ACTA ECONOMICA
Година XIII, број 22 / фебруар 2015.
ISSN 1512-858X, e-ISSN 2232-738X

УДК: 343.326:004.738.5
DOI: 10.7251/ACE1522301S
COBISS.RS-ID 4814104

Жељко Н. Стјепановић[1]
Марко Б. Крсмановић[2]

Заштита и безбједност информационих система у савременом пословању

Protection and Safety of Information Systems in Modern Business

Резиме

Овај рад је писан са жељом да пружи цјеловит увид у стање компјутерског криминала, те презентује тему која с правом изазива све већу пажњу свјетске, а у посљедње вријеме и домаће јавности. С тим у вези, циљ овог рада је да скрене пажњу на различитост ове врсте криминала и да едукује запослене у разним предузећима о опасностима које су присутне у условима глобализације пословних процеса. Заштита информација је неопходна компонента савременог пословања која на жељени ниво редукује опасности везане за лаку доступност и брзу размјењивост огромних количина података и информација. У оквиру овог истраживања обрађене су веома актуелне теме као што су заштита података у електронском пословању, врсте нападача и методе напада, основне технике заштите података и информација, однос законске регулативе и рачунарског криминала и друге теме везане за заштиту и безбједност података. Актуелност теме има посебан значај у процесу едукације заинтересованих корисника чији је основни циљ

[1] Универзитет у Источном Сарајеву, Саобраћајни факултет Добој, stjepanoviczeljko@yahoo.com
[2] Фонд ПИО Бијељина

подизање заштите и безбједности података на значајно виши ниво, усклађен са свјетским стандардима везаних за ову област.

Кључне ријечи: *рачунарски криминал, информациони системи, електронско пословање и заштита података.*

Summary

This paper has been written in order to provide a complete insight into computer criminal presenting the subject which increasingly causes the attention of the public in our country and worldwide. The aim of this paper is to draw attention to the diversity of this type of crime and to educate employees in various companies about the dangers inherent in globalization processes.Protection of information is an essential component of modern business that treduces the risks associated with easy access and quick interchangeability of huge amounts of data and information to a desired level. In the framework of this research issues such as data protection in electronic business, types of attackers and attack methods, basic techniques to protect data and information, legislation, computer crime and other topics related to the protection and security of data have been dicsussed. Significance of the topic has special placein the process of education of users whose primary goal is to raise the protection and security of data at significantly higher levels, harmonized with international standards related to this issue.

Keywords: *computer criminal, information systems, e-business, data protection.*

Увод

Процес реиндустријализације има за циљ стварање нових предузећа и њихово укључивање у глобалне свјетске токове. Узимајући у обзир значај информационих система у процесу реиндустријализације, у оквиру овог истраживања презентована су основна теоријска и практична достигнућа непосредно везана за безбједност и заштиту података. С обзиром на прогресиван раст рачунарског криминала на глобалном нивоу, заштита и безбједност информационих система има изузетан утицај на ефикасност пословања предузећа. Креирање новог и снажног привредног амбијента захтијева континуирану едукацију људских ресурса везану за заштиту и безбједност података. Њихово укључивање у глобалне пословне процесе неизбјежно намеће потребу за новим сазнањима у процесу информатизације. Узимајући у обзир наведено, можемо закључити да се процес реиндустријализације не може ни замислити без развоја савремених информационих

система, који треба да обезбиједе неопходне информације у процесу доношења пословних одлука. Стога, заштита и безбједност података у оквиру ових система има изузетан значај за успјешно функционисање како информационог система, тако и пословног система у цјелини. Према томе, ово истраживање представља изузетно значајан допринос креирању нових сазнања неопходних у процесу реиндустријализације као основног фактора даљег економског и друштвеног развоја Републике Српске.

Основни услов за ефикасан раст и развој сваког предузећа представља развој интегралних информационих система који имају задатак да обезбиједе цјеловиту информациону подршку предузећу. С тим у вези, информатизација пословних система предузећа представља подршку менаџменту предузећа у процесу рјешавања стратешких, тактичких и оперативних питања које намеће све интензивнија конкуренција на глобалном тржишту производа и услуга. Информациони системи у интеграцији са модерним телекомуникацијама промијенили су и промијениће у знатној мјери начин пословања како на локалном, тако и на глобалном нивоу. Цијела планета постала је глобално село испреплетано разним телекомуникационим, сателитским и другим везама неопходним за личну и пословну комуникацију на глобалном нивоу. Широм свијета присутна је интензивна промјена начина пословања захваљујући коришћењу новог глобалног система комуницирања уз активан развој савремених система информисања. Стога, уколико предузећа настала у процесу реиндустријализације и уопште, имају за циљ развој пословања на међународном тржишту рада и капитала, морају прије свега имати развијен савремен информациони систем.

Виртуални свијет постаје све више природни амбијент у коме предузеће свакодневно живи и дјелује. Уз помоћ информационих технологија предузеће задовољава своје потребе свестраном комуникацијом на глобалном нивоу. Наведено представља почетак новог епохалног свјетског заокрета који информационо друштво значајно мијења, па се поред позитивних могу уочити и бројне негативне појаве везане за ове промјене. Уобичајена и сада већ прихваћена синтагма обухвата свеукупност почињеног рачунарског криминала који значајно утиче на коришћење програмске подршке и базе података. Нови облици рачунарског криминала убрзано се развијају са појавом рачунарских мрежа, уз веома интензивну експанзију глобалне интернетске мреже. Посебан утицај на развој рачунарског криминала омогућује дигитални облик доступних података и информација, као и могућност да се злоупотреба оствари коришћењем података са удаљених локација.

Развој интернета и његов утицај на свакодневну егзистенцију предузећа значајно је утицао и на прогресиван развој рачунарског криминала и његово ширење на подручје привредног развоја, уз значајан утицај на ра-

звој техника оперативне криминалистичке контроле и развијених метода оперативне криминалистичке аналитике. Економске посљедице отказа или злоупотребе интернетских технологија могу бити директни финансијски губици као посљедица преваре, затим губитак вриједних и повјерљивих информација, губитак послова због недоступности сервиса, неовлашћена употреба ресурса, губитак пословног угледа и повјерења комитената као и додатни трошкови изазвани неизвјесним условима пословања. Овај комплексан процес захтијева ангажовање стручњака из различитих области, као и значајне новчане инвестиције. Чињеница је да информационе технологије пружају одређене предности, али и одређене ризике који се односе на заштиту и сигурност података и информација. Истраживања Гартнер организације указују на чињеницу да се годишње свјетска економија оштети за 1,6 милијарди долара због проблема које узрокује 20 милиона хакера. Да би се привредни субјекти у процесу реиндустријализације заштитили од оваквих посљедица, потребно је успоставити, примјењивати и одржавати одговарајуће технике заштите података и информација.

