Мр *Зоран МИЛАНОВИЋ*
Криминалистичко-полицијска академија, Београд
Проф. др *Радован РАДОВАНОВИЋ*
Криминалистичко-полицијска академија, Београд

UDK – 681.518:343.983
Прегледни научни рад
Примљено: 20.06.2013.

Дигитална форензика у контексту заштите информационих система*

Апстракт: *Иако се о заштити информационих система и корисника интернета често говори и пише, мали број менаџера и корисника информационих технологија су свесни значаја овог проблема. То може довести до појаве ризичних инцидентних ситуација у којима су угрожени пословни информациони системи. Њихова неадекватна заштита може имати катастрофалне последице на сам пословни процес. Циљ рада је да се на јасан и транспарентан начин успоставе и доведу у везу методе и технике заштите информационих система са дигиталном форензичком истрагом, као и да се скрене пажња на безбедносну свест и културу као есенцијалне елементе циклуса управљања ризиком и заштитом.*

Кључне речи: *заштита информационих система, безбедносни ризик, дигитална форензика, дигитални доказ.*

Увод

Настанак и развој информационих технологија (ИТ), а посебно интернета, сматра се најважнијим технолошким достигнућем 20. века, а већ почетак овог века је означен као улазак у „дигитално доба“. Главне одлике времена у коме живимо су примена напредних ИТ у свим сферама живота и рада, при чему више од 90 одсто информација настаје у дигиталном облику (http://newyorkcomputerforensics.com/learn/ index.php, доступан 22. 5. 2013), више од 70 одсто организација своја документа чува у електронском облику, а 30 одсто информација у електронском облику се никада не одштампа (Симић, 2008:124). Функционисање и остваривање пословних циљева организације почива на сложеним ИТ, које перманентно снабдевају информацијама све нивое управљања,

* Овај рад је резултат реализовања два интерна пројекта Криминалистичко-полицијске академије у Београду, и то: 1) *Национална безбедност Републике Србије и безбедносне интеграције* и 2) *Структура и функционисање полицијске организације – традиција, стање и перспективе.*

одлучивања и процеса рада, чиме се свакодневно повећава количина података и информација (Ђикановић, Сивчевић, 2011:149). Према томе, може се рећи да је „дигитално доба“ промовисало информацију и знање као стратешке ресурсе организација, па и друштва у целини (*Борба против сајбер-криминала,* 2011:288). Самим тим, њихова безбедност постаје приоритетна за очување пословних и свих других друштвених процеса, а познавање безбедносних проблема се намеће као један од елемената опште културе, тим пре ако се има у виду друга (мрачна) страна дигитализације, која се огледа у употреби ИТ као криминалног алата и премештање криминалне сцене из просторне у дигиталну димензију (види Урошевић, 2010). Поједностављено речено, ИТ постаје Ахилова пета информационог друштва (Петровић, 2010а:1).

Оно што је сигурно, ИТ криминал је резултат људске активности. Они су заиста најслабија карика и у ситуацијама када је систем беспрекорно имплементиран, а једини прави узрок проблема лежи у њиховом незнању или намери.

Према подацима Internet World Stats (http://www.internetworldstats.com/stats.htm, 30. 6. 2012), од укупног броја становника 7.017.846.922 скоро једна трећина (2.405.518.376) користи интернет, а на основу закона великих бројева може се претпоставити да је значајан проценат ових корисника спреман да злоупотреби моћ и могућности које су им постале доступне. Посебан подстицај томе је, с једне стране, све већа осетљивост, односно рањивост друштвене заједнице, а са друге стране изузетно висок степен анонимности присутан у дигиталном простору. Потврда изнетој тврдњи је и то да је свако од корисника интернета бар једном био жртва неког од извора проблема у раду са рачунаром, да ли због *spam* порука у *mailbox*-у или вируса који значајно могу да оштете податке на рачунару, потпуно је свеједно (види Урошевић, 2009.).

„Међутим, никоме није циљ да се због опасности одриче повољних могућности, већ да те могућности максимално, али осмишљено и контролисано, експлоатише ради сопствене добробити. Управо због тога технолошке иновације намећу императивну потребу адаптирања новим условима, правилима, могућностима и препрекама. При томе се мора бити свестан да промене нуде прилику, али да носе и врло велики ризик. Тај ризик претпоставља да би кибер-напади доводили у опасност интелектуална, материјална и финансијска добра, пословне операције, инфраструктурне сервисе, поверење потрошача и много тога другог“ (Петровић, 2010б:213).

Имајући у виду и то да цена информација на тржишту стално расте, као и да напади постају изузетно софистицирани, можемо констатовати да је потребно изузетно ангажовање не само информатичког сектора,

него и свих других запослених који користе ове технологије, како би се спречила њихова злоупотреба.

Решавањем наведених проблема, а у циљу смањења степена ризика и обезбеђења амбијента потребног за постизање високог нивоа информационе безбедности, неопходно је дефинисати процесе заштите информационих система и дигиталне форензике, као и њихове везе и интеракције.

Заштита информационих система

Заблуде и уверења корисника ИТ да се непријатности чији су узроци првенствено на интернету дешавају другима, као и мишљење да о заштити нема шта ново да се научи, највећи су савезник злонамерника који своје жртве траже и проналазе на интернету. Заштита великих рачунарских мрежа и база података, које су незаменљиво средство за обраду података и информација, у нашој земљи још увек је готово страна тема. Последњих година томе највише доприноси велика миграција стручњака из ове области ван граница наше земље, као и веома мала обрада ове теме у нашем образовном систему. Може се сматрати да је ово последица непостојања осмишљене националне политике и стратегије на овом пољу, што се посебно истиче као проблем на научностручним скуповима.

С обзиром на директан утицај информационе технологије на пословање (види De Lone, 1992), неопходно је обезбедити континуалну заштиту његовог интегритета, поверљивости и расположивости. Међутим, код нас је врло распрострањена пословна политика која се своди на интензивно форсирање квантитета на рачун квалитета: реализовати што пре и што више појединачних пројеката. Основне одреднице оваквог приступа су превелики захвати, кратки рокови, недовољан кадровски потенцијал и мноштво различитих решења (опција), а све то драстично утиче на безбедност информационог система.

Пројекат заштите информационих система поставља врло сложене захтеве пред целокупну организацију, а нарочито структуру, с обзиром на многобројне интеракције између различитих ентитета, док са друге стране убрзани развој технологије генерише нове проблеме, што захтева и нове приступе у њиховом третирању.

