УДК: 004.738.5
. 343.9.024:336.7

Оригинални научни рад

ПОСЛОВНА ЕКОНОМИЈА
BUSINESS ECONOMICS
Година VI
Број I
стр. 97 - 118

**др Драган М. Ранђеловић[1], ванредни професор**
Криминалистичко-полицијска академија, Земун –Београд

**др Жељко Никач[2], ванредни професор**
Криминалистичко-полицијска академија, Земун –Београд

**Милена Стефановић[3],свршени студент специјалистичких студија**
Криминалистичко-полицијска академија, Земун –Београд

# СОФТВЕРСКИ АЛАТИ И ПРАЊЕ НОВЦА КАО ОБЛИК ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА*

**САЖЕТАК:** Данас када је већина човечанства у информатичкој епохи развоја људског друштва са доминантно присутном глобализацијом, нужна веза прања новца као криминалног догађаја и визуалајзера као сврсисходне методе криминалистичке истраге је актуелна тема научно-стручног разматрања и зато и предмет проучавања овог рада. Када је у питању област финансија, криминална активност се не би могла остварити без коришћења компјутерске технологије, нарочито код дела код којих је услов обрада великог броја информација у кратком периоду. Компјутер се показао као средство којим се могу извршити најразноврснија и најсложенија кривична дела, као што су: пљачке, проневере, финансијске малверзације, шпијунажа, тероризам, као и сви облици злоупотреба. Све ово указује на један новији

1 dragan.randjelovic@kpa.edu.rs
2 zeljko.nikac@kpa.edu.rs
3 stmilena@yahoo.com

* Рад подржало Министарство за просвету и науку Републике Србије/пројекти III44007, TR 34019

(савременији) облик вршења кривичних дела који карактеришу својства велике динамике и посебних форми појавних облика и видова испољавања, а то је високотехнолошки криминал. На крају овог рада је на конкретној студији случаја размотрена употреба алата визуелајзера у детектовању и анализи прања новца и на том примеру предложен један од могућих начина коришћења.

*Кључне речи*: прање новца, визуелајзери, *NodeXL, i2 Analyst's Notebook*, високотехнолошки криминал…

## УВОД

Разни облици криминала, као што су: сива економија, прање новца, утаја пореза, трговина дрогом, људима, оружјем и други који се веома брзо шире и јачају, добијају интернационални карактер. Учесници прања новца врше реинвестирање средстава тамо где очекују да неће бити откривено његово порекло, не у послове са већим профитом. И управо последице тога могу бити смањена монетарна стабилност због неодговарајуће алокације средстава, неочекиване промене у потражњи новца, повећане нестабилности девизних курсева, каматних стопа и међународних токова капитала, услед чега је тешко спроводити стабилну и ефикасну економску политику.

Истовремено, прање новца може имати потенцијално разорне економске, политичке и социјалне последице на сваку земљу, као и угрожавање програма реформи и стабилизације, односно опадања репутације земље. Да би се зауставиле и спречиле такве појаве у области националних и светских финансија, предузимају се одговарајуће мере на превентивном и репресивном плану.

Подразумевана дефиниција новца била би да је он „све оно што је општеприхваћено као начин подмиривања трошкова"[4]. Традиционално се прањем новца сматра чишћење прљавог новца произашлог из незаконитих активности које су у колективној свести вероватно повезане с продајом дроге[5].

„Прљави" новац који циркулише кроз „машину за прање новца" ствара се криминалним радњама које се обављају далеко од надзора легалних

4 Љутић, Б. Ж., "Ревизија. Теорија и пракса" ,Београд, 2002., стр. 15.

5 Ehrenfeld, R., "Evil Money: Encounters Along the Money Trail", Harper Collins Publishers, New York, 1992., стр.566-571

органа власти. Свакако, прање новца није нов феномен, јер егзистира паралелно с постојањем црног тржишта, односно сиве економије. „Прљави" новац, у већини случајева, плод је производње и промета дрога, крађе аутомобила, проневера, инсајдерске трговине, илегалног промета оружја и нуклеарног материјала, дечје порнографије и проституције

Чињеница је да је прање новца немогуће зауставити. Оно се не може ни спречити ни искоренити. Илегалном, прљавом, сивом, нерегуларном, криминализованом новцу немогуће је стати на пут. Тај процес се може делимично контролисати, јер прање новца конвенира банкама, које тобоже не могу да наруше тајност улога. То одговара и одређеним државама које на томе зарађују, чак и правно ваљано уређене државе део своје финансијске полиције не специјализују за праћење и откривање сумњивих и спорних трансакција. Такве државе се, у суштини, највише залажу за потпуну финансијску либерализацију и дерегулацију. А то је фактички први искорак у званичну свеопшту амнестију актера и прљања и прања новца у форми мондијализације криминализованог новца и глобализације опраних финансија.

Када је у питању област финансија, криминална активност се данас не би могла остварити без коришћења компјутерске технологије, нарочито код дела код којих је услов обрада великог броја информација у кратком периоду. Компјутер се показао као средство којим се могу извршити најразноврснија и најсложенија кривична дела, као што су: пљачке, проневере, финансијске малверзације, шпијунажа, тероризам, као и сви облици злоупотреба.