1. Развој и структура рачунарског криминала

С обзиром да се ради о глобалном проблему, за ефикасно сузбијање нису довољни само стручњаци за сигурност, експертне групе и остали органи за спречавање и сузбијање рачунарског криминала, већ је потребно остварити потпуну координацију и свеобухватну акцију законодавства и снага реда у превенцији рачунарског криминала у области електронског пословања. За развој разних метода напада на информационе системе, кључну улогу има већа злоупотреба комуникационих средстава која претходи конкретном криминалном дјелу, бржи развој и ширење телекомуникационих уређаја, развој и све теже коришћење оперативних метода и техника криминалистичке аналитике, све већа доступност рачунара особама без великог стручног знања, појава медија који често неоправдано величају хакерске вјештине и нападе, спорост и релативна сложеност доношења правне регулативе у циљу превенције рачунарског криминала. Рачунарски криминал је противправна повреда имовине код које се рачунарски подаци с предомишљајем мијењају (манипулација са рачунара), разарају (рачунарска саботажа), до њих се неовлаштено долази из користи (рачунарска шпијунажа) или се користи заједно са хардвером (Веиновић, Милосављевић и Грубор, 2009).

С тим у вези, Нортон у свом извјештају за 2013.годину наводи да рачунарски криминал нема граница и да се највећи број жртава налази у Русији (85%), Кини (77%), Јужној Африци (73%). Годишњи број жртава рачунар-

ског криминала, процјењује се на 378 милиона (енгл. *Securitu affairs*, 2013). Процјена је да финансијски трошкови који се појављују као посљедица рачунарског криминала износе: САД (38 милијарди долара), Европа (13 милијарди долара), Кина (37 милијарди долара), Бразил (8 милијарди долара), Индија (4 милијарде долара), Мексико (3 милијарде долара), Аустралија, Јапан и Русија (1 милијарда долара) итд. Најчешћи облици рачунарског криминала који се користе у поменутим земљама су: *преваре* (38%), *крађа података* (21%), *измјена података* (24%) и остали облици (17%). Поред тога, Нортон наводи да развој и употреба мобилних телефона значајно утиче на повећање обима рачунарских напада.

1.1. Појам и врсте рачунарског криминала

Успјех у борби против рачунарског криминала подразумијева, како сталну заштиту информационог система, тако и заштиту података и информација које се при његовом раду похрањују, обрађују и преносе. Рачунарски криминал може се дефинисати као свеукупност казнених дјела. почињених на одређеном подручју. кроз одређено вријеме, којима се неовлаштено утиче на коришћење, цјеловитост и доступност техничке и програмске подршке, као и на интегритет и тајност дигиталних података. Надаље, рачунарски криминал у области електронског пословања обухвата сљедеће категорије криминала:

- *Крађа услуга* - овлаштена особа користи рачунарско вријеме за неовлаштене потребе или за неовлаштеног корисника, те на тај начин остварује имовинску и другу корист.
- *Информациони криминал* – починилац користи информације похрањене на рачунару да би остварио личну добит.
- *Финансијски криминал* – користи се рачунар да би се остварила финансијска корист.
- *Имовински криминал* – рачунар се користи за остварење имовинске добити.
- *Традиционални криминал* – рачунари се могу такође користити за реализацију разних криминалних радњи.

1.2. Врсте нападача и методе напада

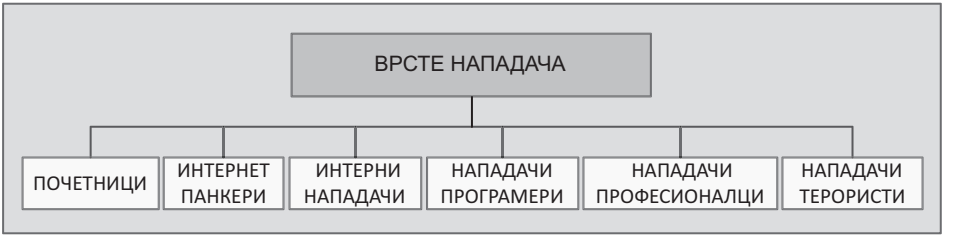
Информациони криминалци су врло интелигентни и образовани људи који досљедно прате развој савремене технологије. Самоувјерени и сигурни у своје знање, теже да још дубље продру у виртуални свијет како би остварили своје циљеве. Убрзаним развојем савремене технологије, повећава се и број криминалних радњи као и број њихових извршилаца. Сваким даном

број сајбер напада је све већи, те негативно утиче на савремено пословање како на локалном, тако и на глобалном нивоу. Ријеч је о озбиљном проблему, кога већина људи није ни свјесна. Свијет се данас сусреће са млађим особама, тзв. *хакерима*, који добро познају савремену технологију и који детаљно прате њен развој. Док се на једној страни налазе појединци са великим знањем о информационој технологији, на другој страни се налази већи број људи који о овој технологији имају веома скромна знања. С тим у вези, познато је да рачунарски криминал данас прави већу штету него трговина дрогом.

Нападачи на информатичке ресурсе могу се подијелити у низ група, узимајући у обзир њихове мотиве за напад. С тим у вези, постоји низ студија које се баве психолошко--социолошким аспектом рачунарског криминала. Разним анализама не иде у прилог чињеница да већина нападача не буде никада откривена, што доводи до закључка да су до сада изведене анализе недовољно вјеродостојне, јер се темеље на релативно малом броју оних који су изведени пред лице правде. За разлику од класичних криминалаца, у информатици се сусрећемо са особама знатно вишег коефицијента интелигенције, из чега се лако може закључити да због изузетних интелектуалних способности они углавном користе нове облике напада. Нападачи на информатичке ресурсе не налазе се на мјесту извршења, што им даје лажан осјећај сигурности, па је зато све већи број оних који се почињу бавити незаконитим радњама у виртуалном свијету. Класификација нападача на информатичке ресурсе приказана је на сљедећој слици.

Слика 1.

