ДУШАН АЛЕКСИЋ
ПУ Нови Сад
СТАНКО ЉУБИЧИЋ
Интернационална полицијска асоцијација
Секција Србија
Регија Нови Сад

УДК 339-98:347.7
Монографска студија
Примљен: 17.08.2013
Одобрен: 22.09.2013

КОРПОРАТИВНА ШПИЈУНАЖА; НОРМАТИВНО - КРИМИНАЛИСТИЧКИ АСПЕКТ САВРЕМЕНОГ ПОСЛОВАЊА

Сажетак: Питања и проблеми који су везани за корпоративну шпијунажу се у највећој мери јавља у новинским чланцима, док ову тему научна и стручна јавност у Републици Србији веома стидљиво обрађује. Имајући у виду наведено циљ рада је да укаже на широко распрострањен феномен корпоративне шпијунаже, као и на неке основне њене аспекте у савременом пословању. Корпоративна шпијунажа представља најефикасније и разорније средство економског ратовања у чему је и садржан њен криминални аспект. Иако је историјат корпоративне шпијунаже веома дуг, она данас посебно добија на значају услед наметнуте потребе за константним иновирањем и развојем знања, јер да би остао „у игри“ пословни систем мора непрестано да иновира и улаже у технику и технологију, а како је то врло скупо јавља се јаз између жеље за профитом и могућности за његовим стварањем. Жеља, тј. похлепа води ка посезању неетичних и незаконитих активностима који пословни систем могу коштати знатна средства или учешћа на тржишту. Са нормативног аспекта решавања проблема може се рећи да се у Републици Србији корпоративној шпијунажи не придаје велики значај, тј. законодавна решења не дају минимум претпоставки за успешно супростављање овом феномену, што у пракси тржишно развијених земаља није случај.

Кључне речи: Корпоративна шпијунажа, конкурентност, криминал, норме, знање, информације

Свет је свакако постао веома комплексно и конкурентно место. Поједине мултинационалне компаније су постале моћније од читавих нација и тежиште економске моћи се преноси на корпорације, унутар којих су идеје и информације постале најцењенија роба, са већом вред-

ношћу него сам производ и физичка имовина. Морамо увек имати на уму да повећање вредности одређене информације неминовно доводи и до тога да она постаје мета оних који желе да је украду. Информације и знања, као плод дуготрајног и скупог развоја унутар организације, јесу главне мете крађе управо због тога што коштају много[1]. Поред тога, погодан су објекат напада јер су виртуелног карактера и тешко их је контролисати. Информације краду различити људи и различите организације, из различитих разлога. Ипак, најчешћи извршиоци крађе пословних знања и информација су незадовољни појединци унутар организације, бивши запослени који желе да науде свом некадашњем послодавцу, или они који желе да остваре зараду на уштрб организације од које краду информацију. Са друге стране, тиме се баве и одређене интересне групе, као што су конкуренција, стране владе и криминални фактори, који циљају одређену организацију и инфилтрирају се у њу како би једнократно или константно крали информације. За овакве активности појединаца или група користи се израз економска, корпоративна или индустријска шпијунажа. Иако је шпијунажа најчешће коришћена ради откривања војних тајни, све више се користи у сврху откривања економских и привредних потенцијала државе и пословних система.

Након престанка хладног рата, индустријска шпијунажа постала је главни задатак традиционалних шпијуна које државне институције и предузећа сада ангажују да краду информације. У многим случајевима то су бивши војни шпијуни који су прешли на мешетарење индустријским информацијама. Они имају потребно знање и искуство па лако искоришћавају организације, нарочито оне које не примењују мере обезбеђења података и не образују свој кадар у том правцу.[2]

Постоји одређен, неуједначен, став у стручној и научној јавности у погледу означавања ове врсте шпијунаже. Међутим, већина је сагласна да је то најефикасније и најраспрострањеније оружје савременог економског ратовања.

Веома велики број аутора из ове области препознаје две врсте шпијунаже која се користи у комерцијалне сврхе, економску шпијунажу која је окарактерисана и која се спроводи под окриљем одређене државе и има међународни оквир, док је корпоративна или индустријска шпи-

[1] Један Апелациони суд у Америци је у случају Rockwell Graphics Systems Inc v DEV Industries et al (925 F 2d 174, 180 (7th Cir 1991)) у својој изреци навео: „...Заштита пословне тајне је важан део власништва над интелектуалним капиталом као формом власништва, која је од велике важности за конкурентност Америчке индустрије... Будућност нације зависи о малим деловима ефикасности индустрије, а ефикасност индустрије зависи о малим деловима заштите интелектуалног капитала…“

[2] Kevin D. Mitkin, *Уметност обмане*, Микро књига, Београд, 2003, стр 243.