Решење ових проблема се нуди кроз системски приступ који подразумева дефинисање веза и утицаја унутар система, утицај окружења на систем, као и потенцијалне опасности унутар и изван система, а потом, на основу анализе ситуације, дефинисање и примену адекватних организационих и безбедносних мера. Те мере усмерене су на избор најповољнијих организационих форми и односа између производних чинилаца, њихово складно распоређивање и међусобно повезивање

у јединствену функционалну целину, избор адекватне методологије планирања, методологије рада и техника рада, стандарда и документације, техника и метода мерења и вредновања рада, дефинисање права и одговорности, као и неопходних санкција. Све ово мора бити уобличено и нормативно регулисано како би се постигао крајњи циљ − јединственост рада и резултата, жељени квалитет, ниски трошкови и висок степен безбедности и поузданости целог система (Петровић, 2004:59).

У оцењивању степена остварене заштите мора се имати у виду да је апсолутна заштита неостварљива (Петровић, 2004:24), те да не постоје потпуно безбедни информациони системи. Постоје само системи који су мање или више безбедни. Поштовање безбедносних стандарда није гаранција потпуне заштите информационог система, већ минимум који мора да буде испуњен да би рачунаре у мрежном окружењу уопште имало смисла користити. У том смислу, сваки реалан систем заштите захтева континуирану надоградњу и усавршавање, без обзира на до тада остварени квалитет.

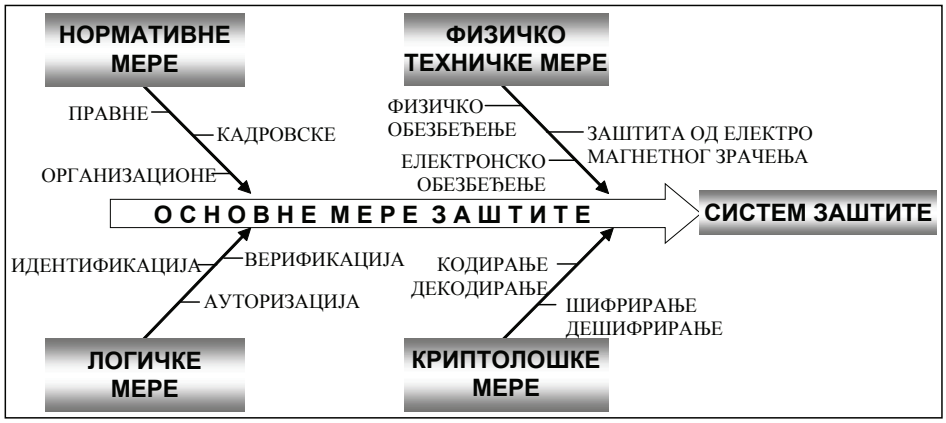
„Када се размишља о заштити, полази се од чињенице да било који систем заштите има смисла ако и само ако се њиме НЕШТО, од НЕЧЕГА и ЗБОГ НЕЧЕГА штити, а да би исти постигао циљ, он своју функцију мора са НЕЧИМ и на НЕКИ НАЧИН извршавати. Из овакве опште констатације није тешко уочити логичке целине и њихов логички редослед. Ове логичке целине се могу исказати кроз „златна питања“ о заштити информационог система, на која треба дати што ПОТПУНИЈЕ одговоре: 1. ШТА штитити? 2. ОД КОГА или ЧЕГА штитити? 3. ЗБОГ ЧЕГА штитити? 4. ЧИМЕ штитити? 5. КАКО штитити?

Одговор на прво питање (ШТА штитити?) подразумева утврђивање ОБЈЕКАТА заштите, на друго (ОД КОГА или ЧЕГА штитити?) подразумева ИДЕНТИФИКАЦИЈУ ПРЕТЊИ (ОПАСНОСТИ) које, у мањој или већој мери, могу угрозити објекте заштите, на треће (ЗБОГ ЧЕГА штитити?) подразумева утврђивање ПОСЛЕДИЦА које нека претња може изазвати у односу на неки објекат, на четврто (ЧИМЕ штитити?) подразумева ИЗБОР МЕРА које ће се користити, и на последње питање (КАКО штитити?) подразумева ДЕФИНИСАЊЕ ПОЛИТИКЕ ЗАШТИТЕ“ (Милановић, 2006:18).

У изградњи и реализацији целовитог и поузданог решења заштите, са становишта ефикасности и трошкова, неопходно је спровести следеће нормативне, физичко-техничке, логичке и криптолошке мере (слика 1).

Методологија за спровођење заштите и информационе безбедности темељи се на међународној норми фамилије стандарда ISO/IEC 27000, која се односи на ИТ, технике заштите и систем за управљање информационом безбедношћу (ISMS – *Information security management system*), али и на друге важеће норме, стандарде и професионалне препоруке специјализованих организација за информациону безбедност.

Тренутно у Србији само тридесет две организације (*Привредна комора Србије*, 2013) имају уведен стандард ISO/IEC 27001, што иде у прилог чињеници да се веома мала пажња данас посвећује заштити и управљању информационом безбедношћу. Тој чињеници се може придодати и коментар Специјалног тужиоца за високо технолошки криминал, Лидије Николић, која каже да „свест о технолошком криминалу у Србији још увек није на довољно високом нивоу". Она истиче да је „непостојање свести код грађана мање опасно од непостојања свести код државних органа, који треба да се баве превентивом и борбом против високо технолошког криминала", као и да „држава није свесна озбиљности коју носи технолошки криминал" (Николић, 2008:3).



Слика 1 – *„Рибља кост" основних безбедносних мера заштите* (Милановић, 2006)

Подизање свести о ИТ безбедности има за циљ подићи свесност свих корисника о безбедности на свим хијерархијским нивоима, а ефикасно је само ако је планирано, спроведено, евалуирано и унапређено према одређеним организационим смерницама. У склопу оваквог програма кориснике је потребно континуирано упознавати са актуелним темама на подручју информационе безбедности, те их наводити на примерено коришћење информационог система које ће смањити ризик од потенцијалних безбедносних инцидената (види Петровић, 2007).

Такође је неопходно да корисници имају обавезу да на својим рачунарима користе резидентну заштиту од вируса и других малициозних програма и редовно их ажурирају, затим да буду дужни да изаберу и користе лозинке и повремено их мењају. Ово су само неке од препоручених мера као обавезних, које подразумева имплементација превентивне заштите информационих система.

Организације које немају овако дефинисана решења и препоруке налазе се у критичној високоризичној зони, подложној безбедно-

сним инцидентима, у којој ће скоро сигурно доћи до компромитације, недоступности и уништења виталних података и информација. Догодили се то, последице ће у најбољем случају бити период изузетно тешког пословања и високи трошкови опоравка од насталих штета. У најгорем случају, последице могу бити катастрофалне за организацију. Узрок томе лежи у чињеници да коришћење информационих технологија чини корисника неопозиво зависним од њих.