С обзиром на огромну количину информација у савременим компјутерским и другим комуникационим мрежама, могућност њихове злоупотребе и размере које ова врста криминалитета сваким даном све више поприма, постаје сасвим извесно да ће се формирањем специјализованих јединица државних органа за сузбијање високотехнолошког криминалитета и конституисањем специјализованих правосудних органа, ефикасност у откривању, разјашњавању, гоњењу и доказивању овог криминала бити значајно увећана, што ће генерално допринети бољој заштити многих угрожених добара, а што за крајњи резултат има већи осећај сигурности и поверења у институције и унапређивање амбијента за инвестиције у привреди и пословању привредних субјеката.

Сама свест припадника полиције мора бити на вишем степену разумевања према техничким достигнућима. Образовни профили се морају прилагодити новим трендовима и могућностима нових софтвера, јер

програм без квалитетног полицијског службеника који уме и жели да га користи не даје никакав допринос.

Циљ овог рада јесте да приближи јавности потребу и могућности употребе софтверских алата у пре свега оперативној аналитици чијим се методама и техникама управља криминалистичким истрагама у области прања новца, свеобухватно разматрајући правни, технолошки и технички аспект и могуће начине примене расположивих различитих врста тих алата.

Сходно томе, овај рад је подељен на три дела:

- У првом делу се говори о правној регулативи, сходно нашим интеграцијама у ЕУ.
- У другом делу рада разматра се технолошки аспект прања новца.
- Последњи, трећи део, тиче се техничког аспекта тј. примене визуалајзера као сврсисходне методе криминалистичке истраге.

На крају, на конкретном случају прања новца, проституције и кријумчарења дроге на југу Србије размотрена је примена два алата-визуелајзера. У закључку рада, а на основу разматрања са правног, технолошког и техничког аспекта и резултата примене на студији случаја даје се један предлог начина употребе расположивих алата визуелајзера у откривању и анализи прања новца.

## ПРАВНА РЕГУЛАТИВА ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

Правна регулатива компјутерског криминала (Стефановић, 2011) у свету датира од друге половине осамдесетих година када је 1973. године у Шведској донет пропис који познаје кривично правну заштиту од компјутерског криминалитета (*Swedish Data Akt,* допуњен 1982. год.) у којем је у члану 21 предвиђено кривично дело „неовлашћени програмски приступ". Од тада па до данас многе земље су измениле своје кривичне законе и донеле низ својих законских прописа у вези са овом материјом.

Опасност од компјутерског криминалитета поспешила је настојање да се превазиђу различита ограничења у националним законодавствима која доводе у питање делотворност правне заштите, као и да се законодавства међусобно што више ускладе што је важна оријентација наше земље, владе и демократских институција[6].

6 Часопис Пословна политика, јул-август 2003., стр. 19-21

С обзиром на своју природу, компјутерски криминалитет врло брзо након своје појаве добија карактер међународног криминалитета, што захтева и организовање одговарајуће међународне сарадње у циљу његовог што успешнијег сузбијања. У том смислу од велике важности је доношење међународних аката. Ове активности одвијају се преко Организације уједињених нација, Организације за европску сарадњу и развој (ОЕЦД), Савета Европе, а значајни су и многобројни акти донети од стране органа ЕУ.

### Уједињене нације

Од аката донетих од стране Организације уједињених нација у овој области свакако су најзначајнији Резолуција о компјутерском криминалитету из 1990. године и Конвенција ОУН о транснационалном организованом криминалитету из 2000. год., (тзв. Палермо конвенција).

Резолуција о компјутерском криминалитету 8. Конгреса ОУН (*Resolution on Computer rileted Crime odn the 8th United Nation Congress on Crime and Treatment of Offenders*) из 1990. године предлаже прихватање следећих мера:

1. модернизација права и процедура у смислу обезбеђења да постојећа кривична дела и права обухвате адекватно осигурање доказа у судским споровима и уколико је нужно мењају своја права на одређени начин;

2. побољшање компјутерске сигурности и предузимања превентивних мера заштите, водећи рачуна о проблемима везаним за: заштиту приватности, људских права и основних слобода и сваком регулаторском механизму који се одности на коришћење рачунара;

3. прихватање мера којима ће се људи убедити о нужности заштите од компјутерског криминалитета;

4. усвајање мера неопходне обуке свих учесника у процесу кажњавања везаног за компјутерски криминалитет, почевши од судија, службеника и чланова тела одговорних за заштиту, истрагу и пресуђивање починиоцима овог криминала;

5. израда и прихватање сета норми компјутерске етике, при чему се очекује потпуна сарадња са заинтересованим организацијама и асоцијацијама и обавезно укључивање ових принципа и норми у редовно образовање и обуку у информатици и

6. прихватање политике да жртве компјутерског криминалитета које потпадају под Декларацију о основним принципима правде за жртве криминала и злоупотреба ОУН-а, буду укључене у реституисање и легализацију захтева и мера за њихово охрабрење у обавештавању (за то предвиђених дела) о претрпљеном нападу.

Конвенција ОУН о транснационалном организованом криминалитету (тзв. Палермо конвенција), из 2000. године, коју је наша земља ратификовала 2001. године, такође спада у битније акте ове организације, а која се између осталог, односи и на компјутерски криминалитет и примењује се на спречавање, истрагу и судско гоњење тешких кривичних дела и злочина, учињених од стране организоване групе криминалаца, састављене од три или више лица, која делују континуирано и споразумно ради прибављања финансијске или друге материјалне користи.