Основне врсте нападача на информатичке ресурсе



Извор: аутор

Почетници (енгл. *newbies*) представљају групу нападача коју чине млађе особе које су изузетно опасне за информациони систем. Ове групе нападача шире се експоненцијалном брзином, али су у принципу технички врло ограничене и углавном не посједују никакво знање из области програмирања. Мотиве за извођење разних врста напада проналазе у оквиру своје генерације са намјером да привуку пажњу појединаца у непосредном окру-

жењу. Углавном користе интернет алате које бесплатно набављају разним каналима или директном размјеном са појединцима из непосредног окружења. Ова врста нападача се релативно лако може открити, али уколико су њихови напади успјешно реализовани, могу изазвати знатну штету на информатичкој инфраструктури.

Интернет панкери (енгл. *cuber-punks*) су нападачи који уз скромну техничку подлогу посједују и одређено знање из области програмирања. Углавном релативно добро познају програмске језике као што су Ц++, Јава, Visual Basic и друге. Уз добро осмишљену стратегију напада, интернет панкери нападе изводе уз криминалну мотивацију усмјерену на потпуно или дјелимично уништење података, рушење информационог система, генерисање идентификационих бројева кредитних и других платних картица и слично. С обзиром на стратегију и методологију напада, заштита од ове врсте нападача реализује се углавном успјешно.

Нападачи изнутра (енгл. *insiders*) представљају најбројније нападаче на информационе системе разних привредних и друштвених субјеката. Према искуствима стручњака за откривање и спречавање рачунарског криминала, готово 80% напада реализује се уз помоћ помагача који имају легалан приступ информатичким ресурсима који су објекат напада. Ову групу нападача чине појединци који поред изузетног знања из области информационих технологија, детаљно познају комплетну инфраструктуру информационог система. У пракси је потврђено да су нападачи на информациони систем понекад и сами систем администратори. Администратори база података углавном посједују солидно програмерско знање, као и знање везано за администрацију информационог система, те су у могућности да изведу и сложене облике напада. Узимајући у обзир информатичка знања и позицију нападача, ова врста нападача веома се тешко открива.

Нападачи програмери (енгл. *coders*) представљају нападаче који углавном реализују криминалне намјере у оквиру предузећа у коме су запослени. Ова врста нападача посједује посебна знања из области програмирања користећи савремене програмске језике (Java, C++, VisualBasic и други), уз значајно познавање хардверске подршке информационом систему предузећа. Мотивација за ову врсту криминала углавном је базирана на осјећају моћи и престижа у информатичким круговима, док алате које углавном пишу лично реализују као тајна оружја. Одређени дио софтверских алата неопходних за реализацију криминалних радњи објављују и на интернету, најчешће у облику тројанских коња, скрипти и вируса. Ова врста нападача веома је опасна због посједовања изузетних знања из области информационих технологија, као и дјеловања у оквиру предузећа, због чега је откривање ових нападача доста неуспјешно.

Професионалци (енгл. *proffessionals*) су истински криминалци чији је мотив искључиво новац. Ова врста нападача углавном користи опрему високе технологије, док њихово подручје дјеловања представљају разни облици шпијунаже. У току своје активности избјегавају било какав облик медијске промоције, на интернету су углавном пасивно присутни, док су углавном оријентисани на прислушкивање комуникационих канала. У току припреме и извођења напада веома се тешко откривају, јер углавном не понављају методе напада, док су припреме за напад дуготрајне и детаљне.

Терористи (енгл. *cuber-terrorists*) представља групу нападача који се као и професионалци веома тешко открива. Мотивација ове врсте нападача налази се у интеграцији политичке реторике, криминалне дјелатности и финансијске користи. За разлику од професионалаца који су више оријентисани на привредно-економску шпијунажу, ова групација оријентисана је на обавјештајну шпијунажу. Сајбер терористи углавном користе најновије информационе технологије за разлику од професионалаца који су углавном школовани у државним системима за ово подручје дјеловања.

Узимајући у обзир наведено, уз интензивно коришћење искустава из прошлости непосредно везаних за рачунарски криминал, уочено је да напади по правилу започињу са прикупљањем основних информација. Нападачи су првенствено заинтересовани за распон адреса на којима се налази објекат напада, оперативне системе на корисничком и десктоп дијелу, сегментацију и топологију рачунарске мреже, рачунарску конфигурацију, присутност веб-страница, системе раног откривања напада ИДС (енгл. *Instrusion Detection System*), присутност енкрипције, сигурносну политику, имена и презимена запослених у информатичком сектору и слично. Значајно је напоменути да извођење ове почетне фазе напада није у конфликту са законом, јер се подаци прикупљају јавно, директно с интернета путем алата за његову претрагу, укључујући базу података са подацима о интернет адресама додијељеним физичким лицима. Ову базу могуће је јавно претраживати на адреси *http://www.ripe.net*. Претраживање ове базе се не наплаћује, анонимно је и представља основни извор података приликом планирања напада.

Након прикупљања основних информација о објекту напада, слиједи претрага цјелокупног интернет окружења. У току претраживања могуће је прикупити енормну количину информација о субјекту напада. Развој информационих технологија обезбиједио је значајан број могућности за успјешно извођење напада без контакта са улазним уређајима рачунара. Надаље, веома често се у контејнерима за смеће предузећа налазе изузетно значајне информације које нападачу обезбјеђује успјешно извођење напада. Ова стратегија напада није специфична за информатичко окружење, ме-

ђутим у пракси се показала изузетно ефикасном, јер се у већини случајева у смећу могу наћи комплетне кореспонденције и предмети који нису уништени: информације о електронској пошти, важним уговорима, телефонском адресару и слично.

Наведене мјере прикупљања података представљају пасивне мјере прикупљања података без контакта са информатичком инфраструктуром потенцијалног објекта напада. Поред пасивних мјера, нападач ће у току припреме напада веома интензивно користи и активне мјере напада као што је енумерација система која укључује активне конекције на информациони систем који се испитује директним упитима. У току енумерације система постоји реална опасност да ће нападач бити откривен уколико су имплементирани системи раног упозорења како на корисничком, тако и на мрежном сегменту. Веома често систем администратори не обраћају посебну пажњу на *логе* датотеке које садрже податке да се над њиховом инфраструктуром изводи енумерација која обухвата прикупљање података о мрежним ресурсима, групама корисника, корисничким рачунима, оперативном систему, дијељеним дисковима, верзијама апликација и слично. Лог фајлови се могу сматрати за очевице дигиталног кривичног дјела и морају бити обезбијеђени уколико постоји пријетња да могу бити избрисани прије него што се систем физички ископира (Грубор и Милосављевић, 2009). На велику жалост, највећи број систем администратора не обраћа пажњу на ове активности, иако оне врло јасно указују на чињеницу да се припрема напад на информатичке ресурсе.