У већини случајева у развијеним ИТ организацијама у чијим се информационим системима десио инцидент прво се покушава решавање проблема сопственим снагама и прикривање догађаја од јавности, те руководство организације ангажује свог администратора мреже и заштите, а ако то није довољно, доноси се одлука о позивању специјализованих консултаната из те области. Они прво утврђују природу догађаја, процењују последице догађаја и доносе одлуку, да ли је у питању грешка у програму оперативног система, грешка оператера, или намерни напад. У случају да је безбедносни инцидент настао као намеран напад који је нанео штету информационом систему, главни менаџер или руководство организације доносе одлуку о наставку истраге, обустави или подношењу пријаве званичним органима МУП-а. Бројни су разлози зашто организације у старту не позивају званичне органе истраге безбедносног инцидента, почев од страха од губитка клијената и компромитације организације, до зазирања од превеликог уплитања званичних органа.

Фамилија стандарда ISO/IEC 27000 је прихватила већ постојеће ставове да се безбедност и безбедносни инциденти не прикривају по сваку цену, већ да је њихово решавање у неким случајевима нужно кроз овлашћене институције. Комуникација с другим стручњацима кроз безбедносне и професионалне групе умногоме може помоћи организацијама при спречавању интерних инцидената или при њиховом решавању.

Процесни модел заштите информационог система

Проблеми заштите са којима се свакодневно сусрећемо у пракси далеко су већи од појединачних техничких решења или безбедносних производа. Заштиту информационог система треба посматрати као процес који обухвата различите аспекте рада и коришћења информационих технологија, а пре свега се то односи на поступак дефинисања одговорности и овлашћења за све учеснике у коришћењу информационог система, као и на процедуре пре и после појаве безбедносног инцидента. Експлозивни развој нових ИТ и њихов снажан утицај на пословање намећу као нужну потребу да се утврди и успостави ланчана веза између превентивне заштите, детекције безбедносног инцидента и дигиталне

форензике, из којих ће проистећи низ нових корективних мера, правила и техника за унапређење заштите информационе имовине.

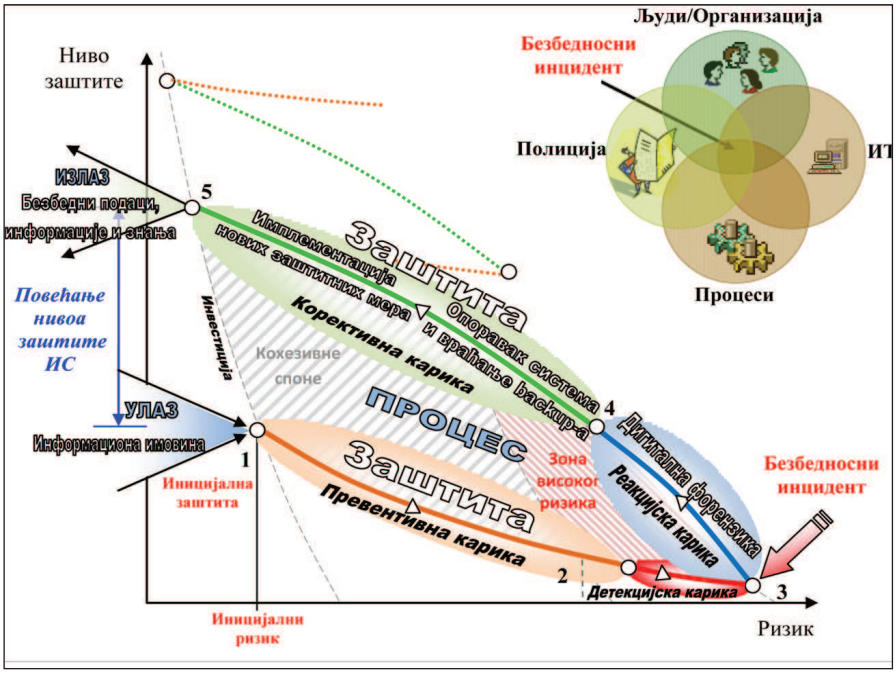
На основу изнетих теоријских разматрања могуће је формирати процесни модел (слика 2) који улаз (ИС са свим својим базама података, информацијама и знањима) трансформише (процес) у излаз (безбедни подаци, информације и знања). Интересантно је приметити да на улазу штитимо целокупан ИС како би на излазу имали испуњен постављени циљ – безбедност дигиталних ресурса.

Елементи процесног модела састоје се из четири активности (карике) које су међусобно повезане и које утичу једна на другу, и то:

- превентивна (*Prevention*) активност која делује у смислу спречавања неовлашћених активности (нпр. антивирусни програми, *firewall*, контрола приступа и сл.);
- детекцијска (*Detection*) активност која омогућава откривање неовлашћених активности (нпр. *Intrusion detection system* – Систем за детекцију упада, алати за проверу интегритета и сл.);
- реакцијска (*Reaction*) активност која представља скуп механизама који помажу при реакцији на детектоване неовлашћене активности (нпр. форензичка анализа);
- корективна (*Correction*) активност која представља опоравак система (*Restore point*) и враћање обрисаних датотека (*Recovery files*) и/или недоступних сервиса, или пак инсталирање новог система (*Install system*) и враћање бекапованих података (*BackUp data*). Затим се имплементирају нове заштитне мере, тестира систем и пушта у рад.

Предложени процесни модел показује међузависност између нивоа остварене заштите и величине ризика, који се у потпуности никад не може избећи. То значи да је неопходно тежити и успоставити баланс (равнотежно стање) између ове две варијабле и имати у виду оптимални ниво заштите, тј. улагање у заштиту мора бити у складу са вредношћу система који се штити. Неравнотежно стање подразумева или недовољну заштиту или превелике (непотребне) инвестиције.

Коначно, сваки реалан систем заштите захтева континуирану надоградњу и усавршавање, без обзира на већ остварени квалитет. Корективне акције треба усмерити на модификацију решења са уоченим слабостима у прихватљива и задовољавајућа решења или, у немогућности модификације, на њихову елиминацију из система, као и на изналажење, развијање и примену сопствених оригиналних решења на плану заштите.



Слика 2 – *Процесни модел у заштити података, информација и знања*

Управљање инцидентним ситуацијама и безбедносним ризиком

Управљање инцидентним ситуацијама подразумева скуп софтверских алата и методологија чији је циљ ефикасан и адекватан одговор на сваки безбедносни инцидент. Управљање инцидентним ситуацијама захтева да сваки корисник у ланцу одговара на инцидент, тачно зна шта се дешава на терену и какве се реакција од њега очекују.

Безбедносни инцидент представља појединачни или низ догађаја који могу нарушити пословање и угрозити информациону безбедност, док се под рачунарским безбедносним инцидентом подразумева употреба рачунарских или умрежених система за разне нелегалне, неприхватљиве или неауторизоване радње (види Dan, 2003).

