Дарко Голић ванредни професор	Др Маја Суботин доцент
Др Јоко Драгојловић ванредни професор	

За издавача:

Др Мирко Кулић, редовни професор

Уредник:

Др Милан Почуча, редовни професор

Штампа:

НС Мала књига плус, Нови Сад

Тираж: 150

ISBN 978-86-86121-51-6

Научни одбор:

ПРОФ. ДР МИЛАН ПОЧУЧА - председник Научног одбора

Продекан за науку, квалитет и развој и шеф Грађанскоправне катедре на Правном факултету за привреду и правосуђе, Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР МАРКО ЦАРИЋ

Ректор Универзитета Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР МАРИЈАНА ЦАРИЋ

Председник Савета Универзитета Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР МИРКО КУЛИЋ

Декан Правног факултета за привреду и правосуђе, Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР МАРИЈАНА ДУКИЋ МИЈАТОВИЋ

Редовни професор на Правном факултету за привреду и правосуђе Универзитет Привредна академија у Новом Саду и ванредни професор Факултета техничких наука Универзитета у Новом Саду | Република Србија

ПРОФ. ДР ПРЕДРАГ МИРКОВИЋ

Продекан за наставу и ванредни професор на Правном факултету за привреду и правосуђе, Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР МАРИЈАНА МЛАДЕНОВ

Продекан за међународну сарадњу и ванредни професор на Правном факултету за привреду и правосуђе, Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР ЗОРАН ПАВЛОВИЋ

Шеф Кривичноправне катедре на Правном факултету за привреду и правосуђе, Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР ДАРКО ГОЛИЋ

Шеф Теоријске и јавноправне катедре на Правном факултету за привреду и правосуђе, Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР ЖЕЉКО БЈЕЛАЈАЦ

Редовни професор на Правном факултету за привреду и правосуђе, Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР ЈЕЛЕНА МАТИЈАШЕВИЋ

Редовни професор на Правном факултету за привреду и правосуђе, Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР ВЛАДИМИР КОЗАР

Редовни професор на Правном факултету за привреду и правосуђе, Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР САЊА ШКОРИЋ

Ванредни професор на Правном факултету за привреду и правосуђе, Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР ДУШАНКА ЋУРЂЕВ

Редовни професор на Правном факултету за привреду и правосуђе, Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР ВЛАДИМИР ЦАТИЕВ

Шеф катедре Кривичноправних наука Руске академије за адвокатуру и нотаријат | Руска Федерација

АКАДЕМИК ДР НЕДЕЉКО СТАНКОВИЋ

Европски универзитет Брчко дистрикт и Ректор Европског универзитета „Kallos” Тузла и | Босна и Херцеговина

АКАДЕМИК ДР БРАНКО ВУЧКОВИЋ, ЕМЕРИТУС

Универзитет „Адриатик“ – Бар, Факултет за пословну економију и право | Република Црна Гора

АКАДЕМИК ДР ВЕСНА ВУЧКОВИЋ

Судија, в.д. председника Врховног суда Црне Горе, Универзитет „Адриатик“ – Бар, Факултет за медитеранске пословне студије, Тиват | Република Црна Гора

PROF. DR DR. WOLFGANG ROHRBACH

Akademik Evropske akademije nauka u Salzburgu | Austrija

PROF. DR VANO TSERTSVADZE

Georgian Institute of Public Affairs | Gruzija

PROF. DR. AMER FAKHOURY

Dean College of Law American University in the Emirates | Ujedinjeni Arapski Emirati

ПРОФ. ДР РУДИКА ГМАЈНИЋ

Професор на Медицинском факултету у Осијеку и члан Хрватске академије медицинских наука | Република Хрватска

ДОЦ. ДР ЈАН ЈАНАЋ

Доцент на Факултету за менаџмент, Универзитет Коменски Братислава | Република Словачка

ДОЦ. ДР БРАНИСЛАВ ДУДИЋ

Доцент на Факултету за менаџмент, Универзитет Коменски Братислава | Република Словачка