Активни напади су усмјерени на уништење података, лажно информисање, успоравање рада рачунарског система, засићење меморијских капацитета и друго. Најпознатије врсте активних напада су *вируси, црви и логичке бомбе*. Рачунарски вирус је дио програмског кôда који је придодан нормалном програму чијим се извршавањем инфицирају други програми. С тим у вези, вируси чине и додатне штете у виду брисања датотека или исписивања непотребних порука. Заштита од вируса обезбјеђује се употребом помоћних антивирусних програма. Међутим, они се могу користити само за познате врсте вируса. Без обзира на ефекте који се могу обезбиједити употребом антивирусног софтвера, ипак је најбоље предузети одређене мјере заштите информационог система и на тај начин спријечити губитак веома важних података за предузеће. Црви су програми који се шире у рачунарској мрежи користећи предности дијељења мрежних ресурса, те користећи грешке у стандардној програмској подршци инсталираног рачунарског система.

Ова врста вируса може довести до загушења мрежног саобраћаја користећи операције на мрежи у властите сврхе. Логичка бомба представља не-

активан програм који се активира кад се испуни неки услов и тада почиње уништавање података и елиминисање програмске подршке рачунарског система. Услови за активирање овог програма могу бити разни догађаји као што су приступ одређеном податку, покретање неког програма одређени број пута, неки специфични датуми и слично. Активни напади, за разлику од пасивних напада, не чине видљиву штету информационом систему, па се зато веома тешко могу на вријеме открити. Основни циљ пасивних напада је прикупљање информација без ометања рада информационог система. Пријетње које су усмјерене на угрожавање сигурности тока информација у рачунарским системима и мрежама генерално се могу класификовати у четири основне категорије: *прекидање, пресретање, измјена и фабриковање* (Плескоњић, Мачек, Ђорђевић и Царић, 2007).

2. Заштита информационих система

2.1. Хронолошки развој заштите података

Упоредо са развојем људског друштва, долази до повећања могућности записивања и претраживања података. Са појавом шире употребе рачунарских система неопходно је било обезбиједити физичку заштиту и сигурност рачунара. Рачунарска опрема имала је релативно високу цијену, стога је примарна улога њене заштите била заштита од физичког уништења, док се другим облицима заштите и сигурности података још увијек не придаје посебна важност.

Касних 60-их година прошлог вијека започиње период који карактерише пад цијена рачунарске опреме, што позитивно утиче на повећање броја корисника информационих технологија. Све више података се похрањује на нове медије, што утиче на промјену фокуса са физичке заштите рачунара на заштиту и сигурност података и информација.

У току 70-их година прошлог вијека долази до употребе рачунарских лозинки, као и појаве нових метода похрањивања података, информација и програма на екстерне медије с циљем заштите од евентуалног уништења. Убрзани развој информационих технологија доводи до производње бржих и јефтинијих рачунара. Надаље, развој нових технологија у овој области обезбиједио је функционисање информационих система у реалном времену, уз интерактиван начин рада користећи веома моћан графички интерфејс.

Почетком 80-их година прошлог вијека започиње нова ера развоја сигурности, односно ера *„сигурности информација"* која наглашава сигурност информација као најважнијег, али и најрањивијег привредног ресур-

са. У савременом пословању посебан значај има *„сигурност знања”*, као и заштита интегралних информационих система у цјелини.

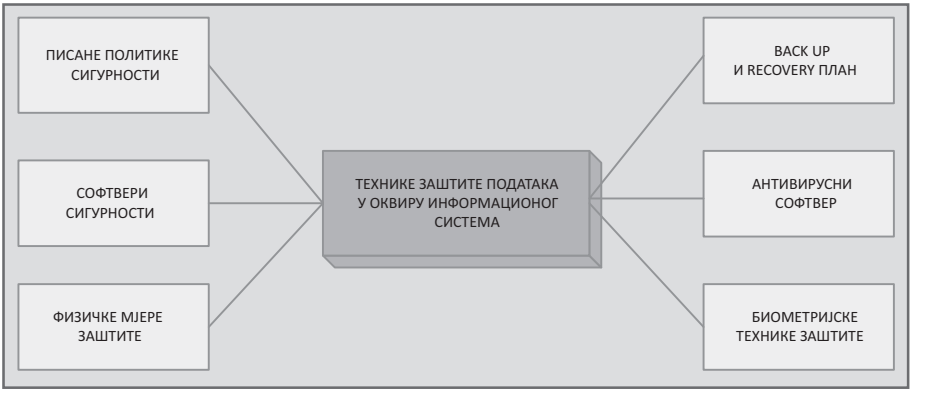
Циљ заштите информационих система јесте сигурност у процесу прикупљања, обраде, преноса и похрањивања података и информација.

2.2. Основне технике заштите података у оквиру интегралних информационих система

Основна карактеристика интегралних информационих система представља повезаност свих података, информација, процеса и других компоненти информационог система. Питање сигурности података у оквиру интегралних информационих система зависи од информационих технологија које подржавају дјеловање ових система. Узимајући у обзир чињеницу да је рачунарски криминал стварност компјутерског доба у којем живимо, може се констатовати да се рачунари користе као средство за реализацију криминалних радњи. У том смислу, питање заштите односи се на физичку заштиту која подразумијева заштиту хардвера, документације, запослених и друге неопходне мјере физичке заштите, као и логичку заштиту која укључује заштиту података и софтвера који су у нематеријалном облику. На сљедећој слици презентоване су одређене технике заштите података у оквиру интегралног система информисања.

Слика 2.