Инцидент не мора бити само последица намере, већ и нехата, грешке или деловања више силе, елементарне непогоде. Сваки инцидент мора бити саниран. Први корак у санацији је такозвана форензичка обрада инцидента, где се истражује, пре свега, одговорност за инцидент, а затим дијагностикује и отклања узрок у систему који је евентуално дозволио да дође до инцидента. Након тога се санирају последице инцидента и

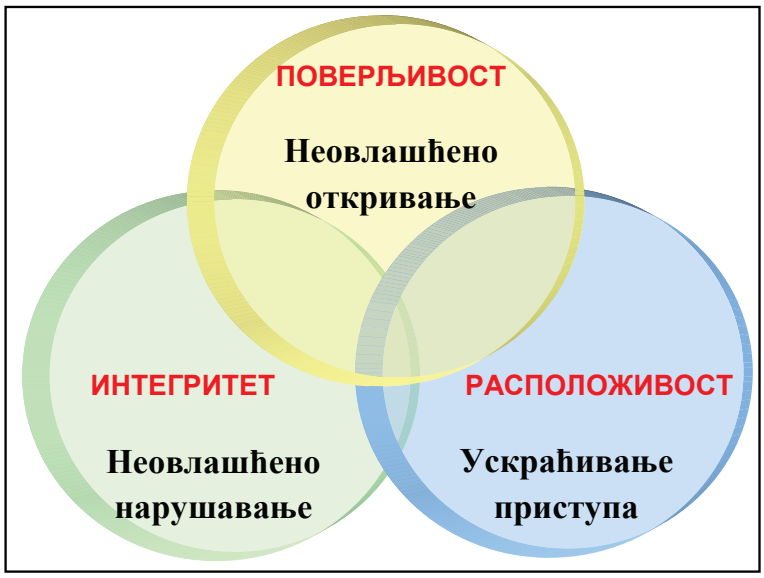
информациони систем се враћа у стање које гарантује његово безбедно функционисање.

Око 80 одсто стварних безбедносних инцидената остане непријављено (http://www.history.navy.mil/library/online/computerattack.htm, доступан 22. 5. 2013), јер у већини случајева организације нису могле да открију да је њихов информациони систем подривен/нападнут, или организације нерадо говоре о томе.

Чињеница је да после сваке инцидентне ситуације долази до скоковитог повећања опрезности код свих радника, чиме се значајно сужава простор за настајање наредног инцидента. Међутим, познато је да се инцидентне ситуације не јављају често, па опрезност код свих, а код појединаца и драстично, временом опада. На неутралисање овакве нежељене појаве највећи утицај управо имају надзор и контрола, јер ако запослени очекују периодичне контроле, онда су свесни и могућих последица, па ће зато знатно већу пажњу поклањати спровођењу свих прописаних поступака заштите.

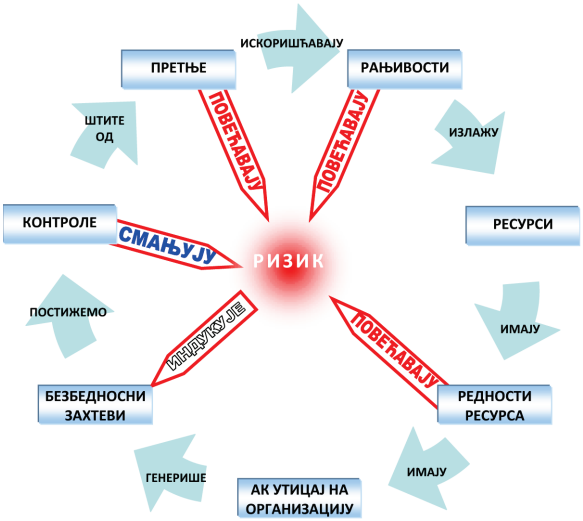
Као најчешћи безбедносни инциденти наводе се: недоступност сервиса и информација, неауторизовани приступ рачунарским системима, пиратерија софтвера, откривање, крађа и измена рачунарских података, крађа рачунарских услуга, злоупотреба украдених лозинки, неовлашћени приступ базама података, губитак WEB-а и мрежног приступа, стварање и дистрибуција вируса, слање нежељене електронске поште, претећих и дискриминишућих мејлова, дечија порнографија, јавне неугодности, лош публицитет и победа супарника у тржишној трци. Све то су претње интелектуалном власништву, знању и информацијама, а међу бројним облицима деловања посебно су изражене као економска шпијунажа, крађа информација и кршење ауторских права. Њихов је извор занимљивост информационих садржаја на темељу којих појединци или групе могу остварити корист. Сви до сада наведени облици злоупотребе ИТ се, у зависности од циља који имају, могу груписати у три категорије: „кибер тероризам, обавештајно деловање (шпијунажа) и информационо ратовање“ (Петровић, 2009:76).

Безбедносни ризик се дефинише као могућност да неке претње искористе слабост(и) елемента информационог система. Данас су посебно важне претње ризиком нематеријалним деловима информационог система, где се говори о потенцијалу којим одређена претња може проузроковати губитак или штету на информацији, користећи њихове рањивости. Реализација претњи може негативно утицати на поверљивост (*confidentiality*), интегритет (*integrity*) и расположивост (*availability*) информационе имовине (слика 3). Под информационом имовином, према стандарду ISO/IEC 27001, подразумевају се сва она средства која организација користи у сврху остваривања својих пословних циљева (информације,



Слика 3 – *Основни елементи информационе безбедности* (Милановић, 2006)

хардвер, софтвер, људи, сервиси и нематеријална имовина). Прецизна идентификација, односно класификација информационе имовине први је и врло важан корак процеса управљања безбедносним ризиком, будући да се на основу њега одређује који ресурси захтевају посебан третман са становишта безбедности. Неприкладно обављена идентификација ресурса може цели процес одвести у погрешном правцу, чиме се у потпуности губи његов значај и смисао.



Слика 4 – *Управљање ризиком* (Милановић, 2006:77)

Улагање у информациону безбедност потребно је посматрати као инвестицију. Од сваке инвестиције, па тако и од улагања у информациону безбедност, очекује се позитиван салдо и повратак средстава. У том контексту управљање безбедношћу се може посматрати у смислу смањења оперативних трошкова, као превенција од потенцијалних трошкова или других негативних утицаја на пословни процес.