ПРОФ. ДР НЕЂО ДАНИЛОВИЋ

Редован професор Универзитет Никола Тесла у Београду и председник међународног удружења методолога друштвених наука у Београду | Република Србија

ПРОФ. ДР АЛБИНА ФАЗЛОВИЋ

Ванредни професор Европском универзитету Брчко дистрикт на Европском универзитету „Kallos” Тузла | Босна и Херцеговина

ПРОФ. ДР ЗОРАН ФИЛИПОВСКИ

Проректор за међународну сарадњу, Интернационални „Vision” Универзитет | Северна Македонија

PROF. DR ALEXIOS PANAGOPOULOS

University Neapolis Paphos Cyprus, master studys in public law and administration | Republika Kipar

ПРОФ. ДР НЕБОЈША ШАРКИЋ

Декан Правног факултета, Универзитета Унион у Београду | Република Србија

ДР МИШО ЂУРКОВИЋ

Научни саветник, Директор Института за Европске студије у Београду | Република Србија

ПРОФ. ДР ВЛАДИМИР ЧЛОВИЋ

Директор Института за упоредно право у Београду | Република Србија

ПРОФ. ДР БОГДАН ВУКОСАВЉЕВИЋ

European Research Institute for Strategic Studies | Словенија

ПРОФ. ДР МИЛОШ МАРКОВИЋ

Редовни професор на Правном факултету за привреду и правосуђе, Универзитет Привредна академија у Новом Саду | Република Србија

Организациони одбор:

ПРОФ. ДР ЈОКО ДРАГОЈЛОВИЋ - Председник Организационог одбора

ПРОФ. ДР ИВАН ЈОКСИЋ

ПРОФ. ДР ЈЕЛЕНА СТОЈШИЋ ДАБЕТИЋ

ПРОФ. ДР НЕНАД БИНГУЛАЦ

ДОЦ. ДР НЕНАД СТЕФАНОВИЋ

ДОЦ. ДР МАРКО СТАНКОВИЋ

ДОЦ. ДР ДАЛИБОР КРСТИНИЋ

ДОЦ. ДР МАЈА СУБОТИН

ДОЦ. ДР ВЛАДИМИР ШЕБЕК

МСР ИСИДОРА МИЛОШЕВИЋ

МСР АЊА КОПРИВИЦА

МСР МАРА ДЕСПОТОВ

МСР ТАМАРА КРСТИЋ

Секретар:

МСР АЊА КОПРИВИЦА, асистент

Др Јоко Драгојловић, ванредни професор
Правни факултет за привреду и правосуђе у Новом Саду
Универзитет Привредна академија у Новом Саду
e-mail: jdragojlovic@pravni-fakultet.info

Мср Ања Копривица, асистент
Правни факултет за привреду и правосуђе у Новом Саду
Универзитет Привредна академија у Новом Саду
e-mail: anja.koprivica@pravni-fakultet.info

Др Марија Станковић, доцент
Правни факултет за привреду и правосуђе у Новом Саду
Универзитет Привредна академија у Новом Саду

СПЕЦИФИЧНОСТИ РАЧУНАРСКОГ КРИМИНАЛИТЕТА УЗ ПОСЕБАН ОСВРТ НА РАЧУНАРСКУ САБОТАЖУ

Апстракт:

Компјутери и компјутерски системи нашли су своје место у многобројним активностима људи на свакодневном нивоу. Експанзија технологије донела је са собом низ позитивних ствари као што су брз проток информација, робе и услуга, држа комуникација, лакше и држе обављање одређених делатности путем интернета. Међутим, поред многобројних предности које са собом доносе рачунари и рачунарске технологије, постоје и оне негативне стране које се огледају пре свега у виду злоупотребе рачунарских података вршењем кривичних дела из ове области. Имајући у виду све специфичности рачунарске криминалистике, откривање и доказивање ових кривичних дела је изузетно сложено и захтевно из разлога што је за откривање и доказивање рачунарске криминалистике неопходно поседовање одређеног знања из ове области, дрзина у предузимању доказних радњи, као и јака међународна сарадња, имајући у виду његов транснационални карактер. Предмет овог рада јесу специфичности рачунарске криминалистике, са посебним освртом на кривично дело рачунарске саботаже.