## ОЕЦД

Организација за економску сарадњу и развој (ОЕЦД) кроз своје активности на успостављању економске сарадње и на јачању културе безбедносне заштите информационих система и мрежа утиче да земље у процесу економске транзиције што пре успоставе нивое заштите који се користе у развијеним земљама. Од аката ОЕЦД-а везаних за ову материју вредни помена су свакако Студија о међународној примени и хармонизацији кривичног права везаног за проблеме компјутерског криминала и злоупотреба из 1983. године, Смернице за политику криптографије из 1996. године, а 2002. године у оквиру утврђених оквира за дигиталну економију донете су Смернице за сигурност информационих система и мрежа, као и за јачање безбедносне културе.

Као основни циљ Смерница ОЕБС-а за сигурност информационих система и мрежа из 2002. године, прописује се:

1. промовисање културе безбедности међу свим учесницима, као средства заштите информационих система и мрежа;

2. подизање свести о ризику по информационе системе и мреже, политици, деловању, мерама и процедури за уклањање ових ризика, као и потребе за усвајање и извршавање ових мера;

3. повећање поверења међу учесницима у информационе системе и мреже и начин на који је предвиђено њихово коришћење;

4. стварање општег оквира препорука које ће помоћи учесницима разумевање безбедносних одлука и поштовање етичких вредности у развоју и имплементацији доследне политике, праксе, мера и процедуре у заштити информационих система и мрежа;

5. промовисање сарадње и размене информација, као подесних, међу свим учесницима у развоју и имплементацији безбедносне политике, праксе, мера и процедуре;

6. промовисање разматрања безбедности као важног циља међу свим учесницима, укључујући развој и имплементацију стандарда.

### Европска унија

На сличан начин, у оквиру Европске уније , одлукама Европске комисије, и Савета министара, настоји се деловати на подизању нивоа безбедности информација које се преносе компјутерским мрежама и похрањују у компјутерима, као и на усклађивању тзв. материјалног кривичног законодавства држава чланица. Многобројни, а у исто време и веома значајни акти донети су у оквиру Европске уније:

- Студија о правним аспектима компјутерског криминала у Информационом друштву ( *Legal Aspects of Computer-releted Crime in the Information Society – COMCRIME study)* из 1998. године;
- Препоруке о стратегији за нови миленијум у заштити и контроли компјутерског криминала из 2000. године;
- Исте године је донета и директива о електронском пословању *(Directive on electronic commerce)*;
- Европски акциони план (*Europian Action Plan)* из 2000. године, везан је за активности обезбеђења сигурности мреже и успостављање сарадње земаља чланица и њиховог заједничког приступа компјутерском криминалу;
- Одлуке Савета министара ЕУ о спречавању дечије порнографије на Интернету из 2000. године;
- Веома важна Конвенција ЕУ о међусобној помоћи у кривичним стварима, донета је такође 2000. год., и њоме се предвиђа не само сарадња, већ и усклађивање правних и правосудних система земаља чланица, а потом следе:
- Предлог правног оквира одлучивања везаног за нападе на информационе системе *(Proposal for a Council Framework Decision on attacks againsts informational systems)* и

- акт Европске комисије који треба да обезбеди сигурније информационо друштво кроз сигурност информационе структуре и борбе против криминала везаног за компјутере, *(Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime)* тзв. *EC Cybercrime communication* из 2001. године.
- У новије акте Европске уније свакако треба споменути:
- Оквире одлука Савета министара из фебруара 2005. године о нападима на информационе системе (*Council Framework Decision on attacks againsts informational systems).* Овај оквир се односи на све земље чланице, које имају обавезу да уједначе законодавство у области компјутерског криминала, описивањем специфичних врста понашања које би требало инкриминисати у појединим законодавствима, а један од најважнијих аката Европске комисије донет у скорије време јесте:
- Студија према генералној политици у борби против сајбер криминала *(Communication towards a general policy on the fight againists cyber crime)* из маја 2007. године, где се као основни предмет ове студије намећу три врсте обавеза:

    - побољшање и олакшавање координације и сарадње између органа гоњења у борби против сајбер криминала, других релевантних ауторитета и експерата у Европској унији;

    - развијање координације са земљама чланицама, релевантним организацијама у Европској унији и међународним организацијама, на доследним политичким оквирима у борби против сајбер криминалитета;

    - подизање свести о штетама и опасностима које потичу од сајбер криминалитета.

Европска комисија је основала Форум ЕУ о сајбер криминалу, који је повезао многе институције, провајдере, мрежне операторе, групе корисника, представнике фирми за заштиту података, невладине организације и друге заинтересоване учеснике са циљем повећања међусобног разумевања и сарадње на нивоу ЕУ.

**Савет Европе**

Један од најзначајнијих међународних докумената донет у области борбе против компјутерског криминалитета који је од посебног значаја и за прописивање ове групе кривичних дела у домаћем законодавству, јесте Конвенција Савета Европе о високотехнолошком криминалу из 2001. године и Додатни протокол уз Конвенцију о високотехнолошком криминалу који се односи на кажњавање аката расизма и ксенофобије учињених путем компјутерског система из 2003. године.

Државе чланице Савета Европе усвојиле су у Будимпешти 23.11.2001. године Конвенцију о високотехнолошком криминалу „убеђени у потребу да се као приоритетна спроводи заједничка казнена политика у сврху заштите друштва од високотехнолошког криминала, те признавајући потребу сарадње између држава и приватних предузећа у борби против високотехнолошког криминала и потреби заштите легитимних интереса у коришћењу и развоју информационе технологије“, како се, између осталог , истиче у уводу ове конвенције.