Основне технике заштите података у оквиру информационог система



Извор: аутор

Заштита и сигурност података и информација може се класификовати у оквиру заштите и сигурности од случајних или намјерних пријетњи физичкој или логичкој цјеловитости база у којима се подаци чувају. Да би одржали сигурност, Мајкрософтово особље, свакодневно дјелује против више од 1.500 покушаја провала у њихов интерни информациони систем

(Microsofts Management Reporting: SAP, Data Warehousing & Reporting Tools, 2013). Занимљив податак је добијен истраживањем које је провела компанија MessageLabs, а које указује на чињеницу да већина европских компанија сматра да ће се у сљедећих десет година број вируса удвостручити. Нека истраживања су показала да су информациони ризици које су ревизори информационих система оцјењивали много виши у ЕРП системима него у системима који нису окарактерисани као интегралне пословне апликације. Очекује се да ће ови ризици бити знатно већи у случајевима виртуелног пословања. Дакле, бројне су пријетње које се адекватним мјерама заштите предузећа могу свести на прихватљиву мјеру. Заштита и сигурност података и информација једна је од водећих тема на подручју информационих технологија. Уз појмове заштите и сигурности података и информација, потребно је размотрити питање приватности и неовлаштеног приступа подацима. Уобичајено је да се као темељни принципи приватности коришћења информација наводе:

- *упозорење/свјесност* – у ову сврху потребно је изградити политику приватности података како би корисници постали свјесни да су ти подаци приватна имовина предузећа;
- *избор/одобрење* – обезбјеђује заштиту приватности података на начин да се сваком кориснику информационих технологија, у складу са одређеним правилима, омогући избор хоће ли поједини подаци и информације бити приватне или јавне;
- *приступ/партиципација* – омогућава сваком учеснику у комуникацији да сагледа које све податке о њему имају остали учесници;
- *цјеловитост/сигурност* – представља одређене контроле које обезбјеђују заштиту података и одржавање њиховог интегритета;
- *наметање/успостављање правила* – има за циљ обликовање регулатива која ће приморати могуће преступнике на поштовање успостављених правила.

Чињеница је да информационе технологије пружају одређене предности, али и одређене ризике који се односе на заштиту и сигурност података и информација. Да би предузећа успјешно заштитила своје информационе системе, потребно је успоставити, примјењивати и одржавати одговарајуће технике заштите података и информација. Савремене технике заштите података и информација су: успостављање писане политике сигурности података и информација, физичка заштита, софтвери сигурности, односно системи за превенцију и детекцију од неовлаштеног приступа, биометријске технике заштите, криптографске технике заштите, план стварања си-

гурносних копија и план опоравка (енгл. *back up*[3] и *recovery* план[4]), лозинка и лични идентификациони број, едукација запослених и слично. Заштита података и информација може се остварити уколико се дефинишу подаци о корисницима појединих модула, њиховим овлашћењима и одговорностима и писаним процедурама понашања, што подразумијева да предузеће треба овакве процедуре и правила понашања записати у облику политика и правила сигурности. Ове политике представљају стратегију заштите информационих система која презентује постављене захтјеве од управе предузећа у облику политика, стандарда, препорука и процедура. Хијерархијски, политике представљају највиши степен стратегије заштите, јер обухватају одлуку о правцу обликовања и развијања заштите, као и функционалне политике заштите информационог система. Пошто се важност рачунарске обраде у оквиру пословне организације континуирано повећава, ефекти могућег прекида рачунарског система потенцијално су вишеструко штетни.

Основне мјере заштите информационих система су организационе, техничке и комуникационе мјере заштите. Организационе мјере заштите обухватају обезбјеђење услова за рад рачунара и особља, стручног кадра, технологије обраде података, медија за чување података и слично. Техничке мјере заштите обухватају физичке мјере заштите и мјере заштите рачунарског система. Физичке мјере заштите података обухватају заштиту од неисправних инсталација, пожара, поплава, загађења околине, штетних зрачења, неадекватног напајања електричном енергијом и слично. Док у мјере заштите рачунарског система убрајамо заштиту: хардвера, системског софтвера, апликативног софтвера, заштиту база података, контролу радних поступака и друго. Одлука о томе на којим ће се подручјима примијенити технике физичке заштите у непосредној су зависности од потреба предузећа, али и од правила одређених струка. Технике заштите информационих система обухватају и системе за превенцију и детекцију од неовлаштеног приступа. Системи за превенцију од неовлаштеног приступа обухватају антивирусне програме, ватрени зид (енгл. *firewall*[5]), а у новије вријеме препоручује се и употреба система за превенцију од неовлаштеног приступа IPS (енгл. *Instrusion Prevention System*). Мјере заштите података у телекомуникационом преносу обухватају основне двије методе:

– софтверску методу (*шифровање података и посебне протоколе заштите*) и
– техничку контролу (*посебну опрему–firewall, односно ватрени зид*).

[3] *Backup план* представља план заштите података.

[4] *Recovery план* означава план опоравка система и повратак изгубљених података.

[5] *Firewall – Ватрени зид.* Уобичајени акроним за "заштитни зид" који представља систем са обје компоненте, односно хардвер и софтвер који управља током информација између интранета и интернета.

Антивирусни програми представљају сигурносни софтвер са задатком одбране информационих система од пријетњи рачунарских вируса. Мјере заштите од вируса који могу да отежају рад информационог система у предузећима проводе се помоћу антивирусног софтвера. Уколико вирус доспије у информациони систем, потребно је што прије извршити његову идентификацију, а затим помоћу одговарајућих антивирусних програма обавити његово уклањање. У циљу што ефикасније заштите од вируса потребно је користити и континуирано освјежавати антивирусни софтвер. Начело отворености, односно потпуне компатибилности интранета и интернета се прихвата да би се искористиле предности које пружа интернет. Средство заштите тајности информационог садржаја и процеса у интранету од неовлаштеног приступа и злоупотреба је тзв. *„ватрени зид"*. Извршавањем функције управљања прометом података између интранета и интернета firewall контролише комуникацију која се одвија између двије мреже, те пропушта или блокира информације.

3. Заштита и безбједност података у електронском пословању

3.1. Сигурносни аспекти електронског пословања

Ризици који прате електронско пословање могу се избјећи употребом одговарајућих мјера везаних за заштиту података и информација. Безбједносни сервиси генерално представљају скуп правила која се односе на све активности предузећа везане за његову безбједност, а реализују се у оквиру информационог система. С тим у вези, информациони системи чију базу чини електронско пословање, изложени су потенцијалним пријетњама од стране злонамјерних нападача. Потенцијалне пријетње информационим системима који садрже подсистем за електронско пословање могу да буду неке од наведених: инфилтрација у систем, суплантација, промјена података на комуникационој линији, прислушкивање, прекорачење овлашћења, одбијање сервиса и негација трансакције. Са економске тачке гледишта, посљедице отказа технолошке природе или злоупотребе информационих технологија од стране корисника у области електронског пословања могу бити сљедеће: директни финансијски губици као посљедица преваре, губитак вриједних и повјерљивих информација, губитак послова због недоступности сервиса, неовлашћена употреба ресурса, губитак пословног угледа и повјерења комитената, те трошкови изазвани неизвјесним условима пословања. Због наведених проблема, комитенти који користе ове сервисе могу сносити директне или индиректне финансијске губитке.