Кључне речи: компјутерски криминалистички, рачунарска саботажа, рачунарски системи, технологија, безбедност.

УВОД

Рачунар као електронски уређај који је створен да на основу програма аутоматски размењује податке, представља можда и најзначајнији напредак технологије, а данас готово да не постоји сфера друштвеног и пословног живота у којој он нема примену. Развојем технологије, рачунари данас имају масовну примену где се користе на свакодневном нивоу, независно од старосне доби и делатности корисника коју помоћу њега обављају. Велике могућности примене као што су брз проток информација, обављање новчаних трансакција, промет робе и услуга, вршење пословних делатности на разним нивоима, довеле су неизбежно и до злоупотребе рачунара и рачунарских система.

Рачунарски криминалитет подразумева различите облике криминалног понашања која подразумевају злоупотребу савремене технологије, где се рачунар јавља као средство али и објект извршења кривичног дела. Имајући у виду све специфичности рачунаског криминалитета, немогуће је издвојити једну дефиницију која би ову појаву дефинисала на адекватан начин. Сходно томе у теорији се могу наћи различите врсте рачунаског криминалитета.

Компјутерски криминалитет представља облик криминалног понашања, код кога се коришћење компјутерске технологије и информатичких система испољава као начин извршења кривичног дела, или се компјутер употребљава као средство или циљ извршења, чиме се остварује нека у кривичноправном смислу релевантна последица.¹⁾ Поред тога, Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала²⁾, по први пут је и у домаћем законодавству дефинисан појам високотехнолошког криминала и то као: вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику.³⁾ Дакле, можемо разликовати кривична дела у којима се рачунари користе као средство извршења, објекат извршења као и кривична дела која се врше на основу незаконитог коришћења интернета.⁴⁾

Појавни облици ове врсте криминалитета су различити а најчешће се односе на неовлашћено брисање, мењање, оштећење или прикривање рачунарских података или програма, оштећење рачунара или других уређаја за електронску обраду, вршење рачунарских превара, саботажа, прављење рачунарских вируса, итд. Циљ вршења ових кривичних дела између осталог јесте ометање и оштећење електронске обраде и преноса података, прибављање противправне имовинске користи и наношење штете другом. Начин и облици извршења кривичних дела рачунарског криминалитета су све разноврснији из разлога што је развој технологије нешто што се стално мења и усавршава, па самим тим се усавршавају и мењају модалитети извршења истих.

Многобројне специфичности прате ову криминалну појаву и дефинитивно се разликују од вршења класичних кривичних дела. Неки од разлога огледају се у самом простору у ком се врше кривична дела, а то је тзв. *cyber* простор који не познаје државне границе, те је најчешће реч о транснационалном виду криминалитета. Извршилац кривичног дела углавном мора поседовати одређена значајна вештине приликом вршења кривичних дела, а нешто што је карактеристично за овај облик криминалитета јесте да се дела врше веома брзо, чак и у секундама.

Посебну опасност коју ова појава доноси са собом односи се и на повезаност транснационалног организованог криминалитета са високотехнолошким криминалитетом, где организоване криминалне групе постојање савремене технологије виде као средство којим ће доћи до свог примарног циља, односно стицања нелегалног профита. Овакав амбијент организоване криминалне групе користе првенствено за циљане нападе на жртве у богатим регионима, када остварују и знатно веће добитке него што би их остварили у сопственој држави.⁵⁾ Сходно томе, криминалне групе су спремне да ангажују стручњаке који располажу одређеним знањем из области рачунара, како би лакше и ефикасније вршили кривична дела.

1) Лилић, С., Прља Д. (2011). Правна информатика вештина, Правни факултет Универзитета у Београду, Београд, стр. 104.

2) Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, *Сл. гласник РС*, бр. 61/05 и 104/09.

3) Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, *Сл. гласник РС*, бр. 61/05 и 104/09, члан 2. став 1 и 2

4) Драгојловић Ј., Данојлић М., (2015). Кривично дело прављење и уношење рачунарских вируса као облик угрожавања рачунарских система», Зборник радова XII традиционалног научног скупа „Правнички дани проф. др Славо Царић“, Правни факултет за привреду и правосуђе, Нови Сад, стр. 640.

