УНИВЕРЗИТЕТ У БЕОГРАДУ

ФАКУЛТЕТ БЕЗБЕДНОСТИ

Дејан Н. Тепавац

ЗАШТИТА ПОСЛОВНИХ ИНФОРМАЦИЈА У ФУНКЦИЈИ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ

докторска дисертација

Београд, 2018

UNIVERSITY OF BELGRADE

FACULTY OF SECURITY STUDIES

Dejan N. Tepavac

PROTECTION OF BUSINESS INFORMATION IN THE FUNCTION OF NATIONAL SECURITY

doctoral dissertation

Belgrade, 2018

КОМИСИЈА ЗА ОЦЕНУ И ОДБРАНУ ДОКТОРСКЕ ДИСЕРТАЦИЈЕ

МЕНТОР:

др Ивица Ђорђевић, ванредни професор, Универзитет у Београду, Факултет безбедности

ЧЛАНОВИ КОМИСИЈЕ:

др Радомир Милашиновић, редовни професор, Универзитет у Београду
др Младен Милошевић, доцент, Универзитет у Београду, Факултет безбедности

ДАТУМ ОДБРАНЕ_____.

ЗАШТИТА ПОСЛОВНИХ ИНФОРМАЦИЈА У ФУНКЦИЈИ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ

Резиме: Поуздане информације представљају основ смисленог људског деловања, успостављања међуљудских, међународних и пословних односа. Информације посебно добијају на значају са напретком информационо–комуникационих технологија и настајањем глобалних пословних мрежа, односно умрежавањем институција и присутношћу неког од видова информационо–комуникационих технологија у животу највећег дела људске популације. Добра селекција и правовремена употреба информација доприносе развоју људског знања и квалитетнијег деловања човека у свим подручјима његовог интересовања. На основу расположивих знања поткрепљених актуелним информацијама, државници доносе одлуке од важности за развој читавог друштва и човечанства. Посебно место и улогу у свету информација имају пословне информације јер од њих зависи ефикасност функционисања информационо–комуникационог система (ИКС) националних држава, као и привредних субјеката. Прикупљање квалитетних информација представља сложен задатак организационих целина које се баве обавештајном делатношћу. Појава великог броја пословних информација намеће следећа питања: како из мноштва информација извући потребне и корисне; како расположиве информације употребити тако да се постигне најбољи пословни резултат; како онемогућити злоупотребу информација и ИКС–а; и како заштитити информације и обезбедити сигуран и несметан рад ИКС–а.

Заштита пословних информација је активност која се реализује у циљу обезбеђивања несметаног и континуираног рада ИКС–а, сводећи ризике и претње на минимум. Заштита пословних информација представља заједнички задатак пословних субјеката и државних институција. Државне службе, обавештајне и контраобавештајне, као део државног система, на тај начин штите и националне интересе будући да је пословање великих привредних субјеката уско повезано са интересима националних држава. Квалитетна заштита пословних информација, између осталог, подразумева

стандардизацију информационе безбедности, а савремени стандарди који се данас употребљавају односе се на генерисање, пријем и чување података унутар ИКС–а. Нормативно правне мере заштите пословних субјеката требало би да буду утемељене на међународним и националним прописима, нормама и стандардима и усклађене са специфичностима организација.

Истраживање у области развоја мерљивих индикатора и подиндикатора нарушавања људске безбедности налази оправдање у потреби за извештавањем, стратешким и оперативним потребама и свим другим захтевима који се упућују пословним субјектима и националним државама у циљу њихове свеобухватне заштите. Сваки од индикатора и подиндикатора осветљава стање безбедности у одређеној области пословних активности.

Анализа стања у области заштите пословних информација кроз призму концепта људске безбедности даје могућност квантификације утицаја нивоа заштите информација на квалитет живота грађана, као и на свеукупно стање националне безбедности држава.

Кључне речи: национална безбедност, пословне информације, информациона безбедност, информационо-комуникациони систем, људска безбедност, индикатори, заштита.

Научна област: интердисциплинарне, мултидсциплинарне и трансдисциплинарне студије

Ужа научна област: студије безбедности

УДК број:

PROTECTION OF BUSINESS INFORMATION IN THE FUNCTION OF NATIONAL SECURITY

Summary: Reliable information are the basis of meaningful human action, establishing interpersonal, international and business relations. Data are especially important with the advancement of information and communication technologies (ICT) and the emergence of global business networks and networking of institutions and the presence of some of the aspects of ICT in the life of most of the human population. Good selection and timely use of information contribute to the development of human knowledge and the quality of human activities in all areas of his interest. Based on the available knowledge substantiated current information, statesmen make decisions of importance for the development of the whole society and mankind. A special place and role in the world of information have business information because of them depends on the efficient operation of theinformation and communication system of national states and business organization. Obtaining quality information is a complex task of business entities, which requires a professional approach to organizational units that deal with business intelligence activities. The emergence of a large number of business information raises questions: how to extract information from a multitude of necessary and useful; how to use the available information so as to achieve the best business results; how to prevent the abuse of information and information and communication system; how to protect information and ensure a safe and smooth operation of the information communication system.

Protection of information is an activity that is being implemented in order to ensure smooth and continuous operation of information and communications systems, reducing the risks and threats directed towards them at a minimum. Protecting your business information is a common task of businesses and government institutions. Civil service, intelligence and counterintelligence, as part of the state system, thereby protect the national interests toot since that the business of big business entities is closely linked to the interests of nation states.
Protecting business information includes standardization of information security, contemporary standards used today are related to the generation, reception and

storage of data within the information and communication system. Normative legal measures to protect businesses should be based on international and national regulations, norms, standards and specifics of the organization.

Research in the field of development of measurable indicators and sub-indicators of human security takes into account the needs for reporting, strategic and operational needs, and any other requirements that are placed in front of businesses to ensure their comprehensive protection. Each of the indicators and sub-indicators lightens the security situation in a particular area of business activities.

Analysis of the situation in the field of protection of business information and the concept of human security provides the possibility of quantifying the impact of the level of protection of information on the quality of life of citizens, but also on the level of national security.

Key words: National security, business information, information security, information and communication system, human security, indicators, protection.

Scientific domain: inter-disciplinary, multi-disciplinary and trans-disciplinary studies

Narrower scientific domain: Security studies

UDK Number:

САДРЖАЈ:

1. УВОД

Друга половина двадесетог века прошла је у знаку великих технолошких достигнућа и примене информационо-комуникационих технологија у многим областима. На основу многих параметара, могло би се закључити да се кроз призму информационо–комуникационих технологија преламају резултати научних достигнућа фундаменталних природних наука, који су кроз своју операционализацију и практичну примену довели до увођења нове пословне и друштвене праксе. Значајно достигнуће огледа се у конструисању уређаја који омогућавају ефикасну пословну организацију и ван уобичајених простора омеђених националним границама и географским препрекама. Међутим, научна достигнућа природних наука, реализована путем нових технологија и техничких решења, нису добила одговарајућу подршку у друштвеним наукама. Временом, због максималне комерцијализације, информационо-комуникационе технологије, упркос свом позитивном потенцијалу, постају уместо решења део проблема. Неадекватна регулатива области која је по свим својим карактеристикама глобална, а у највећем делу регулације ослања се на национална законска решења, отворила је велики простор за манипулацију у оквиру постојећих институционалних система и њихову инструментализацију. Важност заштите тајности критичних података за функционисање система није проблем само на нивоу пословних целина, већ постаје једно од кључних питања безбедности читавих народа и њихових држава.

Стабилност државе и успешност пословних субјеката зависе од тога колико су у стању да уоче везу која постоји између опстанка на тржишту,

националне безбедности и степена заштићености пословних информација. Свеприсутност информационо-комуникационих технологија код пословних субјеката, у државним институцијама и домовима доводи до тога да однос према информацијама није више само питање конкурентности и добре информисаности. Нематеријална природа информација код најширег круга корисника ствара погрешан однос према њиховој вредности. Многи појединци су још увек фокусирани на очување и вредновање материјалних добара јер не постоји свест о томе да вредност привредних субјеката, функционисање пословног или државног система може бити угрожено и крађом материјала који не морају да имају физичку форму.

Перформансе савремених компјутера, који обрађују велику количину података у кратком року, омогућавају да се путем укрштања наизглед безначајних података може доћи до закључака који откривају суштину неког процеса или појаве, а коју би неко желео да сачува као тајну. Разлика између успешних и неуспешних пословних система или држава све чешће се уочава у њиховој способности да спрече отицање и компромитацију информација битних за функционисање система.

Сложеност актуелних друштвено–економских прилика на почетку XXI века онемогућава квалитетну и свеобухватну анализу овог проблема помоћу класичних теоријских приступа. До промена је највише дошло у сфери безбедности, где је ограничавање анализе на територијалну безбедност или безбедност појединих институција давно превазиђено. С обзиром на глобални карактер промена и све већи број екстериторијалних фактора који утичу на квалитет живота грађана неопходно је проширити оквире анализе. Како се класичан концепт безбедности не показује довољним у разматрањима која се тичу безбедносних проблема савременог друштва, неопходно је проблем посматрати и анализирати кроз друге теорије и концепте безбедности. У датом контексту, аналитички потенцијал концепта људске безбедности може да допринесе квалитету анализе и бољој перцепцији савремених безбедносних изазова и претњи. Концепт људске безбедности омогућава квалитативну анализу стања и процеса путем модела који има седам димензија (економска безбедност, лична

безбедност, политичка безбедност, еколошка безбедност, безбедност заједнице, безбедност исхране и безбедност здравља) и у оквиру сваке од њих низ индикатора.

Операционализација концепта људске безбедности може да допринесе отклањању недостатака анализа базираних на државној, односно националној безбедности. Притом, треба имати у виду да концепт људске безбедности није у колизији са класичним приступима безбедности, већ отклања њихове недостатке.

1.1. ПРОБЛЕМ ИСТРАЖИВАЊА

Рад је структуиран тако да омогућава квалитативну анализу веза које постоје између националне безбедности и степена заштићености пословних информација. Информатизација пословних система и државне управе створила је ситуацију у којој је проблем заштите пословних информација од пресудног значаја за функционисање система. Основне карактеристике информација као што су њихова нематеријална природа и чињеница да се најчешће налазе у дигиталној форми, код најширег круга корисника ствара погрешан однос према њиховој вредности. У свести већине наших савременика остала је тежња да се вредност нечега мери на основу органолептичких перцепција предмета. Данашња структура вредности пословних система показује да се њихов највреднији део налази у информатичким мрежама, односно у дигиталном облику.

Отицање битних информација из пословних система може да угрози њихово функционисање, доведе до великих губитака, чак и пропасти. Уколико резултати истраживања нових производних процеса и стратешки дугорочни планови дођу у погрешне руке могу да омогуће конкуренцији стратешку предност на тржишту. С обзиром на велика улагања у креирање нових производа и на значај тренутка у којем се они пласирају на тржиште, способност очувања пословних тајни би могла да буде услов за успех, односно неуспех. Неуспех би, у поменутом случају, могао да представља и

пропаст система што би за последицу имало на стотине незапослених радника. На овом примеру се види условљеност између заштите пословних информација и социјалне стабилности државе на чијој је територији пословни субјект.

Компромитација информација унутар система државних институција може да има још драстичније последице. Почев од тога да се може угрозити приватност грађана, чије се информације налазе унутар информатичких мрежа државне управе, па до тога да се откривањем садржаја стратешких докумената директно угрожава национална безбедност.

Савремени свет са процесом глобализације, чије је основно обележје масовна примена информационо-комуникационих технологија, постаје повезаније и динамичније окружење. Актуелна ситуација подразумева сложен и интерактиван однос међу државама који је додатно оптерећен утицајем транснационалних компанија и неформалних центара моћи. Заштита интереса грађана и држава као њихових заједница захтева одговарајући систем мера како би се у врло сложеној међународној арени обезбедила неповредивост тајности критичних информација. Није проблем само доћи до корисних сазнања и употребљивих података него је још важније резултате њихове анализе адекватним мерама заштитити. Спречавање неовлашћеног приступа информацијама и њихове употребе у складу са интересима њихових поседника пружа шансу за пословни успех и развој шире заједнице.

Једно од основних обележја глобализације је анархичност која проистиче из недостатка адекватне институционалне контроле процеса. Још увек нема глобалних институција и утврђених правила са одговарајућим системом санкција за прекршиоце усвојених декларација. Неолиберални концепт уређења друштвено–економских токова продубљује постојећи развојни јаз и угрожава стабилност неразвијених држава. Технолошка зависност најчешће подразумева контролу привредних система од стране центара моћи изван простора под контролом националних институција. Функционисање привреде се одражава на прилике у систему националних институција (јавне службе, систем безбедности и одбране) јер

недостатак средстава угрожава рад читавог система. Уклањање традиционалних граница између домаћих и међународних послова доводи до ограничавања функција суверених држава и наглашавања спољних утицаја у области безбедносне политике. Тиме на значају добија међузависност институционалних обавештајно-безбедносних система, као инструмената државне политике и система обезбеђења привредних субјеката.

Актуелна пракса показује да се на прикупљању података од значаја за положај државе и развој компанија ангажују посебно обучена лица и институције које имају усвојене и разрађене одговарајуће методе и системе. У савременом међународном окружењу, посматрајући најразвијеније земље света, појмови економске и националне безбедности се скоро поистовећују, јер управо економија одређује стабилност простора и динамику развоја једне земље.

У циљу прикупљања података о привреди једне земље, пословању неког привредног субјекта и политичким приликама унутар једне државе, наведене институције користе се одговарајућим методама и техникама које се у најширем смислу могу поделити на легалне и илегалне. Легалне методе прикупљања података се реализују кроз истраживања јавних медија, слањем упитника компанијама и институцијама од интереса за матичну компанију или државу, пословним сусретима и разговорима, посетама привредним субјектима и институцијама, учешћем на међународним активностима као што су сајмови и симпозијуми. Легалне методе прикупљања података реализују се у складу са законском регулативом земље домаћина и углавном нису предмет заштите надлежних служби или организација унутар привредних субјеката.

За разлику од легалних метода прикупљања података, корисници илегалних метода су подложни законским санкцијама и ради тога се наведена активност реализује тајно и изазива много већу штету по државни систем земље домаћина, то јест за пословни статус привредног субјекта. Прикупљање података реализује се кроз продор у забрањену зону информационих система државних институција или привредних субјеката

и/или ангажовањем посредника за прибављање информација (поткупљивањем поседника, односно руковаоца критичним информацијама, отпуштених или процесуираних кадрова итд). Претпоставља се да је за прикупљање таквих информација неопходан виши степен обучености и знања из области обавештајног деловања за онога ко је ангажован на том послу. На основу квалификоване безбедносне процене и процене ризика, корисник доноси одлуку која би требало у највећој мери да заштити интересе државне институције односно привредног субјекта којим руководи.

На крају би се могло закључити да је глобализација отворила питање глобалне перспективе безбедности држава у његовом суштинском смислу, јер се у савременим међународним односима безбедност дефинише као одсуство претњи и такво стање политичких, економских, правних и других услова којима се минимизира опасност по систем.

Анализом стања националне безбедности кроз призму концепта људске безбедности утврдиће се узрочно–последична веза безбедности државе и појединца са аспекта заштите пословних информација.

1.2. ПРЕДМЕТ ИСТРАЖИВАЊА

Истраживање проблема је усмерено на анализу актуелног система заштите пословних информација у Републици Србији. Постојеће стање је приказано кроз анализу системских решења и праксе. Истраживање показује колико је ефикасан постојећи модел заштите пословних информација у Србији. Анализа постојећег стања и изучавање страних искустава као резултат дају модел заштите пословних информација који је у складу са потребама институција и привредних субјеката који послују на простору Републике Србије.

Дефинисањем индикатора и подиндикатора нарушавања безбедности омогућава се квантификација нарушавања безбедности и доказује се веза између степена заштите пословних информација и безбедности пословног

субјекта. Потреба за контраобавештајним радом постоји у сваком пословном и институционалном систему, а његов највећи значај је у превенцији. Једино правовремено реаговање на могућност компромитовања значајних података може да спречи угрожавање безбедности државних институција и привредних субјеката.

Такође, истраживањем се утврђује колико је рад безбедносних служби Републике Србије у складу са релевантним законским решењима. У том контексту, анализиран је и рад основних елемената институционалног система безбедности Републике Србије (БИА, МУП, ВБА и ВОА). Истраживање на нивоу привредних субјеката утврђује које су законом прописане обавезе и како функционише њихова контраобавештајна заштита. Посебно је анализирана пракса великих система где постоје посебни сектори намењени заштити од разних облика угрожавања (на пример: Дирекција за корпоративну заштиту привредног субјекта). Предмет анализе је и рад Народне скупштине као законодавног органа Републике Србије надлежног за доношење нових и измену постојећих закона. У наведеним оквирима, посебно је значајан Одбор за одбрану и безбедност задужен за контролу поштовања законских норми у процесу рада безбедносних структура Републике Србије, а који делује у оквиру Народне скупштине.

1.2.1. Просторно, временско и дисциплинарно одређење предмета истраживања

Истраживање обухвата временски период од завршетка Хладног рата до данас. Просторно одређење предмета истраживања је у ужем смислу везано за територију Републике Србије, а у ширем смислу обухвата и искуства других држава, што анализу чини свестранијом. Сложеност истраживаног феномена захтева интердисциплинарни приступ будући да предмет, садржај и истраживачко подручје дисертације спадају у домен више научних дисциплина, међу којима су наука о безбедности, политичке, социолошке и правне наука.

1.3. ЦИЉЕВИ ИСТРАЖИВАЊА

Основни научни циљ овог истраживања је систематизовање савремених сазнања о заштити пословних информација у условима масовне информатизације људских активности. Циљ је доказати везу између степена заштићености пословних информација унутар система и нивоа безбедности његових елемената. Циљ је доказати како због масовне информатизације људских активности расте значај обавештајне заштите. У истраживању је обухваћена анализа најбитнијих аспеката заштите информација: обавештајна делатност, с једне, и контраобавештајне мере, с друге стране. Такође, циљ је да се путем прецизног дефинисања скупа индикатора омогући квантификовање нивоа безбедности пословних и институционалних система у односу на степен заштићености пословних информација. Избор адекватних параметара омогућава креирање модела чијом би применом безбедност система могла да се подигне на виши ниво.

Општи циљ истраживања јесте проучавање и критичка анализа постојећег стања система заштите пословних информација и облика решавања инцидената повезивањем сазнања из различитих научних дисциплина. Посебни циљеви су:

— анализа страних и домаћих искустава у области заштите пословних информација;

— проучавање стања и праксе у области заштите пословних информација на нивоу пословних субјеката и у институционалним системима;

— утврђивање корелације између степена безбедности људи у односу на ниво заштите пословних информација;

— указивање на факторе успешности система заштите пословних информација и подизања општег стања безбедности људи;

— утврђивање сета индикатора на основу којих се може анализирати и квантификовати стање безбедности у односу на степен заштите пословних информација;

— креирање модела за предвиђање могућих промена стања на основу промене степена утицаја појединих варијабли;

— анализа студија случаја пословних политика у области заштите пословних информација и њиховог утицаја на степен угрожености пословног система.

Практични циљеви истраживања огледају се у могућности коришћења резултата истраживања за:

— осавремењивање рада специјализованих државних институција у области заштите пословних информација;

— унапређење законодавног оквира и креирање адекватног система заштите пословне тајне.

Друштвена оправданост истраживања се огледа у јачању доприноса у подизању нивоа безбедности заједнице путем модела заштите пословних информација, а у складу са постојећим условима и потребама праксе.

1.4. ХИПОТЕТИЧКИ ОКВИР ИСТРАЖИВАЊА

Основна хипотеза од које се полази у истраживању је да: *Постоји корелација између ефикасности система заштите пословних информација и стања безбедности система*.

Из опште полазне хипотезе могу се извести следећи ставови чија ће се утемељеност испитивати:

— *Обим информатизације пословних активности захтева сразмерно ангажовање на контраобавештајној заштити пословања јер позитивни ефекти увођења информационо-комуникационих технологија у пословне системе зависе од њихове адекватне заштите.*

— *Усвајањем и применом адекватне законске регулативе од стране надлежних државних институција, постиже се виши степен заштите пословних информација.*

— *Квалификована безбедносна процена са јасно дефинисаним елементима и индикаторима угрожавања подиже ниво безбедности система.*

1.5. НАЧИН ИСТРАЖИВАЊА

Начин истраживања и избор метода условљени су проблемом истраживања, теоријским оквиром, операционализованим предметом истраживања и постављеним хипотезама. Имајући у виду комплексност проблема и предмета истраживања неопходан је интердисциплинарни приступ у анализи доступних материјала и комплементарна анализа доступних извора података. Ово истраживање има карактер комбинованог теоријско-емпиријског приступа. У циљу свеобухватног сагледавања проблема примењене су различите методе истраживања, а подаци добијени коришћењем сваке од њих омогућују анализу различитих аспеката везаних за овај проблем, а који се односе на нормативне инструменте, техничке предуслове и могућности, као и друштвене потребе.

У раду су коришћене следеће методе истраживања:

— *Анализа садржаја* је омогућила да се на систематичан и објективан начин дође до постојећих сазнања, резултата и анализа о предмету истраживања. Анализа садржаја је коришћена приликом изучавања релевантних законских решења.

— *Компаративна метода* је употребљена како би се извршила упоредна анализа стања теорије и праксе у различитим системима. Односно, коришћена је како би се установила промена стања у истом систему пре и после промене анализираних варијабли (законских решења и примене одговарајућих стандарда).

— *Студија случаја* је примењена на комплексним истраживањима како би се почетна хипотеза тестирала на конкретним примерима. Овај метод служи да покаже у којој мери је успех система у корелацији са применом адекватних решења у области заштите пословних информација.

— *Статистички метод* је примењен у квантитативној обради података. Статистички метод се користио у истраживању претежно квалитативних садржаја. Ова метода је у истраживачком поступку служила за: груписање

података на основу врста обележја у статистичке групе и низове, приказивање података уз помоћ табела и графикона.

— *Метод синтезе* служи да се повежу парцијална испитивања и да се донесу валидни закључци о истраживању као целини. Конкретно када говоримо о феномену шпијунаже, метод синтезе је омогућио да на основу сазнања о њеном настанку, узроцима и примени установимо и последице по безбедност пословних субјеката који делују на територији Републике Србије, као и саме националне државе.

— *Хипотетичко–дедуктивна метода* је као научно сазнајна основа представљена кроз укупно друштвено и научно искуство. Метода је заснована и изведена из искуства, односно омогућила је изградњу аксиома верификованих искуством.

— *Местод апстракције и конкретизације* је употребљен за разумевање глобалног система безбедности и повезивања проблема заштите пословних информација са постојећим нормативним одредбама.

— *Метод триангулације* представља комплементарну примену различитих истраживачких приступа или њихових посебних елемената у истраживању једног проблема.

1.6. САДРЖАЈ ДИСЕРТАЦИЈЕ

Дисертација садржи десет целина које би укратко могле да се прикажу на следећи начин:

1) Први део рада односи се на теоријско–методолошки оквир истраживања. У форми увода приказани су: предмет и проблем, односно циљ истраживања, хипотезе од којих се полази, методе које ће се примењивати у истраживању и кратки приказ садржаја.

2) Други део рада даје кратки приказ савремених процеса који утичу на амбијент у којем живе и раде људи. Глобализација и процеси који су

довели до њене форме и нивоа са којим се ми данас сусрећемо биће обрађени кроз призму научно-технолошког прогреса и утицаја информационо-комуникационих технологија на стварање глобалних мрежа. У овом делу рада се разматрају и појаве нових међународних субјеката као што су регионалне интеграције и транснационалне организације.

3) У трећем делу су приказани безбедносни проблеми савременог света у условима глобализације, као и могуће последице које они могу да проузрокују по безбедност државе и човека као појединца. Између осталог, тежиште у овом поглављу дисертације је на установљавању узрочно-последичних веза глобалног тероризма и организованог криминала, проблема екологије и одрживог развоја, и проблема енергетске нестабилности. Посебно место у постојећим безбедносним проблемима заузима феномен шпијунаже који је детаљније анализиран. Обрада актуелних извора угрожавања безбедности требало би да допринесе разумевању проблема који се јављају у контексту теме дисертације. Израженија свест о постојећим проблемима савременог света водила би ка адекватној реакцији надлежних институција и појединаца, што би за последицу имало бољу заштиту заједнице од наведених облика угрожавања.