Конвенција о високотехнолошком криминалу састоји се од три дела, при чему први део садржи материјално правне одредбе, други процесноправне, а трећи – одредбе којима се регулише међународна сарадња.

Одредбе првог дела обавезују државе чланице на предузимање одговарајућих законодавних мера у циљу прописивања кривичних дела која за објект заштите имају поверљивост, интегритет и доступност компјутерских података и система, а то су:

- „недозвољени приступ“ (члан 2 Конвенције), под којим се подразумева бесправно приступање компјутерском систему као целини или неком његовом делу, када се учини намерно;
- „недозвољено пресретање“ (члан 3 Конвенције), које представља уз помоћ техничких уређаја и са намером учињено бесправно пресретање преноса компјутерског преноса компјутерских података који нису јавне природе, ка компјутерском систему, од њега или унутар самог система, у шта спада и електромагнетна емисија из компјутерских система, којом се преносе такви подаци;
- „ометање података“ (члан 4 Конвенције) која обухвата бесправно оштећење, брисање, кварење, мењање или прикривање компјутерских података уколико се учини са са намером;
- „ометање система“ (члан 5 Конвенције) које постоји када се бесправно и у већем степену омета функционисање компјутерских

система путем уношења, преношења, оштећења, брисања, кварења, мењања или прикривања компјутерских податакакада је учињено са намером;

- „злоупотреба уређаја“ (члан 6 Конвенције) које се састоји у производњи, продаји, набављању ради употребе, увозу, дистрибуцији и другим видовима стављања на располагање средстава и опреме који су намењени извршењу неког од кривичних дела прописаних у чл. 2-5. Објект радње овде такође могу бити и компјутерске лозинке, шифре за приступ или слични подаци путем којих се може приступити компјутерском систему као целини или неком његовом делу уколико се нека од напред предвиђених радњи извршења предузима са намером да буде употребљена у неком од кривичних дела предвиђених у чл. 2-5.

У другом одељку за државе чланице је предвиђено прописивање посебих облика кривичних дела фалсификовања и преваре који постоје, уколико су инкриминисане радње предузете посредством компјутера. Наиме, реч је о:

- „компјутерском фалсификовању“ (члан 7 Конвенције) под којим се подразумева уношење, мењање, брисање или прикривање компјутерских података, без обзира да ли су ти подаци директно читљиви и разумљиви, са циљем да се они сматрају аутентичним и да се са њима у том смислу уобичајено поступа и
- „компјутерској превари“ (члан 8 Конвенције) која обухвата било какво уношење, мењање, брисање или прикривање компјутерских података или на било какво ометање функционисања компјутерских система са намером прибављања противправне имовинске користи за себе или друга лица.

У трећем одељку предвиђено је прописивање посебних облика кривичних дела:

- дечију порнографију (члан 9 Конвенције).

У четвртом одељку кривична дела која се односе на:

- кршење ауторских и сродних права (члан 10 Конвенције) који као и у претходним случајевима постоје уколико су дата кривична дела остварена посредством компјутерског система.

Надаље се у петом одељку:

- чланом 11 Конвенције прописује кажњавање за покушај, подстрекивање и помагање побројаних кривичних дела компјутерског криминалитета;
- чланом 12 Конвенције прописана је одговорност правних лица, а
- у члану 13 санкције и мере које би требало предузети према учиниоцима.

Државе чланице Савета Европе и остале државе потписнице Конвенције о високотехнолошком криминалу из 2001. године, потписале су у Стразбуру 2003. године Додатни протокол уз Конвенцију о високотехнолошком криминалу који се односи на кажњавање аката расизма и ксенофобије учињених путем компјутерских система. У том смислу је појединим одредбама протокола предвиђено да државе потписнице у националним законодавствима инкриминишу следећа понашања: ширење расистичког и ксенофобичног материјала посредством компјутерских система; расистички и ксенофобично мотивисану претњу упућену посредством компјутерских система; увреду мотивисану расизмом и ксенофобијом остварену посредством компјутерских система и оспоравање и минимизацију у већој мери или одобравање геноцида или другог кривичног дела против човечности.

### Даљи правци развоја правне регулативе

Наша земља је Конвенцију о високотехнолошком криминалу као и додатни протокол уз Конвенцију потписала 2005. године, а до тог момента Конвенцију и Додатни протокол је већ потписало 38 чланица Савета Европе, а поред њих и Јапан, САД, Канада, Аустралија и Јужна Африка.

Будући да превентивне мере (општег и специјалног карактера) често нису довољне нити једине мере којима се друштво супротставља нараслим и набујалим облицима злоупотребе[7] компјутера у различите сврхе, то је логично да сва савремена кривична законодавства у систему инкриминација

7 Петровић, Р. Слободан, Компјутерски криминал, Београд, 2001., стр.153.

познају једно или више компјутерских кривичних дела за које су прописане различите врсте и мере кривичних санкција.

Компјутерски криминал, због свог специфичног карактера, велике друштвене опасности и високе стопе раста, у све већој мери постаје озбиљан друштвени проблем, и то не само у националним већ и у међународним размерама. У том смислу систем заштите мора имати двоструку функцију: одвраћање од злоупотребе рачунара и стварање услова за брзо откривање и доказивање у случајевима када је злоупотреба извршена.