Основни циљеви безбједносних мјера у информационим системима су: повјерљивост, интегритет, доступност и употреба система искључиво од стране овлашћених корисника. Безбједност комуникација односи се на заштиту информација у току процеса комуникације, док безбједност рачунара означава заштиту информационог система. Мјере безбједности комуникација и безбједности рачунара се комбинују са другим мјерама ради остварења поменутих циљева. Развој електронског пословања условљен је одређеним технолошким претпоставкама као што су развијена информатичка магистрала, односно инфраструктура задовољавајућег капацитета. Поред технолошких предуслова, потребно је континуирано развијати законске претпоставке које ће омогућити несметан развој електронског пословања, заштиту ауторских права и приватности, те осигурати универзални приступ мрежи, као и адекватну политику одређивања цијена за коришћење информација. Међу најважнијим разлозима убрзаног развоја електронског пословања су изузетно брз технолошки развој, развој нових сервиса и пословних модела, као и развој националних и међународних стандарда у области електронског пословања.

Да би се стекло повјерење у интернетско окружење, потребно је успоставити политику безбједности. Политика безбједности треба да покаже да је интернет сигурно средство и да нема разлога за бригу. Најмања грешка или пропуст за сајбер криминалца представља пун погодак да на лак начин злоупотријеби или украде повјерљиве информације. У оквиру интернетског окружења уочено је низ проблема који се односе на сигурност података у процесу комуникације. Успјешно рјешавање ових проблема позитивно ће утицати на висок ниво повјерења у дигитално окружење. Налазимо се у дигиталном добу које полако улази у сваки сегмент људског живота. Пошто се важност компјутерске обраде унутар пословне организације континуирано повећава, ефекти могућег прекида компјутерског система потенцијално су вишеструко штетни (Крсмановић и Полић, 2008).С тим у вези, информациони системи треба да обезбиједе политику безбједности како би се стекло повјерење појединаца у пословање путем интернета.

3.2. Криптографија као темељ заштите и сигурности података у електронском пословању

Криптографија је наука о прикривању информационих садржаја и онемогућавању њиховог разумијевања, модификовању и употреби од стране неовлаштених субјеката, те дефинисању математичке технике која треба да обезбиједи сигуран проток информација кроз телекомуникационе канале. Назив потиче од грчких ријечи криптос (која значи сакривен) и графеин (писати). Основни задатак криптографије као науке јесте да обезбиједи вје-

родостојност, тајност, провјеру поријекла информације и идентитета корисника, те доказивање одговорности корисника за одређену радњу која уједно представља и најважнији аспект при успостављању система заштите електронског пословања.

Вјеродостојност (енгл. *gata integrity*) обезбјеђује да не дође до неовлаштеног убацивања, брисања и замјене информација. Да би се осигурала вјеродостојност, мора постојати начин провјере да ли је информација промијењена од стране неовлаштене особе.

Тајност (енгл. c*onfidentiality*) подразумијева да је садржај информација доступан само онима који су за то овлаштени. Постоје бројни начини заштите тајности, почев од физичке заштите до математичких алгоритама који скривају податке од неовлаштених особа.

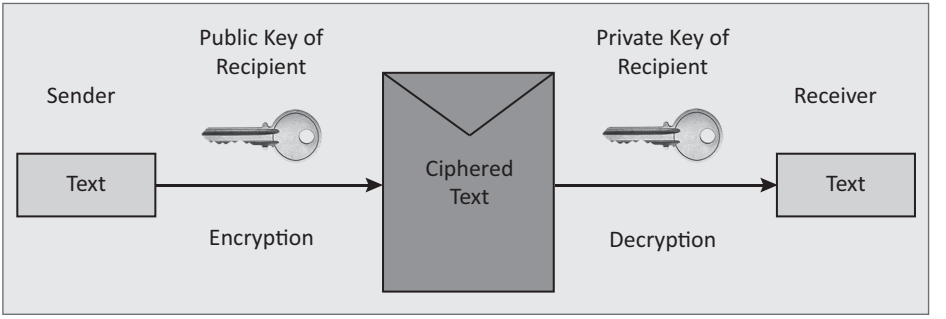
Провјера идентитета (енгл. *autentification*) може да се реализује како на нивоу корисника, тако и на нивоу информације. Пријаву и представљање корисника захтијева већина информационих система да би се могао одредити допуштени сигурносни ниво рада. Представљање на нивоу информације захтијева провјеру података о власнику информације, времену и типу информације и друге информације релевантне за њену сигурност. Дакле, аутентификација је поступак утврђивања идентитета корисника, а изводи се прије него што се кориснику допусти приступ ресурсима. Поступак аутентификације се састоји од два дијела: *идентификације и потврде*. Идентификација је процес гдје корисник даје свој идентитет, док је потврда процес потврђивања датог идентитета. Исправност поступка аутентификације највише зависи о употријебљеној процедури потврде. Главни типови аутентификације су:

- *пријава корисника* (енгл. user login authentication) - системска провјера идентитета корисника у вријеме пријаве,
- *једносмјерна аутентификација* (енгл. one-wayauthentication) - провјера идентитета једног корисника од стране другог корисника и
- *двосмјерна аутентификација* (енгл. two-wayauthentication) – обострана провјера идентитета корисника који комуницирају.

Провјера идентитета путем знања (енгл. *proof byknowledge*) представља приступ гдје аутентификација садржи потврду нечега што зна само ауторизовани корисник (нпр. аутентификација лозинком, односно пасвордом). Овај приступ садржи два типа аутентификације: директну методу (енгл. *direct demonstration method*) и методу изазов- одговор (енгл. *challenge-response method*). Код директне методе корисник потврђује свој идентитет дајући одређену лозинку коју систем упоређује с раније потхрањеном лозинком. Код друге методе корисник тачно одговара на питање (енгл. *challenge*) које поставља систем. Најзначајнија компонента инфра-

структуре јавног кључа јесте цертификациони ауторитет (енгл. *certification authority*) који издаје дигиталне цертификате и управља цертификатима током њиховог животног циклуса (Марић и Стојановић, 2003). Сљедећа слика нам приказује заштиту података у интернетског окружењу помоћу инфраструктуре јавног кључа.