4) Четврто поглавље је посвећено теорији информација. Кроз изношење основних теоријских поставки излаже се аргументација у прилог тезе да пословне информације заслужују озбиљно место у стратегијама привредних и друштвених система. У овом поглављу поред дефинисања основних појмова као што су подаци и информације, посебно је прецизиран појам пословне тајне.

5) Безбедност пословних информација обрађена је у петом делу путем приказа извора и облика њиховог угрожавања. Анализирани су и основни субјекти у процесу заштите, али и у процесу угрожавања значајних информација за опстанак и функционисање система. У овом поглављу стављен је посебан акценат на мере и системе заштите кроз приказ постојећих стандарда за заштиту пословних информација. Обрађени су међународни стандарди из система ISO, као и адекватни национални стандарди. У склопу ове целине приказан је и законодавни оквир који ствара

амбијент у коме се реализује процес заштите, као и права и обавезе институција и привредних субјеката.

6) Шести део дисертације садржи приказ до сада препознатих метода обавештајног рада. У овом поглављу објашњена је разлика између легалних и илегалних начина прикупљања података и доласка до информација. Начини обраде података приказани су путем обраде изабраних метода и кроз приказ обавештајног рада у области политике, безбедности и привреде, као најзначајнијих сегмената за функционисање система националне безбедности.

7) У седмом делу рада приказани су основни принципи контраобавештајне заштите пословних информација. Значај заштите сагледаваће се са аспекта индивидуалног нивоа (појединца), преко привредних субјеката и државе до глобалне заједнице у настајању. Могућности злоупотреба и манипулације подацима о појединцима могу да угрозе функционисање привредних система, националних држава, али и стабилност на глобалном нивоу.

8) У осмом поглављу дисертације анализирана је узајамна веза стања заштите пословних информација и безбедности грађана, базирана на поставкама концепта људске безбедности. Анализа свих седам димензија људске безбедности има задатак да потврди везу између индикатора о стању безбедности и нивоа ефикасности заштите пословних информација. Свака од димензија безбедности илуструје се одговарајућим примерима о везама које постоје између степена заштите пословних информација и стања безбедности на конкретном простору.

9) Девети део представља покушај да се резултати истраживања искористе за креирање модела који би показивао како промена битних параметара везаних за заштиту пословних информација утиче на стање безбедности људи на неком простору. Модел би требао да укаже на утицај свих релевантних елемената на стање у области заштите пословних информација. Структуру модела чине узајамне везе и односи, повратне спреге и утицаји институција, грађана, нивоа технолошког развоја, локалне

културе, спољних и унутрашњих извора угрожавања, стручне квалификације управљачких структура и стратегије развоја.

10) Десети део дисертације чине закључна разматрања. Ова целина даје одговор на питања: шта се може закључити на основу резултата истраживања, које нове проблеме истраживање отвара, који су недостаци установљени током истраживања и како их у будућности отклонити. Закључком је такође обухваћена анализа којом се потврђују или оспоравају постављене хипотезе.

2. САВРЕМЕНИ СВЕТ КАО УМРЕЖЕНИ ПРОСТОР

Завршетак Хладног рата није означио раскид са праксом примене силе у међународним односима, крај свих непријатељстава нити је светском становништву обезбедио дуготрајан мир и стабилност. Иако неолиберални концепт друштвеног организовања отвара низ могућности технолошког, економског и демократског развоја, исти показује негативне тенденције успостављања глобалног друштва кроз повећање глобалне нестабилности, несигурности и, у крајњем смислу, небезбедности. Прелазак постиндустријског друштва у инофрмационо друштво намеће афирмацију нових облика безбедносне заштите, како националних држава тако и привредних субјеката који послују унутар једне или више националних држава.

2.1. ТЕХНОЛОШКЕ ПРЕТПОСТАВКЕ ГЛОБАЛИЗАЦИЈЕ

Технолошки развој омогућава данашњој цивилизацији опстанак. Укидањем технолошких и научних достигнућа створио би се ризик по опстанак људске врсте, који би могао битно да утиче на бројно стање становника и насељеност планете Земље. Могло би се рећи да се почеци технолошке револуције бележе шест хиљада година пре нове ере, развојем металургије и производњом алатки од метала. Међутим, развој технологије започиње експоненцијално после Другог светског рата. Главни показатељ високог технолошког развоја представља развој полупроводничке и

информатичке технологије, нанотехнологија, телекомуникација и интернета, свемирских и нуклеарних технологија.

Били смо сведоци надметања великих нуклеарних сила у циљу унапређења нуклеарног оружја и оружја за масовно уништење чији је развој свакако узрокован технолошким напретком. Надметање у развоју нуклеарног оружја посебно је било изражено у периоду после Другог светског рата и представљало је окосницу војне надмоћи између великих сила, тадашњег СССР-а и САД-а. Војна индустрија је, као и у многим другим случајевима, била покретач развоја напредних технологија које се користе и у другим областима људског живота и омогућују људској популацији квалитетнији живот. С друге стране, поставља се питање безбедности човека и његов опстанак у новонасталим условима. Експерименти који су спровођени у циљу тестирања нуклеарног програма негативно утичу на здравље људи настањених у близини подручја где се таква истраживања спроводе. Примећене су негативне импликације по здравље људи који су на било који начин долазили у додир са програмом нуклеарних испитивања.

Тек по завршетку Другог светског рата нови концепт безбедности укључује и невојне претње усмерене према држави и појединцу, као што су климатске промене и слично. (Abrahamsson, 2008)

Глобализација је процес који је ствари поставио у потпуно нову раван посматрања. То је „процес економског, политичког, социјалног и културног деловања на наднационалном нивоу, који на глобалном нивоу мења устаљене политичке, привредне, социјалне и културне односе. Битна детерминанта овог процеса је технолошки развој који омогућава просторно и временско смањивање света.“ (Глигорић и сар., 2007: 95)

Глобализација (мондијализација) представља процес успостављања критеријума, услова и правила понашања у продукционој, финансијској, спољнотрговинској, банкарској, али и политичкој и свим другим сферама живота, од стране најразвијенијих земаља Запада, као и њихово универзално наметање, посредством међународних економских и политичких организација и институција, како званичних (Светска трговинска организација (СТО), Европска Унија (ЕУ), Уједињене Нације (УН), Савет

Европе) тако и оних незваничних или „невидљивих“ (Г-8, трилитерала, масонске ложе и др.). (Првуловић, 2010: 43)

Неки од позитивних ефеката глобализације узроковани научно технолошким развојем су: савремене методе лечења, развој транспортних средстава који омогућава већи степен мобилности људи, развој комуникација и информатике, развој космичке и нуклеарне технологије. Нажалост, поред позитивних аспеката технолошког прогреса постоје и негативне импликације као што су: загађивање животне средине и стварање ефекта стаклене баште и наглог отопљења, радиоактивне падавине узроковане нуклеарним експериментима, уништавање необновљивих природних ресурса, уништавање екосистема и друштвена отуђеност.

2.1.1. Научно–технолошки прогрес

Појмови технологије и науке су неодвојиви. Развој науке могао би се поделити у три фазе. Прву фазу, која се односи на временски период до Првог светског рата, обележавају најзначајнија научна достигнућа (открића парне машине, аутомобила, авиона, наизменичне струје, електричне сијалице, телефона и остварених домета у грађевинарству). У другој фази, између два светска рата, долази до јачања машинске и металуршке индустрије. Индустрија повољно утиче на развој бродоградње, што узрокује јачање експлоатације угља и нафте као погонског горива. У трећој фази научног развоја, од завршетка Другог светског рата до данас, најзначајнија открића се односе на развој информатичких система, који представљају основ за развој великих научних открића модерног доба. За развој индустријског, постиндустријског, а пре свега информационог друштва, највећи значај имају научна открића која су омогућила стварање система аутоматских машина и нових индустријских технологија, прогресивних средстава аутоматизације производње и управљања. Следи развој рачунара са којим се уводи димензија вештачке интелигенције и информационих технологија, чиме се остварују претпоставке за уобличавање информационог друштва. (Марковић, 2007:

14-24) Могућности брзих комуникација, електронске трговине, размене података широм света, унапредиле су пословање и утицале су да дође до смањења трошкова у наведеном процесу. Овим су профити мултинационалних и транснационалних привредних субјеката постајали многоструко већи. Међутим, њихова рањивост, посматрано из безбедносног угла, постаје много осетљивија. То што је комуникација лако остварљива путем информационо–комуникационих технологија и што се складиште пословни подаци у електронским базама, омогућава неовлашћеним и злонамерним лицима и организацијама са високим нивом знања о инфрормационим технологијама, лакши приступ и долазак до заштићених података. Недовољно обезбеђени подаци у привредним делатностима омогућавају предност конкуренту и боље позиционирање на тржишту у односу на њиховог власника. Када је у питању национална безбедност, приступ недозвољеним подацима може да угрози виталне интересе државе. Позитивни и негативни ефекти технолошког развоја информационо–комуникационих технологија у одређеним ситуацијама представљају предност, а у другим рањивост неког система. Међутим, развој информационо–комуникационих технологија и других технологија има далеко више позитивних ефеката по општељудски развој у односу на присутне негативне ефекте. Проблем се решава заштитом пословних информација од неовлашћеног приступа, применом и развојем програма заштите и омогућавањем селективног приступа информацијама од стране запослених лица у оквиру пословног субјекта.

Утицаји науке и технолошког развоја, посебно информационо–комуникационих технологија, омогућили су многоструко бржи привредни развој и убрзали су процес глобализације. Конкретно, масовна употреба мобилних телефона омогућила је бржу комуникацију међу корисницима без обзира на њихову локацију на Земаљској кугли. Интернет је постао један од основних видова комуникације међу људима широм света. С обзиром да омогућава реализацију пословних активности на даљину, интернет је заслужан за обављање многобројних трговинских, маркетиншких, брокерских и других врста пословања. Могло би се рећи да је

простор у којем се склапају пословни договори виртуелан, што не значи да промет производа и услуга није стваран. Степен виртуелности ограничен је од стране увида администратора којем је омогућено да прати пословне трансакције, контролише, а у одређеним ситуацијама и да мења исход пословања.

Уградња уређаја за даљинско праћење (Global Position System — GPS) у аутомобиле или у мобилне телефоне у циљу њиховог лакшег проналажења у случају крађе, омогућава произвођачу прецизну информацију о кретању појединца који их користи. Поставља се питање колико су такве ствари и у којој мери неопходне просечном човеку. Да ли су у питању стварне потребе и захтеви човека или је потреба наметнута од стране носиоца процеса глобализације. Једно је извесно, процес глобализације свакако без научно-технолошког развоја не би постигао ефекте које сада бележи. (Првуловић, 2010)

2.1.2. Информационо–комуникационе технологије (ИКТ)

Информационо–комуникационе технологије — ИКТ (енгл. *Information Communitation Tehnology* — IT) су технологије које користе рачунаре за прикупљање, обраду, чување, заштиту и *пренос* информација. Тешко је у модерном друштву, које прати висок степен технолошког развоја, замислити живот без њихове примене. Појмови ИТ и ИКТ су нераздвојиви, јер је готово незамисливо да се врши анализа употребе рачунара без његовог повезивања у мрежне системе. Високо развијене и развијене земље употребљавају ИКТ у обиму који је одавно премашио спознају просечног човека и његов однос према употреби рачунара. Овде се не ради само о економском аспекту употребе ИКТ у циљу повећања производње и продуктивности или о коришћењу ИКТ у циљу маркетинга и промоције, већ о употреби напредних рачунарских технологија које омогућавају лакше свакодневно

функционисање друштва и човека као појединца[1]. Коришћењем мрежних апликација које омогућавају online куповину или подизање личних докумената, живот човека је добио нову димензију. Стратегија развоја информационог друштва у Републици Србији наглашава да мотор развоја информационог друштва чине: развијено е–пословање, укључујући е–управу, е–трговину, е–правосуђе, е–здравље и е–образовање (Службени лист, 51/2010).

Процес развоја ИКТ–а није изузет од свеукупног напретка човечанства и научно технолошког прогреса као његовог саставног дела. Развој науке је развојем ИКТ–а постао далеко бржи, као и само ширење и унапређивање нових технологија. Основне предности ИКТ–а у односу на традиционални начин комуникација су: време, ажурност и брзо реаговање. Анализирајући аспект времена, довољно је упоредити некадашње комуникације путем размене писама и размену података употребом email–а. Систематизација и ажурност електронских података су на много вишем нивоу, а коришћењем адекватних програмских пакета и употребом претраживача, електронски складиштени подаци су доступни кориснику за неколико делова секунде. Ова чињеница је изузетно важна када су потребе за брзим реаговањем од стране корисника такве да је време лимитирајући фактор успеха активности. (Јаворовић и Биланџић, 2007) То посебно долази до изражаја у великим пословним и државним системима где од брзине реаговања понекад зависе и животи људи.

Посматрајући економски аспект развоја информационих система може се извести закључак да је информатичко доба наступило 80–их година прошлог века, када је окончано такозвано индустријско доба. То је време

[1] Према истраживању Гемиуса (лат. Gemius), компаније која се бави интернет истраживањима, 3 милиона грађана у Србији узраста од 15 година и више користи интернет. Око 19 % корисника интернета купује робу преко наведене мреже неколико пута годишње, док 57 % корисника скоро никада или веома ретко купује робу преко интернета. Када се узме у обзир образовна структура, интернет највише користе грађани са четворогодишњом средњом школом, вишом школом и факултетом, нешто мање од тога су основци а најмање грађани са завршеном трогодишњом средњом школом. E–banking је спремно да користи 28 % испитаника, док већина (72 %) није заинтересована за наведену услугу. (http://pt.uninp.edu.rs/wp-content/uploads/2014/01/INFORMACIONE-TEHNOLOGIJE-I-SAVREMENI-TRENDOVI-POSLOVANJA-U-SRBIJI.pdf)

када је окончана традиционална економија и када почиње развој нове економије. Ако узмемо у обзир да је основна предност нове економије у односу на традиционалну, глобализација као њен главни тренд, виртуелност, дигитализација и доминантност услуга у односу на производне процесе, онда може да се закључи да је развој ИКТ–а врло тесно повезан са свеукупним економским развојем савременог друштва. Јуричић сматра да је глобализација претварање Земљине кугле у јединствен економски простор, тако да су појмови међународни маркетинг, финансије, економија и политике замењене префиксом глобални (Јуричић, 2013: 117-128).

Трендови развоја ИКТ–а у свету у наредном периоду могли би се поделити у следеће категорије:

- Развој бежичног интернета у неразвијеним и земљама у развоју уз одговарајућу едукацију корисника о могућностима угрожавања;
- Развој преносивих рачунара и њихово коришћење у свим деловима света које насељава људска популација;
- Развој примене ИКТ–а у систему здравствене заштите уз очување приватности и поверљивости личних здравствених података;
- Побољшање могућности бржег приступа информацијама кроз развој програма за брзо претраживање и укрштање више параметара, што омогућује бржи проток информација и нуди кориснику могућност за брзо (ситуационо) реаговање;
- Усвајање јединствених идентификационих ознака којим би се пратио транспорт робе у транзиту чиме би се систем безбедности подигао на виши ниво;
- Примена биометрије у циљу побољшања безбедности путника на аеродрому и другим местима на којима је присутно веће окупљање људи;
- Покривеност насељених делова Земљине кугле камерама у циљу превентивног деловања и откривања починилаца дела усмерених против безбедности људи;

- Развој роботских система који ће замењивати активност људи у услужним друштвеним делатностима;
- Развој мобилне телефоније;
- Уградња имплатаната којим ће се утицати на мишљење и поступке појединаца који са аспекта безбедности представљају претњу по безбедност људи.

2.2. НАЦИОНАЛНА ДРЖАВА У ПРОЦЕСУ ГЛОБАЛИЗАЦИЈЕ

Актуелна питања, која се односе на положај државе у условима глобализације, јесу да ли је држава изгубила своју моћ и суверенитет и да ли је њен опстанак угрожен процесом глобализације. Опстанак националних држава се још увек не доводи у питање, али би се са оправдањем могло констатовати да је њихов суверенитет делимично ограничен. Исто тако, улазак националних држава у интеграције, као што је на пример Европска унија (ЕУ), подразумева да се држава добровољно одриче дела суверенитета у циљу постизања општих, али и сопствених интереса, што наведени проблем ставља у потпуно другу димензију.

Другу половину 20. века обележила је експанзија међудржавног повезивања, али и експанзија мрежног повезивања појединаца, компанија, пословних система. Развој интернета одвијао се уз наглашавање ефикасности и слободе, међутим растуће везивање за интернет није било праћено напорима да се он очува безбедним. Безбедност у сајбер простору обухвата изазове који превазилазе државне границе, док одговори на њих остају претежно у националним видокрузима, који су, очигледно, недовољни. Неразумевање проблема и недовољно развијене техничке и системске способности наглашавају потребу квалитетнијег реаговања. Поред тога, проблеми демократског управљања, нарочито кад је реч о питањима контроле и транспарентности, не изазивају довољну пажњу јавности. Државе су, разуме се, нарочито забринуте за националну безбедност и због ризика да државни или недржавни актери или групе украду, промене, униште или на

неки други начин компромитују кључне информације и информационе инфраструктуре. У том смислу, за националну безбедност је нарочито значајан проблем ометања телекомуникација, преноса електричне енергије, функционисања енергетских цевовода, рафинерија, финансијских мрежа, здравствених система и других служби од посебне националне важности. (Buckland et al., 2010)

2.2.1. Транснационалне привредне целине

Транснационализација делатности у привреди представља најзначајнији елеменат развоја глобалне светске економије у 21. веку. Транснационализација је убрзала прожимање различитих система, култура и тржишта националних држава, што је привредним целинама које делују изван своје матичне државе омогућило квалитетније пословање и стицање већег профита.

По дефиницији, транснационална корпорација (ТНК; енгл. TNC) је корпорација која послује или је регистрована у више од једне земље. Корпорација има своје седиште у матичној држави, али њено пословање је присутно и у другим земљама које о резултатима пословања подносе извештај седишту корпорације. Суштина транснационалног пословања јесте у смањењу трошкова који произилазе из проширеног нивоа производње и повећања учешћа на тржишту. Иако културне баријере могу да проузрокују непредвидиве препреке, са искусним особљем и квалитетним техничким експертизама, могуће је стратешко пословање пренети у различите земље. (Encyclopedia Britannica) Поред растуће глобалне економске моћи ТНК у савременим међународним односима, наведене привредне целине све више испољавају утицај и на политичку, културну па, у неким сегментима, и на војну моћ појединих националних држава. Управо таква чињеница је проузроковала да присуство ТНК у неким државама, најчешће неразвијеним, буде окарактерисано као лоше по одржање националне државе. Ако при том узмемо у обзир да поједине транснационалне компаније поседују буџет који

се мери десетинама или стотинама милијарди долара, што премашује целокупан буџет појединих држава, таква бојазан се може сматрати оправданом.

У наступима на страним тржиштима ТНК имају неколико фаза: извоз производа, производња у иностранству и транснационална експанзија. (Петковић, 2009: 34) У првој фази, транснационална компанија оснива представништва или филијале у другој држави у циљу лакше дистрибуције властитих или других врста производа. У овој фази ТНК увозе поједине производе у компонентама које у земљи домаћина склапају и дистрибуирају на тржиште. Друга фаза наступа ТНК представља оснивање производних капацитета у земљи домаћина или продају лиценци (франшизинг) којима се обезбеђује присуство на неком тржишту без директног улагања. Мотив за овакво деловање може да буде јефтина радна снага, високе царинске стопе земље домаћина као и регионалне интеграције којима је земља домаћина већ приступила, а интересантне су за улагање од стране ТНК. Трећа и најважнија фаза наступа ТНК представља експлоатацију и прераду сировина тамо где је њихова цена најповољнија, затим њихову прераду и продају на местима на којима она подразумева најмање трошкове чиме се остварује највећи профит. Маркетиншким активностима производи се у одређеној мери прилагођавају укусима циљне потрошачке групе, међутим данас се све више укуси потрошача прилагођавају већ постојећим производима ТНК. У таквим ситуацијама ТНК, избегавајући диверзификацију производа, стиче многоструко већи профит[2].

Фактори који су омогућили раст ТНК у свету могли би се поделити у неколико категорија: (према UNCTAD, World Investment Report, 2016, 2. март)

- динамичан раст светске привреде;
- научно–технолошки прогрес;
- либерализација светске трговине;
- либерализација међународне размене услуга;

[2] 500 највећих ТНК контролише 42 % светског богатства са тенденцијом раста (Ћатовић и сар., 2013: 139-150).

- стандардизација у различитим областима усвојена од стране већине земаља у свету;
- конвертибилност великог броја валута;
- приватизација;
- унификација међународног привредног права.

Иако широм света постоји више покрета и организација које неблагонаклоно посматрају долазак транснационалних компанија на тржиште њихових држава, ТНК имају и позитивне ефекте на привредни развој неразвијених земаља. ТНК својим присуством и учешћем у привреди једне земље уносе свежи капитал без којег је привредни раст незамислив, доносе нове технологије, доприносе повећању запослености земље домаћина отварањем нових производних капацитета и повећањем радних места. Као крајњи, али не и најмање важан ефекат присуства ТНК у некој држави, јесте пораст извоза те државе и позитиван утицај на њен спољнотрговински биланс.

У табели бр. 1 дат је приказ десет највећих транснационалних компанија по укупном приходу у 2014. години.

Табела бр. 1: Приходи десет највећих компанија у свету у 2014. години

Ред. бр.	**Компанија**	**Држава**	**Делатност**	**Приход у доларима (милијарде)**
1.	Walmart	САД	Малопродаја	$476.3
2.	Royal Dutch Shell	Холандија Велика Британија	Бензин	$459.6
3.	Sinopec	Кина	Бензин	$457.2
4.	China National Petroleum Corporation	Кина	Бензин	$432.0
5.	ExxonMobil	САД	Бензин	$407.7
6.	BP	Велика Британија	Бензин	$396.2
7.	State Grid Corporation of China	Кина	Енергија	$333.4
8.	Volkswagen	Немачка	Аутомобили	$261.5
9.	Toyota	Јапан	Аутомобили	$256.5
10.	Glencore	Швајцарска	Роба	$232.7

(http://fortune.com/global500/, 2016, 3. април)

У циљу заштите од негативних ефеката деловања ТНК, националне државе доносе прописе, односно правила којим се уређује режим пословања са иностранством. То су по правилу спољнотрговински прописи, односно правила којима се уређује режим пословања са иностранством, али и прописи о девизном и царинском режиму. Овим прописима се уређују општи и посебни услови које субјекти међународног пословања морају испунити, са аспекта јавног поретка одређене државе, да би уопште могли да ступе у послове са елементом из иностранства. (Вукадиновић, 2006)

Нови односи моћи, нове технологије, као и нови типови финансијских инструмената, знатно отежавају економску улогу државе у привредном тржишном систему, односно знатно отежавају увођење ефективне контроле кретања капитала. Раст и доминација транснационалних компанија чини бескорисним увођење или одржавање трговинских баријера. Процес глобализације, где правила игре намећу велики и моћни, веома је тешко зауставити. (Петровић, 2004: 2)

2.2.2. Регионалне интеграције

Регионална интеграција представља чврсто повезивање земаља у целину у циљу остваривања економских и политичких интереса, те изналажење путева за ефикасну сарадњу привредних субјеката земаља у интеграцији. (Унковић, 2007: 269) Регионалне интеграције су у прошлости биле фокусиране на укидање баријера око слободне трговине, повећање прекограничног кретања људи, робе и новца, контролу регионалних оружаних сукоба, усвајање ставова који се односе на животну средину, климатске промене и миграције људи. Лук Ван Лангенхове (Langenhove, L. V.) истиче да регионалне интеграције треба да испуњавају најмање шест важних функција (према Slocum & Langenhove, 2004: 227-252):

- Јачање трговинских интеграција у региону;
- Стварање одговарајућег окружења за развој приватног сектора;

- Развој инфраструктурних програма за подршку економском расту и регионалним интеграцијама;
- Развој снажних јавних институција и владиног сектора;
- Смањивање социјалних раслојавања и јачање цивилног друштва;
- Јачање мира и безбедности у региону;
- Изградња програма животне средине на регионалном нивоу;
- Јачање регионалне сарадње са осталим регионима у свету.