5) Sofaer, A. D., & Goodman, S. E. (2001). Cyber crime and security. The transnational dimension. The transnational dimension of cyber crime and terrorism, 6-7.

Поред различитих кривичних дела који се могу извршити путем рачунара и рачунарске технологије, аутори ће у раду посебну пажњу посветити кривичном делу рачунарске саботаже, које се врши са намером да се онемогући или знатно омете поступак електронске обраде или преноса података који су од значаја за државне органе или друге субјекте.

КАРАКТЕРИСТИКЕ РАЧУНАРСКОГ КРИМИНАЛИТЕТА

Међународна организација криминалистичке полиције – Интерпол, је прва међународна организација која се проблематиком компјутерског криминала и кривичноправном регулативом у овој области почела бавити још 1979. године, на Конференцији одржаној у Паризу. Интерпол је том приликом покренуо дискусију о најбитнијим питањима, а Упитник о компјутерском криминалитету циркуларно је послат свим земљама чланицама Интерпола. Пројекат је одобрен од стране Генералне скупштине 1980/1981. године, што је пропраћено организацијом Првог Интерпол тренинг семинара за истражитеље компјутерског криминала. Закључци са овог семинара представљају први корак на развоју усаглашавања кривичноправних решења, који се односе на компјутерски криминалитет, широм света.⁶⁾ У почетној фази борбе против рачунарског криминалитета организоване су многобројне конференције, именоване стручне комисије о разматрању ове проблематике, где су донете одређене Препоруке, Протоколи и међународни документи, са циљем развоја националних законодавстава, односно усклађивања кривичних закона и препознавања криминалних делатности овог, релативно новог облика криминала.

Најзначајнији међународни акт о решавању овог питања јесте Конвенција Савета Европе о високотехнолошком криминалу усвојена 23. новембра 2001. године у Будимпешти, која је ступила на снагу 1. јула 2004. године. Република Србија је ову Конвенцију ратификовала Законом о потврђивању Конвенције о високотехнолошком криминалу⁷⁾. О њеном изузетном значају говори и то, да поред држава чланица које су је потписале, приступиле су јој и многе државе које нису чланице Савета Европе.

Поглавље II Конвенције, у Првом делу говори да свака Страна уговорница треба да усвоји законодавне и друге мере које су неопходне, да би се у домаћем праву прописала следећа кривична дела. На првом месту то су *дела у вези са рачунарима*, што подразумева све радње фалсификовања у вези са рачунарима⁸⁾ и превара у вези са рачунарима⁹⁾, након тога *дела у вези са садржајем*, што се односи на кривична дела у вези са дечијом порнографијом¹⁰⁾ и дела у вези са кршењем ауторских и сродних права.¹¹⁾

Вршење рачунарских тј, сајбер кривичних дела, без обзира о ком делу је реч, одликује једна јако битна карактеристика а то је анонимност. Иста се постиже коришћењем VPN-а¹²⁾ путем интернета, при чему се IP адреса рачунара који се користи неће видети, већ ће се заправо видети IP адреса VPN-а који се користи.¹³⁾

⁶⁾ Бјелајац, Ж., Матијашевић, Ј., Димитријевић, Д. (2012). Значај успостављања међународних стандарда у сузбијању високотехнолошког криминала, Међународна политика, Институт за међународну политику и привреду (МПП), Београд, вол 63, бр. 1146, стр. 73-74

⁷⁾ Закон о потврђивању Конвенције о високотехнолошком криминалу, *Сл. гласник РС*, бр. 19 од 19. марта 2009.