јунажа инструмент пословних система и одражава се на националном нивоу. Корпоративна шпијунажа се јавља у много облика и форми, и упућена је на прикупљање осетљивих информација о пословној конкуренцији[3].

Аутори као што је Владимир Првуловић користе израз економска шпијунажа и дефинишу је као комплексан низ активности агресивног карактера, усмерених а приори против конкурената у циљу њиховог истискивања или уништења у процесу економског ратовања на унутрашњем и светском тржишту. Економска шпијунажа се служи легалним, али и скривеним нелегалним средствима, ради прибављања поверљивих економских информација, као и другим методама проваљивања у пословне тајне, планове и стратегије конкурената, њиховог представљања у негативном светлу и намерног онемогућавања у њиховим плановима и акцијама. Подразумева се да су активности економске шпијунаже, неспојиве са етичким нормама и стандардима пословања, лојалне конкуренције и регуларног економског надметања. Економска шпијунажа, је дакле, par exelance, средство и метода економског ратовања[4].

Стив Ален (*Steve Allen*) даје своју дефиницију и дели је на *индустријску шпијунажу*, која представља предузимање незаконитих напора конкуренције како би се скупиле информације о компанијама и индивидуалцима, као што су брокерске информације, информације о конкуренцији и слично и *економску шпијунажу*, која представља државно спонзорисано прикупљање информација која се често изводи у сарадњи са обавештајном службом[5].

Сагледавајући наведене, али и друге ауторе, можемо рећи да се корпоративна шпијунажа може дефинисати као скуп обавештајних мера и радњи усмерених на прикупљање економских и комерцијалних информација кроз активности које су тајне и забрањене законом. Она углавном не подразумева легалне изворе и легално прикупљање информација, али ни то није стран метод ове врсте шпијунаже. Корпоративна шпијунажа се може још дефинисати као облик шпијунаже који се користи и спроводи у комерцијалне сврхе, уместо у сврху националне безбедности.

---

[3] Competitive intelligence and economic or industrial espionage, 15. oktobar 2010. http:// finance.reachinformation.com/Industrial_espionage .aspx, i Economic Espionage, 18. novembar 2010. http://www.fbi.gov/about-us/investigate/counterintelligence /economic-espionage

[4] Владимир Првуловић, *Економска дипломатија*, Мегатренд универзитет, 2006, Београд, стр. 147

[5] Steve Allen, "Safeguarding proprietary information the protection of intangible asset", Financial Crime Review: Strategies to Combat Money Laundering and Fraud, BDE Global, London, 2001, п. 3.

Циљ корпоративне шпијунаже је да прикупи сва потребна знања о организацији, а то може да подразумева крађу интелектуалног капитала, али и прибављање основних података о економској снази, стратешким плановима пословног система или личним подацима запослених, њиховим склоностима, навикама, слабостима и примањима.

Што се тиче Републике Србије, проблем корпоративне шпијунаже је у многоме сложеније од индустријски развијених земаља. Наиме, преласком из планско-диригованог у тржишно-конкурентски систем привређивања, пословни системи у Републици Србији морају да се прилагоде новонасталим захтевима и процесима које намеће окружење капиталистичког друштвеног уређења (а посебно твз. Неочибералног уређења). У условима транзиције, где долази до трансформације привредног система и усклађивања правних норми са жељеним системом, долази до великих раскорака, недостатака и празнина у функционисању привреде, а то је погодно тло за активност нелојалне конкуренције и криминалног фактора који константно покушавају да на јефтин и незаконит начин дођу до интелектуалног потенцијала других пословних система.

Према подацима Факултета организационих наука у Београду, наша привреда је веома подложна корпоративној шпијунажи. Код нас о корпоративној шпијунажи нико не говори као о претњи, јер се обично сматра да је читава привреда Републике Србије већ одавно снимљена из ваздуха, па да због тога више и нема много чега што би у склопу ње некоме било интересантно. Истина је, међутим, да су сва предузећа мета корпоративне шпијунаже. Предмет крађе су, судећи по званичним подацима ФОН-а, информације о новим производима, производним процесима и пословању предузећа, финансијски извештаји, стручни пројекти, маркетиншки пројекти, резултати истраживања, разне рецептуре, формуле, најразличитије развојне стратегије, подаци о запосленима, тендерске информације… листи нема краја, јер свака информација има свог купца.