Прве три функције се односе на економски аспект интеграција. Заједнички именитељ наведеним функцијама је *подизање нивоа привредне ефикасности*. Могло би се закључити да су управо економске интеграције много заступљеније у односу на друге врсте регионалних интеграција. Поред економских интеграција, изузетно важну улогу у савременим друштвеним односима имају безбедносне интеграције које долазе до изражаја посебно у условима и у регионима у којима се нарушава мир и безбедност људи. Основа и суштина повезивања националних држава у безбедносне интеграције јесте заједничко деловање у новонасталим глобализацијским условима, против носиоца екстремистичке, терористичке и других врста субверзивне делатности, чијом активношћу се доводе у питање основна људска права и слободе људи. Регионалне интеграције би у безбедносном смислу требало да омогуће бржи и квалитетнији проток информација о непријатељским активностима терористичких група које делују на транснационалном нивоу. Управо због такве делатности носиоца субверзивних делатности, потребно је развијати међудржавну сарадњу између земаља у региону. Заједничким снагама и капацитетима, безбедност националних држава у условима глобализације, подиже се на виши ниво. Једна од највећих организација која делује по наведеном принципу јесте НАТО пакт (енгл. *North Atlantic Treaty Organisation* — NATO). Земље чланице НАТО-а су приказане на слици бр.1.

Слика бр. 1: Земље чланице НАТО–а
(https://europeandisarmament.wordpress.com/maps/nato-countries/)

Распадом Варшавског уговора, једине организације која је представљала противтежу НАТО–у, изгубила се равноправност два света у доношењу политичких, војних и других одлука. Данас се поставља питање оправданости или неоправданости приступања великим војним савезима од стране малих и неразвијених земаља које нису у могућности да се самостално супротставе озбиљнијим терористичким и другим безбедносним изазовима и претњама. Регионалне интеграције и глобализација тиме постају феномени који изазвају промену глобалног поретка заснованог на суверенитету националних држава.

Често се безбедносне интеграције тумаче као апсолутна сарадња међу државама чланицама са максимално указаним поверењем и отвореним приступом ка њиховом решавању. Безбедносна пракса је показала другачије резултате. Обавештајна делатност држава унутар савеза се често не смањује, већ се, напротив, појачава. Упоредно са тим, појачава се и контраобавештајна заштита поверљивих информација, иако је споразумима дефинисано да је приступ заштићеним информацијама од стране неовлашћених лица унутар савеза строго кажњив и да ће лица, носиоци таквих активности, сносити одговарајуће законске и дисциплинске последице. Интеграција, дакле, не пружа у потпуности отворен и равноправан приступ информацијама од значаја свим чланицама, што посебно компликује ситуацију око сарадње обавештајно–безбедносних структура.

Ситуација око економских интеграција је на први поглед једноставнија, међутим треба бити свестан чињенице да равноправност

између великих и малих држава у таквим интеграцијама не постоји.[3] Пример објашњен у фусноти јасно указује колико су интеграције важне у области економског пословања, али и да је равноправност међу чланицама интеграција дискутабилна. Само са прецизно усвојеним и прихваћеним споразумима свих страна међусобни пословни односи могу да се развијају на позитивној основи. (Dunkley, 2004)

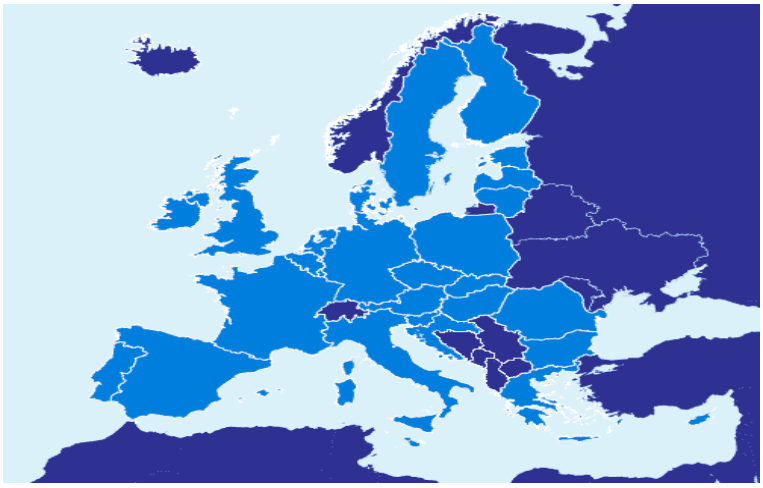
Економске интеграције су свој процват доживеле непосредно после окончања Другог светског рата. Разлог томе је покушај националних влада да у што краћем року санирају настале материјалне штете које су се мериле хиљадама милијарди долара. Највећи део регионалних споразума се односио на формирање слободне трговине међу земљама потписницама. Један, мањи део, односио се на формирање царинске уније, а остало су представљали билатерални и мултилатерални споразуми. Суштина економских интеграција је у повезивању тржишта, подели рада и координацији економских политика чијим остваривањем земље чланице постају значајан фактор развоја савремене светске привреде и међународне економске сарадње.

Организација за европску економску сарадњу (енгл. *The Organisation for European Economic Co–operation* — OEEC; https://www.oecd.org/, 2014, 5. фебруар) основана је 1948. године. Седиште организације је било у Паризу (Француска). Године 1961, новоформирана Организација за економску сарадњу и развој (енгл. *Organisation for Economic Co–operation and Development* — OECD), чији су чланови поред европских држава постале САД, Канада, Јапан и Аустралија, преузела је активности којима се до тада бавила OEEC, а која је

[3] Исказани пример таквог неравноправног односа који је Светску трговинску организацију (СТО) довео у питање, је случај „рата око банана" између САД и Француске. Године 1997. ЕУ на предлог Француске уводи обавезне квоте за увоз банана из САД. Званичници ЕУ праве билатералне споразуме са водећим светским извозницима ове врсте воћа, између осталог са Костариком и Колумбијом. Власник транснационалне компаније „Чикита" (која се између осталог бави прометом и продајом банана), Карл Линднер, преко својих веза у високим круговима САД, обезбеђује подршку да се ЕУ због наведеног поступка уведу економске санкције. СТО се у овом случају у потпуности ставио на страну америчке транснационалне компаније и донео пресуду којом се поступци званичника ЕУ сматрају дискриминаторским и незаконитим. Иако је ЕУ званично одбила да измени режим увоза ове врсте производа, СТО је подржала САД да наметне додатне таксе на широки асортиман производа из ЕУ, на основу чега је створен буџетски прилив у висини од 200 милиона долара. (Првуловић, 2010: 238).

престала званично да постоји. Кроз активност ОЕЕС, САД је чланицама организације додељивала новчана средства у висини од око 14 милијарди долара. Десети део наведене суме је био у виду зајмова, а остатак је дониран у виду поклона и хране, одеће и грађевинског материјала. Поред хуманитарног карактера, САД су кроз активности ОЕЕС прокламовале своје политичке идеје и заступале своје економске интересе. Следећа фаза, након оснивања ОЕЕЦ, подразумевала је интеграцију западноевропских држава, али није спроведена због размимоилажења Енглеске и Француске. Паралелно са оснивањем ОЕЕС, социјалистичке земље у Европи су основале Савез за узајамну економску помоћ, (рус. *Совет экономической взаимопомощи* — СЭВ) управо како би избегле утицај САД–а на њихов, пре свега, политички статус. СЕВ је каналисао спољну трговину земаља чланица, тако да се више од пола трговинских трансакција одвијало унутар савеза.

Године 1957. формирана је Европска економска заједница коју је чинило шест држава, а 1960. године Европско удружење слободне трговине (енгл. *European Free Trade Associati*on — EFTA; http://www.efta.int/about-efta/history, 2014, 8. Фебруар). Назив који данас носи Европска унија (ЕУ; енгл. *European Unio*n — EU) је добила 1992. године. Данас ЕУ има своје органе: Европски парламент, Европску комисију, Европски савет, Савет министара и Европски савет председника. ЕУ за сада не обједињује области спољне политике, одбране, безбедности, образовања и културе њених чланица. Највећи напредак, када говоримо о наведеној организацији, постигнут је у области економије и то усвајањем монетарне, фискалне и спољнотрговинске политике, научно–технолошке политике, политике заштите животне средине и заштите потрошача њених чланица. Република Србија је започела преговоре за придруживање Европској Унији у јануару 2014. године. Данас ЕУ има 28 држава чланица, а последња земља која је приступила интеграцији је Хрватска, у јулу 2013. године. На слици бр.2 су приказане земље које узимају чланство у ЕУ.



Слика бр. 2: Карта земаља чланица ЕУ
(http://ec.europa.eu/ecip/information_resources/links/index_en.htm)

Услови за придруживање Европској Унији могли би се поделити у три целине: правне и институционалне промене и усклађивање прописа са прописима ЕУ, јачање демократије и људских права и економска стабилизација и конкурентност.

Од осталих регионалних интеграција потребно је издвојити Централноевропску зону слободне трговине (енгл. *Central European Free Trade Association* — CEFTA; http://www.cefta.int/, 2014, 8. фебруар). Организација је основана 1992. године у Кракову (Пољска). Званичници ЕУ подржавају ову врсту сарадње пошто су Словенија, Румунија, Бугарска и Хрватска пре приступања ЕУ биле чланице CEFTA–е. Још један од разлога подршке овој организацији представља и усвајање европских стандарда који се пре свега односе на спољнотрговинско пословање земаља чланица. Споразум подразумева либерализацију царинских стопа код великог дела индустријских и пољопривредних производа. Треба истаћи да је пољопривреда једна од најразвијенијих привредних грана у земљама члановима CEFTA–е.

Чланице ове организације (слика бр. 3) су Албанија, Босна и Херцеговина, Македонија, Молдавија, Црна Гора, Србија и УНМИК/Косово као царинска територија у складу са резолуцијом СБ ОУН бр.1244 (http://www.pks.rs/PoslovnoOkruzenje.aspx?id=794&p=1, 2014, 2. фебруар).

Слика бр. 3: Карта земаља чланица ЦЕФТА–е
(https://en.wikipedia.org/wiki/Central_European_Free_Trade_Agreement)

Од великих регионалних интеграција још би требало поменути Северноамерички споразум о слободној трговини (енгл. *The North American Free Trade Agreement* — NAFTA; https://www.nafta-sec-alena.org/Home/About-the-NAFTA-Secretariat, 2014, 9. фебруар) која је основана 1993. године, а истој су приступиле следеће земље чланице: САД, Канада и Мексико. Такође, Удружење југоисточних азијских земаља (енгл. *Association of Southeast Asian Nations* — ASEAN; http://asean.org/, 2014, 9. фебруар), које је основано не само као економска него, за разлику од већ набројаних, као безбедносна и културна заједница.

3. БЕЗБЕДНОСНИ ПРОБЛЕМИ САВРЕМЕНОГ СВЕТА

Вестфалски мир (1648) је означио завршетак религијских ратова и отворио нове сукобе у којима велике силе стално покушавају да прошире своју моћ и утицај. Вестфалски мир је установио систем суверених држава као главних међународних субјеката. Адам Вотсон (Adam Watson) је у својим радовма описивао како вестфалски систем доприноси развоју модерне дипломатије. (Watson, 1982). На првом месту, то је увођење концепта каријерног дипломате, који је развијао специфичне вештине неопходне за ефективно извршавање обавеза. Професионалне дипломате припадале су неформалној групи акредитованих дипломата са дворова широм Европе. Они су следили заједничке циљеве, имали су заједничке привилегије и имунитете, предност у размени информација, посебно код савезничких држава и одржавали су добре односе, чак и када су њихове земље биле у завади. Такође, вестфалским миром је дошло до успостављања дипломатског кора као сталног тела и установљен је систем конгреса којим су се завршавали и регулисали сукоби и ратови.

Може се закључити да се утемељивање територијалног суверенитета везује за Вастфалски мир. Период од 1648. до 1915. године је период у којем суверене државе успостављају дипломатске односе, минимално сарађују, а своје несугласице решавају најчешће силом. Јаз који постоји између начелног признања да су државе једнаке пред законом и стварне асиметрије моћи подстакао је стварање разних савеза и уговора између сила које су тежиле да обликују међународни поредак у своју корист. Овај „систем споразумевања“ после Наполеонових ратова јесте покушај да се створи нови систем безбедности, да се успостави „равнотежа моћи“. Равнотежа моћи, уграђена у

систем споразумевања, тежила је да одржи мрежу великих држава и царства. (Хелд, 1997: 224).

Један од безбедносних изазова који се јавља у новијој историји је наступио после окончања биполаризма, што је на својеврстан начин подстакло и убрзало процес глобализације. Овом процесу је претходио пад комунизма и слабљење источног блока. Актуелна тежња Руске Федерације да заузме место некадашњој противтежи западном савезу је очигледна и несмањеног интензитета, а улога ове државе у борби против Исламске државе иде у прилог претходној тврдњи. Улога појединих великих сила у форми очувања глобалне безбедности наилази на оправдање у борби против глобалног тероризма, што је данас посебно изражено у борби против такозване Исламске државе. Терористички напади су данас погодили део европских земаља које се супротстављају настајању Исламске државе и које су, у целу ситуацију, укључене на директан или индиректан начин. У циљу спречавања злонамерних активности терористичких колективитета, пресудна је улога обавештајних и контраобавештајних служби које су задужене за прикупљање података и извршавање безбедносних процена.

3.1. ИЗВОРИ УГРОЖАВАЊА БЕЗБЕДНОСТИ

У поглављу ће бити анализирано неколико извора угрожавања, а могу да се ставе у контекст теме дисертације:

- Тероризам
- Организовани криминал
    - Трговина људима
    - Трговина оружјем
    - Прање новца
- Оружје за масовно уништавање
- Неравномеран економски развој
- Енергетска нестабилност

- Демографска експанзија и квалитет животне средине
- Еколошка неодрживост
- Локални етнички сукоби
- Шпијунажа

3.1.1. Тероризам

Сам појам *тероризма* је проблематичан, пошто не постоји дефиниција која би била свеважећа и општеприхваћена. Проблем се додатно усложњава не само због неслагања научника око терминолошког одређења већ и због вишеструких интерпретација овог појма од стране различитих држава које се у тумачењу руководе сопственим интересима. У циљу дефинисања овог проблема пожељно је поћи од појма *терор*. Терор (лат. *terror, terroric — страх, ужас*) је планирано ширење страха и ужаса кроз спровођење насиља како би се људи учинили покорнима и послушнима. Димитријевић (1982) сматра да кад год за примену насиља није унапред одређена казна за непожељно понашање, а насиље у виду кажњавања није више само одвраћање потенцијалних преступника које се не односи ни на кога другог, почиње терор. Према Симеуновићу „тероризам је сложен облик организованог, групног и ређе индивидуалног или институционалног политичког насиља обележен не само застрашујућим брахијално физичким и психолошким, већ и софистицирано–технолошким методама политичке борбе којима се обично у време политичких и економских криза, а ретко и у условима остварене економске и политичке стабилности једног друштва системски покушавају остварити‘велики циљеви’ на морбидно спектакуларан начин, а непримерено датим условима, пре свега друштвеној ситуацији и историјским могућностима оних који га као политичку стратегију упражњавају“ (Симеуновић, 2000: 122).

Милошевић закључује да „тероризам представља плански акт насиља или претња применом насиља коју предузимају одређене друштвене групе с

циљем да утичу на друштвени и политички живот одређене заједнице, односно које су усмерене на освајање или очување власти“ (Милошевић 2005: 9).

Дефиниција тероризма америчких аутора је добро прихваћена у стручним круговима у свету. Један од њих је Брајан Џенкинс (Brian Jenkins) који је пре тридесет година дао једну од најбољих дефиниција тероризма која је и данас актуелна:

„Тероризам је у ствари позориште, где су глумци извршиоци напада и њихове жртве, а публика јавност и власт којима се преноси порука. Страх је незаобилазни и централни елемент терористичке стратегије, која постаје све тајанственија за органе државне заштите. Тероризам је, дакле, насиље усмерено на посматраче. Страх је жељени и намеравани ефекат, а не споредни производ тероризма.“ (Jenkins, 1975: 14)

Из ове дефиниције може да се схвати да је за носиоце терористичке акције битно какав је њен учинак на јавно мњење, а не колико је она жртава донела. Један од значајнијих теоретичара тероризма је Алекс Шмит (Alex P. Schmid) који наводи да је тероризам метод системских аката насиља који извршавају полу(скривени) појединци, групе или припадници власти из идиосинкратских, криминалних или политичких разлога, где за разлику од атентата, директне мете тог насиља нису и главне мете. (http://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1400&context=jil,),2014, 08.mart).

Од домаћих аутора најупечатљивију дефиницију тероризма је дао Димитријевић који наводи да је то „акт физичког насиља чији је предмет изабран тако да изазива јаке психичке реакције, у првом реду страх код ширег круга људи у нади да ће она помоћи да се одржи или промени понашање које је важно за постизање политичког циља, ако такав акт није оправдан општим интересима који су одређени независно од њега и ако није извршен по правилима која се уобичајено примењују на друштвене видове вршења власти“ (Димитријевић, 1982: 122).[4]

[4] О утицају терористичких акција на јавност и на промену власти потврђује терористики напад Ал Каиде који се догодио 2004. године у Мадриду у којем је погинуло 200 људи. Напад

Од међународних докумената који дефинишу тероризам најважнија је резолуција Генералне скупштине Уједињених нација, која је усвојена 1999. године, по којој тероризам чине „терористичка дела и активности усмерене ка поништавању људских права, основних слобода и демократије, претње територијалном интегритету и сигурности држава, дестабилизовање легитимно конституисане владе, угрожавање плуралистичког грађанског друштва и негативан утицај на економски или друштвени развитак држава“ (УН Резолуција 54/164 — људска права и тероризам; http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/54/164, 2014, 6. јул).

Савет Европе је 2002. године усвојио Заједнички став о примени одређених мера у борби против тероризма који даје врло децидну дефиницију терористичког дела, при чему је очигледно да су се аутори потрудили да не изоставе ни најмањи елемент посматране појаве: „Терористичким делом сматраће се једно од следећих намерно учињених дела које, с обзиром на његову природу и околности у којима је настало, може озбиљно оштетити неку државу или међународну организацију, а које је дефинисано као преступ према националном законодавству и почињено са циљем да: 1) озбиљно застраши становништво, 2) неоправдано натера владу, односно међународну организацију, да учини, односно да не учини неко дело или 3) озбиљно дестабилизује или уништи основне политичке, уставне, економске или друштвене структуре неке државе, односно међународне организације тиме што: а) насрне на живот неке особе, што може довести до њене смрти; б) насрне на физички интегритет неке особе; в) отме или узме као таоца; г) доведе до уништења неког државног или јавног објекта, транспортног система инфраструктуре, укључујући и информационе системе, фиксиране платформе у приобалном појасу, неко јавно место или приватни посед, уз велику могућност да угрози људске животе и доведе до знатне економске штете (отме летелицу, брод или неко друго средство

је, по признању организатора терористичког акта, извршен како би се шпанске власти приморале да повуку своје оружане снаге из Ирака. Након извршеног терористичког акта, Шпанци су повукли своје трупе из Ирака, а јавност је на изборима, који су убрзо након тога одржани, осудила тадашњу власт те је на изборима остварила знатно слабије резултате.

намењено превозу путника, произведе, поседује, набави, транспортује, снабдева или користи оружје, експлозиве, односно нуклеарно, биолошко или хемијско оружје као и да врши истраживања у циљу развоја биолошког и хемијског наоружања; ослободи опасне материје или изазива пожаре, експлозије или поплаве које угрожавају људске животе; угрожава или ремети снабдевање водом, струјом или неким другим извором природних ресурса чиме угрожава животе људи; прети да изврши неко од дела наведена од а) до г); руководи терористичком групом; учествује у активностима терористичке групе, укључујући и достављање информација, односно материјалних средстава, на било који начин финансира ту групу, знајући притом да такво учествовање доприноси криминалном деловању“ (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33168, 2016, 3. март).

Мијалковски Милан дефинише тероризам на следећи начин: „Тероризам је смишљено, систематско, противзаконито, специфично, самостално или насиље у оквиру неког облика оружаног сукоба извесног људског колективитета (не–државног, државног или транснационалног), чији су припадници у толикој мери уверени у основаност и оправданост властитих екстремистичких циљева и опседнути мржњом у односу на примарну жртву (крајњег, главног непријатеља) да су одлучни да примене или примењују најгрубљу физичку силу над секундарном (непосредном) жртвом, коју преовладавајуће чине приватна лица — цивили — ради њеног бруталног убиства, привременог и трајног повређивања (сакаћења), киднаповања и психичког злостављања, с намером да изазову (произведу) максималан психолошки ефекат (страх) у односу на примарну жртву (влада земље коју нападају) и принуде је да учини захтеване уступке, који значе остварење крајњег политичког циља конкретног терористичког колективитета.“ (Мијалковски и сар., 2012: 36).

Потребно је напоменути да су терористичке организације изузетно добро организоване и да у њиховој структури постоје целине које имају јасна и конкретна задужења. Организацијом може да руководи једно лице (вођа) или већи број лица која обављају функцију руководећег тима. Ради се о лицима која доносе најважније, такозване стратешке одлуке које се односе на

место, време и начин употребе терористичке организације и ефекат који се жели постићи. Следећи елеменат терористичке организације који је такође изузетно битан за доношење одлука руководећег тима јесте обавештајно–безбедносна целина. Овај део организације се бави прикупљањем сазнања на територији земље домаћина која обрађује, процењује и доставља руководећем тиму. Безбедносна целина овог елемента врши непрекидне провере чланова организације и њихових евентуалних веза са припадницима обавештајно–безбедносних служби. У случајевима откривања таквих појединаца примењују се најбруталнији начини лишавања живота, што уједно служи као опомена и упозорење онима који не буду лојални организацији. Дакле сегменат застрашивања се не примењује само ка жртви напада већ и према унутрашњим деловима организације: према члановима за које се сумња да нису лојални или који показују другу врсту непослушности према руководећем тиму. Следећу целину представља тим за подршку, који поред финансијског дела, терористичкој организацији пружа и сваку другу материјалну и нематеријалну врсту подршке. Ова целина између осталог обезбеђује просторије за смештај чланова организације, аутомобиле који служе за превожење чланова и материјално–техничких средстава која ће бити примењена у некој терористичкој акцији, прикупља новчана средства од финансијера који за такву врсту подршке могу да буду различито мотивисани. Како најчешћи мотив представља политичко неслагање са актуелном влашћу земље домаћина, таквим лицима се обећавају висока места у оквиру нове Владе или чине разне врсте привилегија у њиховом пословању чиме им се обезбеђује монопол на тржишту и стицање високог профита. Следећу целину представља тим за операције и смртоносна дејства. У највећем броју случајева ради се о бившим припадницима специјалних јединица спремним за сваку врсту изазова, који су у директној колизији са актуелном влашћу у држави којој припадају или држави која њиховој држави одузима неко од загарантованих права као што је право суверенитета или територијалног интегритета. Припадници најтврђег језгра организације у терористичким операцијама не презају ни од чега, ни по цену сопственог живота. Једини мотив којим се тада руководе јесте да нанесу што веће

губитке непријатељу и да га доведу до потпуног уништења. Врло често, у оваквим операцијама, терористичке организације користе жене и децу, које снажном индоктринацијом доводе у највише фазе послушности и фанатизма у којима свој живот третирају као средство за постизање виших циљева. Висок ниво индоктринације и фанатизма је највећа претња службама безбедности јер таква индоктринација има форму потпуне непредвидивости и немогућности предвиђања тока догађаја, начина, места и жртве напада.[5]

Први облици тероризма настали су давно о чему сведочи чињеница да је још Аристотел у својим делима оправдавао неку врсту политичког тероризма Оправдавана је ликвидација политичких противника, то јест владара који су својим понашањем према поданицима то и „заслужили". Међутим, тек у 19. веку тероризам постаје учестало средство појединаца за обрачун са политичким неистомишљеницима, тако да се тек од тада може говорити о правим почецима тероризма. Терористички акти у то време углавном су имали карактер појединачног и бивали су усмерени искључиво на носиоца власти, тако да би се могли, на специфичан начин, сматрати моралним у односу на данашње поимање тероризма који за последицу има изазивање што масовнијег нереда и што већег броја жртава, често посве недужних људи и деце.

Тек 60–их година прошлог века долази до експанзије такозваног национал–сепаратистичког екстремизма који у неким државама света, које своје уређење сматрају демократским, и даље тиња и сваког тренутка може да прерасте у озбиљан безбедносни проблем. Циљ терористичких организација јесте промена актуелне власти и довођење нове која одговара мерилима терористичке организације. Употреба силе, бруталност и безобзирност су у таквим случајевима усмерене према сопственом народу. Данас, најозбиљнију терористичку претњу представљају исламски фундаменталисти код којих је присутна највећа доза бруталности икад

[5] Ал Каида, као терористичка организација, свој развој започиње 80–их година 20. века, када САД јачају исту због слабљења тадашњег СССР у рату са Авганистаном. У томе су успели, али само привремено, пошто је Ал Каида, после рата са СССР-ом означила САД као главног непријатеља уједињења свих муслиманских земаља у једну државу. Тренутно се процењује да Ал Каида има око 20.000 чланова широм света.