Управљање безбедносним ризиком релативно је нова дисциплина у подручју безбедности информационих система, која је произашла из потребе за стандардизацијом и формализацијом поступака везаних за управљање безбедношћу. Управљање безбедносним ризиком (слика 4) се дефинише као процес идентификације оних чињеница које могу негативно утицати на поверљивост, интегритет и расположивост информационе имовине, као и њихова анализа у смислу вредности појединих ресурса и трошкова њихове заштите. Завршни корак обухвата предузимање заштитних мера које ће идентификовани безбедносни ризик свести на прихватљиву меру, у складу са пословним циљевима организације.

У којој мери и на којим местима ће се приступити умањивању безбедносног ризика, одлука је првенствено менаџмента, као оне функције која има могућност доношења одлука и право располагања буџетом организације. Безбедносни ризик могуће је третирати на неколико начина: могуће га је прихватити онаквим какав јесте, могуће је приступити његовом умањивању имплементацијом одговарајућих безбедносних контрола, а могуће је и његово посредно решавање, односно пребацивање другим организацијама које су за то специјализоване.

Доношење одлука везаних за управљање ризиком врло је одговоран и захтеван посао који, осим одређеног нивоа стручности, захтева и изузетно добро познавање информационих система и њихове функције.

Дигитална форензика

Дигитална форензика је интердисциплинарно подручје које обухвата различите специјалности и дисциплине, а представља употребу природних наука на правне садржаје. У пракси, дигитална форензика темељи се на начелима и методама природних наука, као што су математика, физика, хемија и биологија.

„Дигитална форензика је област криминалистичке науке која представља спој технологије и знања са циљем утврђивања и доказивања коришћења ИТ у одређеним криминалним радњама. Наука о дигиталној форензици обухвата познавање метода и процедура које се примењују у анализи и прикупљању података (доказа)“ (Милановић, 2010:4). Технологије, с друге стране, представљају разне алате који омогућавају

примену метода и процедура у рачунарској, мрежној, мобилној и интернет дигиталној форензици.

Дигитална форензика је фасцинантно поље, јер како организације постају сложеније и имају велику размену података и информација на мрежи, тако се и високотехнолошки криминал развија − великом брзином и у сталном је порасту. Дигитално доба је произвело много нових занимања, а једно од најнеобичнијих је дигитална форензика, јер се бави применом закона у науци. „Иако је слична другим облицима правне форензике, дигитални форензички процес захтева огромно познавање различитог хардвера и софтвера како би се избегло случајно уништавање доказа, као и очување доказа за касније анализе“ (Solomon, 2005:2).

Дигитална форензичка наука дефинише се као „коришћење научно деривираних и доказаних метода за сакупљање, чување, идентификацију, анализу, интерпретацију, документовање/презентацију дигиталних доказа деривираних из извора дигиталних података, а намењених за лакшу реконструкцију догађаја који се сматрају кривичним делом, или неовлашћеним ометањем планираних операција рачунарских система и мрежа“ (Милосављевић, 2009:90). Ова дефиниција покрива широке аспекте дигиталне форензике, од аквизиције података до легалних акција у правосудном поступку. При томе је важно напоменути да сами медији и подаци не представљају доказ, него су само потенцијални извор доказа. Појам дигитална форензика односи се на квалитет и оригиналност сачуваних и генерисаних дигиталних доказа, као нпр. дигитални аудио и видео записи, дигиталне фотографије, дигитални текстови и сви други дигитални подаци који су смештени на стабилним и преносним рачунарима, серверима, преносним меморијским уређајима и другим медијима, као и доказа са интернета.

Процес дигиталне форензике обухвата четири главне фазе:

- сакупљање (аквизиција): идентификација, валидација, означавање, снимање и извлачење података из могућих извора података, следећи процедуре које штите интегритет података;
- испитивање: форензичко процесуирање сакупљених података коришћењем комбинације аутоматизованих и мануелних метода и процена екстрахованих података од посебног интереса, уз очување интегритета података;
- анализа: анализирање резултата испитивања легално оправданим методама и техникама, идентификовање потенцијалних дигиталних доказа применом научно деривираних и доказаних метода које

могу користити код реконструкције догађаја у истрази компјутерског криминала;

- извештавање: формирају се чврсти докази и припрема њихова презентација пред судом кроз експертско сведочење или вештачење. Извештавање о резултатима анализе може укључити опис примењених акција, који објашњава како су изабрани алати и процедуре, и одређује које друге акције треба да се изврше, нпр. форензичко испитивање додатних извора података, идентификоване рањивости, побољшавање постојећих контрола заштите, препоруке за побољшавање политика, процедура, алата и других аспеката процеса дигиталне форензике (Kent, 2006:16).

Слика 5 – *Фазе процеса дигиталне форензике*

Сваки корак анализе потребно је документовати на одговарајући начин. Израда документације од изузетне је важности, јер омогућава у сваком тренутку увид у радње које су остварене до тог тренутка, те да се исте могу реконструисати ако је то потребно.

Ефикасност и ефективност дигиталне форензике у истраживачко-доказном поступку зависи од: обухвата полазних елемената (аквизиције); коришћења техника и форензичких алата за прикупљање доказа; дефинисања валидних дигиталних доказа; анализирања и приказивања добијених резултата и предвиђања правца даљег развоја превентивне заштите информационих система.

Код полазних елемената потребно је применити „10 златних правила форензичке истраге“:

1. осигурати и изоловати место где се десио инцидент/и;
2. искључити мрежне прикључке и не дирати друге информационе ресурсе, тј. оставити све у стању у коме се тренутно налазило (укључено/искључено);
3. деловати прибрано, процедурално, у правом тренутку и без панике;
4. дефинисати шта се тражи и идентификовати потенцијални доказни материјал, као и у којој ситуацији је проблем настао;
5. дефинисати циљеве анализе;
6. ко је, када и како открио проблем;
7. који су, како су повезани и администрирани рачунарски ресурси;
8. ко су њихови корисници, која су њихова задужења и делатности;
9. пажљиво записати све важне податке и запажања на папир;
10. обавестити најуже руководство и позвати овлашћене експерте за ову област.

Поступци форензичке анализе могу се поделити зависно од стања у којем се налази систем који се анализира. Сваки систем има два основна стања, а то су укључен (*online*) или искључен (*offline*). Укључено стање представља радно стање неког система у којем он обавља неки задатак. За разлику од укљученог стања, искључено стање је оно у којем систем мирује, односно не обавља никакав задатак (искључено је с напајања). Према томе, форензичка анализа се дели на *online* и *offline*, односно на тзв. *live* (живу) и *post-mortem* (традиционалну) анализу (види Craiger, 2006). *Online* форензичка анализа се огледа у праћењу и надгледању мрежног саобраћаја у реалном времену, а посебно интернет комуникације, док се *offline* форензика обавља по настанку безбедносног инцидента. Код *online* форензике неопходно је планирати и стварати структуру која ће обезбедити наставак посла у случају безбедносног инцидента. Ту треба извршити припрему и тестирање радњи неопходних за заштиту кључних пословних процеса у организацији, као и имплементацију процеса на другом (резервном) месту (види Albert, 2008).