Слика 3.
Графички приказ заштите података на интернету



Извор: аутор

Провјера идентитета путем посједовања (енгл. *proof by possession*) доказује идентитет корисника представљањем предмета који може посједовати само ауторизовани корисник. Примјер таквог предмета је пластична картица с магнетном траком на којој су уписани битни подаци у електронском облику. Провјера идентитета одређеном особином (енгл. *proof by property*) доказује идентитет провјером неких физичких особина корисника које није лако кривотворити. Мјерна особина мора бити јединствена за сваког корисника, а може бити отисак прста, глас, потпис и слично. Провјера идентитета корисника помоћу знања и посједовања има широку примјену за све типове аутентификације у децентрализованим мрежним системима, док је провјера идентитета особином генерално ограничена на аутентификацију људи у системима опремљеним посебним инструментима. У пракси, системи могу користити комбинацију двије или више аутентификационих метода. Крађа идентитета наставља се употребом прикупљених података за извршење кривичних дјела која су у највећем броју случајева везана за стицање противправне имовинске користи лицима која злоупотребљавају украдени идентитет (Милошевић и Урошевић, 2009).

Основни концепти електронског пословању су повјерљивост, интегритет, доступност, аутентификација и немогућност порицања (Haagand Cummings, 2002). Немогућност избјегавања одговорности (енгл. *non-repudiation*) представља врло важну особину сигурносног система у савременом пословању. С тим у вези, неопходно је обезбиједити потпуну иден-

тификацију обављања одређене трансакције, без могућности порицања. Ова особина сигурносног система посебан значај има у условима обављања пословних трансакција електронским путем.

4. Управљање информационим ризицима

4.1. Методологија управљања информационим ризицима

Сигурносни информациони ризик дефинишемо као опасност од примјене информационих технологија која може да произведе нежељене посљедице у предузећу или његовој околини. Будући да су ризици саставни дио процеса пословања, треба настојати развити и провести методологију управљања ризицима у предузећу. Као и сваки управљачки процес, и процес управљања ризицима обухвата сљедеће активности:

- идентификацију ризика,
- испитивање вјероватноће и квантификацију ризика,
- утврђивање приоритета ризика,
- идентификацију мјера које умањују ризик,
- утврђивање односа трошкова и користи од примјене протумјера,
- избор најефикаснијих протумјера,
- имплементација изабраних протумјера,
- дефинисање мјера отклањања насталих штета,
- контрола, ревизија и промјена плана и поступака.

Најважнији задатак сигурносне политике подузећа је да сигурносне мјере које се проводе на нивоу подузећа морају бити формализоване, а сигурносна политика треба да представља обавезујући документ за све запослене у предузећу. Наравно, већ при самом креирању сигурносне политике потребно је размишљати о могућностима њене имплементације, што подразумијева познавање нивоа одговорности сваког запосленог. Дакле, уз само познавање степена одговорности, запослени су дужни извршавати одређене процедуре дефинисане сигурносном политиком предузећа. Узимајући у обзир наведено, реализују се сљедеће процедуре везане за сигурносну политику предузећа: процедуре за превенцију сигурносних проблема, процедуре за препознавање недопуштених активности и комуникационе процедуре.

Сигурносни инциденти представљају неизбјежну нуспојаву електронског пословања сваког предузећа, с тога предузеће мора имати унапријед разрађене процедуре управљања инцидентима како би се спријечила штета и отклонили њихови негативни учинци. Узимајући у обзир наведено, хронолошки редослијед активности постављања приоритета заштите је:

– заштита људи и њихова сигурност,
– заштита тајних података,
– заштита осталих података,
– спречавање физичких оштећења система,
– минимизирање могућности злоупотребе информационих ресурса.

Наравно, након предузетих мјера заштите и ревизије насталих штета усљед појаве инцидената, сљедећи корак јесте провођење прописаних мјера санације и то:

– инвентура ресурса предузећа,
– обнављање ресурса предузећа,
– идентификација услова под којим је настао инцидент,
– процесуирање особе (особа) одговорних за настајање инцидента,
– анализа инцидента и уклањање евентуалних пропуста који су омогућили његов настанак.

Приликом планирања и креирања сигурносне политике подузећа неопходно је у потпуности ускладити елементе сигурносних процедура са законским и другим одредбама и прописима. Под наведеним подразумијева се примјена општих начела законитости, казненог и грађанског права, подзаконских прописа, уговорних обавеза, унутрашњих правила у предузећу, те прихваћених пословних обичаја и узанси. Између осталог, нужност представља и примјена етичких норми које нису формално прописане, а односе се на приватност појединаца. Дакле, у одређеној мјери требало би санкционисати информациони садржај који се односи на преношење пријетећих и лажних информација које могу негативно утицати на односе међу запосленима, ширити расну, националну или вјерску нетрпељивост, те угрожавати приватност појединца.

4.2. Законска регулатива у интернетском окружењу

Уласком у „беспапирни" свијет пословања, уважавајући свјетски слоган *„papers is dead"* односно *„папир је мртав"*, значај законске регулативе у вези са информационим технологијама постаје неизбјежан императив за редовно и регуларно пословање предузећа. С обзиром на значај интернета у савременом пословању, посебно је потребно представити постојећу законску регулативу у овој области која је развијена у земљама Европе и Сједињених Америчких Држава. Глобални систем комуникације, какав је интернет, захтијева ажурне правне оквире који треба да дефинишу потребе пословних субјеката и корисника услуга. Законска регулатива у вези с интернетом и пословањем на њему разликује се од земље до земље. У Европској унији постоји најмање 15 директива, приједлога и препорука које покушавају да

регулишу ову област. Два економски најразвијенија дијела свијета Америка и Европска унија, имају различите ставове о питањима законске регулативе на интернету. Европска унија има далеко либералније ставове о приватности пословања у односу на Сједињене Државе. Усаглашавање њихових ставова о законској регулативи на интернету од великог је значаја за комплетну свјетску привреду. Постоје двије могуће варијанте за рјешење законске регулативе у пословању на интернету:

– прва варијанта, за коју се залаже Европска унија, либералног типа је и заснива се на потпуној аутономности и приватности пословања;
– друга варијанта, за коју се залажу Сједињене Државе, заснована је на комплетној контроли пословања трансакција и података од стране државних органа.