Имајући у виду сву сложеност спречавања, откривања, разјашњавања и доказивања компјутерског криминала, у борби против овог феномена на располагању су, генерално гледајући, три типа механизама који могу помоћи да се успешно одговори на ове изазове: алати за заштиту, етика и закони. Ови механизми имају превентивни и репресивни карактер, при чему би се у њиховој примени изразита предност морала дати превентивним у односу на репресивне мере.

Основне мере заштите информатичких система односе се на: 1) заштиту уређаја и материјалних средстава; 2) заштиту електронских веза у оквиру система – његове садржинске компоненте која се превентивно огледа у примени одређених компјутерских програма и меморисању одређених (унетих) информација.

На једном ширем превентивном плану, неопходно је да у друштву заживи свест да компјутери, као и већина других технолошких достигнућа, могу да осим своје корисне функције послуже и као ефикасно средство у рукама вештих криминалаца. Неопходно је и да сва службена лица која се баве сузбијањем компјутерског криминала, стекну основна информатичка знања као предуслов његовом ефикасном супротстављању. Осим тога, нужно је развијати свест да се овом опасном виду криминала који према свим показатељима представља и деликвенцију будућности, друштво може на ваљан начин супротставити само благовременим улагањем у стварање високообразованих кадрова, компетентних за борбу против изузетно вештих, лукавих и интелигентних учинилаца, као што су то компјутерски деликвенти. Поред тога, у конкретном деловању у сузбијању компјутерског криминалитета, мора се увек остварити и тимски приступ, уз ослањање на помоћ компјутерских стручњака (Петровић, 2001; Ранђеловић,2010; Ранђеловић, 2011).

Може се закључити да је неопходно да се сузбијање и превенција високотехнолошког криминала одвија упоредо на четири нивоа:

1. међународном – кроз сарадњу са страним државама ради што ефикасније примене низа конвенција и међународних стандарда у овој области, као и олакшаној сарадњи по питању правне помоћи, екстрадиције и решавања низа других питања правне и практичне природе;

2. институционалном – кроз адекватну примену материјалних и процесних одредби кривичног права, као и Закона о организацији и надлежности државних органа у борби против високотехнолошког криминалитета;

3. кадровском – кроз специјализацију свих службених актера супротстављања криминалитету, при чему је свако потребно формирање посебног одељења унутар полиције, као специјализоване службе у оквиру органа унутрашњих послова и

4. корисничком – преко развијања основних правила понашања (компјутерске културе) за сва лица која употребљавају рачунаре (нарочито када су они повезани у глобалне информатичке мреже).

## ТЕХНОЛОШКИ АСПЕКТ ПРАЊА НОВЦА

Разни облици криминала, као што су: сива економија, прање новца, утаја пореза, трговина дрогом, људима, оружјем и други, који се веома брзо шире и јачају, добијају интернационални карактер. Учесници прања новца врше реинвестирање средстава тамо где очекују да неће бити откривено његово порекло, не у послове са већим профитом. И управо последице тога могу бити смањена монетарна стабилност због неодговарајуће алокације средстава, неочекиване промене у потражњи новца, повећане нестабилности девизних курсева, каматних стопа и међународних токова капитала, услед чега је тешко спроводити стабилну и ефикасну економску политику, а да би се зауставиле и спречиле такве појаве у области националних и светских финансија, предузимају се одговарајуће мере на превентивном и репресивном плану[8].

По дефиницији, прање новца је скривена активност (Бошковић, 2001; Гиунио,1998; Циндори, 2007). „ Прљави“ новац који циркулише кроз „ машину за прање новца“ ствара се криминалним радњама које се обављају далеко од надзора легалних органа власти. Свакако, прање новца није нов

8 Giunio, M.,Мере за спречавање прање новца, Београд, 1998.– чланак

феномен, јер егзистира паралелно с постојањем црног тржишта, односно сиве економије. „Прљави" новац, у већини случајева, плод је производње и промета дрога, крађе аутомобила, проневера, инсајдерске трговине, илегалног промета оружја и нуклеарног материјала, дечје порнографије и проституције.

На пример, нека истраживања показала су да „прање" новца полази од технике прикривања правог порекла новца и власништва средства плаћања, преко технике легалног долажења у посед новца после обављеног „прања" новца, до технике промене облика средстава и ослобађања од велике количине новца, која је стечена криминалом (Стефановић,2011.). Ова техника „ прања" новца садржи три етапе:

(1) етапа пласмана,

(2) етапа „пресвлачења" и

(3) етапа интеграције.

У етапи „пресвлачења" одвија се најзначајнија операција „прања" новца, у којој се фактички врши „прерушавање" порекла, односно „заметање трагова" власништва средстава. У тој етапи се користе тзв. оквирне компаније, које поседују легална средства и пословни легитимитет. Најпогодније су за то оф-шор рачуни инвестиционих или пензионих фондова. Шаљу се, затим, налози за трансфер да би се средства у потпуности уклопила у међународни систем плаћања. Коначно, врши се (успешно и легално) препродаја или робе или хартија од вредности.

Прање новца из сиве економије је изум америчких транснационалних компанија које су, бежећи од високих пореза и државне контроле, измислиле оф-шор државе, пореске рајеве на свету, у којима се порез плаћао максимално до 4,23 одсто. Ти порески рајеви углавном су отварани на егзотичним острвима да би турбо менаџери могли без проблема да узму милијарде долара опљачканог новца и да се на миру одморе и окупају.