Дигитална форензика данас има широку примену и није ограничена само на званичне истражне органе (полицију – борба против високо технолошког криминала, тужилаштво, судство и војно-обавештајне активности), већ је користе и неки други друштвени сектори, као нпр. веће организације које желе да управљају безбедносним инцидентима сопственим снагама, затим, професионалне организације за опоравак података из случајно/намерно оштећених рачунарских система.

Такође, све је више великих, приватних компанија које користе дигиталну форензику као вид унутрашње контроле својих запосле-

них, правдајући то превенцијом. Прикупљање и чување дигиталних форензичких доказа је уређено Међународним стандардом у ISO/IEC 27037 (http://www.iso27001security.com/html/27037.html, доступан 22. 5. 2013) и кроз: *SWGDE – Scientific Working Group on Digital Evidence* и *IOCE – International Organization on Computer Evidence* (http://www.albany.edu/crccp/resources.html, доступан 22. 5. 2013). У оквиру њих су издате препоруке за основне принципе форензичке анализе дигиталних доказа, критеријуми, стандардне радне процедуре за заплену рачунара, форензичку аквизицију и анализу, чување, копирање оригиналних дигиталних доказа и др.

Дигитални докази

Да би се доказало неко кривично дело, неопходно је прикупити доказе. Међутим, када је реч о рачунарским криминалним делима мора се имати у виду да „дигитални докази често нису једнаки осталим облицима физичких доказа“ (Sieber, 1986:139) у односу на које су осетљивији и подложни мењању структуре и садржаја, те се према њима треба посебно односити.

Доказ је оно што раздваја хипотезу од неосноване тврдње. Докази могу потврдити или оборити хипотезу, па је њихов интегритет кључна ствар у њиховом прихватању, односно одбацивању пред судом. Постоји неколико специјалних карактеристика дигиталних доказа које их чине посебно изазовним. Пре свега, потребно је јасно и прецизно дефинисати дигитални доказ. Дигитални доказ је информација ускладиштена или преношена у дигиталној форми која учествује у судском процесу или неком другом спору. Дигитална форма по својој природи подразумева да се ради о неком електронском или магнетном уређају, па то могу бити подаци у оперативној меморији, на хард диску, флеш картицама, али и подаци који се налазе у трансмисији, нпр. радио таласи. Дигитални доказ није нешто што људи могу на први поглед протумачити. У буквалном смислу, дигитални доказ представља низ нула и јединица које неки електронски уређај преводи у људима разумљиву форму коју они могу користити као поткрепљење својој хипотези у оквиру неког судског случаја (види Стевановић, 2006). Дигитални доказ може бити било који податак, односно информација која је релевантна за случај који се анализира – помаже у решавању случаја.

У раду са дигиталним подацима, у процесу аквизиције и анализе, форензичар се мора придржавати главних принципа за рад са компјутерским дигиталним доказима, које су, са незнатним варијацијама, прописале бројне међународне организације: IOCE, NIST, FBI (више Kenneally, 2009; Mocas, 2009):

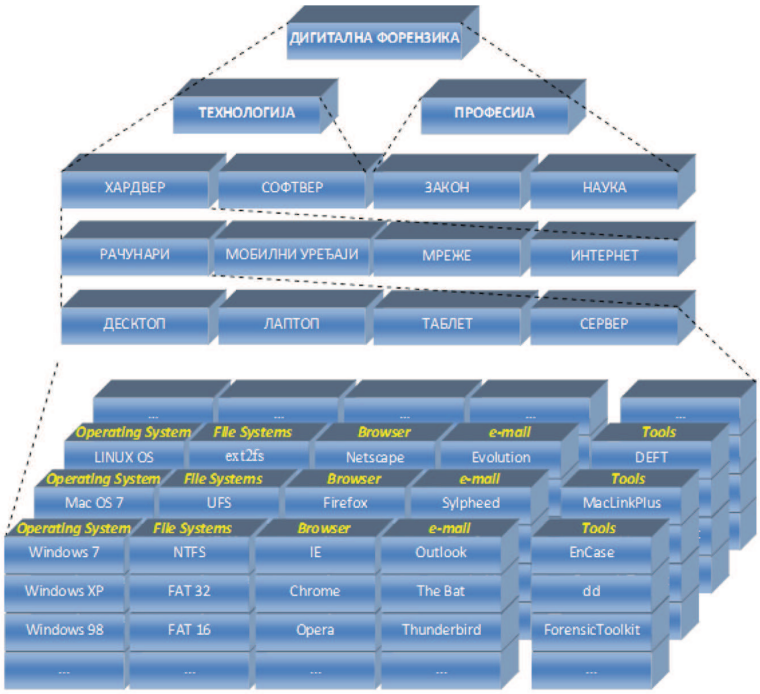
- *Принцип* 1: Ни једна активност агенције или форензичара не сме изменити податке који се налазе у рачунару или медијумима за складиштење и који могу бити потенцијални докази за суд.
- *Принцип* 2: У посебним околностима када орган истраге, форензичар или друго лице мора приступити оригиналним подацима, то лице мора бити компетентно и мора дати доказ који објашњава значај и импликације те активности.
- *Принцип* 3: Треба креирати и чувати у целокупном ланцу истраге контролне трагове и друге записе свих процеса извршених над компјутерским електронским доказима, да би се обезбедила независна форензичка анализа тих процеса са истим резултатима.
- *Принцип* 4: Лице надлежно за истрагу случаја компјутерског криминала одговорно је за обезбеђивање спровођења свих активности форензичке истраге, аквизиције, анализе и презентације у складу са законском регулативом и овим принципима.

Генерално, дигитални докази који су потребни за истрагу налазе се анализом и евалуацијом свих података сакупљених у фази аквизиције дигиталних података. Као и у истрази класичног криминала, да би открили истину, дигитални форензичари морају идентификовати податке који формирају:

- оптужујуће доказе, верификују постојеће податке и теорије (хипотезе);
- ослобађајуће доказе, супротстављају се постојећим подацима и хипотези, и
- индикаторе покушаја скривања података.

Потенцијални дигитални докази

Комплексност проблема на које форензичари наилазе (слика 6) условила је специјализовање стручњака за различите области. У напреднијим срединама форензичари се баве одређеним оперативним системом, специјализују се за Windows, Linux, Mac и др. Форензичари, као уосталом и сви информатичари, морају редовно пратити развој технологије. Разлике између различитих верзија истог програма, а поготово оперативног система, често су суштинске природе.