Потпуно анониман систем пословања на интернету могућ је захваљујући систему енкрипције података, који гарантује анонимност у слању свих порука путем интернета. На овај начин систем штити приватност пословања појединца или предузећа што је уједно и основно правило електронског пословања и добра страна овог система. С друге стране, мане овог система су што омогућава избјегавање плаћања пореза, царинских обавеза, прање новца и пребацивање капитала у друге земље, и то мимо знања финансијских, царинских, пореских и осталих државних органа. Интернет пословање, уз одсуство законске регулативе, могло би уздрмати не само државне органе, него и читав пословни систем најразвијенијих земаља свијета. Други систем рјешења законске регулативе за пословање путем интернета заснива на комплетној контроли и евиденцији трансакција, пословања и података на интернету од стране државних органа. Овај систем би омогућио државним органима комплетан увид у све интернетске трансакције и кореспонденцију путем електронске поште. Слобода и приватност појединаца, као и основна правила пословног понашања, овим системом била би прекршена на најгори могући начин. Оба приказана система имају своје добре и лоше стране. Комбиновањем њихових најбољих елемената добило би се оптимално рјешење законске регулативе за пословање на интернету.

Сигурно је да ће још много времена протећи док се не усагласе међудржавне законске регулативе које су у вези с пословањем појединаца и предузећа на интернету. Недостатак међудржавне законске регулативе спречаваће одређене сегменте пословања, док ће, с друге стране, омогућавати примјену широког спектра незаконитих активности у пословању појединаца и предузећа на интернету. Кредибилитет електронског пословања ће у цјелини зависти од капацитета домаћих законодаваца да дефинишу и створе чврсто и свеобухватно правно окружење за електронско пословање које би изградило повјерење. Правне активности на домаћем нивоу треба про-

водити у тијесној координацији с међународним развојем и иницијативама да би се обезбиједила међусобна усклађеност. Земље које желе да обезбиједе да су електронске трансакције правно важеће, обавезујуће и спроводљиве, морају да дају одговоре на сљедећа три питања:

– Да ли је трансакција примјенљива у електронском облику?
– Да ли партнери у трансакцији вјерују поруци?
– Која правила важе за трансакцију реализовану електронским путем?

Полазећи од наведеног, кључне области које треба да буду размотрене приликом изградње правног оквира за електронско пословање обухватају заштиту података, регулисање интернетског окружења, пуноважност електронског потписа, електронску приватност, право интелектуалне својине, прописе о регулисању садржаја на интернету, закон о електронском документу, закон о електронском архивирању, закон о слободном приступу информацијама и друго. Најчешћи типови злоупотреба у оквиру електронског пословања представља неовлаштен приступ, пиратерија софтвера, откривање и измјена пословних података и информација, неовлаштен приступ базама интегралних информационих система, злоупотреба лозинке, као и пренос деструктивних вируса. Наиме, ове врсте злоупотреба усмјерене су против безбједности информационог система у цјелини или у његовим појединим дијеловима на различите начине и разним врстама информатичких и других средстава у намјери да себи или другом прибави корист, или да се другоме нанесе штета.

Новије америчке студије указују на чињеницу да се информатички криминалитет у области електронског пословања пословања дешава 40 пута чешће од класичног криминалитета, а да 90% злоупотреба остаје практично неоткривено. Ова врста злоупотреба се развија таквом брзином, да практично нема преседана у пракси. Узимајући у обзир наведено, можемо закључити да се развој информационих технологија у области савременог пословања знатно брже одвија у односу на промјене које се дешавају у области правне регулативе која прати ову област. С тим у вези неопходно је напоменути да доношење законских прописа који су везани за савремене облике електронског пословања углавном настају као одговор на разне облике злоупотреба, које се дешавају у овој области тек након њиховог настанка.

Закључак

Постојећа заштита података у нашем окружењу још увијек је на веома ниском нивоу, углавном везана за хијерархијски прилаз појединим базама података путем лозинке, тако да у тренутку када нека особа открије ло-

зинку, практично има цјеловит увид у податке и информације које креира информациони систем. С тим у вези, информациони систем треба да обезбиједи политику безбједности како би се стекло повјерење појединаца у пословање путем савремених информационих технологија као што је глобална интернет мрежа. Због пораста рачунарског криминала и других ризика, предузећа треба да развијају многобројне безбједоносне технике заштите информационих система.

У оквиру овог рада презентоване су основне опасности које пријете информационим системима, врсте нападача који се појављују у пракси, методе напада криминалних особа и друге компоненте које се односе на безбједност података и информација, с циљем унапређења развоја ефикаснијег система заштите у оквиру наших предузећа. Сматрамо да боље познавање самих нападача, као и методологија самог напада обезбјеђује свим заинтересованим да изградњом савремених система заштите података и информација обезбиједе ефикасно пословање и интеграцију у глобални систем пословања, као императив који обезбјеђује континуиран раст и развој предузећа. С тим у вези можемо закључити да се заштити и безбједности података у предузећима која послују у непосредном окружењу не приступа одговорно, што би могло да има изузетно негативне посљедице на њихову ефикасност пословања, посебно у тренутку када она постану дио глобалног привредног система. Изузетак представљају домаће банке које посједују веома ефикасне системе заштите података и информација, те могу представљати добар примјер и другим привредним субјектима у непосредном окружењу како се овај проблем рјешава.

Развој система заштите података и информација посебан значај има у условима када се пословање обавља електронским путем, уз веома интензивно коришћење глобалне интернет мреже. Стога се намеће као императив развој ефикасног система заштите података и информација у оквиру разних привредних субјеката и банака. Резултати овог рада треба да упознају кориснике информационих система са реалним опасностима које су присутне у савременом пословању, као и мјерама и методама заштите које треба предузети како би се обезбиједило ефикасно пословање предузећа и банака. С тим у вези сматрамо, да је едукација корисника везана за заштиту и безбједност података и информација још увијек недовољна и да ће овај рад подстаћи многе кориснике информационих система на размишљање како побољшати безбједност властитог система информисања.

Литература

Веиновић, М., Милосављевић, М. и Грубор, Г. (2009). *Информатика.* Београд: Универзитет Сингидунум.

Грубор, Г. и Милосављевић, М. (2009). *Истрага компјутерског криминала*. Београд: Универзитет Сингидунум.

Крсмановић, Б. и Полић, С. (2008). *Информационе технологије у рачуноводству и ревизији*. Бијељина, Бања Лука: Факултет спољње трговине, Финрар д.о.о.

Марић, В. и Стојановић, Д. (2003). *Информациони системи.* Бања Лука: Економски факултет.

Милошевић, М. и Урошевић, Б. (2009). Крађа идентитета злоупотребом информационих технологија.У *Безбједност у постмодерном амбијенту. Зборник радова књига VI.* Београд: Центар за стратешко истраживање националне безбједности.

Haag, S. M., Cummings, D. J. & McCubbrey. (2002). *Management Information Systems for the Information Age*. Irwin, McGraw-Hill.