забележена[6]. У својим нападима они користе најсавременија оружја која захтевају примену специфичних знања и искустава и која условљавају деобу данашњег тероризма у следеће подврсте: био–тероризам, еко–тероризам и сајбер–тероризам. С обзиром на то да су циљеви терористичких акција против њихових непријатеља углавном слични, тј. наношење таквих губитака који ће изазвати високи степен незадовољства код становника довољан да изврши промену актуелне власти, терористичке организације се често повезују и ван граница држава у којима егзистирају. Развој ИКТ–а је свакако повољно утицао на ову околност тако да се данас може говорити о транснационалним терористичким организацијама и активностима.

Многи покрети широм света, који су касније називани терористичким, зачињу своје активности као герилски покрети. Иако у почетку оспоравани и игнорисани, упорношћу и стрпљивом борбом они су успевали да дођу до постављеног циља који је у први мах представљао почетак преговора са представницима власти. У Немачкој се јавља покрет *Црвена Зора*, у Италији *Црвене Бригаде* (ит. *Brigate Rosse*), у Ирској *Ирска Републиканска Армија* (ИРА), у Шпанији *ЕТА* (Слобода за баскијску домовину), на Блиском истоку *Хезболах* (Божја партија) и *Хамас* (Исламски покрет отпора). Ради остваривања својих циљева терористичке организације користе различита средства: отмице авиона, узимање талаца, подметање бомби и сл, што их доводи у везу са деловањем организованих криминалних група. Ипак, постоји основна и суштинска разлика између ових организација, а огледа се у њиховој мотивацији. Док су организоване криминалне групе мотивисане искључиво новцем, терористичке организације су мотивисане вишим циљевима који могу бити политички, идеолошки и религијски. Самим тим, много је теже предвидети активности терористичких организација. Идеолошка посвећеност организацији је у великом броју случајева толико изражена да је у контраобавештајном смислу тешко применити мере којим би се испољени фанатизам неутралисао и спречио, јер он не познаје границе људске милосрдности и толеранције. У том смислу Купер (Cooper) сматра да су у

[6] Одсецање глава страним држављанима, деца самоубице итд.

психолошком смислу „терористи људи који не могу прихватити живот у несавршеном свету“ (Cooper, 1978: 26), што на неки начин појашњава претходно изведени закључак. Уколико томе додамо да је за религијски мотивисаног терористу смрт почетак новог живота, а не његов крај, онда постаје сасвим јасно колико је тешка мисија спречавања деловања таквих јединки у нашем окружењу.

У циљу одбране од тероризма, државе данас предузимају одговарајуће мере и активности које су прописане и обавезујуће за све њене институције и друштвене субјекте. Држава доноси низ закона којима се уређују права и обавезе државних институција и органа који се баве противтерористичким делатностима, али и законе који прописују санкције за починиоце кривичних дела у вези са тероризмом.

Према мишљењу Мијалковског садржаји противтерористчке стратегије се могу разврстати у три категорије: превентивни, офанзивни и дефанзивни (Мијалковски и сар., 2012: 99-106):

- Превентивна делатност је изузетно важна, јер се иста предузима правовремено док терористичка акција још увек није доживела своју кулиминацију. У превентивној фази, најинтензивнији је рад обавештајно–безбедносних служби потенцијалне земље напада у којем се прикупљају сазнања о финансијерима терористичке операције, појединцима који на било који начин узимају учешће, а све у циљу „пресецања“ недозвољене делатности.
- Офанзивна стратегија се реализује у моменту када противтерористчке снаге, на основу обавештајних информација о локацијама терористичких колективитета, предузимају мере на њиховом онеспособљавању и потпуној елиминацији.
- Дефанзивни садржаји противтерористичке стратегије наступају у условима када је држава доживела изненађење од стране терористичке организације. Ради се о привременој дефанзиви, која након консолидације сопствених ресурса прелази у офанзиву до потпуне елиминације извршиоца терористичког акта.

Дакле сви елементи државе који учествују у противтерористичким активностима имају своје место и улогу у систему одбране од такве врсте претње. Ипак, намеће се закључак да је најзначајнији обавештајно–безбедносни сегмент будући да је његов задатак да доносиоцу одлука, државном руководству, правовремено пружи сазнања о планираним мерама руководећег тима терористичке организације, како би офанзивним деловањем приотиветроористичких снага непријатељ био спречен да учини дело терористичког акта и по могућству у потпуности био онеспособљен за такве и сличне делатности у будућности.

Када се ради о Републици Србији, снаге за одбрану од тероризма се могу поделити на руководећи и на извршни или оперативни сегмент ових снага. Руководећи сегмент представља Савет за националну безбедност, којим руководи Председник Републике Србије. Оперативни сегмент противтерористичке делатности представљају снаге за превентивну делатност (БИА – *Безбедносно информативна агенција*, ВБА – *Војнобезбедносна агенција* и ВОА – *Војнообавештајна агенција*) и снаге за офанзивно деловање (САЈ – *Специјална антитерористичка јединица* и Жандармерија - МУП Републике Србије, Специјална бригада Војске Србије).

3.1.2. Организовани криминал

У актуелним међународним околностима криминал се јавља и испољава у готово свим облицима друштвене делатности, те самим тим представља озбиљну претњу по безбедност друштва и заједнице. О организованом криминалитету у ширем смислу може се говорити увек када одређене криминалне делатности обавља група људи. У ужем смислу, организовани криминалитет поред постојања групе криминалаца, подразумева још неке услове и то: постојање (чврше или еластичније) криминалне организације са јасном поделом посла између чланова, организовање континуиране привредне (легалне и нелегалне) делатности усмерене на стицање профита, употреба (или претња) насиља као средства за

постизање циљева, контакте са полицијом, правосуђем и извршном влашћу засноване на њиховом корумпирању ради обезбеђења политичког имунитета од кривичног гоњења (Игњатовић 1988: 25).

Специфични, уједно и најопаснији облик криминала у савременом свету представља организовани криминал, који је данас предмет проучавања експерата из разних научних дисциплина.[7]

Око дефинисања појма *организованог криминала* постоје и данас велике полемике. Једна од општеприхваћених јесте Албанезеова (Albanese J. S.) дефиниција: „Организовани криминал је трајан криминални подухват који се рационално обавља ради профита од нелегалних активности. Његово трајно постојање одржава се коришћењем силе, претњама, контролом монопола, и/или корумпирањем јавних званичника." (Albanese, 2000: 409). Елиот (Eliot, M. A.) сматра да организовани криминалитет у свом садржају, поред организованости, планирања, поделе задатака, дисциплине и одговорности унутар криминалне организације чији је циљ остваривање добити и профита, обухвата и одређену везу са државом и појединим њеним органима и то у виду сарадње органа који примењују закон са онима који га не поштују и желе да га изиграју. (Eliot, 1962: 114)

С обзиром на то да се дефиниција и одређење организованог криминала у свету разликује од државе до државе и да у међународним институцијама не постоје јасне и прецизне одредбе према овој врсти друштвене опасности, могло би се рећи да такав приступ погодује носиоцима ових делатности. Узимајући у обзир да су и законске одредбе у вези организованог криминала подељене и неунифициране, носиоци овакве делатности користе поменуте околности и проналазе такозване „рупе" у законима како би спроводили своје активности.

У Републици Србији појам организованог криминала је дефинисан у Закону о кривичном поступку, Кривичном законику и Закону о организацији

[7] Израз *организовани криминал* први пут је употребљен почетком 18. века у Енглеској, а односио се на делатност организоване банде лопова којом је руководио Џонатан Вајлд (Johnatan Wild) и која је деловала тако што је вршила крађу ствари, а затим их „проналазила" и уз новчану надокнаду враћала њеним власницима. Специфичност ове банде била је у томе што је неоткупљене ствари продавала ван граница матичне државе, а све то уз знање тадашњег енглеског краља Џорџа I. (Shmalleger, 1996: 348)

и надлежности државних органа у сузбијању организованог криминала, корупције и других посебно тешких кривичних дела. Закон о кривичном поступку (Службени гласник Републике Србије, 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014) дефинише да се организовани криминал односи на случајеве постојања основане сумње да је кривично дело резултат деловања три или више лица удружених у криминалну групу која врши кривична дела ради стицања добити или моћи, када су, поред тога, испуњена још најмање три од следећих услова: да је сваки члан криминалне организације, односно криминалне групе имао унапред одређени, односно очигледно одредиви задатак или улогу, да је делатност криминалне организације планирана на дуже време или за неограничени временски период, да се делатност организације заснива на примени одређених правила унутрашње контроле и дисциплине чланова, да се делатност организације планира и врши у међународним оквирима, да се у вршењу делатности примењују насиље или застрашивање или да постоји спремност за њихову примену, да се у вршењу делатности користе привредне или пословне структуре, да се користи прање новца или незаконито стечене добити, да постоји утицај организације или њеног дела на политичку власт, средства јавног информисања, законодавну, извршну или судску власт или на друге важне друштвене или економске чиниоце. Закон о организацији и надлежности државних органа у сузбијању организованог криминала, корупције и других посебно тешких кривичних дела (Службени гласник Републике Србије, 42/2002, 27/2003, 39/2003, 67/2003, 29/2004, 58/2004, — др. закон 45/2005, 61/2005, 72/2009, 72/2011, — др. закон 101/2011, — др. закон 32/2013) дефинише организовани криминал као вршење кривичних дела организоване криминалне групе или њених припадника. Под организованом криминалном групом подразумева се група од три или више лица, која постоји одређено време и делује споразумно у циљу вршења једног или више кривичних дела за која је прописана казна затвора од четири године или тежа казна, ради стицања, посредно или непосредно, финансијске или друге користи.

Један од истакнутијих домаћих аутора који се бави овим феноменом, Игњатовић, разврстава организовани криминал на: 1.) Илегалне делатности: рекет, коцкање, трговина дрогом, лихварење, одлагање опасних материја и остале незаконите делатности, 2.) Инфилтрирање у легални бизнис: грађевинарство, тржиште меса, рекетирање у области запошљавања, лажна банкротства и преваре у осигурању, прање новца и 3.) Обављање „прљавих" послова за државу и корумпирање носилаца јавних функција. (Игњатовић 1988: 69-92)

Бошковић под појмом организованог криминалитета подразумева „врсту деликвенције и типологију криминалних појава везану за активност професионалних криминалних организација. То је делатност 'привредног типа' коју врше криминална удружења са строго утврђеном хијерархијом, дисциплином и нормама понашања. Појава се испољава у виду деловања организованих или полуорганизованих група и других облика удруживања, колективног вршења кривичних дела, у спрези са представницима локалне или виших степена државне власти, односно њених органа и институција. Осим тога, носиоци организованог криминалитета могу бити у посредној вези 'пословног односа' са представницима финансијских институција, привредних компанија и политичких странака." (Бошковић, 2002, 129).

Године 2004. организација Уједињених нација доноси конвенцију Уједињених нација против транснационалног организованог криминала, усвојена Резолуцијом Генералне скупштине Уједињених нација 55/25 од 15. новембра 2000. године. Конвенција представља базични инструмент међународног карактера у сфери борбе против транснационалног организованог криминала, а ступила је на снагу 29. септембра 2003. године. Уз Конвенцију су усвојена и три протокола која регулишу транснационални организовани криминал у појединим областима: Протокол о спречавању, сузбијању и кажњавању трговине људским бићима, нарочито женама и децом, Протокол против кријумчарења миграната копном, морем и ваздухом и Протокол против незаконите производње и трговине ватреним оружјем, његовим деловима и муницијом. Да би држава постала уговорница неког од протокола, она мора бити уговорница Конвенције. Република Србија постала

је уговорница Конвенције 6. септембра 2001. године. (https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf, 2016, 4. јул)

Године 2010. организација Уједињених нација UNODC (енгл. *United Nations Office on Drugs and Crime*) доноси извештај у којем се предлаже предузимање координисане акције против прања новца и корупције у циљу супротстављања овим елементима организованог криминала https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA Report 2010 low res.pdf, 2016, 4. јул). Србија се у извештају помиње у деловима о трговини кокаином, хероином, о трговини људима, као и у делу о поседовању ватреног оружја. Извештај указује да криминалне групе сваке године зарађују милијарде долара од трговине дрогом, оружјем, људима, фалсификованом робом, као и од пиратских напада и сајбер криминала. Криминалне радње не представљају претњу само у економском смислу, већ омогућивши криминалцима завидан профит дале су им и моћ да утичу на изборну вољу и битне политичке одлуке. У циљу супротстављања појави организованог криминала, по наведеном извештају, потребно је сучити се са „саучесницима криминала", односно са онима који „покривају" нелегалне активности и перу илегално зарађени новац (адвокати, рачуновође, агенти за некретнине и банкари). У извештају UNODC се такође наводи да је око 400.000 жртви трговине људима у Европи, од чега организатори кријумчарења имају годишњу „зараду" од три милијарде долара. Како се наводи, Европа је тржиште на којем се највише заради од хероина (20 милијарди долара), док је Русија земља која је највећи конзумент те дроге на свету (70 тона). Једна од земаља на рути трговине хероином од Авганистана до Русије и Европе је Србија.

3.1.2.1. Трговина људима

У 19. веку се бележе прве правне основе укидања ропства и од тада у многим земљама света оно постаје забрањено. Иако је, формално, престало да

постоји у свету, евидентно је да су још увек присутни извесни облици ропства у појединим муслиманским земљама, као што је то случај у Авганистану где су жене талибана, такозваних „божијих ратника“, лишене основних људских права.

У данашње време, најчешћи облик злоупотребе људи у ропству представља такозвано проституционо ропство у којем криминалне организације, нажалост, све више користе децу узраста до 12 година. Процењује се да су европски и азијски педофили данас на овај начин у послове проституције увукли око два милиона деце широм света. (Петковић 2009: 240-251) Путеви дроге, користе се и за трговину људима који у овом случају представљају робу коју је потребно присилним путем испоручити из једне државе у другу. За наведене активности, поред класичних отмица, користе се и разне врсте огласа за рад у иностранству, као што су нафтне платформе, чување деце и сл. Жртва трговине људима у тим ситуацијама не слути каква је судбина очекује, а обично се заврши као ропски однос у којем будући власник експлоатише жртву сексуално или радно, или и једно и друго. Зарада од ових нелегалних делатности износи неколико милијарди евра, тако да се може слободно рећи да је трговина људима једна од најуноснијих врста организованог криминала. Жртве се транспортују у своја одредишта на разне начине, од посебних скривених места у средствима превоза, до ангажовања туристичких тура у којима се налази једна жртва или више њих. Многе од жртава на послетку бивају подвргнуте захватима вађења органа, који се касније илегалним каналима продају по високим ценама, док жртва губи свој идентитет, губи јој се сваки траг и престаје да постоји.[8]

По дефиницији УН–а трговина људима „означава врбовање, пренос, премештање, скривање или прихват лица уз примену претње или силе или других облика принуде, отмице, преваре, обмане, злоупотребе овлашћења или угрожености или давањем или примањем новчаних средстава или друге користи ради добијања пристанка лица које има контролу над другим лицем

[8] У Мексику годишње нестане око 20.000 деце, која се касније користе за препродају органа или транспорт дроге у њиховим телима. Велики број отете деце се користи за трансплантацију органа унутар САД–а, што потврђује чињеница да је највећи број нестале деце у подручјима Мексика која се граниче са САД–ом. (Чомски и сар., 1999)

у циљу експлоатације. Експлоатација, у најмању руку укључује, искоришћавање проституције других лица или друге облике сексуалног искоришћавања, присилан рад или пружање услуга, ропство или праксу сличну ропству, вађење људских органа.“ (https://www.coe.int/t/dghl/monitoring/trafficking/Source/PDF_Conv_197_Trafficking_Serbian.pdf , 2014, 23. август).

Посебно интересантно би било дефинисати које информације би могле бити предмет интерсовања криминалних организација које се баве овом врстом криминалне делатности. Пре свега, основу трговине људима представља добра логистичка подршка у вези организације транспорта жртава трговине људима. Информација о распореду безбедносних снага, пре свега полицијских, распоређених у земљи домаћина кроз коју је потребно извршити транспорт, омогућава носиоцу ове противзаконите активности несметану реализацију започете активности. Следећа информација која свакако представља предмет интересовања криминалних група које се баве трговином људима јесте порозност државне границе и пропусти у раду царинских и безбедносних служби које су распоређене на прекограничним прелазима. Овакве информације омогућавају криминалним организацијама несметан прелазак преко границе. Злоупотреба жртава у земљи домаћина кроз разне врсте противзаконитих активности, нпр. сексуално искоришћавање, преношење и транспорт недозвољених материја као што су наркотици, подразумева, такође, перманентно прикупљање информација о систему безбедности јер оне своде степен ризика на минималан ниво. Врло често се за прибављање потребних података користе запослена лица у државним службама, која пристану на одговарајућу новчану надокнаду или другу врсту противуслуга. Један од најважнијих задатака служби безбедности, када је у питању организовани криминал ове врсте, јесте заштита информација које би у случају доласка у посед организованих криминалних група омогућиле спровођење противзаконите активности. Контраобавештајна заштита не подразумева само елиминацију људи из система који свесно пружају информације криминалним групама, већ и заштиту информационих система, који садрже податке о распореду

безбедносних снага у одређеном простору, распореду службених лица на смени, спровођењу контрола, распореду камера и других техничких средстава физичко–техничке заштите, као и податке о распореду патрола унутар територије у којој се организује транспорт жртава трговине људима.

Године 2013. је спроведено истраживање од стране тима научника које се, између осталог, односило на злоупотрбу ИКТ–а у сврху трговине људима — подаци о жртвама (Урошевић, 2014: 558–615). Истраживање је показало да је први контакт са жртвама био личан, директан, непосредан или преко посредника, али без употребе ИКТ–а. То показује, у овом случају, да приступ ИКТ–и од стране жртве није имао битног утицаја на њену виктимизацију.

Наведени подаци представљају пресек ситуације у тренутку истраживања и свакако не могу бити основ за доношење поузданог закључка да у Републици Србији нема случајева врбовања жртава трговине људима путем злоупотребе ИКТ–а.

3.1.2.2. Трговина оружјем

Трговина оружјем представља једну од водећих индустријских грана високоразвијених држава у свету, пре свега САД–а и Руске Федерације, те се оне тренутно сматрају највећим произвођачима и извозницама наоружања и војне опреме. О томе сведочи чињеница да је САД за систем одбране 2003. године потрошила 400 милијарди евра, односно 3,5 % америчког бруто националног производа. Да се издвајања за војни буџет из године у годину повећавају сведочи податак да је 2006. године САД у војни буџет инвестирала 530 милијарди долара. Највећи купац војне опреме произведене у САД–у представљају арапске земље: Саудијска Арабија, Уједињени Арапски Емирати и Катар, које за војна опремања троше енормне количине новчаних средстава. Профит који стиче војно–индустријски комплекс САД–а је изузетно важан за њен свеукупни економски развој. Војно–индустријски комплекс Руске Федерације је једно време био у стагнацији, посебно у време распада СССР-а. За време Хладног рата СССР је успевао да одржи баланс у

производњи и продаји наоружања и војне опреме, али ја за то морао бити спреман да издвоји половину бруто националног производа. То је „коштало“ развој других привредних грана који се компензовао експлоатацијом извора нафте и течног гаса којим је СССР изузетно богат. Војно–индустријски комплекс поново почиње да се развија 2003. године, када Русија уговара веће количине извоза оружја у Кину и Индију. (Петковић, 2009)

Данас се поставља питање да ли трка за модернизацијом војног наоружања и опреме треба и даље да буде циљ или би требало новчана средства преусмерити у друге мирнодопске области људског живота, као што је случај са развојем здравства. Ако узмемо у обзир претпоставку да би 30 до 50 милијарди долара годишње решило проблем глади у свету, а да је то тек 8 % финансијских средстава који САД улаже у војни комплекс, јасно је да би се проблеми болести и сиромаштва савременог света могли решити једноставним преусмеравањем новца у друге новчане токове (http://www.vreme.co.rs/cms/view.php?id=640079, 2016, 23. април).

У свету се око извоза и куповине наоружања воде тајни ратови. Циљ је онемогућити противника да располаже најразвијенијим врстама оружја као што су нуклеарне ракете и сателитско навођење. Тако је САД више пута, захваљујући обавештајним подацима, спречавала набавку и куповину савременог оружја Кине од Израела, а у циљу спречавања Кине да преузме улогу светског лидера. Процењује се да би се таква промена могла догодити 2025. године, уколико САД не изврши реформу у државним сферама и промену спољне политике. (Бжежински, 2013: 3)

У циљу спречавања наставка негативних трендова и последица у свету, Уједињене нације су основале Канцеларију УН–а за питања разоружања. Основана је 1982. године на другој седници Генералне скупштине о разоружању, а 1992. године њено име је промењено у Центар за питања разоружања који се налазио под Одељењем за политичка питања. На крају, 1997. године, Центар је преименован у Одељење за питања разоружања, а 2007. године постао је Канцеларија УН–а за питања разоружања. Канцеларија промовише: нуклеарно разоружање, јачање регулативе у области разоружања оружја за масовно уништење као и хемијских и биолошких

оружја, напоре око разоружања у области конвенционалног оружја, посебно мина и лаког оружја који се користе у савременим сукобима. (https://www.un.org/disarmament/about/, 2016, 15. јул)

Генерална скупштина УН–а је 6. децембра 2006. године донела Резолуцију 61/89 под називом „Према Уговору о трговини оружјем: утврђивање заједничких међународних норми за увоз, извоз и пренос конвенционалног оружја" и тиме покренувши процес УН–а за израду Уговора о трговини оружјем („процес УТО"). Главна скупштина УН–а, одржана 2. децембра 2009. године, доноси Резолуцију 64/48 под називом „Уговор о трговини оружјем" којом је одлучено да ће се 2012. године сазвати Конференција УН–а о Уговору о трговини оружјем како би се разрадио правно обвезујући инструмент о највишим могућим заједничким међународним стандардима преноса конвенционалног оружја. Седница је одржана у јулу 2012. године, али споразум на истој није постигнут. Споразум је постигнут тек у јуну 2013. године и потписале су га све чланице УН-а. (http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32013D0768, 2016, 16. јул)

Посебан безбедносни проблем представља извоз неперспективног наоружања и војне опреме у земље „трећег света" што у одређеним ситуацијама може да прерасте у међународни инцидент. Извозом технолошки застарелог наоружања јавља се могућност да, посредовањем разних сумњивих привредних субјеката и израдом лажних докумената, такво оружје заврши у некој од земаља које су обухваћене међународним санкцијама на извоз наоружања и војне опреме. У тим условима и држава из које потиче то наоружање постаје предмет интересовања међународних истражних институција, што често узрокује нарушавање њеног угледа у међународној јавности као и кредибилитета безбедносно–обавештајних структура.

Превентивним радом обавештајних и контраобавештајних структура земаља, које привлаче пажњу будућих трговинских извозника наоружања, потребно је предупредити таква настојања и онемогућити ескалацију сукоба

на сопственој државној територији будући да они могу да проузрокују озбиљне и несагледиве последице по живот њеног становништва.

3.1.2.3. Прање новца

Термин „прање новца“ је настао тридесетих година прошлог века у САД–у, у време прохибиције, када су криминалне групе (гангстери) новац зарађен на нелегалан начин приказивали као профит остварен у легалним активностима — ресторанима, кафе клубовима или перионицама.

„Прање новца” представља данас једну од најзаступљенијих организованих криминогених активности у свету. Вредност промета „прљавог новца“ која се у светским размерама средином деведесетих година прошлог века процењивала на око 500 милијарди $ у току једне године (Петковић, 2009: 209), увећала се на 1000 милијарди долара годишње десетак година касније. Половина од тога је новац који потиче од шверца наркотицима. (Петковић, 2009, 261) „Прљав новац“ је термин који се данас најчешће користи у круговима који се баве овом врстом нелегалне активности, а ради се о новцу који је зарађен на илегалан начин (трговина наркотицима, трговина људима, тешке крађе, трговина оружјем), а налази се изван званичних финансијских токова. „Прање новца” је процес поновног озваничења новца и његовог враћања у легалне токове и спроводи се реализацијом купопродајних уговора (изградња или куповина некретнина), депоновањем у банке и другим начинима улагања капитала. Посебан проблем је што ова врста криминалитета, у највећем броју случајева, излази ван граница националних држава, тако да су међународне безбедносне институције (ISPAC, CICAD, FATF[9]) важне са аспекта његовог сузбијања и отклањања.