Иван Остојић, саветник IBM-а за индустријску шпијунажу на источном Балкану каже да је, на основу истраживања стручног тима IBM-а, у Републици Србији утврђено да млади, неафирмисани стручњаци за компјутерски инжењеринг немају решен нити пословни нити финансијски статус, тако да се лако опредељују да своје знање уновче и „шпијунирају" у корист страних и домаћих клијената, којима су наше фирме примамљиве за улагање.[6]

---

[6] „Индустрјска шпијунажа као пошаст над планетом", http:// www.mediacenter.org.yu/ code/ navigate.asp, 19/01/2007.

Нормативни аспект заштите од корпоративне шпијунаже

Заштита економских потенцијала Републике Србије од корпоративне шпијунаже али и од свих видова злоупотреба, било да су оне криминалног карактера, или су дело нелојалне конкуренције, која крши све норме пословног морала, максимално ће повећати конкурентске способности сваког пословног система. Смањење или елиминисање губитака, насталих деловање разних извора угрожавања те безбедни услови рада, чиниоци су за које су и пословни системи и друштво и целини природно заинтересовани. Како би се остварио овај интерес друштва реагују (држава) репресивним мерама, док је на пословном систему да делује превентивно. Иако се често говори о превентивном деловању државе у Републици Србији још увек акценат стоји на репресивном деловању које се спроводи путем норми понашања уоквирених у законодавним решењима.

Како би се размотрио нормативни аспект заштите од корпоративне шпијунаже у Републици Србији, најпре се треба осврнути на стратегијског опредељење у области економске безбедности и заштите економских потенцијала. У том смислу Скупштина Републике Србије, је 26.10.2009. године, усвојила Стратегију националне безбедности Републике Србије. Стратегија националне безбедности Републике Србије представља најважнији стратешки документ којим се утврђују основе политике безбедности у заштити националних интереса Републике Србије. У делу Стратегије која се односи на глобално окружење утврђено је да су последњу деценију прошлог и почетак овог века обележила нова безбедносна кретања у свету. Безбедност је из претежно војне сфере проширена и на друге области, првенствено економску, енергетску, социјалну и еколошку безбедност, укључујући безбедност појединца и друштва у целини. Стратегија указује да је Република Србија још увек суочена са значајним изазовима, ризицима и претњама које угрожавају њену безбеднсот. Као један о главних елемената економске политике у стратегији је истакнута економска стабилност као основни предуслов за реализацију циљева политике националне безбедности Републике Србије. Такође је као национални интерес између осталог истакнут и економски развој, који уз очување животне средине и природних ресурса, представља услов за просперитет грађана и држава и заштиту националних вредности[7]. Са друге стране у Стратегији развоја Министарства

[7] „Стратегија националне безбедности Републике Србије", http://www.mod.gov.rs /cir/dokumenta/strategije/usvojene/Strategija%20nacionalne%20bezbednosti%20Republike%20Srbije.pdf, 20/02/2011.

унутрашњих послова 2011 – 2016 у делу стратегијске анализе економског окружења Републике Србије у првој реченици дословце се наводи да је: „приоритет Србије ради убрзаног економског развоја јесу развој економије засноване на знању….”.[8]

Ова два кључна стратешка документа само у назнакама указују на важност економског развоја, што је недовољно и може се закључити да Република Србија у овом тренутку нема Стратегију економске безбедности или макар стратегијско опредељење заштите економских потенцијала, ма какви они били.

Привредно-правни оквир заштите од корпоративне шпијунаже

Пословни системи који послују у Републици Србији су практично препуштени сами себи, јер се анализом законодавног оквира може видети да нема прецизног оквира који би правно регулисао заштиту података, информација и знања, као привредног потенцијала уопште. Ова изузетно важна област је до сада била делимично регулисана Законом о привредним друштвима, што је било недовољно, а тако постављена решења су била неадекватна, непотпуна и недовољна. Овим Законом пословна тајна се одређује као:

Пословну тајну представљају исправе и подаци утврђени одлуком управе предузећа чије би саопштавање неовчашћеном лицу било противно пословању предузећа и штетило би њеовим интересима и пословном угледу – Дефиниција према Закону о предузећима (“Службени лист СРЈ”, бр. 29/96, 33/96, 29/97, 59/98, 74/99, 9/01, 36/02), који је престао да важи.

Пословном тајном сматра се информација о пословању одређена оснивачким актом, актом или уговором ортака или уговором чланова друштва, односно оснивачким актом или статутом акционарског друштва, за који је очигледно да би проузроковала знатну штету привредном друштву ако дође у посед трећег лица – Дефиниција према Закону о привредним друштвима ("Службени гласник РС", бр. 125/2004).