Слика 6 – *Сложена структура дигиталне форензике*

Информациони системи сами за себе садрже значајне количине података који се могу искористити као доказни материјал. Потрага и прикупљање дигиталних доказа могу се обавити на следећим ХАРДВЕРСКИМ уређајима/компонентама (http://carfield.com.hk/document/Forensics/ComputerForensics.pdf, доступан 22. 5. 2013):

• стандардним рачунарским системима (десктоп, лаптоп, сервери, таблети);	• преносним чврстим дисковима;
• мрежној опреми (*firewall, router, wireless access point*);	• compact flash, micro drives, smart media, memory stick;
• рачунарским периферијама (локалним и мрежним штампачима);	• PCMCIA картицама;
• личним дигиталним помоћницима (*PDA, iPod, iPhone, GPS*);	• backup тракама, и

• флопи, *CD, DVD, BD* дисковима;	• мобилним (телефонима, конзолама и видео играма, дигиталним аудио плејерима, дигиталним видео-рекордерима, диктафонима)

Потенцијални СОФТВЕРСКИ докази који су:

- Направљени од стране корисника:

• електронски адресар;	• омиљене интернет странице;
• *email* датотеке;	• базе података;
• аудио/видео датотеке;	• електронске табеле, и
• слике/графичке датотеке;	• документи или текстуалне датотеке.
• електронски календар;	

- Заштићени од стране корисника:

• компресоване датотеке;	• датотеке заштићене лозинком;
• погрешно назване/преименоване датотеке;	• сакривене датотеке, и
• енкриптоване датотеке;	• стеганографске информације и датотеке.

- Направљени од стране рачунара:

• бекап датотеке;	• скривене датотеке;
• лог датотеке;	• системске датотеке;
• конфигурационе датотеке;	• *history* датотеке;
• *printer spool* датотеке;	• темпорари датотеке;
• *cookies*;	• линк датотеке, и
• *swap* датотеке;	• логови извештаја.

- Неки други подаци:

• лоши кластери;	• време, датум и лозинке на рачунару;
• друге партиције;	• системски простор;
• скривене партиције;	• изгубљени кластери;
• обрисане датотеке;	• недодељен простор;
• резервисан простор;	• метаподаци, и
• *slack* простор;	• записи о покретању система.
• слободан простор;	

Дигитални форензички алати

Избор алата је од суштинског значаја у процесу дигиталне форензичке истраге. Само они алати који дају тачне, потпуне и поуздане резултате могу обезбедити дигиталне доказе који су прихватљиви на суду.

Иначе, добро је познато да деструктивни корисници покушавају да прикрију и уклоне трагове, тако да су најквалитетнији дигитални докази по правилу увек невидљиви за стандардне алате из оперативног система. Неки аутори користе модел „**леденог брега**“ (слика 7) како би презентовали проблем садржаја дигиталног доказа, при чему се у литератури могу срести различите интерпретације, али сви мали видљиви врх леденог брега поистовећују са елементима који се лако препознају и откривају на једном рачунарском систему уз стандардне алате оперативног система, док се испод површине или у „дубокој води“ налазе тешко доступни елементи и дигитални докази који су скривени у привременим фајловима/фолдерима, обрисаним партицијама диска, обрисаним мејловима итд.

Слика 7 – *Ледени брег, видљиви и невидљиви ниво дигиталних доказа* (Grunwald, 2004)

Данас постоји много развијених техника и алата који се користе у форензичком поступку, а њихов превелик значај повезан је са већ изнетом чињеницом „да је данас преко 90 одсто свих нових информација произведено у дигиталном облику“ (http://www.paho.org/ English/DPI/ Number14_article4_5.htm и http://www.isaca.org/Con-tent/ContentGroups/ Member_Content/Journal1/20023/Computer_Forensics_Emerges_as_an_Integral_Component_of_an_Enterprise_Information_Assurance_Program.htm), и да се такво богатство мора на адекватан начин контролисати, надгледати и чувати.

Развој форензичких алата усавршавао се кроз три генерације. Прву генерацију су сачињавали разни алати за слике, документа, претраживање и опоравак система; другу генерацију су чинили посебно дизајнирани и развијени професионални алати (*Encase, SANS, FTK, Helix* итд.), као и велики број бесплатних алата отвореног кода који се могу наћи и преузети са интернета; трећу генерацију чине интелигентни алати који у реалном времену безбедно и ефикасно надгледају целокупан мрежни саобраћај.

EnCase је један од најпознатијих професионалних форензичких алата који је нашао свој пут и у многим државним институцијама које се баве информационом безбедношћу и форензичким активностима. Статистика каже да око 90 одсто на територији USA користи управо *EnCase* алат за обављање форензичких истрага. Наравно, ова статистика није случајност, јер стручњаци из фирме „*Guidance software*“ (http://www.guidancesoftware.com, доступан 22. 5. 2013) своја дугогодишња искуства из ове области уграђују у овај програмски пакет, прилагођавајући га специфичним потребама и различитим категоријама корисника, и то како по питању методологије истраге, тако и по питању потребних врста претрага које алат мора подржавати. *EnCase Forensic* је постао практично индустријски стандард када су у питању дигиталне форензичке истраге.

Оно што је потребно да би се неки форензички алат користио у истрази, је да буде сертификован и признат од државних судских органа, како би дигитални докази били валидни у судском процесу.

Препоруке професионалаца су да се форензички алати и технике не примењују на „живим“ подацима, већ да се направе њихове копије; да треба поштовати правила: оригинал додирни једном, копију два пута, а радну копију онолико пута колико је потребно; и никад, баш никад, не експериментишу корисници који нису за то обучени, јер ће скоро сигурно оштетити или изгубити потребне дигиталне доказе.

Завршна разматрања

Информациона писменост је у све већој мери главна одредница времена у којем живимо, познавање елемената заштите постаје насушна потреба свакодневице, а за информатичаре и неке специфичне професије (војска, полиција, судство, тужилаштво) и део њихових професионалних обавеза.

Из досадашњих теоријских и емпиријских разматрања може се констатовати да је у Србији мало информационих система који су заштићени према препорукама струке или прописаних стандарда, нарочито ако прихватимо дефиницију информационе безбедности као процеса, а не скупа техничких мера. Поштовање безбедносних стандарда није гаранција апсолутне заштите информационог система, већ минимум

који мора да буде испуњен да би рачунаре у мрежном окружење уопште имало смисла користити, при чему треба имати у виду да је заштита информационих система једина ствар која не би смела бити страни, већ домаћи производ.