⁸⁾ Закон о потврђивању Конвенције о високотехнолошком криминалу, Одељак 2, члан 7

⁹⁾ Закон о потврђивању Конвенције о високотехнолошком криминалу, Одељак 2, члан 8

¹⁰⁾ Закон о потврђивању Конвенције о високотехнолошком криминалу, Одељак 3, члан 9

¹¹⁾ Закон о потврђивању Конвенције о високотехнолошком криминалу, Одељак 4, члан 10

¹²⁾ Virtual Private Network – Виртуелна приватна мрежа

¹³⁾ Лутовац, С., Рачић, Ј., (2021). Компјутерски криминал као савремени облик криминалитета, Право и нове технологије, Правни факултет ФППНТ, Београд, вол. 18, бр. 4, стр. 286.

Анонимни извршилац кривичног дела има одређени циљ напада који може бити: хардвер, софтвер, одређени програми, подаци, заштита, услуге, док би се бројне активности које могу имати карактер криминалних радњи могле груписати на следећи начин:

- атак на хардвер (уништење, оштећење или отуђење рачунарског система или његових компоненти),
- атак на софтвер (уништење, оштећење, отуђење и неовлашћена измена, објављивање или коришћење софтверских производа),
- атак на програм (уништење, оштећење, отуђење и неовлашћена измена, објављивање или коришћење програмских производа),
- атак на податке (уништење, оштећење, отуђење и неовлашћена измена, објављивање или коришћење података),
- атак на заштиту (нарушавање или пробијање система заштите), и
- атак на услуге (неовлашћено коришћење информационих ресурса).¹⁴⁾

Оно што је специфично за овакве активности криминалног деловања, јесте временска димензија извршења која омогућава да се рачунарска кривична дела врше невероватном брзином, чак и у деловима секунде. Такође, место извршења кривичног дела везано је за локацију рачунара, што са собом повлачи чињеницу да се најчешће место извршења кривичног дела налази у једној држави а настала последица у другој. Разлог за то је у виртуелни *cyber* простор у ком се извршиоци крећу, а који не познаје државне границе. Самим тим долази до потешкоћа при процесуирању овако специфичног криминалног деловања где је од круцијалног значаја сарадња међународне заједнице, а на првом месту откривање и препознавање разних облика криминалног деловања која обучени извршиоци врше.

Неки од облика рачунарског криминалног деловања су:

- Употреба информационог система у случајевима кршења пословне и безбедносне политике фирме или предузимању корака противно безбедносној политици фирме и тиме излагање система и података фирме сајбер нападима;
- Класичне облике криминала који укључују примену рачунара или других ИТ комуникационих или евиденционих средстава као подршку нелегалним активностима;
- Онлајн преваре као што су фишинг напади, спуфинг, спиминг, форминг или другим облицима дела којима се покушавају преварити лица с циљем остваривања противправне имовинске користи;
- Хакерисање, крековање шифара, недозвољени упад у рачунар с сврхом крађе или незаконитог увида у шифре администраторских и других налога или с циљем упада у рачунаре или информационе системе како би се вршили други незаконити акти офлајн или онлајн;
- Прибављање малициозних и дистрибуирање других рачунарских програма или кодова, који у себи садрже активности стварања, копирања и/или испуштања злоћудних програма (на пример, деструктивне или ометајуће вирусе, тројанце, црве, адвертајзинг програме – адвере, или шпијунске програме – спајвере). Пиратерија (дигитална) музике, видео-записа (филмова);

¹⁴⁾ Васић, Г., Шарић, Б., Јованић, В. (2012). Компјутерки криминалитет, У: Зброник радова, Сузбијање криминала и Европске интеграције, с освртом на високотехнолошки криминал, Висока школа унутрашњих послова, Бања Лука, стр. 183

- Сајбер узнемиравања, узнемиравања, претње, интенциона излагања порузи, изнуде укључујући и сајбер злостављања;
- Онлајн прогањања и ухођења, као и друга дела сајбер сексуалне конотације;
- Организовани криминал који подразумева злоупотребу интернета етнички везаних и организованих банди у омогућавању комбинованих илегалних и легалних активности као на пример купопродају људских бића, њихово кријумчарење, али и других нелегалних роба – оружја и наркотика;
- Кибертероризам извршен од стране особа које намеравају да створе „социјалне, религиозне или политичке циљеве наношењем страха и панике путем оштећивања или ометања критичких информационих структура”.¹⁵⁾

Посебан *modus operandi* ових кривичних дела нам указује на то да лица која га врше морају поседовати одређена знања и вештине из области рачунарске технологије¹⁶⁾, која се развија и усавршава невероватном брзином, самим тим, и надлежни органи морају бити обучени и поседовати одређено знање како би могли препознати и стати на пут овој криминалној активности.