[9] ISPAC — *International Scientific and Professional Advisory Councilof the United Nations Crime Prevention and Criminal Justice Programme* — Међународни савет за научне и професионалне консултације програма криминалне превенције и криминалног правосуђа Уједињених Нација, CICAD — *The Inter-American Drug Abuse Control Commission* — Интерамеричка комисија

Петковић разликује четири типична начина „прања новца" (Петковић, 2009: 211). Прва техника се састоји из три фазе, и то:

- *Етапа „пласмана",*
- *Етапа „пресвлачења",*
- *Етапа „интеграције".*

У првој фази, *етапи* „пласмана", нелегално зарађен новац се већ поменутим кривичним и противзаконитим радњама депонује у одређене финансијске институције или се користи за куповину хартија од вредности. Целокупна активност се реализује уз помоћ банкарског службеника или брокера, који уклања евентуалне почетне проблеме (доказивања порекла). Таква средства се депонују на банкарски рачун ван граница земље, а касније се користе за куповину некретнина и покретних добара као легална.

У *етапи „пресвлачења"* нелегалан новац се пребацује компанијама које регуларно послују на одређеном тржишту и поседују такозвани „пословни легитимитет". На овај начин нерегуларно стечен новац званично улази у промет пословања привредних субјеката који послују у званичним националним и међународним финансијским токовима.

Етапа „интеграције", представља издавање лажних или нереално увећаних фактура за робу и радове који нису изведени, а обухваћени су фактуром, или су вишеструко нереално увећани. Тиме се нелегалан новац брже ослобађа и улази у редовне финансијске токове привредног субјекта који га фактурише.

Међународна федерација рачуновођа дефинише „прање новца" као „пресвлачење" готовине или других новчаних средстава насталих илегалним активностима кроз легитимне финансијске институције, употребом најразличитијих и најразноврснијих финансијских инструмената и других достигнућа, у циљу прикривања извора тих средстава. (International Federation of Accountants: Anty money loundering, 2004: 4)

за контролу злоупотребе дроге, FATF — *The Financial Action Task Force* — Група међународне акције против прања новца.

У даљим разматрањима биће објашњена још једна техника „прања новца" која је у свету позната под називом „метод веш машине". Овај метод, као и претходно објашњени, подразумева три фазе реализације:

- *Фаза претпрања,*
- *Фаза прања,*
- *Фаза рециклирања.*

Прва фаза (*фаза претпрања*) подразумева отварање банкарских рачуна у земљама у којима је финансијска контрола слаба или уопште не постоји. Истовремено се у земљама са ригорозним системом поштовања тајности банкарских рачуна отварају рачуни и региструју пословни привредни субјекти. Развојем ИКТ–а и применом савремених ИС–а у сфери банкарског пословања, ова фаза реализације је знатно олакшана пошто је целокупну активност отварања рачуна и регистровања привредног субјекта могуће завршити на даљину, без личног присуства носиоца активности.

У другој фази (*фази прања*) у земљама са слабом финансијском контролом, врши се куповина и продаја покретне и непокретне имовине. Новац који прође ову фазу, сада поседује порекло, депонује се у земљама са ригорозним поштовањем тајности рачуна, чиме новац добија легитимитет.

На послетку, у трећој фази (*фази рециклирања*) новац се фиктивно улаже у привреду неке земље као што је то случај са приватизацијом код земаља у развоју, тако што прође кроз текуће рачуне и враћа се у земљу из које је дошао. Проценат који се за такве активности наплаћује износи од 10 до 50 % од опране количине новца (Петковић, 2009: 213).

Овде треба напоменути да се само 1 % од 1000 милијари долара, колико се годишње нелегалног новца у свету опере, заплени од стране надлежних безбедносних институција, а остатак новца одлази у редовне новчане токове. Међународна агенција за борбу против прања новца сваке године објављује „црну листу" земаља које толеришу или у којима је присутно прање новца у већим размерама.[10]

[10] На наведеној листи по подацима објављеним у „Дневнику" (22.03.2003. године) нашле су се Русија, Либан, Бахами, Кајманска острва, Кукова Острва, Маршалова Острва и Лихтенштајн.

„Прање новца" које проистиче из сиве економије потекло је из транснационалних компанија које су у циљу повећања профита креирале пореске земље са великим олакшицама, то јест земље које представљају такозвани „порески рај". Сива економија заузима своје место и учествује одређеним процентом у укупном друштвеном производу свих држава. (Telser, 1981: 24)

Данас у свету постоје делатности преко којих се „прљави новац" може најлакше „опрати", то јест легализовати, међу којима су најпознатије: коцкарнице, хотели, туристичке агенције, ноћни клубови, медији, трговина уметничким предметима. Вредност неког уметничког дела на тржишту уметнина је релативна и зависи од поступка лицитације који се у најчешћем броју случајева спроводи да би се реализовала трговина. Намештеним лицитацијама вредност уметнина се подиже и до неколико десетина пута, чиме се стиче могућност „прања" веће количине нелегалног новца.

У следећим разматрањима наводе се и објашњавају штетне последице које економија једне земље трпи због спровођења ове делатности:

- Економски поремећаји и тржишна нестабилност

Проблем економског поремећаја наступа због неадекватног улагања власника легализованог „прљавог новца", као што је улагање у друштвене делатности које немају производни потенцијал. Ради се дакле о делатностима које власницима таквог капитала служе за наставак финансијских манипулација, а највећи део новца полажу на банкарске рачуне и улажу у некретнине у иностранству. Није редак случај да власници такве врсте капитала у земљама у којима постоји уређен финансијски систем купују читаве спортске клубове, а каснијом трговином са играчима, врше додатне сумњиве послове око „прања новца". Нестабилност наступа оног момента када, на пример, улагањем у област грађевинарства дође до засићења тржишта, због превелике понуде или због непостојања куповних потенцијала. Тада се такве делатности прекидају или напуштају остављајући за собом нерешена дуговања и потраживања са заједничким улагачима. У

Као репрезентативан пример наводе се Кајманска Острва која имају свега 40.000 становника, а 34.000 регистрованих компанија и 590 банака.

таквим ситуацијама највећи губитници су купци који због законске регулативе о одговорности привредног субјекта, а не власника капитала, остају заувек без свог новца.

- Слабљење пословања легалног сектора

Конкурентност компанија које располажу са већим количинама нелегално стеченог новца је много већа у односу на компаније које су капитал стицале постепено и преко легалних пословних активности. Дешава се да су цене производа првих компанија испод стварних цена коштања неког производа („дампинг цене“). Обезбеђујући својим добављачима такве цене и дајући им нереално високе рабате гуше конкуренцију и елиминишу је са тржишта.

- Негативан утицај на програме реформи и на приватизацију

Овај проблем је посебно изражен код земаља у развоју које поступак реформи нису спровеле до краја. Власници сумњивог капитала нуде веће количине новца за куповину циљног привредног субјекта, без намере да наставе са инвестирањем у његов развој и опстанак, што у каснијој фази доводи до угрожавања самог процеса економских реформи и до масовног отпуштања радника.

- Смањење угледа националне државе у међународној јавности

Поједине државе су означене од стране неких финансијских институција као земље „пореског раја”. С обзиром на ниво корупције, неуређеност финансијских институција и слабости законске регулативе, такве земље ретко буде интересовање за права улагања, већ искључиво за финансијске малверзације од којих и опстају.[11]

[11] Европске државе постају све мање интересантне светским финансијским манипулантима, а пре свега оне које нису формално приступиле ЕУ. Један од разлога за неприступање јесте управо отежана контрола финансијких токова од стране међународних организација које се баве сузбијањем „прања новца“. Једна од земаља која је често помињана као погодна за вршење такве активности јесте Швајцарска. Међутим, након афере око бившег заирског председника Мобутуа и скидања ознаке тајности са његових рачуна депонованих у швајцарским банкама, као и после скидања тајни са рачуна нациста из Другог светског рата и исплате штете страдалим јеврејским породицама, Швајцарска све мање бива интересантна за спровођење ове врсте недозвољене активности. Тренунто се сматра да на простору Европе, Кнежевина Линхенштајн и Кнежевина Монако толеришу незакониту активност „прања новца“. О томе сведочи афера у Кнежевини Линхенштајн која се односи на покренуту истрагу од стране државног тужиоца поводом пословања банке *LGT*, иначе у власништву

„Прање новца", међутим, добија посебну пажњу у међународној јавности када се са њим финансирају терористичке организације. Међународне институције које су делом побројане, посебну пажњу посвећују пресецању и откривању ове врсте криминала, који свакако има елементе организованости. Један од начина којим се међународне институције боре против ове врсте криминала јесте евиденција великих новчаних трансакција и обавеза пријављивања истих од стране банака. Поједине државе, као што је то случај са Руском Федерацијом, законом су уредиле обавезу пријављивања финансијских трансакција које прелазе суму од 100.000 долара. Посебна владина агенција проверава такве трансакције као и порекло новца. Не треба сметнути с ума да су пословне банке и истражни државни органи често у сукобу интереса када је у питању сузбијање делатности „прања новца". Усвајањем законских процедура којима би се делимична одговорност за такве трансакције пребацила на терен банака, представља једно од могућих решења које би требало применити. „Прање новца", као један од облика организованог криминала, заступљено је и у нашој земљи, а у том смислу Република Србија је под будним оком институција Европске уније које пажљиво прате активности наше земље на супротстављању наведеној криминалној активности. У циљу превазилажења уочених проблема, Скупштина Републике Србије је донела Закон о спречавању „прања новца" и финансирања тероризма који је усаглашен са критеријумима Европске уније.

принца регента Ханса Адама II. У спроведеној акцији заплењен је велики број досијеа који могу представљати доказе забрањених операција светски познатих криминалаца и вођа мафијашких кругова. Кнежевина Монако броји свега 30.000 становника од којиха су 20% староседеоци. У држави, по подацима из 1999. године постоји 49 великих банака на чијим рачунима је наведене године уплаћен новац у висини од 50,5 милијарди евра. Један од разлога насељавања великх светских звезда из области музике, филма и спорта у ову државу лежи управо у пореским олакшицама које она нуди. До сада, нико није осуђен за „прање новца" у Монаку, а велики приливи и капитал правдају се финансијским и пореским повољностима улагања које ова држава нуди улагачима. (Првуловић, 2010: 260-261).

3.1.3. Оружје за масовно уништење

Употреба отровних материја у војне сврхе забележена је још пре неколико векова коришћењем отровних стрела у племенским ратовима на подручју Јужне Америке. Почеци употребе оружја за масовно уништење се јављају у Првом светском рату употребом бајонета затрованих цијанидом од стране пруске војске, пуњењем топовских граната дериватом арсеника од стране британских и француских војних трупа. И у Другом светском рату забележена је употреба оружја за масовно уништење са катастрофалним последицама. Концепт рада бацача пламена је дао научницима идеју да развију један много опаснији систем за масовно уништење који се и данас користи — напалм. У целокупној историји светске цивилизације бацање атомских бомби од стране оружаних снага САД–а на јапанске градове Хирошиму и Нагасаки (1945) представља најрепрезентативнији пример примене оружја за масовно уништење. У овим нуклеарним нападима усмрћено је преко 200.000 људи. (http://www.newsweek.rs/foto/54057-u-hirosimi-obelezen-dan-secanja-na-zrtve-atomskih-bombi-foto-video.html, 2016, 12. фебруар)

Владе појединих земаља света су оружје за масовно уништење развијале у толикој мери да је његова намена одавно превазишла потребе одбране тих земаља. Када оружје за масовно уништење постане предмет интересовања терористичких организација, које у својим настојањима не презају од употребе и ове врсте оружја, наступа озбиљан проблем. Иако је употреба оружја за масовно уништење забрањена међународним споразумима, сведоци смо догађаја у Русији који се десио 2002. године, када је чеченска терористичка организација у московском позоришту заробила око 600 талаца. У противтерористичкој акцији оружаних снага Руске Федерације, поред терориста, смртно је страдало и 130 недужних грађана (http://ruskarec.ru/articles/2012/10/26/rusija se seca zrtava nord-osta 17681.html, 2016, 13. фебруар).

Свет се данас суочава са проблемима контроле ширења нуклеарног оружја. Посебан проблем представљају државе чије Владе финансирају

међународне терористичке организације. Неке државе већ деценијама покушавају да развију сопствени нуклеарни програм, који би им омогућио снажнију позицију на међународној сцени. Поједини теоретичари заступају мишљење да развој нуклеарног програма у свету не треба спречавати већ само контролисати од стране надлежних међународних институција. Основ за овакве ставове представља размишљање да је мир између двеју највећих светских сила, САД-а и тадашњег СССР-а, одржан управо захваљујући паралелном развоју нуклеарног програма обеју страна (Waltz, 2010). Са друге стране, постоје теоретичари који се оштро противе ширењу нуклеарног програма јер сматрају да такав процес може да произведе само негативне импликације по мир и безбедност у свету. Један од аутора који заступају такво мишљење је Скот Саган (Sagan, 1994: 66-107). Поред САД-а и Руске Федерације, нуклеарно оружје данас поседују и Француска, Велика Британија, Кина, Индија, Израел, Пакистан и Северна Кореја. Међутим, Индији, Израелу, Пакистану и Северној Кореји није признат статус нуклеарне силе у међународним уговорима (Новичић, 2005-2006: 505-528). Поред наведених земаља, опсежне мере за развој и поседовање нуклеарног наоружања предузима и Иран, држава за коју постоје сумње да већ поседује технологију за производњу нуклеарног оружја.

У циљу спречавања развоја нуклеарног оружја, посебно у земљама које би могле на било који начин бити повезане са терористичким организацијама у свету, водеће светске нуклеарне силе су постигле неколико споразума — уговора којима се ограничава или потпуно прекида пролиферација нуклеарног програма. Тако је 1963. године између САД–а, СССР–а и Велике Британије, потписан Уговор о делимичној забрани нуклеарних проба (енгл. *Partial test ban treaty*), којим се оне ограничавају на извођење искључиво под земљом. Године 1968. на иницијативу САД–а и тадашњег СССР–а, покренут је нацрт уговора за нешириење нуклеарног оружја, који је усвојен исте године на Генералној скупштини УН–а (енгл. *Treats on the Non–Proliferation of Nuclear Weapons*). Затим следе уговори о ограничењу стратешког офанзивног оружја (SALT I — 1972. године, START I — 1991. године, START II — 1993. године и SORT — 2002. године). Међутим, и

поред иницијативе да се нуклеарно оружје, које представља данас најопаснији вид оружја за масовно уништење, ограничи и спречи његов развој, поједине нуклеарне силе, као што је САД, мењају одреднице стратешке употребе нуклеарног оружја. Наиме, исте године када је потписан Московски споразум, (SORT), САД су „омекшале“ услове око употребе нуклеарног оружја дозволивши његову употребу искључиво против држава које су га прве употребиле. (Dekker & Coppen, 2012: 25-47)

Поред нуклеарног оружја, као врсте оружја за масовно уништење, посебна пажња се поклања биолошком, хемијском и радиолошком оружју. Доспећем такве врсте оружја у посед терористичких организација ствара се безбедносни ризик по светску популацију највишег степена. За разлику од нуклеарног оружја, биолошко оружје одликује релативно јефтина производња, а у исто време изузетно висок степен смртности приликом употребе. Производња ове врсте оружја лако се може прикрити и оправдати, под изговором употребе и развоја производње биолошких агенаса у медицинске и друге сврхе, а последице њиховог доспевања у „погрешне руке“ могу бити јако опасне. За разлику од нуклеарног оружја за чији је развој неопходна примена савремених технологија која је лако уочљива, те је прикривање таквих активности у данашњим условима готово немогуће, код биолошког оружја је ситуација у потпуности другачија. Управо због тога, у циљу борбе против биотероризма, на значају добијају обавештајне и контраобавештајне службе које оперативним радом и прикупљањем података долазе до информација о производњи, транспорту и евентуалној примени таквих агенаса у терористичке сврхе. Развој интернета је допринео стварању услова за израду импровизованих отровних хемијских агенаса за које је некад била потребна висока стручност. Данас, просечан корисник интернета могао би да направи средство којим се може угрозити живот неколико десетина, па и стотина људи.

Први случајеви употребе биолошког оружја забележени су у Првом светском рату када су у борбеним дејствима зараћених страна коришћени нервни гасови са бактеријама и вирусима који су исцрпљујуће деловали на снаге непријатеља. Године 1926. у Женеви потписан је Женевски протокол о

забрани употребе биолошког оружја. Пошто наведени протокол није подразумевао забрану производње, у Другом светском рату забележени су бројни случајеви употребе биолошког оружја за масовно уништење. Тек 1972. године у Лондону потписана је Конвенција о забрани развоја, производње и складиштења биолошког и токсичног оружја (енгл. *Convention on the prohibition of the development, production and stockpiling og bacteriological and toxin weapons and on their destruction*). Једна од земаља за коју се претпостављало да крши међународне одредбе о забрани производње нуклеарног оружја је Ирак, за коју је Специјална комисија УН–а (UNCOM) 1995. године установила да је још 1974. започела програм развоја ове врсте оружја. Управо је то био повод за војну интервенцију НАТО–а на Ирак 2003. године, који је резултирао свргавањем тадашњег државног руководства са власти. Повод за интервенцију је процена која говори да би у посед биолошког оружја које производи Ирак могли да дођу припадници терористичке организације Ал Каида за коју се претпостављало да одржава интензивне и блиске везе са ирачком владом. Наведене претпоставке никада нису потврђене, а активности САД–а у Ираку нису ни дан–данас окончане. (Милић, 2010: 103-116)

У циљу одбране од биотероризма, државе су у обавези да предузимају низ мера како би се последице од таквих напада ублажиле или у потпуности неутралисале. У том смислу потребно је радити на едукацији становништва како би препознавали симптоме примене биолошких агенаса, затим на унапређивању здравственог сектора како би могао стручно да одговори на потенцијалне ризике и претње. Ипак на првој линији одбране од ове врсте тероризма налазе се службе обавештајно–безбедносног сектора које благовременим прикупљањем информација о месту и јачини напада треба да неутралишу терористичку претњу или да је сведу на последице које представљају минималан безбедносни ризик. (Јовић и Савић, 2012: 62)

Употреба хемијских средстава у терористичке сврхе није новост на светској сцени. Последњи забележен случај те врсте догодио се у подземној станици у Токију када је секта „Аум Шинрикио“ употребила нервни гас „сарин“ што је изазвало тренутну смрт код дванаест лица, а последице је

претрпело више стотина људи који и данас пате од разних врста нервних оштећења. Предност употребе ове врсте агенаса у терористичке сврхе јесте лака доступност, релативно јефтина производња, као и могућност лаког прикривања делатности. (Гаћиновић, 2012: 1-18) Њихова предност је, као и у случају употребе биолошких агенаса, одложено дејство на објекте угрожавања што омогућава носиоцу такве делатности контролисано извлачење из зоне употребе, без последица по личну безбедност. Одбрана од ове врсте тероризма је слична као и у случају одбране од биотероризма. Улога безбедносних служби у такозваној „раној фази" откривања потенцијалних извршилаца хемијских терористичких напада је најважнији вид борбе против хемијског тероризма.

Данас се све више у свету помиње примена такозваног климатског оружја чија је употреба застрашујућа, а последице и ефекти те употребе представљају потенцијални безбедносни ризик коме се тешко, а понекад и немогуће, супротставити. Године 1992. САД почињу изградњу радарског комплекса HAARP (енгл. *High Frequency Active Auroral Reseach Program*) на Аљасци, који је у првобитној фази био намењен за проучавање јоносфере. Према истраживањима научника, зрачење HAARP-а негативно утиче на земљину атмосферу, екологију, као и сеизмичку активност. О последицама по здравље људи и могућим безбедносним претњама показаће будући токови развоја догађаја (https://www.zeitenschrift.com/artikel/haarp-das-wetter-als-waffe-wahn-oder-wirklichkeit, 2016, 13. март).

3.1.4. Неравномеран економски развој

Фактори економског развоја једне земље представљају: акумулација капитала укључујући инвестиције и природна богатства (земљиште, горива, минерали), број становника (образовање, знање, мотивисаност) и технички прогрес (научна достигнућа, степен развоја предузетништва, техничка примена која подразумева и развој ИКТ–а).

Раст људске популације се кроз историју развијао врло споро, све до друге половине 18. века када почиње такозвана индустријска револуција. Од тада, захваљујући пре свега побољшању услова живота и повећању производње хране, започиње експоненцијални раст светског становништва, а прогнозе су да ће 2050. године светско становништво досегнути бројку од 9.7 милијарди. Процена је да на свету данас живи око 7.1 милијарди становника. (http://www.novosti.rs/vesti/naslovna/reportaze/aktuelno.293.html:456820-Sredinom-veka-u-svetu-97-milijardi-ljudi, 2016, 17. март)

Управо је индустријска револуција условила снажан економски развој земаља које се и данас сматрају лидерима економског развоја, а међу њима прве кораке ове врсте започела је Велика Британија. У Великој Британији су забележени први почеци експлоатације парних машина и развој железнице, који су позитивно утицали и на развој индустрије. Могло би се рећи да је ова земља покретач индустријске револуције у свету. Без образованог и стручно оспособљеног становништва нема ни економског развоја, јер управо су људи незаменљиви елеменат производног процеса који покреће економски развој. Зато је улагање у квалитетно образовање и побољшање социјалног статуса становништва један од најважнијих задатака сваке државе. Технологија и сировине могу да се позајме или купе, међутим куповина квалификоване и високообразоване радне снаге данас је привилегија само најбогатијих држава у свету. У том смислу, сведоци смо великог одлива становништва из најнеразвијенијих земаља, што је посебно карактеристично за земље у развоју. То је посебно изражено код одлива школованих кадрова, пошто, у потрази за бољим и квалитетнијим животом, а понекад и ради обезбеђивања основне људске егзистенције, напуштају своју домовину и насељавају државе које им нуде квалитетнији живот. У литератури се таква врста миграција назива „одливом мозгова“, управо због чињенице да таквој врсти промене животне средине прибегавају најобразованији појединци. Случај миграција становништва данас имамо и у оквиру једне државе, када из слабије развијених региона становништво мигрира у развијеније регионе или градове. У многим земљама света, па и у нашој земљи, имамо случај развијених и неразвијених региона, што условљава прекомерно насељавање

појединих области, проблеме незапослености, нелојалне конкуренције и смањење цене рада. Такви проблеми, углавном у земљама нижег степена економског и културног развоја, могу да узрокују и озбиљне безбедносне проблеме.