На основу списка земаља које су означене као порески рај, по „улагањима" предњаче Уједињени Арапски Емирати, Монголија, Северна Кореја, Девичанска острва, Сејшелска острва, Лихтенштајн, Гибралтар и Маршалска острва. Високо се котирају и острво Ниуе, острва Белизе, Вануату, Свалбард и Јан Мајен острва, Конго, Бахами, Обала Слоноваче, Либан, а поред других помиње се и Монако. Кајманска острва, за која многи и не знају где се налазе, постала су пети светски финансијски центар после Њујорка, Лондона, Токија и Франкфурта, управо спровођењем великих операција прања криминогеног новца пристиглог у локалне банке из свих

крајева света. У Џорџтауну, престоници Кајмана, у неким тренуцима банке и осигуравајуће компаније „седеле“ су на имовини од око 700 милијарди долара. На Кајманским острвима, са само 40.000 становника, има око 34.000 регистрованих компанија и преко 600 банака.

Процењује се да „опрани новац“ данас чини од два до седам одсто укупне светске производње, а процена Међународног монетарног фонда је да сада „бруто криминални производ“ у свету премашује 1.000 милијарди долара годишње.

Прање новца у Сједињеним Америчким Државама, и уопште гледајући шире међународно, чини кључ проблема. Од милијарди долара који се потроше на куповину кокаина, 91одсто остаје у Америци. Он се депонује у амерички и канадски банковни систем. Трговина дрогом помаже акумулирању чврстих валута у америчкој и канадској економији. Обим прања новца у Америци може се схватити на основу тога што практично свака новчаница у оптицају садржи „микроскопски траг“ кокаина. Трагови кокаина на свакој америчкој новчаници означавају интензивну употребу кеша као основног средства плаћања у пословању са дрогом. Cesar Gaviria Trujillo, бивши председник Колумбије и бивши генерални секретар Организације америчких држава, је изјавио: „Ако је Колумбија крупна риба у трговини дрогом, онда је Америка кит“ и захтевао је од америчке владе да се обустави прање новца у самој Америци и да ставе више ресурса за обуставу конзумирања опијата у Америци.

За генераторе нове индустрије прања новца важна је и употреба кеша у трансакцијама, иако је рефлексија индекса несигурности правно-финансијске природе. Кеш је постао атрактиван и зато је нагло увећан број земаља у којима се трансакције обављају готовином (а не путем кредитних и потрошачких картица, чекова, електронског трансфера и сл.). После вишеструког обртања кеша, власници „опрани“ новац теже да пребаце у земљу – државу у којој влада „пластика“, на пример Сједињене Државе, због атрактивности платних, кредитних и пластичних картица. Зато се новац пребацује по „сваку цену“ у банку да би се даље трансферисао по свету. Међутим, сада се родила и фаза прања новца у којој се користи новац за куповину читаве банке или за оснивање нове банке.

Чињеница је да је прање новца немогуће зауставити. Оно се не може ни спречити ни искоренити. Тај процес се може делимично контролисати, јер прање новца конвенира банкама, које тобоже не могу да наруше тајност улога. То одговара и одређеним државама које на томе зарађују.

Последњи ратови који се воде на етничкој и релеигиозној основи у неразвијеним државама довели су до отварања нових тржишта црног пословања и стицања прљавог новца. Примери за то су илегална продаја оружја на Косову, у Авганистану, Ираку, Либији и Сирији, као и продаја људских органа у Албанији.

## ТЕХНИЧКИ АСПЕКТИ – ПРИМЕНА ВИЗУЕЛАЈЗЕРА

С обзиром на чињеницу да је прање новца све већи проблем, како у свету тако и код нас, и да се прањем новца жели заварати траг разних компанија и појединаца који се баве незаконитим пословима, потребно је у откривању и доказивању оваквих кривичних дела користити одређене алате. За превенцију ових дела постоје одређени софтвери (комерцијални и некомерцијални) – визуалајзери који омогућавају утврђивање односа између појединаца, кључних догађаја, фирми, а помоћу њих откривају се и информације које недостају у процесу аналитичког разматрања.

Последњих година визуализација је присутна у подручју претраживања информација као препознатљива карактеристика семантичког веба[9]. Постоје специјализовани претраживачи који визуализирају резултате, али они нису предмет разматрања овог рада у коме ћемо ми између многих алата за визуалну аналитику разматрати два: комерцијални – *Analsyst's Notebook* (I2) и некомерцијални – *Node XL* алат.

Познато је и може се наћи у литератури (Ранђеловић и др.,2011) да са становишта цене и могућности лаке обуке, *NodeXL* нуди боље могућности, јер је бесплатан за коришћење са добром подршком, док са становишта могућности – *I2 Analyst's Notebook* нуди много веће могућности али је скупљи и тежи за обуку.

### Analsyst's Notebook (I2)

*Analsyst's Notebook* (I2) је врло користан аналитички софтвер који омогућава јасну визуелизацију у криминалистичким или обавештајним анализама. Овај софтвер омогућава сређивање и приказ информација из различитих извора, као и њихову организацију на смислен начин, а потом и њихову анализу употребом различитих техника.

9 Randjelović, Dragan, Popović, Brankica, Visual analytics tools and theirs application in social networks analysis, Telfor2011 Proceadings, pp. 1341,Belgrade

Да би се приказали жељени ентитети и везе између њих, потребно је најпре унети ентитете који могу бити различити, нпр. људи, места, догађаји, трансакције новца итд. Изабрани подаци се уносе у радни лист који је по стартовању I2 визуалајзера празан. Кључне карактеристике овог изузетног софтвера су:

Широк асортиман визуализације и аналитички алати који омогућавају брзо идентификовање веза и утврђивање и израду шема у сложеним скуповима података. Флексибилно прикупљање података омогућава брз унос података, уз динамичне аналитичке процесе. Једноставно приказивање комплексних информација помоћу графикона који омогућавају брзо и прецизно информисање, а на основу њега и одлучивање (Раду, 2008).