Тек се у новом Закону о привредним друштвима (Службени гласник РС 36/2011, 99/2011), који је на снагу ступио дана 01.02.2012. године, може видети јасна дефиниција појма пословне тајне која је садржана у члану 72. и која гласи: Пословна тајна је податак чије би саопштавање

[8] Стратегије развоја Министартства унутрашњих послова 2011 – 2016 http: //www. http://www.mup.rs/cms_cir/sadrzaj.nsf/Strategija%20razvoja%20MUP-a%202011-2016.pdf, 22.04.2012, стр. 6.

трећем лицу могло нанети штету друштву, као и податак који има или може имати економски вредност зато што није опште познат нити је лако доступан трећим лицима која би његовим коришћењем или саопштавањем могла остварити економска корист, а у погледу којег су од стране друштва предузете разумне мере у циљу чувања његове тајности.

Пословна тајна је податак који је законом, другим прописом или актом друштва одређен као пословна тајна. Актом друштва из става 4. овог члана се:

1) као пословна тајна може одредити само податак који испуњава услове из става 1. овог члана; и
2) не могу као пословна тајна одредити сви подаци који се односе на пословање друштва. Податак из става 3. овог члана може бити производни, технички, технолошки, финансијски или комерцијални, студија, резултат истраживања, као и документ, формула, цртеж, објекат, метод, поступак, обавештење или упутство интерног карактера и слично. Поред тога, чланом 73. утврђени су изузеци од дужности чувања пословне тајне и чланом 74. последице повреде дужности чувања пословне тајне.

Анализом ових решења може се видети се да су предходна законска решења, који је до сада били на снази, а посебно последњи Закон о привредним друштвима, уопште није регулисао ко је и на који начин дужан да чува пословну тајну. Такве одредбе су веома штуре, недовољне и конфузне у погледу заштите пословне тајне. Предходни закони нису дали довољну нити прецизну дефиницију пословне тајне као категодије, већ је то остављено самој организацији да регулише својим интерним актима. Дефиниција пословне тајне је уопштена и не даје довољно објашњења шта је заиста пословна тајна и која је њена сврха. Предходни закони нису предвидели санкцију за одавање пословне тајне. Поред тога, нити једним законским решењем се не дефинише одговорност треће особе у случају крађе или присвајања пословне тајне, а што је, како је то приказано у ранијем излагању, од велике важности. Веома велики напредак је направљен ступањем новог Закон о привредним друштивма, али аутори указују да су ова решења и поред тога што модернија, упућена на савремене законе других – развијених земаља, ипак недовољна, обизорм да се комплексност теме корпоративне шпијунаже и пословне тајне, не може описати у неколико чланова Закон о привредним друштвима. За правно регулисање ове проблематике потребно је донети Закон о економској шпијунажи, како је то урађено у Сједињеним Америчким Државама. Иако би се овакав предлог могао оповргнутим чињеницма да је наша земља далеко заостала из многих земаља а посебно Сједињених Америчких Држава, ипак се треба фокусирати на стра-

тешке документе, које је држава донела, а чији су делови горе наведени и цитирани, а из чега се јасно види правац којим жели да иде наша земља.

Имајући у виду наведено потребно је нагласити да привредна друштва морају унутрашњим актима да уреде област заштите пословне тајне. На самом привреном друштву је фактички да одлучи који је то опсег и врста података, информација и знања које ће означити као пословна тајна, и да дефинише и пропише њихово чување и заштиту. Унутрашња акта којима се уређује пословна тајна су Статут привредног друштва, Правилник о пословној тајни и Одлука о пословној тајни. При томе Статут, као најважнији општи интерни акт, представља правни извор, док се питање пословне тајне непосредно уређује Правилником и Одлуком као појединачним интерним актом. Њихова непосредна обавеза на запослене мора се спровести Уговором о раду, у коме би се на јасан и недвосмислен начин запослени упознао са постојењем, коришћењем чувањем пословне тајне, односно кључних пословних и економских потенцијала организације.

Кривично-правни оквир заштите од корпоративне шпијунаже

Са аспекта кривично правне заштите, у нашој земљи не постоји посебан систем заштите знања, тј. не постоји јасно дефинисана стратегија борбе против корпоративне шпијунаже и заштите конкурентске привреде. Ипак, оно што је добро је чињеница да је одавање пословне тајне дефинисано Кривичним закоником као кривично дело.