Проблеми миграција и сукоба нису изражени само у новије доба. Пре почетка првих назнака бављења пољопривредом, отприлике пре 12.000 година, човек је стално мењао своје станиште у потрази за храном коју је обезбеђивао ловом, риболовом и сакупљањем плодова у природи. Да би обезбедио боље услове живота, човек је почео да користи природне ресурсе у количинама које су надмашиле могућност одрживог развоја, што је касније доводило до миграција становништва у пределе који су омогућавали задовољавање основних људских потреба. Основне људске потребе су касније, искључиво због несразмерних апетита човека и жеље за наводним побољшањем квалитета живота, прерастале у луксуз и несклад са природом. Миграцијом, унутар или ван своје земље, људи остављајући свој дом и имовину, насељавају подручја богата природним ресурсима и потенцијалима како би себи обезбедили што квалитетније услове за даљи опстанак и развој породице. Неретко се у тим ситуацијама насељавају подручја у којима је већ настањено становништво других обичаја и традиција, што у каснијим фазама доводи до сукобљавања, понекад оружаних сукоба, чак и ратова. (Homer–Dixon, 2010)

Расположивост природним ресурсима се некада односило искључиво на земљиште и климатске услове. Када је у питању земљиште, важно је било каквог је земљиште квалитета, колики је проценат покривен шумским покривачем и каквог је он квалитета, затим његов географски положај и слично. Климатски услови су били унапред детерминисани и нису се много мењали, док данас имамо другачију ситуацију која је условљена великим и снажним климатским променама, а које настају као резултат еколошких проблема и уништавања озонског омотача. Данас се под најважнијим природним ресурсима, у контексту високог техничког и технолошког развоја, подразумева располагање енергетским изворима и рудним богатствима. Сведоци смо и ратова који се воде у циљу лакшег приступа овим врстама

природних богатстава, чији су капацитети лимитирани, а обновљиви извори још увек нису довољни да би надоместили тренутне светске потребе. (Homer–Dixon, 2010) Такође, потребно је истакнути да расположивост природним ресурсима није преко неопходан услов којим би се мерио степен развоја једне земље, о чему сведоче државе као што је Јапан, Швајцарска, Белгија, које не располажу значајнијим природним ресурсима, а налазе са на лествици високо развијених светских земаља. Недостатак природних ресурса у овом случају надомештава се применом стечених технологија и знања (know how), увозом сировина и стварањем производа вишег степена обраде. Развој технологија у директној је корелацији са научним открићима и иновацијама у посматраној области, а у случају Велике Британије и научним открићима која су заувек променила свет. Управо због тога, високо развијене државе, као и транснационалне компаније, улажу велика финансијска средства у научна истраживања која позитивно утичу на њихову пословну позицију и увећање капитала. Резултати таквих истраживања често су на мети носиоца пословне шпијунаже, који у циљу обезбеђења повољнијег конкурентског положаја на тржишту не презају ни од ове врсте делатности.[12]

Ниво развијености производних капацитета, изграђеност путева, уређеност пловних објеката и обала, развијеност инфраструктуре, ниво степена развоја телекомуникација и информатичких технологија утиче на акумулацију капитала. У неким високо развијеним земљама одвајања за ове потребе крећу се и до 20 % бруто друштвеног производа, док су у земљама у развоју неупоредиво мања. Иностране инвестиције су обично у директној корелацији са овом врстом улагања, тако да је у том смислу потребно пронаћи оптималан однос уложеног и очекиваног, а то се пре свега односи на земље као што је Србија. Поједине високоразвијене земље, као што је САД,

[12] Деведесетих година прошлог века познате америчке компаније као што је HONEYWELL покренуле су тужбу против јапанске компаније MINOLTA због неовлашћеног коришћења патента аутофокуса, односно аутоматског изоштравања слике код производње фотоапарата, а захетв за одштету је износио око 96 милиона евра. Иако је MINOLTA једина јапанска компанија која је платила наведену одшету, и друге јапанске екомпаније као што је CANON и NIKON данас користе наведену технологију. Познат је и случај да је америчка компанија TEXAS INSTRUMENTS тужила јапанску компанију FUJITSU због нелегалног коришћења патента за производњу електронских кола, а захтев за одштету је такође био милионски. (Првуловић, 2010: 253-254).

ослањају се на улагања и инвестиције приватног сектора, који у овој врсти капитала учествује у проценту већем у односу на таква улагања у Европској унији. (Samuelson & Nordhaus, 2010)

Проблеми неравномерног регионалног развоја су такође глобалне природе. Примена нових технологија, масовна производња, промене у стилу живота људи, утичу на комплексност овог проблема. Један од основних задатака сваке државе јесте да обезбеди равномеран економски развој на целој својој територији. То би се могло постићи бољим коришћењем природних потенцијала у неразвијеним подручјима и стварањем инвестиционе климе за улагања домаћих и страних привредних субјеката. Инвестиције у неразвијеним деловима се односе углавном на улагања у сировинску и базичне гране индустрије у којима је профит највећи, а ризик пословања сведен на минимум. Велике разлике у паритету цена између, нпр. пољопривредних производа у вишим и нижим фазама прераде, такође иду у прилог додатног богаћења развијених, а осиромашења неразвијених региона. (Ђорђевић, 2008)

Последице диспаритета цена огледају се у смањењу акумулативне и репродуктивне способности примарних пољопривредних произвођача. То се манифестује у недовољној акумулацији, екстензивирању производње и одсуству инвестиционих улагања, пре свега, у обнављање пољопривредне механизације. (Влаховић и сар., 2010)

У Уставу Републике Србије наглашена је потреба равномерног развоја целе територије Републике Србије, а члан 97. се односи на развој Републике Србије, политику и мере за подстицање равномерног развоја појединих њених делова, укључујући и развој недовољно развијених подручја; организацију и коришћење простора; научно-технолошки развој.

Неки од показатеља који неповољно утичу на развијеност делова територије једне националне државе су:

- Демографско старење;
- Недовољан прилив инвестиција;
- Неповољни паритети цена на штету произвођача пољопривредних производа;

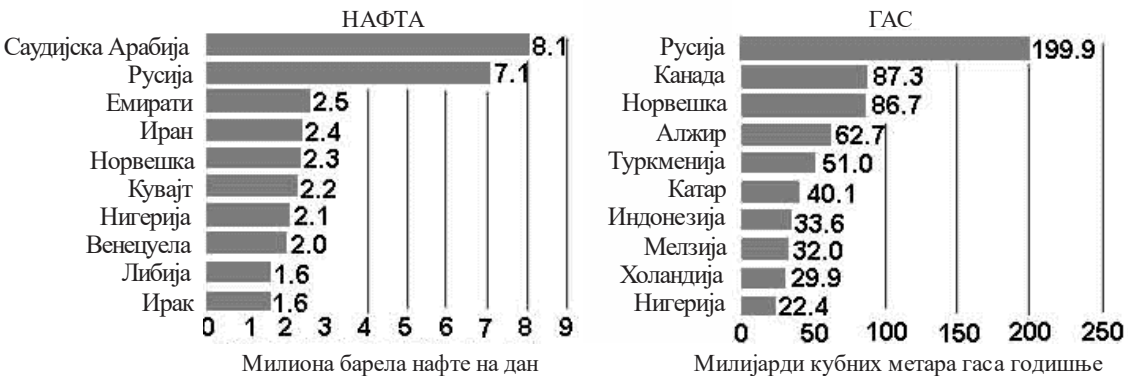
- Заступљеност индустријске производње искључиво у нижим фазама;
- Недовољно развијена инфраструктура (путна, електрична, водоводна, информациона мрежа);
- Слабо развијене услужне делатности (здравствене и образовне установе, трговински објекти);
- Немогућност запошљавања и професионалне афирмације;
- Миграције становништва ка развијенијим регионима и смањење насељености.

3.1.5. Енергетска нестабилност

Енергија је, поред хране, важан ресурс који утиче на развој једне државе. Доступност и расположивост енергетским ресурсима, пре свега фосилним горивима, јесте најважнији чинилац укупног економског развоја државе. Управо је тежња појединих великих сила за контролом и доступношћу енергетских потенцијала утицала на свеукупну безбедносну слику света, а често је узроковала и оружане сукобе и примену силе у циљу обезбеђења енергетских ресурса за сопствене потребе. Са сигурношћу би се могло рећи да располагање енергетским потенцијалима фосилних горива данас представља основ за стицање геополитичке, геостратешке и војне надмоћи. Енергетски ресурси као што су фосилна горива су ограничени, стога су истраживања научника око увођења обновљивих енергетских ресурса најважнија у области енергетике. С обзиром на ограниченост необновљивих природних ресурса и на све веће потребе индустријског сектора за овом врстом енергетских ресурса, у стручној јавности се осамдесетих година прошлог века увео појам енергетске безбедности. Ако при том узмемо у обзир да су предвиђања научника да ће овим темпом експлоатације нафта бити у потпуности исцрпљена до 2050. године и чињеницу да је потражња нових економских сила у експанзији, Индије и Кине, све већа, може да се схвати колико је појам енергетске безбедности данас актуелан. Енергија има

непроцењив друштвено-економски, стратегијски и политички значај за сваку организовану друштвену заједницу. (Радичевић, 1995: 42)

Тренутно у свету, највећу потрошњу нафтних деривата, најзаступљеније врсте фосилних горива, имају САД, Јапан, Кина и Руска Федерација. САД своје енергетске потребе задовољава из сопствених капацитета у висини од 20 %, Кина 50 %, а Јапан целокупне потребе за нафтним дериватима решава увозом. Једино Руска Федерација од набројаних држава, поседује довољне количине нафтних деривата којима измирује сопствене потребе, а још два пута толико извози ван својих граница. (Колев, 2011: 45-47)



Слика бр. 4: Највећи произвођачи нафте и гаса у свету
(http://www.vizijadanas.com/svet_nafte.html, 2016, 13. март)

Највећи светски произвођач нафте у свету је Саудијска Арабија. Државни приход од извоза нафте чини 90 % укупног бруто друштвеног производа ове државе. Држава која у тој мери поседује енергетски потенцијал свакако је и у ранијем периоду била предмет интересовања великих сила, а понајвише САД–а, које су 70–их година прошлог века утицале на политичке промене државног руководства наведене државе. (Perkins, 2006)

Када је гас у питању, највећи светски произвођач је Русија, а иза ње Канада која се не убраја у велике произвођаче нафте. Русија је највећи снабдевач гаса земаља европског континента.

Субјекти енергетске безбедности би се могли поделити у три категорије: власници енергетских налазишта, власници транспортних путева (гасоводи, нафтоводи) и корисници енергетских ресурса.

У стратешким документима готово свих држава света енергетска безбедност третира се као део стратегије безбедности, па је то случај и са Републиком Србијом (Стратегија националне безбедности Републике Србије http://www.mod.gov.rs/cir/dokumenta/strategije/strategije.php, 2016, 11. мај). Појам „енергетска безбедност" се, уопштено посматрано, најчешће одређује као „доступност енергената", при чему се под префиксом „доступности" подразумева потребна количина, континуитет у снабдевању, прихватљиве и стабилне цене, физичка обезбеђеност траса гасовода и нафтовода, политичка стабилност држава из којих се енергенти увозе и слично. (Колев, 2011: 45-62)

О геополитичком утицају појединих држава, које у светским размерама заузимају место највећих произвођача и извозника енергетских деривата, може се говорити са два аспекта. На пример, утицај Руске Федерације на укупна геостратешка и геополитичка кретања и односе са земљама Европске уније битно је условљен и њеним енергетским потенцијалом. Ипак, иако 30 % укупне потрошње гаса у Европи долази из Руске Федерације, однос енергетских привредних субјеката из Руске Федерације, пре свега „Гаспром њефта" као највећег, према земљама увозницама мора бити обазрив. Ако узмемо у обзир чињеницу, садржану у дефиницији о енергетској безбедности, да је континуитет у снабдевању и физичка обезбеђеност траса гасовода и нафтовода важна са аспекта доступности и стабилности у снабдевању, што представља најважнији захтев земаља увозница, схватићемо колики ниво обазривости је потребан од стране испоручиоца како не би натерао увознике да налазе алтернативна решења у снабдевању. Други аспект представља монополистички однос извозника према земљама увозницама, који поред енергетског утиче на политички, економски, па и на војни статус увозника. У циљу превазилажења могућих проблема, седамдесетих година прошлог века формирана је Међународна енергетска агенција (енгл. *International Energetic Agency* — IEA) са седиштем у Паризу, која врши контролу над стратешким залихама нафте у свету, као и мониторинг најважнијих светских енергетских

произвођача. Постојећи систем енергетске безбедности створен је као одговор на ембарго арапске нафте из 1973. године, како би обезбедио координацију међу индустријализованим земљама у случају поремећаја у снабдевању, охрабрио сарадњу у области енергетске политике, избегао негативне последице по снабдевање и извознике одвратио од било какве будуће употребе „нафте као оружја“. (Yergin, 2006: 69)

Од новијих споразума који се односе на смањивање могућности злоупотребе енергената у политичке сврхе и обезбеђење стабилности у снабдевању јесте Уговор о успостављању Енергетске заједнице земаља Југоисточне Европе, који је потписан у Атини 2005. године, а ратификован од стране ЕУ 2006. године. Документ се односи на обавезу креирања заједничког законодавног оквира земаља Југоисточне Европе и ЕУ којим би се дефинисали односи око успостављања јединственог енергетског тржишта уз јачање заштите животне средине.

О утицају енергената на геостратешку слику света сведоче и догађаји који су се дешавали последњих деценија у Либији, Ираку и Авганистану, када је нестабилност појединих државних система, изазвана унутар или споља, искоришћена, између осталог, и за експлоатацију енергетских ресурса од стране појединих великих сила које су под изговором развоја демократичности обезбедиле своје присуство у наведеним земљама. Прогнозе су да ће подручја богата резервама нафте и гаса у будућности бити предмет борбе за геополитичку надмоћ високо развијених земаља. Посебан проблем представљају земље које располажу високим енергетским ресурсима и налазиштима, а финансирају разне светске терористичке и организоване криминалне организације. Уплитање у њихове унутрашње односе је са аспекта међународне безбедности потпуно оправдано, али границу која раздваја уплитање у унутрашњу политику државе у односу на глобалне безбедносне претње није лако одредити.

Производња нафтних деривата у Републици Србији задовољава око 25 % државних потреба. Ситуација око располагања природним гасом је знатно компликованија јер готово све потребе за овим енергетским ресурсом се задовољавају из увоза. Однос државе према енергетским потребама и

потенцијалима са аспекта енергетске безбедности би могао негативно да утиче на енергетску стабилност Републике Србије. Интереси нових власника, и поред чињенице да је већина таквих привредних субјеката у мешовитом власништву, често нису у складу са интересима државе, што у кризним ситуацијама може да имплицира негативне последице по енергетску безбедност државе. (Ђурић и Јегеш, 2011: 80-89) Посебан проблем представља неконтролисано уступање информација од државног значаја таквим корисницима, без претходног усаглашавања са мишљењем надлежних државних институција. Нарочита обазривост је потребна код информација које се односе на тренутне енергетске потенцијале државе, степен искоришћености појединих налазишта, достигнућа око испитивања потенцијалних налазишта и слично. Постављају се питања да ли је код тих привредних субјеката извршено степеновање и класификација података који би могли неконтролисаним одливом да наруше државне интересе и како се такви подаци чувају и штите. Узмимајући у обзир интересе приватног партнера који ће своје пословање у енергетском сектору у перспективи планирати искључиво у складу са расположивим ресурсима, поставља се питање да ли ће експлоатација истих у том случају бити рационална и у складу са дугорочним државним интересима. Око тога да ли у таквим компанијама пословима безбедности треба да се баве искључиво лица запослена од стране већинског власника или би те послове (корпоративне заштите) требало поверити и државним службеницима, сразмерно учешћу у капиталу привредног субјекта, не би смело да буде дилема.

3.1.6. Демографска експанзија и квалитет животне средине

Проблеми демографске експанзије су данас изражени до те мере да представљају један од најозбиљнијих проблема савременог света. Нагли пораст светског становништва који данас бележи бројку од преко седам милијарди, утиче на еколошке проблеме планете као и на успостављање одрживог развоја. Према подацима УН-а процењује се да је почетком нове ере

светска популација бројала између 200 и 300 милиона становника. Милијарду становника светска популација достиже тек почетком 19. века. Године 1927. број становника у свету достиже бројку од две милијарде, а већ 1960. од три милијарде. Четрнаест година касније број становника се пење на четири милијарде, а 1987. године бележи се шест милијарди становника. Ако узмемо у обзир да је највећи пораст становника забележен у сиромашним и неразвијеним земљама, онда је основана претпоставка да ће такав тренд утицати негативно на додатну поларизованост светске популације, односно да ће сиромашни постати још сиромашнијим, а богати богатијим. До Другог светског рата, пораст светске популације код развијених и неразвијених земаља је био уједначен. После тога долази период у коме тренд пораста светске популације преузимају земље у развоју, које данас чине око 97 % укупног раста светске популације. (Спасовски, 2001)

Популациона експанзија додатно утиче на експлоатацију основних људских ресурса, пре свега на доступност хране, воде, енергетских извора и земљишта. Проблем исхране становништва посебно је изражен у Африци, пре свега због смањених површина пољопривредног земљишта које стоји на располагању становништву. Светска популација данас је суочена и са све чешћим проблемима који се односе на доступност воде за пиће, што је такође најизраженије на подручју афричког континента.

Статистички гледано државе у којима се налази највећи број становника по мери површине имају нижи степен развоја, тако да се наведени проблем са исхраном пре свега јавља у сиромашнијим земљама и у земаљама у развоју (Индија, Кина, Индонезија). Миграције становништва узроковане су поменутим проблемима, тежњом за проналажењем бољих услова за опстанак, као и разним врстама природних и других катастрофа које снажно мењају животно окружење. Људи који мигрирају ради стварања повољнијих услова за квалитетнији живот, а квалитетнијим окружењем се у овом смислу сматра здрава средина, све чешће се у међународној литератури називају „еколошким избеглицама“. Иако, међународно право не познаје ову врсту избеглица, тј. немају третман избеглих лица по међународним класификацијама и мерилима, наведени проблем је све присутнији у

међународној јавности. Миграцијом, унутар или ван своје земље, наведена лица остављајући свој дом и имовину насељавају подручја богата природним ресурсима и потенцијалима, како би себи обезбедили што квалитетније услове за даљи опстанак и развој породице. Неретко се у тим ситуацијама насељавају подручја на којима је већ настањено становништво других националности, других обичаја и традиција, што касније доводи до разноврсних непријатељских односа који кат–кад прерасту у оружане сукобе, чак и ратове. Сукоби широм света који се воде због доминације над природним ресурсима све су чешћи и масовнији. Неретко су прикривени другим мотивима и разлозима, јер су Владе појединих држава „падале" због „тврдог става" према експлоатацији природних ресурса. Међународна заједница је чиниоц који би требало да контролише сукобе у свету и ратове који се воде око природних ресурса. Да ли је циљ међународне заједнице пружање помоћи у решавању сукоба или нешто друго, остаје на аналитичарима да процене, али у сваком случају стављање еколошких проблема у исту раван са проблемима националне безбедности дају еколошкој безбедности нову димензију коју до тада није имала.[13]

Недостатак хране је данас, посматрајући то на светском нивоу, проблем који је могуће решити, јер је свеукупна производња хране довољна, али се у високо развијеним земљама расипа и троши преко стварних потреба. У исто време у најнеразвијенијим земљама света је забележено да људи услед недостатка хране умиру од глади. По извештајима UNPFA (енгл. *United Nation Population Fund*; http://www.unfpa.org/, 2016, 11. мај) највећи изазов у свету представља недостатак воде, те су процене наведене међународне организације да ће 2030. године свет бити суочен са дефицитом воде од 40 %. У ком правцу дефинисати популациону политику да би се обезбедио одрживи развој на глобалном, националном и регионалном нивоу, остаје питање са којим ће се суочити светски научници у наредном периоду.

[13] Tomas Homer–Dixon (1999) је еколошке изазове поделио у три групе: изазови који се односе на сукобе међу државама у вези права на коришћење необновљивих природних ресурса, изазови који се односе на миграције становништва који су изазвани „еколошким ударима" што доводи до сукоба међу популацијама различитих етно–религијских идентитета и изазови који доводе до сукоба услед осиромашења природних извора енергије, деградације животне средине и климатских промена. (Homer–Dixon, 2010)

Пораст броја становника у свету такође је снажно утицао на организацију индустријске производње и потрошње, а ови елементи на екосистем. Пораст и омасовљавање индустријске производње утицали су негативно на очување озонског омотача и на климатске промене. Просечна температура у последњих 100 година је порасла за 0,74 степена, што доводи до наглог отопљавања ледених површина на северном и јужном полу и подизања нивоа мора. Наведена дешавања негативно ће утицати на квалитет живота светске популације настањене у приобалним подручјима, тј. у непосредној близини мора, река и језера. У САД–у приближно 75 % становништва живи у приобалним подручјима. (Koren & Butler, 2006: 109-125)

Савремени начин живота свакодневно утиче на промену животне средине. Када се ради о савременом начину живота, пре свега мислимо на употребу техничких достигнућа којима се човек служи како би себи омогућио комфорнији и лагоднији живот, не водећи при том рачуна како та средства утичу на животну средину, на здравље човека као појединца и у крајњем случају на еколошку безбедност људи. Неумерена употреба аутомобила и пловних објеката са емитовањем издувних гасова у спољну средину, утиче на квалитет ваздуха који удишемо и воде коју конзумирамо, што за последицу може имати нарушавање здравља људи. Код популације се јављају проблеми на дисајним путевима, затим проблеми са болестима типа дијабетес I и II, неке врсте канцерогених обољења и слично. Без обзира на ком делу земаљске кугле човек живи, он је изложен утицају хемикалија у ваздуху, канцерогеним средствима у храни и другим опасностима из свог окружења.[14] „Сваки појединац је сваки дан изложен опасностима у животној средини које су невидљиве, а потенцијално смртоносне“. (Corson–Finnerty, 1982)

[14] Употреба азбеста је била изузетно велика у грађевинској индустрији, док је данас у земљама ЕУ забрањен будући да услед дуже изложености и контакта са људским организмом изазива неколико врста канцерогених болести. (http://www.euractiv.rs/odrzivi-razvoj/3578-zabranjeni-azbest-i-dalje-opasnost, 2016, 11. мај)

3.1.7. Еколошка неодрживост

Корени и први почеци идеје одрживог развоја потичу у ловству и шумарству. У ловству се правилним газдовањем, селекцијом, прихраном и контролом прираштаја дивљачи, обезбеђује бројно стање које спречава нестанак појединих врста и одржавање довољног броја јединки за даљу репродукцију на неком простору. Ситуација је слична и у шумарству где се контролисаном сечом шуме обезбеђује природни прираштај и онемогућује дефорестација која за последицу има друге врсте природних и еколошких катастрофа по биљни и животињски свет. Једна од најважнијих међународних институција, када је одрживи развој у питању, јесте Светска комисија за животну средину и развој, познатија под називом Брунтлендова комисија. Ова комисија је одрживи развој дефинисала као „развој који задовољава садашње потребе, не угрожавајући могућности будућих генерација да задовоље своје потребе“.[15] Дакле, одрживи развој представља складан однос екологије и економије како би се природно богатство Земље сачувало за будуће генерације. Одрживи развој садржи у себи три аспекта: 1. економски, 2. социјални и 3. еколошку одрживост, а у даљим разматрањима ће бити више речи о трећем аспекту одрживог развоја.

Циљеви одрживог развоја су задовољавање потреба људи и превазилажење противречности између економије и екологије. При томе, не треба заборавити на потребе за ресурсима наредних генерација, што захтева, између осталог, и подизање еколошке свести свих нас. Наћи оптималну меру између задовољења сопствених потреба и ресурса који остају на располагању наредним генерацијама, представља основну обавезу одрживог развоја гледано са еколошког аспекта.

Проблемима загађења и уништавања животне средине данас се све више у свету баве разне владине, невладине као и међународне организације. Ако узмемо у обзир да једну од највећих претњи по еколошки систем у свету

[15] На „Земаљском самиту“, који је одржан 1992. године у Рио де Жанеиру, у Бразилу, светски лидери су усвојили препоруке Брунтлендове комисије и документ под именом „Агенда 21“ који садржи препоруке за управљање земљишним, воденим и шумским ресурсима у 21. веку. (https://sustainabledevelopment.un.org/content/documents/Agenda21.pdf, 2016, 11. мај)

представљају ТНК које услед емитовања велике концетрације штетних гасова у земљину атмосферу изазивају негативне еколошке последице, онда закључујемо да су еколошки и економски проблеми света данас тесно повезани.[16] ТНК дакле представљају један од основних стубова глобализације, а глобални развој је тренутно незамислив без прекомерног исцрпљивања природних ресурса. У таквој констелацији снага највећу штету трпе земље „Трећег света" које се данас све више суочавају са дужничком кризом и немогућношћу сервисирања зајмова и кредита.

Ипак, најопаснији и најизраженији актуелни еколошки проблем који погађа планету Земљу, јесте проблем глобалног загревања и климатских промена. Велика емисија штетних гасова и стварање такозване „стаклене баште" представља еколошки проблем који узрокује пре свега човек. Према извештајима Националне здравствене академије Америке, ниједна друга еколошка катастрофа неће изазвати толико штетне ефекте као глобално загревање, које за стотинак година може да доведе и до нестанка биљног и животињског света на Планети. Глобално загревање ће утицати на отапање глечера на северном и јужном полу, повећање нивоа мора, појаву природних катастрофа као што су олује, поплаве, смањивања ресурса пијаћих вода и слично. И сами смо сведоци таквих природних несрећа којима је свет био изложен у последњих двадесетак година.