### NodeXL

*NodeXL* је повољан, отворен шаблон за Excel 2007 и 2010 који нам омогућава да унесемо умрежене податке и видимо графикон мреже, а све у Excel прозору. Можемо лако да прилагодимо изглед графикона, зум, обим; динамички филтер за темена и ивице, променимо распоред графикона, нађемо кластер повезаних чворова и израчунамо метрике графикона. *NodeXL* пружа низ основних анализа мреже и визуализацију функције. Овај визуалајзер користи радну свеску која садржи више радних листова за складиштење свих информација потребних за представљање графичке мреже. Однос мреже је представљен као „ивица листа", који садржи све парове чворова који су повезани у мрежу. Остали листови садрже информације о сваком чвору и кластеру.

Ова алатка подржава рад са скромном величином мреже од неколико хиљада чворова, мада неки корисници успешно раде са десетинама хиљада чворова.

## СТУДИЈА СЛУЧАЈА ПРАЊА НОВЦА – ЈУГ СРБИЈЕ

Како би истражили оптималан начин употребе предложена два алата *Analsyst's Notebook (I2)* и *NodeXL* у анализи прања новца у раду, позабавићемо се њиховом употребом на примеру у којем се може видети како се ови софтверски алати могу применити за визуелизацију података битних за расветљавање једног кривичног дела, у конкретном случају у питању је случај прања новца, проституције и кријумчарења дроге на југу

Србије. Због расположивог простора ћемо само једну, прву информацију приказати у пуном формату.

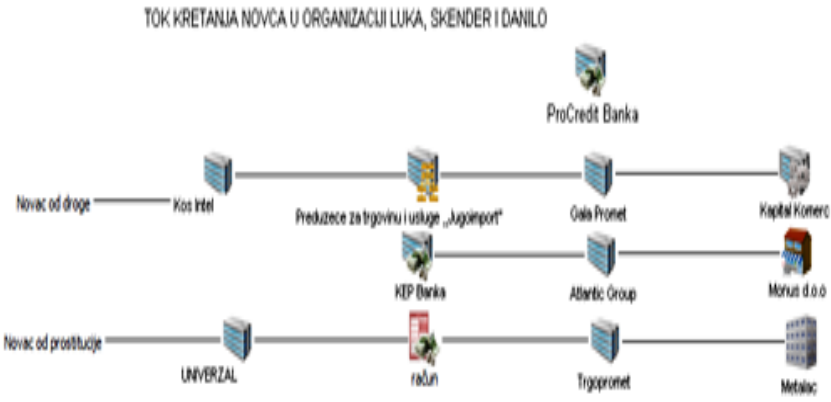
*Слика1. – Изглед форме за приказ информација у студији случаја и почетна од њих*

<table>
<tr><td colspan="2">ПРОЦЕНА ИЗВОРА</td><td rowspan="3">ИЗВОР<br><br>ОГЊЕН<br>234 5066 998</td><td>БРОЈ ИНФОРМАЦИЈЕ</td></tr>
<tr><td>ШИФРА</td><td>C</td><td>MC/1240/10</td></tr>
<tr><td colspan="2" rowspan="2">Свака информација мора бити процењена према извору. Процењује је службеник користећи шифре A, B, C и X</td><td>ДАТУМ ИНФОРМАЦИЈЕ</td></tr>
<tr><td>05.12.2010.</td></tr>
<tr><td colspan="2">ПРЕДМЕТ</td><td>Синдикат проституције</td><td>СЛУЖБЕНИК<br>Владан</td></tr>
<tr><td colspan="3">САДРЖАЈ:<br>Именован је на одслужењу седмогодишње затворске казне у КПЗ Сремска Митровица због оружане пљачке. Недавно је захтевао и одобрен му је разговор са службеником Министарства унутрашњих послова Републике Србије, који је задужен за контакте са осуђеницима. Током разговора именован је тврдио да је био вођа ланца проституције који се бави пратњом и довођењем проститутки у хотелске собе, посетиоцима луксузних хотела на Косову и осталим градовима на југу Србије. У разговору је објаснио како је улога „вође“ да осигура да групе проститутки пошаљу правила која им организација намеће. Према његовој изјави улоге „вођа“ су укинуте, тако да је, с обзиром да нема других знања и искустава, почео да се бави пљачкањем мањих продавница, а током једне пљачке је ухапшен и осуђен.<br>Огорчен због односа организације према њему, спреман је дати информације о активностима Синдиката. Као противуслугу за дате информације захтева повлашћени третман током одслужења затворске казне.<br>За време разговора нису постигнути никакви договори. Разговори ће бити настављени.<br>ДОПУНСКЕ ИНФОРМАЦИЈЕ:</td><td>Процена садржаја (шифра)<br>3</td></tr>
<tr><td colspan="2">ВЕЗЕ</td><td>НАДЗОРНИК<br><br>САША</td><td>Сваки део информације (садржаја) мора проценити службеник који је подноси, користећи шифре: 1,2,3 и 4.</td></tr>
</table>

*Извор – Ранђеловић, Д. и др.,The use of visualization tools in the prevention of the money laundering, Archibald Reiss Days Proceedings, КПА Beograd, 2012., стр. 891*

Следе информације које због ефикасности коришћења расположивог простора за овај рад аутори неће дати, и могу се наћи у (Ранђеловић, Д. и др., 2012), већ ће аутори приказати шеме токова кретања новца по повезаним организацијама осумњичених у разматраном криминалном случају, који ћемо назвати „Организација Лука, Скендер и Данило“ по именима шефова појединих повезаних криминалних група, респективно за проституцију, дрогу и прање новца, и то компаративно добијене i2 Analyst's Notebook и NodeXL визуелајзером .