Недовољна обученост надлежних служби у комбинацији са недовољном информисаношћу потенцијалних жртава о опасностима које прете и мерама превенције, производе ситуацију у којој је могуће и замисливо да највећи број кривичних дела сајбер криминала никада не буде пријављен, па чак ни уочен.¹⁷⁾

КРИВИЧНО ДЕЛО РАЧУНАРСКЕ САБОТАЖЕ

Кривично дело рачунарске саботаже има два облика извршења, па тако, први облик ће постојати уколико неко, унесе, уништи, избрише, измени, оштети, прикрије или на други начин учини неупотребљивим рачунарски податак или програм, док други облик овог кривичног дела постоји уколико неко уништи или оштети рачунар или други уређај који служи 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.¹⁸⁾

Прописана казна за ово кривично дело јесте казна затвора од шест месеци до пет година. Објект радње кривичног дела јесу рачунарски податак или програм, односно рачунар или други уређај за електронску обраду и пренос података. Поред умишљаја као облика кривице, за извршење овог кривичног дела потребна је и намера која мора бити управљена ка ометању и онемогућавању електронске обраде и преноса података наведених субјеката.

Ово кривично дело неће постојати уколико је извршено према другим рачунарима, односно, оним рачунарима који нису од значаја за наведене субјекте, што значи да, у сваком конкретном

15) Бошковић, Г. (2011). Организовани криминал, Криминалистичко – полицијска академија, Београд, стр. 107-108.

16) Више у: Матијашевић Ј., Бингулац Н., Драгојловић Ј., (2014). Психологија хакера и значај њихових активности у интернет комуникацијама савременог друштва, *3rd International scientific conference on „Power of communication 2014”*, Београд, стр. 147-160.

17) Јерковић, Р. (2009). Високотехнолошки криминал: актери и жртве, Ревизија за безбедност – стручни часопис о корупцији и организованом криминалу, Центар за безбедносне студије, Београд, вол. 3, бр. 3, стр. 27-34

18) Кривични законик «Сл. гласник РС», бр. 85/05, 88/05 - испр., 107/05 - испр., 72/09, 111/09, 121/12, 104/13, 108/24, 94/16 и 35/19, члан 299.

случају, треба утврдити да ли се ради о рачунарима, описаних органа и организација таквог значаја.¹⁹⁾

Веома је значајно да безбедност електронских података буде на завидном нивоу како би се смањио ризик злоупотребе, а поготово кад је реч о електронским подацима државних органа, јавних служби, установа, предузећа и других субјеката који обављају одређене дeлатности и користе се подацима грађана читаве државе, поготово данас, када је дошло до умрежавања електронских података на нивоу целе државе и преласка грађана на електронско коришћење услуга путем Е-управе.

Увођење информационо комуникационих технологија у државну управу и прелазак државне управе на електронски режим рада представља велики изазов, значајно унапређује квалитет рада државних органа, смањује трошкове управе, побољшава квалитет живота грађана и пружа нове могућности за утицај грађана на јавни живот. Од државног је интереса да информациони системи државних органа буду адекватно заштићени, а државни службеници буду добро обучени, јер оштећење или уништавање података садржаних у тим системима може имати значајне последице по безбедност државе и животе грађана.²⁰⁾ Колики је значај да информационе технологије и системи које користе државни органи буду добро заштићени говори нам и чињеница да се и наша држава у последње време суочавала са одређеним сајбер терористичким нападима. Сетимо се напада на ЈКП „Информатика” у Новом Саду, као и напада на информациони систем Републичког геодетског завода. Управо ситуације са којима смо се суочили су нам показале који је значај поседовања адекватне заштите ових информационих система као и колико је важно да запослени који се брину о сигурности информационих система буду на висини задатка, а поред њих и сви запослени који користе и управљају тим информационим системима. Иако је настанак великих последица (губитак података, злоупотреба података, измена података и сл.) од напред поменутих случајева, спречен сама чињеница да је део јавних служби био паралисан, а да је опоравак од ових напада трајао и по неколико недеља, свакако указује на додатан опрез и потребу да се овим питањем у будућности детаљније позабавимо.