Према кривичном закону пословном тајном се сматрају подаци и документи који су законом, другим прописом или одлуком надлежног органа денесеном на основу закона проглашени пословном тајном чије би одавање проузроковало или би могло да проузрокује штетне последице за предузеће или други субјект привредног пословања – Дефиниција према Коментару кривичног законика Републике Србије.

Анализом Кривичног законика[9] може се издвојити група кривичних дела која инкриминишу незаконите радње у погледу крађе и оштећења знања и интелектуалног капитала пословног система које су садржане у три главе,а то су:

1. Глава двадесета; кривична дела против интелектуалне својине,
2. Глава двадесет друга; кривична дела против привреде,

[9] Зоран Стојановић, *Коментар Кривичног закона Србије*, Београд, 2009. година, стр. 345

3. Глава двадесет седма; кривична дела против безбедности рачунарских података,
4. Глава двадесет осма; кривична дела против уставног уређења и безбедности Републике Србије

Ова кривична дела, у одређеном свом облику и по начину извршења, се могу класификовати као кривична дела из области корпоративне шпијунаже и високо технолошког криминала, и као таква могу обухватити област крађе знања, заштите конкурентности и интелектуалног капитала.

Корпоративна шпијунажа се заснива на једноставном концепту. Ради се о откривању и крађи нечије пословне тајне - и коришћењу тако добијене информације за производњу сопственог производа. Наравно у то је укључена и крађа интелектуалне својине - односно изума који су заштићени лиценцама или патентним правима. Конкретнска предност у привредном пословању се одувек штити системом пословне тајне. Најранији историјски записи нам показују да се конкурентска предност најефикасније бранила њеним чувањем у тајности, ограничавањем приступа и заштитом путем система пословне тајне.[10]

Заштита конкурентске предности се и у савременим пословним односима најефикасније штити системом пословне тајне и у том смислу наше кривично законодавство је прописало кривично дело Одавање пословне тајне из члана 240. које гласи:

„Ко неовлашћено другоме саопшти, преда или на други начин учини доступним податке који представљају пословну тајну или ко прибавља такве податке у намери да их преда непозваном лицу, казниће се затвором од три месеца до пет година.

Ако је дело из става 1. овог члана учињено из користољубља или у погледу нарочито поверљивих података, учинилац ће се казнити затвором од две до десет година.

Ко дело из става 1. овог члана учини из нехата, казниће се затвором до три године."[11]

[10] Кина је 1713. године изгубила конкурентску предност услед деловања корпоративне шпијунаже. Кина је, наиме, вековима производила висококвалитетни порцелан, и то искључиво кроз процесе који су били познати само њеним алхемичарима, што јој је давало могућност велике зараде. Francusli Jezuit, отац d'Etrecolles, је приликом посете краљевској фабрици порцелана у Кини, успело да запамти – меморише тајне производње порцелана; да их опише и пошаље у Француску – Stevan Dedijer, Development & Intelligence 2003-2053, Paper presented at the Infoforum Business Intelligence Conference, Загреб 25-26 Септембер 2003

[11] Кривични законик

Криминалистички аспект корпоративне шпијунаже

Деловање корпоративне шпијунаже се може класификовати на више начина, али основна подела јесте подела на деловање шпијунаже легалним методама и деловање шпијунаже нелегалним методама.

Легалне методе

Постоји неколико облика корпоративне шпијунаже који се могу назвати легалним. Ове методе у основи се веома тешко могу подвести под активности којима се крши закон, али мотиви њихове примене, тј. прикупљање података, информација и знања их свакако сврставају у активности корпоративне шпијунаже. Легалне методе могу да укључују куповину привредног друштва или производа, чији крајњи циљ није то друштво или производ већ искључиво прибављање одређене технологије легалним стицањем права власништва. У овом случају фокус није на производу или компанији већ на конкретној технологији, јер када се овлада технологијом компанија или производ могу да пропадну а конкурент почиње да прави сопствени.

Други метод прибављања технологије подразумева притисак на привредно друштво да одустане од заштите пословне тајне. У основи, то је поступак када привредно друштво послује у страној земљи, и онда оно мора да обучи домаћу радну снагу у вези са кривичним технологијама, тако да је врло вероватно да ће доћи до одливања до тада добро штићених знања и технологија. Други облик је удруживање са другим привредним друштвом било да је оно страно или домаће. Најизразитији случајеви су joint-venture удруживања, када привредна друштва улазе у пословне аранжмане ради заједничког остваривања једног или више послова, тада је привредно друштво суочено са захтевом да открије своје пословне тајне и осетљиве технологије. На привредном друштву је да одлучи да ли су трошкови обављања оваквог пословања исплативи, јер откривање сопствених тајни може бити једини начин да се уђе на одређено тржиште или да се изради одређени нов производ.