*Слика 2.- Карта кретања новца у организацијама – приказ у i2 Analyst's Notebok-y*




*Извор-Аутори*

*Слика 3.- Карта кретања новца у организацијама – приказ у NodeXL-y*


*Извор-Аутори*

## ЗАКЉУЧАК

На основу разматрања са правног, технолошког и техничког аспекта могуће примене расположивих по основној подели комерцијалних и некомерцијалних алата визуелајзера, и коришћењем познатих и у раду датих података о међусобним предностима и манама два у раду разматрана визуелајзера, аутори предлажу као решење за њихово коришћење хијерархијску мрежу са алатом *I2 Analyst's Notebook*-ом у чворишту организације која врши послове детектовања и анализе прања новца и дистрибуиране алате *NodeXL* на мобилним платформама са комуникацијом у смислу решавања задатака, чиме се омогућава оптимално коришћење обе врсте алата користећи њихове предности.

## SUMMARY
## SOFTWARE TOOLS – TOOLS FOR VISUALIZATION AND MONEY LAUNDERING AS A FORM CYBERCRIME

Today, when most of humanity is in the information era of development of human society with predominantly present globalization, the necessary connection of money laundering as a criminal act and the tools for visualization as meaningful methods of criminal investigation is a hot topic of scientific and professional considerations and because of that the topic of the this paper.

When it comes to finance, criminal activity could not be achieved without the use of computer technology, especially the part where the condition of processing large amounts of information in a short period. The computer proved to be a means to make the widest and most complex crimes such as robbery, fraud, financial fraud, espionage, terrorism and all forms of abuse.

All this points to a recent (modern) form of committing criminal acts that characterize the properties of the dynamics and special forms forms forms and manifestations, and to the high-tech crime. On the end of this paper work on a specific case study considered the use of visualization tools for detection and analysis of money laundering and on this example proposed one possibly way of its using.

Keywords: money laundering, data visualization tools, NodeXL, i2 Analyst's Notebook, high-tech crime

## ЛИТЕРАТУРА


1. Бошковић, М., Актуелни проблеми сузбијања прања новца, *Безбедност*, Вол. 1, 2001.,стр 565.
2. Циндори, С., *Систем спречавања прања новца*, Финансијска теорија и пракса, Београд, 2007.
3. Giunio, M., *Мере за спречавање прања новца*, Слободно предузетништво, Београд,1998.
4. Петровић, Р. С., *Компјутерски криминал-друго издање,* Министарство унутрашњих послова Републике Србије, Београд, 2001.
5. Раду, К. П., *Како открити невидљиве везе*, http://www.media.ba/ bs/alati/ kako-otkriti-nevidljive-veze, 2008.
6. Ranđelović, D., Popović B., Стефановић М., The use of visualization tools in the prevention of the money laundering, *Archibald Reiss Days Proceadings*, КПА Beograd, 2012.,881-902.
7. Ranđelović, D., Popović B.,Visual analytics tools and theirs application in social networks analysis,*Telfor Proceadings*,Belgrade, 2011, pp. 1341-1343.
8. Ранђеловић, Д., *Поређење комерцијалних и некомерцијалних алата дигиталне форензике и њихова употреба*, Научно-техничка информација, Војно-технички институт, Београд, 2011.
9. Ранђеловић, Д., Сигурност рачунарских мрежа као основе за повезаност полиције, безбедности и високотехнолошког криминала, *Тематски зборник Полиција, безбедност и високотехнолошки криминал*, КПА, Београд, 2010.
10. Стефановић, М., *Примена Визуелајзера у прању новца*, Специјалистички рад, КПА Београд, 2011.


## RESUME


The subject of this research is the study of the connection of money laundering as a criminal event and visualization as methods of criminal investigation. Money laundering is the process of disguising the illegal origin of money or property acquired through crime. Therefore, criminals made a series of transactions with the ultimate aim of the money or property is present as legally acquired. The money in this process often changes its shape and is transferred from one place to another which is why you need to use certain tools and methods to detect all illegal acts and thereby reduce the future performance of these crimes. A major role in monitoring and combating this type of crime just play visualiyation that allow to determine the relationship between individuals, key events, firms, companies.

The goal of this research is reflected in the fact that through a comprehensive analysis of the money laundering and legal, technological and technical aspects and proper application of existing software solutions in the two groups are not the best known commercial tools and determine the best solution in order to identify, clarify and prove the offense. So the goal of the research is the optimal choice of the method used to track money laundering because the only possibility of analyst services dealing with this problem depends on which tool to choose.

Using an experiment i.e. case study and comparative method the authors were guided by the aim of answering these questions on the subject of this paper.

Овај рад је примљен **06.09.2012.** а на састанку редакције часописа прихваћен за штампу **10.10.2012.** године.