ЗАКЉУЧАК

Рачунарски криминалитет је вид криминалитета који је константно у порасту, а његова феноменолошка димензија се константно шири. Наиме, различити су начини злоупотребе рачунара и рачунарске технологије, али и мотиви из којих се ова кривична дела врше. Свакако да су најдоминантнији финансијски мотиви, али често они нису једини. Када је реч о кривичном делу рачунарске саботаже, код извршиоца поред предузете радње мора постојати и намера. Намера обухвата свест да се одређена радња предузима ради онемогућавања или ометања електронске обраде података који су од значаја за државне органе, јавне службе, установе, предузећа. Наиме, намера која постоји приликом извршења кривичног дела рачунарске саботаже се састоји у онемогућавања обављања редовне дeлатности државних органа и служби. Дакле, мотив код овог кривичног дела по правилу не мора подразумевати само финансијску корист (али је не треба искључити) већ и намеру да се дестабилизују државни органи, обављање одређених јавних овлашћења, односно редовно функционисање и рад државних органа, служби и установа. Оно што је још карактеристично за ово кривично дело јесте и транснационални карактер, односно да се најчешће дешава да је место предузе-

19) Герке, М., Ђокић, Д., Радловић, С., Петровић З., Лазовић, В., Прах, Р. (2008). Приручник за истрагу кривичних дела у области високотехнолошког криминала, Савет Европе, стр. 117

20) Прља, Д., Ивановић, З., Рељановић, М. (2011). Кривична дела високотехнолошког криминала, Институт за упоредно право, Београд, стр. 146

те радње у једној држави а настала последица у другој. Ово свакако у великој мери компликује поступак откривања и доказивања кривичног дела.

Нажалост, наша држава је имала прилику да се суочи са одређеним сајбер нападима, који су утицали на рад државних органа, а од напада је опоравак трајао и по неколико недеља. Све ово позива на додатни опрез и потребу да се о овој теми све више пише и прича, али и потребу да се уради нешто по питању заштите од ових напада, имајући у виду последице до којих долази услед тога. Такође, сигурно је да у будућности можемо очекивати још покушаја оваквих или сличних напада, где овакви или слични напади у великој мери могу изазвати несигурност код грађана, губитак и крађу података, као и измену и злоупотребу истих, али и паралисање рада јавних служби и државних органа, док мотиви ових напада могу бити различити

Joko Dragojlović, PhD, Associate Professor

*Faculty of Law for Commerce and Judiciary in Novi Sad
University Business Academy in Novi Sad*

Anja Koprivica, LLM, Teaching Assistant

*Faculty of Law for Commerce and Judiciary in Novi Sad
University Business Academy in Novi Sad*

Marija Stanković, PhD, Assistant Professor

*Faculty of Law for Commerce and Judiciary in Novi Sad
University Business Academy in Novi Sad*

SPECIFICS OF CYBERCRIME WITH SPECIAL REFERENCE TO COMPUTER SABOTAGE

Summary:

Computers and computer systems have found their place in many human activities on a daily basis. The expansion of technology has brought with it a number of positive things, such as the rapid flow of information, goods and services, faster communication, and easier and faster performance of certain activities via the Internet. However, in addition to the many advantages that computers and computer technologies bring, there are also negative aspects that are reflected primarily in the form of misuse of computer data by committing criminal acts in this area. Bearing in mind all the specifics of cybercrime, detecting and proving these criminal acts is extremely complex and demanding since these require certain knowledge in the area of cybercrime, speed in undertaking evidentiary actions, as well as strong international cooperation, considering the transnational character of such crimes. The subject of this paper is the specifics of cybercrime, with special reference to the crime of computer sabotage.