Информације из отвореног извора такође нуде богат извор знања за корпоративне шпијуне. Оне могу бити различитих облика, укључујући новинске чланке, корпоративне годишње извештаје, патенте поднеске, судске документе, маркетинг стратегије. На пример, типично корпорацијско понашање је слање истраживача и маркетинг особља на сајмове и конференције како би се прикупили подаци о конкурентима и њиховим најновијим активностима и производима. Они се обично по-

нашају као купци које интересује одређени производ, па испитивањем запослених из конкурентске фирме прикупљају обиље потребних података и информација.

Уобичајен начин прибављања информација и пословних тајни о конкуренту је, свакако, запошљавање стручњака из конкурентског привредног друштва, те искоришћавање његових знања и вештина које је стекао.

Нелегалне методе

Као што је речено многи од претходних метода се изводе на граници криминалне активности. Илегалне методе се најчешће користе јер нису сви спремни или нису у позицији да користе легалне методе, које су и најбезбедније.

Највећи број случајева корпоративне шпијунаже подразумевају коришћење инсајдера, односно запослених у одређеном привредном друштву, како би крали информације за конкуренцију. Мотиви зашто инсајдери пристају да садађују су различити, у зависности од околности могу се поделити на мотиве који су везани за новац[12] и оне који нису везани за новац. У највећем броју случајева као и са традиционалним шпијунским случајевима, регрутовање се обавља подмићивањем, изнудом или уценом. Међутим, постоје и инсајдери који имају друге мотиве, као што су освета послодавцу за лош третман у напредовању или новчаном награђивању. Инсајдери често услед свог положаја злоупотребљавају могућност приступа информацијама или само предају информације које већ поседују у раду. У новије време јављају се и инсајдери који су вођени патриотским мотивима, па се у страној земљи запошљавају у циљаној компанији одакле, некада и годинама, прикупљају податке о критичним технологијама.

Постој мање софистицирани, али ефикасни методи за крађи информација. Корпоративна шпијунаћа може да користи и једноставно проваљивање у зграде и канцеларије одакле се жели украсти тражена

[12] Септембра 1997. године Pin Yen Yang и његова ћерка Hwei Chen Yang су били ухапшени заједно са Dr Ten Hong Lee због покушаја крађе вредних индустријских тајни од компаније Avery Dennison Corporation из Калифорније и њиховог преноса компанији Four Pillars Company на Тајвану. Dr Lee, који је био запослену у Avery Dennison од 1986. године примио је између 150,000 $ и 160,000 $ од Four Pillars i Pin Yen Yang за нелегални трансфер поверљивих производних информација и истраживачких података, те производних инфорамција у периоду од око девет година. Економски губитак за Avery Dennison је утврђена на 50-60 миллион долара. Овај случај означен као прва осуда страног држављана и стране компаније у оквиру the Economic Espionage Act of 1996.

инфорамција. Корпоративни шпијуни савладавају препреке, ограде, откључане и закључане пословне просторе, ормане, касе, те упадају у рачунаре, и обавезно ће испитати незаштићене рачунарске системе, итд. Веома чест метод којим се користе корпоративни шпијуни је претрага контејнера за смеће где ће свакако пронаћи значајну количину информација.[13] На западу је одавно уочено да менаджери и пословни људи који често путују, бивају предмет софистицираних надзора. Амерички руководиоци су изјавили да понекад имају осећај да су им хотелске собе претресане, или да ду им телефонски позиви били праћени, итд. Ово се дешава због вредности информација које поседују, а што имају важнији положај у компанији и приступ осетљивим технологијама самим тим ризик да буду посматрани од стране конкурентске организације је већи.[14] Корпоративни шпијуни могу да прикупљају информације хаковањем рачунара, уношењем вируса и тројанаца, прислушкивањем телефона, видео и аудио надзором, софистицираним криптоанализама, итд. Због ефикасности тренутно познатих метода, мало је вероватно да корпоративни шпијуни морају да развијају нове методе.

Америчка студија о безбедности пословања је указала на најосетљивије информације у организацији које су мете конкуренције:

- Истраживање и развој
- Продаја/маркетинг
- Базе података о клијентима
- Финансије
- Нови производи
- Пословни и стратешки планови
- Производни процеси
- Merger/acquisition
- Цене
- Подаци о запосленима

Директива Енглеског министарства за трговину и индустрију предвидела је следећу листу информација које имају вредност за конкуренцију:

- Преговарачка позиција
- Процена конкруренције
- Информације о купцима
- Пословне и конкуренцијске стратегије
- Маркетиншки планови

[13] Pasternak, G. (1996), The Lure of the Steal, U.S. News & World Report, March 4, p. 45.
[14] White House (1995), Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, Washington, DC: Government Printing Office.