Управљање животном средином, са аспекта очувања еколошке одрживости је врло сложан процес који захтева одговарајуће алате за поуздану процену ризика и претњи, као и касније доношење квалитетних одлука. Нагли раст светске популације и снажан економски напредак, а са друге стране све већи притисци на побољшање животног окружења и услова за здраву животну средину, представљају сложен и тежак задатак институција које се баве еколошком безбедношћу. Безбедност животне средине представља заштиту животне средине и виталних интереса грађана,

[16] Студија Организације за економску сарадњу и развој је показала да се у Кини од последица загађења природне средине годишње разболи и умре око милион људи. Оваква ситуација је посебно изражена у последњих десетак година када је Кина доживела своју економску експанзију. Поред тога, наведена студија је показала да се у Кини годишње разболи од болести респираторних органа око 20 милиона становника, управо из истих разлога. (Живков, 2008)

друштва и државе, од унутрашњих и спољних утицаја, штетних процеса и трендова економског развоја који угрожавају здравље људи и опстанак човечанства, биодиверзитета и одрживост функционисања екосистема. Дакле, било какво нарушавање у том смислу може да доведе и до отворених конфликата међу ентитетима на одређеном простору. Међутим, и кад сукоба нема, само нарушавање и поремећаји у животној средини доводе до проблема који могу дестабилизовати стање локалне, регионалне, а често и националне заједнице. Проблеми и ризици који се јављају у животној средини одражавају се негативно на здравље људи, а ако узмемо у обзир да је ¼ болести у свету узрокована променама квалитета животне средине, схватићемо колико су превентивне мере еколошке безбедности важне за здравље и у крајњем случају, за опстанак човечанства (Wenning et al., 2007: 19–36).

Најчешће дефинисани глобални еколошки проблеми савременог света би се могли поделити у следеће категорије: уништавање озонског омотача и стварање ефекта стаклене баште, квалитет и доступност воде за пиће, загађење ваздуха, неконтролисана сеча шумског покривача, губитак биодиверзитета и дезертификација — ширење пустиња.[17]

Узајамни односи између животне средине, екосистема и људских активности у последњих неколико година изазивају интересовање многих међународних и националних организација које се баве облашћу људске безбедности. Утицај екосистема на људско здравље је такође предмет истраживања и интересовања разних међународних институција. Само правилним, планским и ограниченим односом према екосистему човек може користити капацитете хране, горива и остале природне ресурсе, а да при том не утиче негативно на животну средину. На пример, неконтролисаним крчењем шума, човек изазива појаву ерозије земљишта, што касније доводи до огромних последица и нарушавања животне средине. Међутим, треба имати у виду да на „нестајање“ шума и зелених површина утичу и све

[17] Diamond дефинише дванаест проблема животне средине са којима се суочава савремена светска популација: уништавање природних станишта (углавном кроз крчење шума), смањење извора хране из природних капацитета, губитак биодиверзитета, ерозија земљишта, исцрпљивање природних ресурса, загађивање водених површина (река и језера), инхибиција природних фотосинтетичих ресурса, уношење пестицида у животну средину, вештачко индуковање климатских промена, пренасељеност. (Diamond, 2005)

учесталије климатске промене узроковане загађивањем ваздуха које изазивају појаву такозваних „киселих киша“.

Посебан проблем са аспекта еколошке безбедности представља нерационално коришћење шумског покривача које доводи до појаве ерозија, то јест померања земљишта са једног места на друго. Свакако да је ерозија природни процес, али њена учесталост је последица и деловања човека на природу. Најчешћи облик ерозије који се јавља код нас и у свету представља ерозија узрокована водом.[18]

Поред квалитета земљишта и ваздуха, на човека, посматрано у дужем временском периоду, утиче и биолошка разноврсност гена, врста екосистема на Земљи, биодиверзитет. По дефиницији биодиверзитет обухвата укупну различитост и варирање гена и свих врста микроорганизама, гљива, биљака и животиња, као и сву разноликост екосистема где су жива бића активни извршиоци еколошких процеса. (Radovic, 2005: 17-52)

Складиштење нуклеарног отпада и даље представља један од проблема великих сила, који се решава потписивањем уговора са државама, најчешће сиромашним и земљама у развоју, на основу којег токсична и средства са високим степеном зрачења складиште, доводећи у опасност становништво које живи у непосредној близини. За то стање висок степен одговорности сносе носиоци власти склони корупцији и противзаконитом стицању материјалне користи. Они потписивањем штетних уговора или недовољно прецизно дефинисаних услова у уговорима, стичу материјалну и

[18] Хаити је најсиромашнија земља у западној хемисфери са свега 1.200 $ бруто националног дохотка. Око 80 % становништва Хаитија живи испод линије сиромаштва. Нерационално коришћење пољопривредног земљишта и крчење шума довело до је до тога да је земљиште посебно склоно ерозији. Слаби услови за заштиту животне средине су кроз историју доводили до честих миграција Хаићана (око 1,3 милиона). Од укупне покривености Хаитија шумским покривачем само 2 % је остало од првобитног стања. Један од чиниоца који су проузроковали такву ситуацију су француски колонизатори који су правећи плантаже за кафу и шећер немилосрдно крчили шумске површине. Дрвна индустрија је процветала на Хаитију, међутим драстично смањење шумског покривача довело је до додатних ерозија земљишта што је даље уроковало поплаве. Последња ерозија, 2010. године, проузроковао је огромне материјалне штете и деградацију животне средине. У питање је доведен квалитет земљишта и воде за пиће, што је узроковало миграцију неколико хиљада становника. Догађај је дакле био последица комбинованог деловања природних и људских фактора. Иако није могао да буде спречен од стране човека, неодговоран однос према животној средини и изостанак превентивног деловања проузроковао је многоструко веће штете по живот и здравље људи.

другу врсту користи, не водећи притом рачуна о здрављу и негативним последицама на домаће становништво. Врло често, услед разних врста притисака, потписаних споразума о билатералној и другим врстама сарадње, Владе појединих држава трпе снажне притиске како би прихватили неприхватљиве услове који се касније негативно одражавају на становништво. У оваквим и сличним случајевима снажну улогу имају невладине институције и организације за заштиту права људи, а ако говоримо о еколошким проблемима, то су организације и институције које се баве еколошком безбедношћу.[19]

Посебан проблем представљају ризици природног порекла. Када разматрамо природне појаве и катастрофе, узимамо у обзир, пре свега, климатске промене узроковане порастом температуре, отапањем глечера и порастом нивоа мора, дефорестацију земљишта која узрокује ерозије и клизишта. Највећи проценат светске популације изложен је управо овој врсти ризика. Када је реч о Републици Србији сведоци смо догађаја у мају месецу 2014. године, када је услед поплава, дошло до уништења стамбених објеката у великим размерама, па и до губитка неколико људских живота. Чињеница је да су природним катастрофама најугроженије неразвијене и сиромашне земље, не само због њиховог положаја, већ и због превентивних безбедносних мера које се много успешније и ефективније предузимају у високоразвијеним земљама, а односе се на „управљање ризицима“. Како сматра проф. Радовић Весела катастрофе највише последица имају у неразвијеним и земљама у развоју зато што су најрањивије и имају слабе капацитете... На пример, земљотрес од 6,6 степени по Рихтеру који је 2003. године погодио Иран, усмртио је око 40.000 људи. Насупрот овом, земљотрес од 6,5 степени по Рихтеру који је погодио централну Калифорнију четири

[19] Године 1967. један од власника корпорације FIAT препознаје проблеме везане за квалитет животне средине, ресурса, повећање бројности људске популације и увиђа потребу за проналажењем решења. Око себе окупља тим експерата из различитих области природних, друштвених и техничких наука који трагају за одговором на питање *куда иде ова планета и шта ће бити са човеком?* Као резултат 1972. године излази публикација под називом „Границе раста“ у којој се појављује први компјутерски модел предвиђања развоја човечанства до 2100–те године, у односу на параметре: расположиви ресурси, бројност људске популације, расположивост хране, индустријска производња и загађивање. (Гиденс, 1997)

дана раније, однео је два живота, а повређено је било око 40 људи. (Радовић, 2013)

Један од индикатора одрживог развоја је „еколошки отисак“ (енгл. *The ecological footprint*). „Еколошки отисак” представља процењену величину биолошки продуктивног земљишта и водних површина које треба да се регенеришу (уколико је то могуће), ресурса које људски род користи и апсорпцију отпада које ствара тренутна технологија. Анализирајући „еколошки отисак” дошло се до закључка да потрошња природних ресурса од стране човека превазилази способност планете за њихову рециклажу. (Ишљамовић и сар., 2009)

3.1.8. Локални и етнички сукоби

Реч *етницитет* потиче од старогрчке речи *ethnos* која означава читав низ ситуација у којима неки колективитет људских бића заједно живи и дела и која се данас најчешће преводи као „народ“ или „нација“. (Ценкинс, 2001) Често се у литератури мешају појмови етничког и националног идентитета, тако да је у том смислу потребно рећи да се појам етнички везује за етничку скупину или заједницу, док се појам национални везује искључиво за националну заједницу, тј. нацију у целини. Етнички идентитет је везан за историју човечанства о чему сведоче археолошка налазишта и сачувани писани документи. Дакле, он је старији од националног идентитета који је изграђен тек у епохи модерног друштва (развој индустријског друштва, урбанизације), када људи почињу да се организују у нове целине (образовне, културне, језичке и слично).

Према Бжежинском, 20. век је век халуцинаторне политике и политике стравичног убијања у којем су ратови однели око 87 милиона живота, док се број рањених, осакаћених и страдалих не може ни проценити. (Бжежински, 1994) Ратови и сукоби локалног карактера мотивисани етничким и верским супротностима посебно су погодили подручје Југоисточне Европе, пре свега Балкана. Међутим, пример таквих сукоба имамо и данас који нису

ескалирали искључиво захваљујући реакцији међународне заједнице и присуству међународних снага на угроженом подручју, а ради се о сукобу између Грчке и Турске због недефинисане границе на Егејском мору и због Кипра. Сукоб Албаније са Македонијом, као и насилно отцепљење дела државне територије и стварање државе Косово, представљају такође врсту етничких локалних сукоба и тиме актуелну претњу по безбедност региона. (Таталовић, 1998: 65-78)

Етнички сукоби и односи данас одређују безбедност великог дела националних држава и региона у свету. Ово је посебно важно у регионима света где постоје догађаји из прошлости који су снажно утицали на међуетничке и међунационалне односе њихових насељеника. Западни Балкан је, услед бурних историјских догађаја, интересантан за студију и изучавање о међуетничким односима. Поред тога наведено географско подручје обилује високим степеном етничке разноликости што је последица богате историје насељеног народа, али исто тако и локалних и регионалних ратова вођених на том подручју. Прекрајање граница и миграције становништва узроковали су сложене међуетничке и међунационалне односе, те се ово подручје сматра трусним и безбедносно нестабилним. Раздобље у којем су и међународне организације, као што су Уједињене нације, поред националних држава, усвојиле поједине документе који дефинишу и регулишу етничке односе између и унутар држава, наступа након Другог светског рата. Треба напоменути и то да су инструменти Уједињених нација за заштиту људских права и националних мањина били искључиво у функцији превенције сукоба и њихове стабилизације. У том смислу, посебан проблем представља чињеница да су такви сукоби, поред етничког карактера, у себи садржали и идеолошке, верске и друге врсте узрока. Улога међународне заједнице и институција као што су ЕУ, УН, ОЕБС (Организација за европску безбедност и сарадњу) је изузетно важна како би се изградња Уставних, Законских и подзаконских аката националних држава додатно учврстила и унапредила, а унутар–државни односи према националним мањинама подигли на виши ниво поштовања људских права. Један од услова који позитивно делују на националне државе, када је

поштовање права националних мањина и етничких идентитета у питању за земље Западног Балкана, је чланство у Европској унији. Питање квалитета међуетничких односа данас се везује за снагу државних институција и њихову изграђеност, висину политичке културе и међусобно поверење. Најчешћи узроци и поводи оружаних сукоба широм света биле су територијалне претензије као и унутрашњи политички сукоби. Први су чешће везани за ратове ширих размера, док се други готово увек везују за локалне оружане сукобе. Дакле, локални сукоб је сукоб између две или неколико држава, ограничен на простор на којем се води као и у погледу ангажованих снага и средстава. Готово сви ратови, изузев Првог и Другог светског рата, су према мишљењу многих научника, окарактерисани као локални.

Међутим, етнички сукоби нису увек узроковани прекрајањем граница националних држава и борбом за стицање људских права мањина. Пренасељеност земљине кугле становништвом узрокује проблеме који се огледају и у недостатку хране. Један од основних узрока конфликата јесте однос према природним ресурсима, који је у случају еколошких избеглица, када се имају на уму будуће генерације, флексибилнији. Разлог томе је што се еколошке избеглице у највећем броју случајева на новонасељеном подручју задржавају ограничени временски период па им је и однос према природним капацитетима такав.[20] Изненадни стрес у животној средини може, под

[20] Пример таквог сукоба је случај избегличког кампа „Бонга“ у Етиопији. Камп је формиран уз надзор UNHCR-а (енгл. United Nations High Commissioner for Refugees) и у њему је у почетној фази 1993. године смештено око 11.000 избеглих лица из Судана. Конкретно, ради се о етничкој заједници Удук, која је више пута од 1983. године морала да напусти Судан због грађанског рата који се водио у овој држави. Грађански рат је узроковао уништавање природних ресурса који су обезбеђивали наведеној популацији минимум услова за нормалан живот. Удук своје уточиште, у координацији са UNHCR, у нади да ће се вратити својим домовима, налази у пограничном делу Етиопије ка Судану, регион Гамбела. Камп се налазио у близини око 800 хектара пољопривредних површина и површина богатих шумама. Врло брзо су почеле нетрпељивости локалног становништва према избегличком, које су се односиле на оптужбе у вези крађе шуме и плодова са пољопривредних површина и слично. У исто време, један део земљопоседника, давао је своје земљиште у закуп новопридошлом становништву кампа „Бонго“ које је успевало да постигне веће приносе од домаћег становништва. Још један проблем на који локално становништво није гледало благонаклоно представља чињеница да је избегло становништво имало огроман природни прираштај, тако да је већ 2001. године достигло бројку од 16.000. У исто време међународна заједница UNHCR врши надзор и контролу активности у кампу преко неколико волонтера, држављана Етиопије, који су свакодневно извештавали да је стање у капму уобичајено и без тензија.

одређеним друштвеним условима, бити катализатор за продубљивање социјалног раслојавања и сукоб. (Drury & Olson, 1998: 153-161)

3.1.9. Шпијунажа

Под „шпијунажом се углавном подразумева тајно, потајно, прикривено и на преваран начин прикупљање економских, политичких, војних и техничких података, које држава и покрети означавају као тајне." (Ђорђевић, 1978: 17)

О значају информација говорио је пре 2500 година чувени кинески ратник и мислилац Сан Цу (Sun Tzu). Значај његових речи понајбоље су схватиле војне формације широм света, али и мултинационалне и транснационалне компаније које своје пословање унапређују управо применом филозофије чувеног кинеског ратника. У својој књизи *Умеће ратовања* наведени аутор указује на прве облике појаве шпијунаже међу зарађеним странама. У једном делу књиге наводи потребу доброг познавања непријатеља као претпоставку квалитетнијих припрема за добијање битке или рата. То „предзнање" не може се добити од духова, богова нити аналогијом са прошлим догађајима, већ искључиво од људи који познају ситуацију непријатеља. (Сун, 2007: 232)

Почеци развоја пословне шпијунаже забележени су у 15. веку, када је кинеска принцеза, на капи украшеној цвећем, пренела у Индију чауре свилене бубе и на тај начин предала свом будућем мужу строго чувану тајну о начину производње свиле. Тада Индија започиње производњу свиле и временом постаје један од највећих произвођача свиле у свету. (Дураковић, 2007)

Снажнији развој пословне шпијунаже забележен је почетком 20. века у САД-у, а први европски државник који је схватио њен значај био је Винстон Черчил (Sir Winston Leonard Spencer Churchill), који је 1919. године у Великој

Међутим, ситуација је била сасвим другачија, те је на послетку дошло до сукоба и људских жртава. (Martin, 2005: 329-346)

Британији основао „Обавештајни центар за проучавање индустрије“. Неколико година након тога, сличну установу оснивају Јапанци, који су данас отишли најдаље када је питању индустријска шпијунажа.[21] У актуелном тренутку, у Јапану и у његовим представништима ван матичне државе, овим се послом баве добри познаваоци обавештајних служби, а у неким ситуацијама и бивши припадници обавештајно–безбедносног система државе. Успех јапанске индустрије и привреде неретко се приписује успешном раду пословног обавештајно–безбедносног система. Дакле, почеци појаве пословне шпијунаже везују се за потребе војне шпијунаже. У склопу војне шпијунаже, привреда једне државе је у почетку била усмерена на прикупљање сазнања о производним капацитетима наоружања и војне опреме одређене државе, као и о њиховој технологији израде.

3.2. ТЕОРИЈСКИ ПРИСТУПИ САВРЕМЕНИМ БЕЗБЕДНОСНИМ ИЗАЗОВИМА

До краја двадесетог века, тачније до 1994. године, безбедност се посматрала искључиво са аспекта безбедности државе, превасходно са војног становишта. Појавом и других врста угрожавања опстанка људске цивилизације и човека као појединца, јављају се и други концепти безбедности као што су еколошка, безбедност заједнице, политичка безбедност. Томе је допринела и појава оснивања приватних актера безбедности као што су приватне службе које делују у оквиру пословних субјеката, а држава им није у центру интересовања. „Пракса је показала да се ослањањем на реалистичне теорије безбедности и традиционалним реалполитичким приступом тешко могу решавати савремени безбедносни проблеми. (...) Реализам, као ни либерално–институционалистички приступ

[21] Јапан је острвска земља са специфичним језиком, културом и високим степеном патриотизма. Поред тога ову земљу карактеришу висок ниво лојалности и оданости држави и компанији, а као основни циљ намеће се освајање светског тржишта. Сматра се да без развијене економске шпијунаже Јапан не би могао да оствари такве економске резултате на светском тржишту, а да су за то заслужне пре свега школе, као што је „Мацушито школа за бизнис и менаџмент“ у којој се школује пословна елита ове државе. (Зиндовић, 2008).

не дају, међутим, оквир за решавање постојећих проблема безбедности на нивоу локалних заједница и грађана.“ (Ђорђевић, 2013: 73)

Основна схватања теорија безбедности развила су се под окриљем науке о међународним односима, а најчешће се деле у три основне групе:

1. Реалистички
2. Либерално–институционалистички,
3. Алтернативно–критички приступ. (према Симић, 2007: 165-193)

3.2.1. Реализам

Представници који заступају ову теорију безбедности мишљења су да су „државе главни актери међународних односа који су анархични и неизвесни, пре свега зато што произилазе из људске природе у којој доминира жеља за моћи“ (Димитријевић и Стојановић: 1996: 36). Ратови су резултат политички агресивних државника и њихових присталица који следе експанзионистичку спољну политику. Овај теоријски приступ полази од чињенице да је човек егоистично биће склоно анархији и да је у циљу његове контроле потребно успостављање ауторитета од стране државе, као и изналажење инструмената којима ће се вршити контрола појединаца али и читаве друштвене заједнице. Слична је ситуација и у међународним односима у којима државе константно преиспитују своју моћ у односу на друге државе и на тај начин подижу степен националне моћи на што је могуће виши ниво, а у циљу квалитетнијег супротстављања и отклањања потенцијалног извора угрожавања. Државе такво стање спроводе подизањем степена обуке сопствених оружаних снага и константним наоружавањем. Један од аутора који је заговорник идеје неореализма Волц (Waltz, K. N.), сматра да је анархичност у међународним односима могуће избећи једино јачањем сопствених унутрашњих војних капацитета, пошто на међународном плану не постоји ниједна организација која поседује врховни ауторитет (Waltz, 2010). Неореалисти сматрају да се понашање држава на међународном плану одвија према већ познатим и усвојеним обрасцима, а као пример

наводе односе између Атине и Спарте из даље прошлости и однос САД-а и Руске Федерације у данашње време. Дакле, по среди је теорија безбедности која заступа максималност нивоа моћи. То, између осталог, подразумева да је држава у циљу увећања своје моћи непрекидно у борбеном ставу према другим државама.

3.2.2. Либерализам

За разлику од поборника реалистичке теорије безбедности, либерални институционалисти или либералисти заговарају теорију која истиче значај међународних институција у међународним односима, који је могуће јачати узајамном културном, економском и политичком сарадњом. Чиниоци који су повољно утицали на ову теорију су висок техничко–технолошки напредак и све већи међузависни однос међу државама у свету. Они притом не споре мишљење реалиста да је преовлађујуће стање међу државама у свету стање анархије и да је политика силе у таквом систему могућа. Међутим, док реалисти структуралну анархију међународног система сматрају неизбежном и непроменљивом последицом оштрог разликовања између унутрашње и спољне политике, при чему је у унутрашњим односима могуће достићи правду, заједништво, демократију и друштвени напредак, али не и изван државе, с обзиром на то да у последњем случају изостаје средишњи ауторитет (у међународном систему државе су осуђене на самопомоћ у тежњи да осигурају опстанак), дотле либерални институционалисти одбијају да прихвате њихове закључке у погледу немогућности превазилажења таквог стања у међународним односима и сматрају да политика силе није нужна. (Симић, 2002: 36)

Један од првих заговорника либералног институционализма јесте Имануел Кант (Immanuel Kant) који пропагира државно уређење под називом либералне републике. Кант такво уређење види кроз спровођење неколико ставки: укидање стајаће војске, немешање у унутрашње ствари других држава, забрана шпијунаже, прекид империјалистичких тежњи. Поред тога,

међународни систем види као конфедерацију либералних република што представља повољну околност за стварање глобалног система безбедности. Управо јачање међузависности држава узрокује јачање међународних институција, које би требале свим државама да обезбеде остварење њихових интереса. (Кант, 1995)

Осамдесетих година прошлог века јавља се покрет неолиберални институционализам који наглашава значај међународних институција као што су УН. Према мишљењу ових теоретичара, међународне институције узимају важну улогу у арбитражи и могу да подстичу међународну трговину, а самим тим и односе међу државама, стимулишући њихов повољнији статус или супротно, увођењем санкција и других врста ограничења и квота у трговини. Још једну повољност оснивања међународних институција, неолиберални институционалисти виде у смањењу цене трансакција кроз одређивање јасних правила пословања, у већој доступности информацијама, као и у ефикаснијим решавањима неспоразума и сваке друге врсте конфликата. У оквиру неолибералних теорија у данашње време најзаступљенија је „теорија демократског мира“. За разлику од Кантовог виђења либералног институционализма, ова теорија предлаже и успостављање слободне трговине између либералних држава. Предуслов мира, према теоретичарима који заступају теорију демократског мира, лежи у демократији као друштвеном уређењу.

3.2.3. Алтернативно–критички приступ

Хладни рат није представљао само политичку реалност већ и интелектуални оквир у којем су се развијале нове теорије безбедности, посебно осамдесетих година када је постало извесно да он почиње да се ближи крају. Новонастале околности, распад Берлинског зида и почетак грађанског рата у тадашњој СФР Југославији, затекле су познаваоце безбедности неспремне јер ни једна претходна теорија није могла да објасни развој актуелних догађаја. Нови теоријски приступи и категорије били су

неопходни за разумевање актуелних догађаја што је довело до развоја алтернативно–критичког приступа теорије безбедности.

3.2.3.1. Копенхашка школа

Развој Копенхашке школе почиње 1985. године када је основан Институт за проучавање мира и конфликата. Вевер (Wæver) и Бузан (Buzan) су научници који су дали највећи допринос развоју ове теорије безбедности. Поменути аутори су први направили јасну разлику безбедносних посебности условљених територијом. У том контексту направили су јасну разлику између европске сфере безбедности и безбедности других територија, пре свега САД–а. Аутори су нагласили да су политички и економски односи међу државама у Европи битно другачији од оних у САД–у, стога и да безбедносна ситуација и методологије приступа овој теми морају да се разликују једна од друге. У својој студији (*Идентитет, миграција и нова безбедносна агенда у Европи*) по први пут се уводе и невојни проблеми. Управо ова школа уводи у безбедносну сферу социјалне, економске, политичке претње и оне које су везане за заштиту животне средине. Копенхашка школа је специфична и по томе што област безбедности дели по следећим нивоима анализе (према Buzan et al., 1998):

- Међународни систем обухвата целу планету и изнад њега не постоји нити један системски ниво;
- Међународни подсистем подразумева групе јединица у међународном систему које могу да се деле на територијалне (АСЕАН, ЕУ) или на оне које то нису (УНХЦР, ОЕЦД);
- Јединице се састоје од кохезивних подгрупа, организација и друштава које су међусобно зависне (држава, транснационална компанија);
- Појединци су организоване групе унутар јединица (лобисти, бирократе);

- Индивидуе представљају најнижи ниво анализа у друштвеним наукама.