Keywords: *cybercrime, computer sabotage, computer systems, technology, security.*

ЛИТЕРАТУРА

1. Бјелајац, Ж., Матијашевић, Ј., Димитријевић, Д. (2012). Значај успостављања међународних стандарда у сузбијању високотехнолошког криминала, Међународна политика, Институт за међународну политику и привреду (МПП), Београд, вол 63, бр. 1146, стр. 66-84
2. Бошковић, Г. (2011). Организовани криминал, Криминалистичко – полицијска академија, Београд
3. Васић, Г., Шарић, Б., Јованић, В. (2012). Компјутерски криминалитет, У: Зброник радова, Сузбијање криминала и Европске интеграције, с освртом на високотехнолошки криминал, Висока школа унутрашњих послова, Бања Лука, стр. 181-191.
4. Герке, М., Ђокић, Д., Радуловић, С., Петровић З., Лазовић, В., Прах, Р. (2008). Приручник за истрагу кривичних дела у области високотехнолошког криминала, Савет Европе
5. Драгојловић Ј., Данојлић М., (2015). Кривично дело прављење и уношење рачунарских вируса као облик угрожавања рачунарских система», Зборник радова XII традиционалног научног скупа „Правнички дани проф. др Славко Царић, Правни факултет за привреду и правосуђе, Нови Сад, стр. 639-648.
6. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, *Сл. гласник РС*, бр. 61/05 и 104/09
7. Закон о потврђивању Конвенције о високотехнолошком криминалу, *Сл. гласник РС*, бр. 19 од 19. марта 2009.
8. Јерковић, Р. (2009). Високотехнолошки криминал: актери и жртве, Ревизија за безбедност – стручни часопис о корупцији и организованом криминалу, Центар за безбедносне студије, Београд, вол. 3, бр. 3, стр. 27-34
9. Кривични законик, *Сл. гласник РС*, бр. 85/05, 88/05 - испр., 107/05 - испр., 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 и 35/19.
10. Лилић, С., Прља Д. (2011). Правна информатика вештина, Правни факултет Универзитета у Београду, Београд
11. Лутовац, С., Рачић, Ј., (2021). Компјутерски криминал као савремени облик криминалитета, Право и нове технологије, Правни факултет ФППНТ, Београд, вол. 18, бр. 4, стр. 281-292.
12. Матијашевић Ј., Бингулац Н., Драгојловић Ј., (2014). Психологија хакера и значај њихових активности у интернет комуникацијама савременог друштва, *3rd International scientific conference on „Power of communication 2014”*, Београд, стр. 147-160.
13. Прља, Д., Ивановић, З., Рељановић, М. (2011). Кривична дела високотехнолошког криминала, Институт за упоредно право, Београд.
14. Sofaer, A. D., & Goodman, S. E. (2001). Cyber crime and security. The transnational dimension. The transnational dimension of cyber crime and terrorism, p. 1-34.

CIP - Каталогизација у публикацији
Библиотеке Матице српске, Нови Сад

001:34(082)
316.3:34(082)

**МЕЂУНАРОДНИ научни скуп Правнички дани - проф. др Славко Царић
(19 ; 2022 ; Нови Сад)**

Право, наука и друштво - актуелна питања и перспективе : [зборник радова] = Law, science and society - the current issues and perspectives : [proceedings] / XIX међународни научни скуп "Правнички дани - Проф. др Славко Царић", Нови Сад, 23. септембар 2022. = XIX international scientific meeting "Legal days - Prof. Slavko Carić, PhD" ; [уредник Милан Почуча]. - Нови Сад : Универзитет Привредна академија, Правни факултет за привреду и правосуђе, 2022 (Нови Сад : НС Мала књига+). - 454 стр. ; 24 cm

Текстови ћир. и лат. - Тираж 150. - Стр. 19-20: Уводна реч / Милан Почуча = Foreword / Milan Počuča. - Напомене и библиографске референце уз текст. - Библиографија уз сваки рад. - Резиме на енгл. језику уз већину радова.

ISBN 978-86-86121-51-6

а) Наука - Правни аспект - Зборници б) Друштво - Правни аспект - Зборници

COBISS.SR-ID 74323209