- Информације о запосленима
- Детаљи за велике аквизиције и др.
- Врло осетљиве процене конкуренције, партнера и уговора
- Пословни планови и потенцијалне опције
- Заштита патентних информација

Извештај Америчког конгреса о индустријској шпијунажи из 1995. године навео је листу технологија које су најчешће мете страних обавештајних активности:

- Биотехнологије
- Ваздухопловнно-космичке технологије
- Телекомуникације
- Компијутерски хардвер и софтвер
- Напредне саобраћајне и машинске технологије
- Напредни материјали и премази
- „Невидљиве технологије“

Истраживања су показала да негативан утицај корпоративне шпијунаже може да нанесе озбиљене штете за компанију која је била изложена њеном дејству, у најгорем случају може довести до престанка рада и губитка капитала. Међутим, најчешћи губици услед деловања корпоративне шпијунаже су:

- Губитак конкурентске предности
- Губитак удела на тржишту
- Губитак прихода
- Повећање трошкова истраживања и развоја
- Губитак пословног угледа
- Повећање судских трошкове - трошкови повезани са губитком поверљивих информација
- Повећани трошкови осигурања

Колико је проблем сложен и колике су штете које настају услед деловања корпоративне шпијунаже може се видети из истраживања Федералног истражвног бироа (Federal Bureau of Investigation - FBI), који је изнео тврдње да су Сједињене Америчке Државе (САД), као светски лидер у технологији, данас постале једна од главних мета индустријских шпијуна. FBI процењује да је између 2004. и 2005. године због индустријске шпијунаже привреда САД изгубила између 130 и 330 милијарди долара. FBI сматра да 15 до 16 земаља тренутно има веома агресивне програме чија мета су САД. Међу њима су и Кина и Русија.[15]

[15] Voice of America, U današnjem svetu ratovi se ne vode samo bombama i topovima, http:// www. Voanews .com/ Serbian/ archive/ 2005-05/ 2005 – 05 – 08 -voa3.cfm? moddate=2005-05-08. децембар 2007.

Разматрањем овога облика криминалитета и начина испољавања, уочљиво је да се у суштини цео проблем своди на предузимање мера и радњи у циљу спречавања или ограничавања деликта. Са начином извршења појединих кривичних дела која се могу подвести под криминалну појаву названу корпоративна шпијунажа, нераскидиво је повезана проблематика превенције тога облика криминалитета. У конкретном случају под појмом превенције подразумевамо целокупност разноврсних међусобно повезаних мера, које проводе како државни органи тако и привредни субјекти, а усмерене су на спречавање криминалитета и уклањање узрока његова настајања. Циљ превентивних радњи на спречавању и сузбијању ових деликата је да се предузму сврсисходне и конкретне радње које ће придонети спречавању њиховог извршења. Суштина превенције повезује се са предделиктним и постделиктним спречавањем деликта у виду тзв. антикриминалне акције. Сагледавајући конкретну негативну појаву и заузимајући криминалистичко становиште о најефикаснијем облику борбе против исте изражене у превенцији, потребно је разликовати:

- превентивне мере које се предузимају као акција постављена пред целокупни апарат кривичног гоњења,
- превентивне мере које се предузимају индивидуално или групно и усмерене су на одређено кривично дело, које још није извршено или је већ извршено, али може бити да се и даље наставља.

У првој групи превентивих мера ради се о мерама израђеним на основу материјала из предмета у којима је кривични поступак већ завршен или је у току, а може се одности на околности и сфере извора шпијунског криминалитета у датом раздобљу или начину извршења шпијунаже. У другој групи превентивних мера, ради се о оперативно тактичким мерама и радњама које су усмерене на евентуалног извршиоца корпоративне шпијунаже.

Закључак

Савремени друштвено-економски односи и глобални начин привређивања наметнули су изазове у националној и регионалној економији, као и економији на нивоу пословног система. Савремени пословни системи су суочени са три одлучујућа фактора: конкуренцијом, променама и купцима. Ове три снаге модификују компанијске стратегије, водећи их у дубоко, непознато и застрашујуће. У пословним односима нема *fair-play* и саосећања, те стога пословни системи морају озбиљно да приступе овом широко распрострањеном проблему који је, нарочито у свет-

ским размерама, све више попримио облике тихог, прикривеног рата. Слободно се може рећи да већ годинама траје „глобални економски рат".