Најразвијеније земље света, као лидери глобалног друштва, прве су се суочиле са новим појавним обликом криминала, па су прве и дефинисале нове законске оквире којима би се институционализовала борба против високо технолошког криминала. Међутим, пракса је показала да то није било довољно за ефикасну борбу против ове врсте криминала, а главни проблеми су се огледали, пре свега, у недовољном знању и обучености из области ИТ полицијских службеника који због тога нису били у стању да препознају радње које представљају високо технолошки криминал, или су својим поступањем компромитовали „место злочина“, док тужиоци и судије, без специјализованих знања нису могли на прави начин и у довољној мери да схвате интерпретацију дигиталних доказа ИТ вештака.

С обзиром на констатацију да Србија касни за земљама у којима је развијена примена сертификованих форензичких алата, аутори се надају да ће подстаћи одговорне да убрзају рад на законској регулативи, а до тада апелују на научну и стручну јавност да сви заједно дају свој допринос унапређењу постојећег стања, како кроз едукацију што већег броја корисника ИТ, тако и кроз професионализацију стручних особа које се баве овом научном дисциплином, јер је једина шанса у чињеници да је знање у свему овоме најјаче оружје. Наравно, не може се очекивати да се добро и квалитетно обави данашњи посао са јучерашњим знањима, и да се тако дочека сутра.

Литература

1. Albert, J. M., Robert, S. G., (2008). *CYBER FORENSICS A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, Auerbach Publications, Taylor & Francis Group, New York.
2. An introduction to: *Computer Forensics primary uses*, http://carfield.com.hk/document/Forensics/ComputerForensics.pdf. доступан 22. 5. 2013.
3. *Борба против сајбер-криминала* (превод), Безбедност, год. 53, број 2, Београд, стр. 288-298.
4. Kent, K., Chevalier, S., Grance, T., Dang, H., (2006). *Guide to Integrating Forensic Techniques into Incident Response*.
5. http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf. доступан 22. 5. 2013.
6. Craiger, J. P., (2006). *Computer forensics methods and procedures*, To appear In H Bigdoli, (Ed), Handbook of Information Security, New York,

John Wiley and Sons, 2, pp. 736-755. http://www.ncfs.ucf.edu/craiger.forensics.methods.procedures.final.pdf. доступан 22. 5. 2013.

7. Dan, F., Wietse, V., (2003). *Forensic Discovery*, Addison-Wesley.
8. De Lone, W. H., Mc Lean, E. R., (1992). *Information Systems Success, the Quest for the Dependent Variable*, Information Systems Research, Vol. 3, No. 1, pp. 60-95.
9. Ћикановић, П., Сивчевић, Д., (2011). *Примена Open Source решења у имплементацији портала полицијских службеника*, Безбедност, год. 53, број 3, Београд, стр. 148-159.
10. Internet World Stats, http://www.internetworldstats.com/stats.htm. доступан 22. 5. 2013.
11. Kenneally, E., Brown, Ch., (2005). *Risk sensitive digital evidence collection*, Digital Investigation Vol. 2, No. 2, pp. 101-119.
12. Милановић, Ј. З., Милановић, С. Т., (2010). *Дигитална анти-форензика као криминогено средство заштите кибер криминала*, Саветовање о злоупотреби информационих технологија и заштити, Београд.
13. Милановић, Ј. З., (2006). *Организација заштите рачунарских система*, Магистарски рад, Машински факултет, Београд.
14. Милосављевић, М., Грубир, Г., (2009). *Истрага компјутерског криминала*, Београд.
15. Mocas, S., (2009). *Topics in Computer Science Introduction to Digital Forensics*, CS 483, Washington State Universit.
16. New York Computer Forensic Services, http://newyorkcomputerforensics.com/learn/index.php. доступан 22. 5. 2013.
17. Николић, Л., (2008). *Банкомати на удару сајбер криминалаца*, www.vibilia.rs/ srpski/izvestaj/0508/Lidija%20Nikolic _030 308.pdf. доступан 22. 5. 2013.
18. Петровић, Р. С., (2007). *Полицијска информатика II*, Криминалистичко-полицијска академија, Београд.
19. Петровић, Р. С., (2010). *Знањем против злоупотребе знања*, Саветовање о злоупотреби информационих технологија и заштити, Београд, http://www.singipedia.com/content/1040-Znanjem-protiv-zloupotrebe-znanja. доступан 22. 5. 2013.
20. Петровић, Р. С., (2009). *Кибер простор – изворište нових претњи националној безбедности*, Информациона безбедност, Међународни научностручни скуп, Београд.
21. Петровић, Р. С., (2004). *Заштита рачунарских система*, Виша железничка школа, Београд.

22. Петровић, Р. С., (2010). *Прилог националној стратегији заштите кибер-простора*, Војно дело, Београд, http://www.odbrana.mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/VD_2010-jesen/07-%20Prilog%20nacionalnoj%20strategiji%20zastite%20kiber-prostora;%20Slobodan%20R.%20Petrovic.pdf. доступан 22. 5. 2013.
23. *Привредна комора* Србије, http://www.pks.rs/Aplikacije.aspx?aplikacija=sertifikati. доступан 22. 5. 2013.
24. RFC 3227, (2002). *Guidelines for Evidence Collection and Archiving*, www.faqs.org/rfcs/rfc3227.html. доступан 22. 5. 2013.
25. Sieber, U., (1986). *THE INTERNATIONAL HAND-BOOK ON COMPUTER CRIME*, John Wiley&Sons, New York, pp. 139-142.
26. Solomon, M., Barrett, D., Broom, N., (2005). *Computer Forensics Jumpstart*, SYBEX, San Francisco-London.
27. Стевановић, Б., (2006). *Компјутерска форензика – одговор на инцидент*, Саветовање о злоупотреби информационих технологија и заштити, Београд.
28. Симић, Д., (2008). *Имплементација безбедности података у пословном систему Новосадски сајам а.д.*, International Journal "Total Quality Management & Excellence", Vol. 36, No. 1-2, pp. 123-126.
29. Урошевић, В., (2010). *Коришћење интернет сервиса који пружају злонамерне програме као услугу при извршењу кривичних дела из области високотехнолошког криминала у Републици Србији*, Безбедност, год. 52, број 3, Београд, стр. 177-189.
30. Урошевић, В., (2009). *„Нигеријска превара" у Републици Србији*, Безбедност, год. 51, број 3, Београд, 145-157.

Digital Forensics in the Context of Information System Protection

Abstract: *Although a lot has been said and written about the protection of information systems and users of the Internet, only a small number of managers and users of information technologies are aware of the significance of this problem. This can lead to occurrence of risky situations in which business information systems may be threatened. Their inadequate protection may have disastrous effects on the business process itself. The purpose of the paper is to clearly and transparently establish relations between methods and techniques of information system protection and digital forensic investigation, as well as to raise the security awareness and promote security culture as essential elements of the cycle of risk management and protection.*

Keywords*: protection of information systems, security risk, digital forensics, digital evidence.*