Владајуће мишљење већине пословних људи је да се ради о високо софистицираним активностима обучених шпијуна, који раде или су радили у некој обавештајној служби. То је само донекле тачно, најпре из разлога што услуге таквих шпијуна нису јефтине, а са друге стране корпоративна шпијунажа обично користи једноставне методе које се могу спречити уколико се примени концепт свеобухватне безбедности, а не само физичко-техничко обезбеђење. Заштита од корпоративне шпијунаже се може остварити развојем модела пословања који мора да буде састави део пословне стратегије. Заштита од корпоративне шпијунаже у пословном системи је стаставни део пословања, то је пословна филозофија. Заштита се може остварити само вољом и жељом менаџмента и успех заштите ће искључиво зависити од тога да ли је менаџемант опредељен ка организацији и свестан проблема.

Анализом горе изнетих ставова може се закључити да на светском тржишту владају нова правила пословања и да се у савременом пословању примењују сва могућа средства, дозвољена и недозвољена, како би се остварила конкурентска предност на корпоративном нивоу, или боље речено економска доминација на глобалном нивоу.

Свако ко сматра да капитал нема граница и да он није обележен националним бојама појединих народа веома греши, јер су освајање тржишта и економска домијација дубоко обојене националним интересима појединих народа, а да није тако националне обавештајне службе не би узимале толико учешћа у тзв. "*тржишном надметању"*.

Литература:

1. Allen Steve, "Safeguarding proprietary information the protection of intangible asset", Financial Crime Review: Strategies to Combat Money Laundering and Fraud, BDE Global, London, 2001, p. 3.
2. Competitive intelligence and economic or industrial espionage, 15. oktobar 2010. http:// finance.reachinformation.com/ Industrial_espionage .aspx,
3. Economic Espionage, 18. novembar 2010. http://www.fbi.gov/about-us/investigate /counterintelligence /economic-espionage
4. Kevin D. Mitkin, *Umetnost obmane*, Mikro knjiga, Beograd, 2003, str 243.
5. Prvulović Vladimir, *Ekonomska diplomatija*, Megatrend univerzitet, 2006, Beograd, str. 147
6. Mediacentar, *Industrjska špijunaža kao pošast nad planetom*, http:// www. mediacenter.org.yu/ code/ navigate.asp, 19/01/2007.

7. Zakon o privrednim društvima (Službeni glasnik RS 36/2011, 99/2011),
8. Pasternak George., The Lure of the Steal, U.S. News & World Report, 4. March 1996, p. 45.
9. Stojanović Zoran, *Komentar Krivičnog zakona Srbije*, Beograd, 2009. godina, str. 345
10. „Strategije razvoja Ministartstva unutrašnjih poslova 2011 – 2016“, http: //www. http://www.mup.rs/cms_cir/sadrzaj.nsf/Strategija%20razvoja%20MUP-a%202011-2016.pdf , 22.04.2012.
11. „Strategija nacionalne bezbednosti Republike Srbije”, http://www.mod.gov.rs /cir/ dokumenta /strategije /usvojene/ Strategija% 20nacionalne% 20bezbednosti% 20 Republike%20Srbije.pdf, 20/02/2011.
12. Voice of America, U današnjem svetu ratovi se ne vode samo bombama i topovima, http:// www. Voanews .com/ Serbian/ archive/ 2005-05/ 2005 – 05 – 08 - voa3.cfm? moddate=2005-05-08. decembar 2007.
13. White House (1995), Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, Washington, DC: Government Printing Office.

Corporate espionage; normative - forensic aspect of modern business

Summary: Questions and issues related to corporate espionage is largely occurring in newspaper articles, while scientific and professional community in the Republic of Serbia is very shy handles this subject. Bearing in mind the above mentioned, aim is to show the broad widespread phenomenon of corporate espionage, as well as some of its basic aspect of modern business. Corporate espionage is the most efficient and destructive mean of economic warfare in which it is contained by its criminal aspect. Although the history of corporate espionage is very long, it is now particularly important because of the imposed requirements by constant innovation and development of knowledge, because to remain "in game" operating system must constantly innovate and to invest in equipment and technology, and how it is very expensive, there is a gap between the desire for profit and opportunities for its creation. Desire or greed leads to stepping unethical and illegal business activities that the system can cost significant resources or market share. From the normative aspect of problem solving, it can be said that in the Republic of Serbia corporate espionage does not have great significance, legislative solutions do not provide minimum requirements for successful opposition to this phenomenon, which in practice of developed market countries is not the case.

Key words: corporate espionage, competitiveness, crime, norms, knowledge, information