Копенхашка школа прави јасну разлику између субјективног и објективног схватања безбедности. Објективно схватање се односи на реалну опасност, док је субјективно схватање одређено личним доживљајем. Лични доживљај се формира на основу личних запажања посматрача, тј. на основу информација које добија из спољашњег света. Вивер сматра да главни ефекат изговарања појма *безбедности* представља потенцијал да публика допусти нарушавање правила која би иначе морала бити поштована. (Wæver, 2003) Ради се о томе да, уколико постоји претња неком референтном објекту изражена у тој мери да представља реалну опасност, дозвољено је употребити специјалне мере, мимо установљених правила и прописа у циљу отклањања такве опасности. Овде аутори уводе појам *егзистенцијалне претње* који се односи на универзалне стандарде, утврђујући шта то представља претњу појединачном људском животу посматрајући то кроз различите безбедносне сфере или области. У војној сфери то су претње оружаним снагама од стране других држава или организација. У политичкој сфери претње се односе на нарушавање степена суверености националне државе, а у социјеталном сектору на колективну промену људских идеологија и колективитета услед еволуцијских промена изазваних унутрашњим и спољашњим догађајима који нас окружују. У сфери заштите животне средине егзистенцијалне сфере би се односиле на очување биосфере, еколошке одрживости или појединих врста флоре и фауне. Оно што представља посебну одлику ове теорије безбедности јесте искључивање политике из безбедносног контекста и правила одлучивања. Померање питања безбедносних проблема коришћењем реторике егзистенцијалне претње представља правац за коју се залажу поборници Копенхашке школе.

3.2.3.2. Концепт људске безбедности

Завршетком Хладног рата развијају се нови облици међународних односа међу државама, који доводе у питање дотадашњи аналитички оквир тумачења нових безбедносних претњи. Нови оквир питање безбедности усмерава на два основна правца. Први, који у тумачење појма безбедности укључује и невојне претње (економске, политичке, еколошке) и други правац који у центар поимања безбедности ставља појединца и његову добробит — људска безбедност. (Дулић и сар., 2010: 13)

Такође, један од важнијих проблема који је питање безбедности поставио у раван међународних односа јесте глобализација. Процес глобализације је интензивирао транснационалне токове добара, услуга, финансија, информација, технологије, идеја, али исто тако увео и нове облике угрожавања безбедности појединца, као и нове ризике. То је условило да се преиспита традиционални појам безбедности, а људска безбедност је препозната као концепт који има потенцијал да захвати глобалне безбедносне ризике и претње и понуди прихватљиве стратегије за њихово отклањање. (www.humansecurity-chs.org, 2016, 6. децембар)

Снажан економски развој, посредством примене најновијих технолошких и техничких достигнућа, помера питање капитала ван граница националних држава. Оснивање транснационалних компанија усмерених на максимизацију профита изместило је права и интересе грађана у другу раван која је кат–кад штетна по њих. Код појединих држава, најчешће држава у развоју, чије су државне институције донекле под знаком питања, поједине ТНК–а својим финансијским потенцијалима и стицањем одговарајућег нивоа моћи, утичу на доношење одлука, понекад штетних по грађанство, а у интересу власника крупног капитала (Ђорђевић и Мијалковски, 2011: 338-339).

„Свет може да буде миран само ако су људи безбедни у свом свакодневном животу“ (http://hdr.undp.org/en/content/human-development-report-1994, 2016, 12. јануар) кључна је реченица Развојног програма Уједињених Нација, која указује на потребу развоја концепта људске

безбедности. Посебан значај Извештаја о људском развоју УНДП–а (енгл. *United Nations Development Program*) из 1994. године, огледа се у наглашавању да се ново схватање појма безбедности не односи искључиво на оружје, већ на живот и достојанство човека. Извештај је дао широко одређење људске безбедности кроз седам димензија. У наведеном извештају се наводи да људска безбедност укључује „безбедност у односу на хроничне претње као што су глад, болести и тлачење, као и заштиту од изненадних и штетних поремећаја у одвијању свакодневног живота, било у кући, на послу или заједници." (http://hdr.undp.org/en/content/human-development-report-1994, 2016, 12. јануар)

Основна предност концепта људске безбедности произилази из наглашавања приоритетних претњи усмерених ка појединцу и/или заједници. Приоритетне претње, то јест њихова перцепција и формулација, нису константне, већ варирају у зависности од простора у којем се изражавају, али и од других фактора. (Bosold & Werthes, 2005: 84-101)

Потребно је узети у обзир да посматрана целина (држава, институција, организација) може по усвојеним критеријумима да буде безбедна, али да елементи те целине нису безбедни на задовољавајућем нивоу. Уколико је нпр. држава заштићена од угрожавања споља, то не значи да су њени грађани безбедни у обављању својих свакодневних активности. Претње у том смислу могу да буду узроковане високом стопом уличног криминала, породичним насиљем, неадекватним условима у радном окружењу и животном амбијенту. „Последица неједнакости у погледу стања безбедности и сигурности на одређеном простору најчешће долази као последица структуралних поремећаја." (Ђорђевић, 2013: 84)

Један од првих аутора и родоначелника студија мира, јесте Јохан Галтунг (Johan Galtung), који је у својим радовима тежио да направи јасну разлику између очигледног и суптилног насиља. Ради се о насиљу које није изазвано споља ка држави као предмету заштите носиоца националне безбедности, па су самим тим овим структурама наведене појаве мање интересантне, као и теоретичарима класичних теорија безбедности. Галтунг разматра десет линија које означавају потенцијалне облике структурног и

културног насиља, а односе се на међусобне интеракције између човека — човека и човека — природе (Табела бр.2). (Галтунг, 2009: 91)

Табела бр. 2: Галтунгова класификација структурног насиља према контексту поделе

Контекст поделе	Термин
Људи / нељуди	Врстизам
Род (мушки/женски)	Сексизам
Генерација (стари/млади)	Ејџизам
Раса (белци/обојени)	Расизам
Класа (виша/нижа)	Класизам
Народ (виши/нижи)	Национализам
Земље (центар/периферија)	Територијализам
Држава – грађанско друштво – капитал	Етатизам - анархизам – капитализам

(Ђорђевић, *Људска безбедност, глобални контекст и примена у Србији,* 2013)

Сваку од наведених врста насиља Галтунг посебно објашњава и прави компаративну анализу садашње људске цивилизације и онога што се дешавало кроз људску историју. Класификацију територијалног насиља Галтунг образлаже све већим раслојавањем светске популације на богате и сиромашне.[22] Почеци ове врсте насиља забележени су колонијалним аспирацијама великих сила, које су довеле до готово потпуног истребљења аутохтоних народа. Основа у спровођењу ове врсте насиља лежи у економској експлоатацији. Расизам као критеријум насиља се може јасно анализирати кроз пример расне нетрепељивости у империји Адолфа Хитлера названој Трећи рајх, у којој је исказана бруталност расистичког безумља спровођеног према другим народима, а пре свега Јеврејима и Ромима. Заговарање такозване надљудске популације (нем. übermensch) и примена насиља према другим народима издвојило је ове облике расизма као најизраженије и најбруталније у људској цивилизацији.

Једна од најутицајнијих теорија по развој концепта људске безбедности представља теорија одрживог развоја која одрживост посматра са три аспекта: економског, еколошког и социјално–политичког. Теорија

[22] Према подацима организације Oxfam, осамдесет пет људи на планети посеудје богатство које се мери укупном количином богатства којима располаже сиромашнија половина становника на Земљиној кугли. (http://www.novosti.rs/vesti/planeta.299.html:474249-Osamdesetpet-najbogatijih-ima-para-kao-i-35-milijardi-najsiromasnijih, 2016, 12. мај).

одрживог развоја је добила на значају после Брунтлендовог извештаја у којем је наглашена потреба развоја који задовољава потребе садашњости без угрожавања могућности будућих генерација да задовоље своје потребе. (World Commission on Environment and Development, 1987: 43) Човек је наставио са експлоатацијом животне средине, индустријализацијом и технолошко–техничким развојем чиме је допринео угрожавању животног окружења, у тој мери да се поставља питање могућности изласка из новонастале ситуације. Такође, поставља се питање опстанка биљног и животињског света на Планети, јер су већ сада поједине врсте на прагу изумирања.

Концепт виталног језгра[23] је, такође, често присутан при теоријским расправама о садржају појма људска безбедност. Концепт је усмерен на заштиту људи од претњи које су изван њихове контроле, као што су финансијске кризе, насилни сукоби, неодговорна национална политика која угрожава систем јавних служби (здравство, образовање), тероризам, недостатак исправне воде за пиће, хронично сиромаштво. С обзиром на непредвидљивост последица, захтева се проактивна улога система која није шаблонска и која предвиђа могући развој догађаја и благовремену реакцију у складу са конкретним условима. Дакле, циљ је заштитити људе на одређеном простору, а не стриктно се придржавати процедура. (Дулић, 2009: 91)

Дулић Драгана наглашава следеће предности концепта људске безбедности на међународном плану (према Дулић и сар., 2010, 19):

- Фокусирањем на појединца и заједнице у оквиру концепта људске безбедности, промењен је политички пејзаж савременог света у погледу дискурса о хуманитарним и развојним последицама либералног схватања мира, безбедности, фундаменталних људских права, владавине закона и одрживог развоја. Шире концептуално разумевање слободе треба да послужи као инструмент свима онима који се баве практичном реализацијом програма намењених сиромашним, али и другим категоријама људи.

[23] Витално језгро чини скуп људских права и способности које морају да буду заштићене у свим условима. (Ђорђевић, 2013: 97)

- Концепт људске безбедности наглашава универзалност и примат људских права и слобода, тј. он не прави разлику између различитих врста људских права — грађанских, политичких, социјалних и културних.
- Концепт људске безбедности указује на негативне индикаторе развоја безбедности на неком локалитету. Тиме указује на проблеме и изазива промене од стране политичких структура, чиме се ситуација у вези људских права подиже на виши ниво.
- Концепт људске безбедности може да представља значајну подршку у политичким одлукама које се односе на постконфликтне ситуације настале као последица ратова и других кризних ситуација. Посебно уколико узмемо у обзир да наведени концепт представља модел за анализу и пројектовање приоритета у кризним ситуацијама.
- Оквир људске безбедности посвећен је вредностима као што су сигурност, стабилност и развој. Правовременим извештајима о небезбедностима и лишавањима права људи који егзистирају на одређеном простору, концепт људске безбедности постаје снажна подршка програму људског развоја, а самим тим подршка смањењу друштвених тензија.
- Концепт људске безбедности пружа основу за мониторинг и рано упозорење за кризне и посткризне ситуације. Идентификацијом главних претњи, систему раног упозорења даје додатну димензију и допуњује традиционалне социо–економске индикаторе.
- Концепт људске безбедности може да узме активно учешће приликом решавања постконфликтних ситуација у земљама у којима дубоко укорењени проблеми онемогућавају решавање питања људских права и безбедности појединца.
- Концепт подразумева следеће фазе, то јест полазишта приликом поступања у решавању проблема:

- Идентификација главних проблема са којима се сучава држава значајних са аспекта националног извештаја о људском развоју и људској безбедности;
- Конципирање националних приоритета;
- Дефиниција људске безбедности;
- Дефинисање најрелевантнијих облика људске небезбедности и њихово довођење у везу са људским развојем;
- Прикупљање података релевантних за стање људске безбедности;
- Истраживања грађана у вези перцепције о различитим врстама и облицима угрожавања, претњи и утицају на њих;
- Анализа и процена садашњих и бивших политичких иницијатива које представљају различите претње људској безбедности;
- Препоруке за будуће токове (циљеви, статегије) и мерење њиховог утицаја.

- Концептом људске безбедности ствара се подршка широком партнерству на међународном, националном и локалном плану.
- Концепт може да укаже који су изазови развоја, „суочени“ са класичним концептом безбедности, остали ван пажње медија, а имају важност за националну безбедност државе.
- Концепт људске безбедности допуњује миленијумске циљеве развоја кроз три димензије Миленијумске декларације: мир и безбедност, развој и људска права, демократија и добра владавина.

Мерење појава у оквиру људске безбедности представља тежак и сложен задатак и често је предмет расправа о могућностима и сврсисходности оваквог приступа. Проблем је додатно изражен због тога што се аналитичари и политички чиниоци не могу сложити у вези дефиниције људске безбедности која би створила услове за прикупљање и каснију анализу емпиријских података. Ако притом узмемо у обзир да људска

безбедност није искључиво листа објективних индикатора већ и субјективних искустава људи, проблем додатно долази до изражаја. Иако постоје критике на рачун овог концепта, он представља добар аналитички оквир који може да допринесе отклањању слабости у систему заштите пословних информација.

Лурент (Laurent) наводи: „Потребно је развити инструменте и методе мерења појединих специфичних студија људске безбедности, потребно је развити инструменте и методе мерења, специфичних ситуација људске безбедности и тако пружити специфичну слику о томе како људи укључени у истраживање перципирају своје безбедносно окружење. (...) Све у свему, потребна су даља побољшања у смислу партиципативне методологије која се користила, као и дизајнирања адекватних студија случаја“ (Laurent, 2005, www.security-and-peace.de/archiv/PDF/2005-1/SuF_01_2005_5.pdf, 2016, 9. мај).

Постоји неколико методологија мерења људске безбедности које произилазе из различитих схватања овог појма. Једна од њих је GECHS (енгл. *The Global Environmental Change and Human Security*) индекс људске небезбедности (IHI) који су предложили Лонерган и сарадници (Дулић и сар., 2010: 45). Они људску безбедност дефинишу као узрочну везу између еколошке и личне безбедности, а индекс људске безбедности се мери преко четири индикатора за сваки од друштвених, економских, еколошких и институционалних домена. Индекс људске небезбедности се дефинише у терминима претњи, као и могућност да се оне анулирају, ублаже или да се људи њима прилагоде. Могуће претње су: деградација земљишта, однос трошкова државе за куповину наоружања и војне опреме у односу на трошкове који се користе на образовање становништва, смртност деце, смртност мајки, стопа неписмености, увоз енергије, безбедност воде, доходак по глави становника, инвестиције. (Дулић и сар., 2010: 45–46)

Многи предлози за мерење људске безбедности се заснивају на годишњим Извештајима о људском развоју Уједињених нација. Извештај подразумева сложен индекс људске безбедности заснован на индикаторима

као што су: број смртних случајева у оружаним сукобима, учесталост криминалног насиља, број избеглица и други.

Андрју Мак (Andrew Mack) се фокусира на уску дефиницију људске безбедности ослоњену на термин насиља. Он за индекс људске небезбедности предлаже следеће елементе: смрт и повреде настале усред рата, геноцида и других тешких кршења људских права; податке о криминалном насиљу; погоршање индикатора здравља као последица рата и криминалног насиља; прилив избеглица и интерно расељених лица; штета причињена друштвеној инфраструктури која је у вези са насилним сукобом (прим. трговина људима). Према наведеном аутору кључни индикатори људске небезбедности су: смртност настала у току оружаних сукоба, геноцида и других видова насилне репресије, као и самоубиства. Подаци за ову методологију би се црпели из Светске здравствене организације. (Andrew, 2002: 515–525)

Методологија коју су предложили Кинг (King) и Марej (Murray) 2000. године дефинише људску безбедност као очекивање појединца да води такав живот који га неће довести у стање општег сиромаштва. У том смислу људска безбедност се мери индикацијом индивидуалног благостања путем индикатора: прихода, здравља, образовања, политичке слободе и демократије, наглашавајући развојни аспект људске безбедности. (Дулић и сар., 2010: 42–49)

Према извештају УНДП-а (Програма Уједињених Нација за развој), за анализу стања безбедности неопходна је анализа седам димензија концепта људске безбедности, а то су:

1. *Економска безбедност*, која анализира утицај економских прилика и трендова на неком простору и њихово дејство на стање безбедности људи и човека као појединца. На основу анализе степена развоја неког друштва, увођења ИКТ, техничко-технолошког развоја, затупљености класичне индустријске производње у односу на високо развијену, могуће је одредити колико је привреда једне земље конкурентна на међународном тржишту, што директно утиче на стање запослености и економску сигурност њених грађана. Анализом заступљености сиве

економије у укупној економији једне државе и корупције као болести система, фактор економске безбедности се може додатно дефинисати.

2. *Безбедност исхране* се може посматрати са аспекта доступности довољне количине хране неопходне за задовољавање основних људских потреба и са аспекта њеног квалитета који подразумева довољну количину протеина, витамина, минерала и других суплемената, као и исправност хране која директно утиче на здравље конзумената.

3. *Безбедност здравља* параметре за анализу узима из података који се односе на дужину живота, стопу природног прираштаја и ферилитета, али и на стање здравственог система. Управо ови показатељи дочаравају тренутно стање у здравственом систему једне државе и квалитет услуга које пружа.

4. *Еколошка безбедност* се посматра са аспекта анализе квалитета ваздуха, воде, земљишта и стања биодиверзитета одређене средине. Стање у законској регулативи државе и њена усклађеност са међународним нормама и активностима институција које се баве овом проблематиком такође представља област коју је потребно анализирати у циљу доношења закључка о стању безбедности у области животне средине.

5. *Лична безбедност* анализира безбедност индивидуа које егзистирају у неком друштву без обзира на достигнути степен безбедности њихове матичне државе. Често имамо ситуацију да је национална безбедност једне државе доведена на завидан ниво, међутим лична безбедност њених грађана се налази на много нижем нивоу. У том смислу, као параметри који утичу на стање личне безбедности, анализирају се следеће појаве у друштву: криминал (организовани, привредни, корупција), саобраћај (квалитет саобраћајница, број саобраћајних несрећа, квалитет и старост моторних возила), етничка структура, мањине и међуетнички односи (број етничких заједница на некој територији, проценат у укупној популацији).

6. *Безбедност заједнице* се посматра кроз анализу следећих параметара: насиље у породици (психичко, физичко, сексуално) које се посебно

испољава у кризним ситуацијама услед недостатка основних егзистенцијалних потреба за живот, квалитет становања (структура и квалитет животног простора, проценат личних примања који се издваја за стамбено збрињавање), стање медија и комуникација (квалитет медијске понуде, структура медија, распрострањеност и доступност медија), локална заједница (локална самоуправа, религија, државне институције), невладине организације (НВО) и синдикати.

7. *Политичка безбедност* се анализира кроз факторе политичког уређења, институције система, демократске одговорности носиоца власти и владавине закона. Она у том контексту анализира политичке партије и изборни процес, судство и правосуђе, јавну и државну управу, војску, полицију, избеглице, имигранте, права особа са инвалидитетом.

4. ТЕОРИЈА ИНФОРМАЦИЈА

Човекова опсерверско–слушна активност је тежишно усмерена ка сазнавању стања у свом окружењу, односно прикупљању информација чијим коришћењем настоји да успешно опстане и развија своје капацитете. Информација представља моћ за сваког човека, која долази до пуног изражаја у оквиру људског колективитета чији је он члан. Заправо, моћ једног људског колективитета одражава његову способност да опстане у објективној средини (природној и друштвеној) коју карактерише неизвесност. То подразумева способност субјекта да одреди, успостави, показује и одражава своје субјективно хтење (циљеве, вредности и интересе) у складу са објективним условима. Тиме, производи промене које обезбеђују његов опстанак и одрживи развој. Реч је о сложеном процесу ефикасног решавања бројних и разноврсних проблема (изазова, претњи и ризика) заснованом на сазнањима (подацима и информацијама) за доношење адекватних одлука.

„Реч је о управљачком процесу у коме одлучивање и реализација одлука једног људског колективитета вишеструко зависи од облика и карактера његове обавештености о другим људским колективитетима са којима је у некаквој комуникацији, наравно, и, од познавања својих чланова друштвених скупина.“ (Мијалковски и Томић, 2013: 23)

Када се анализира значај информација у савременом свету довољно је поћи од тога да човек на основу расположивих информација свакодневно доноси одлуке, обавља послове и задатке, усмерава сопствене активности, успоставља међуљудске односе, решава проблеме, планира будућност. Схвативши значај информација, човек је у прошлости тражио решења како би

их ставио у функцију бољег искоришћавања, чиме је иницирана појава више научних дисциплина које проучавају информације.

Теорија информација (енгл. Information Theory) проучава законитости повезане са предајом, пријемом, чувањем и обрадом информација. За разлику од теорије информација, теорија комуникација (енгл. Communication Theory) је научна дисциплина која проучава вероватност преноса података уз присутност шума и других сметњи на преносном путу, што значи да је за ову теорију важан преносни систем, а не само информација која се преноси. Обе теорије се темеље на поставкама научника Клода Шенона (Claudea Shannon) које је објавио у раду *Математичка теорија комуникација* (1948). (Јаворовић и Биланџић, 2007: 57)

Комплексно схватање информације претпоставља узимање у обзир њених следећих аспеката: појма, значаја, развоја, обраде, коришћења и чувања који се своде на одлучивање (Шема бр. 1).

Шема бр.1: Карактеристике пословних информација

4.1. ОД ПОДАТКА ДО ИНФОРМАЦИЈЕ

Централно место у теорији информација заузима *информација* као феномен и *комуникација* као процес. (Милосављевић и Адемовић, 2013: 11) Милосављевић и Адемовић у својој књизи издвајају следеће дефиниције информација:

- Информација је инкремент знања, њеним постојањем је наше знање о нечему увећано;
- Информација је значење које додељујемо податку;
- Информација је скуп података у неком контексту;
- Информација је примљена и схваћена порука.

Како би се суштински схватио појам *информације* важно је направити јасну разлику између *податка* и *информације*. Податак представља чињеницу предочену у формализованом облику (број, реч, слика) погодну за комуникацију, интерпретацију и обраду уз помоћ људи и машина. Могло би се рећи да је то порука која може, а не мора да се искористи. Тек када тој поруци доделимо неко значење и када она добије неки смисао онда податак постаје информација.

Човек као мисаоно биће има потребу за развојем нових информационо- комуникационих способности од постанка па до данас. Развој комуникације је свој први велики напредак доживео појавом писма, пре око пет хиљада година. Појавом папируса и писма прекинута је дотадашња пракса бележења информација и стварања цртежа на каменим плочама или у пећинама, и управо тај догађај представља основ за развој напредних врста комуникација у будућности. И у Библији, која је настајала пре три хиљаде година, у књижевном детаљу Мојсијевог слања извидника у Кананску земљу, забележена је потреба прикупљања информација и нешто што би се данас могло поистоветити са обавештајним деловањем. О важности информација говори и чињеница да се људска цивилизација не би развијала истим степеном и капацитетима да није било размене информација између различитих култура и да се искуства једне цивилизације нису користила за

развој друге цивилизације. Тек појавом папира и изумом машине за штампање, започиње револуција коришћења информација. Доступност књига различитог садржаја (верске књиге, филозофске студије, књижевна дела, путописи итд.) омогућавала је људима широм света стицање нових поимања и сазнања која су им до тада била делимично или у потпуности непозната. Тада настају и прве велике библиотеке, које у својим фондовима средином прошлог века броје и до неколико милиона наслова из различитих области људског живота. Међутим, информације саме по себи нису довољне, посебно у условима када су се почеле појављивати у великој мери коју човек није могао апсорбовати одједном. Човек је тада схватио потребу обраде информација чији се почеци јављају са развојем првих рачунара као што је „ENIAC", а касније и персоналних рачунара, „лап топ" рачунара, таблет уређаја и слично. Појавом телефона, радија, телевизије, а крајем 20. века и интернета, стварају се услови за развој науке, технике, технологије и привреде у обиму који је незапамћен у историји човечанства.

Тофлер (Toffler, A.) је међу првима препознао важност информација у модерном добу. Овај аутор у свом делу наводи да је човечанство у свом развоју прошло три информационо–технолошке фазе. (Toffler 1981: 32-33) Прва фаза обухвата период од постанка човечанства па до половине 19. века, када су се људи бавили углавном пољопривредом и живели у мањим заједницама. Информације су у том времену преношене усмено или путем курира. Проблем је представљала велика неписменост светске популације, а самим тим и немогућност стицања нових знања писаним путем. Друга фаза, према овом аутору, настаје другом половином 19. века и траје до педесетих година прошлог века. Ради се у периоду великог индустријског развоја човечанства и највећих открића која су снажно утицала на будући ток развоја човечанства. Концентрација светског становништва у градовима и развој терцијалних делатности, дао је напретку човечанства нову димензију која истиче значај информација за потребе даљег напретка и развоја. Везе међу људима подстакнуте развојем свих врста саобраћаја, изумом телефонских комуникација, постале су једноставније, брже, а повећање писмености и образовања светке популације створило је услове за ширење информација

без обзира на ком месту се на земљиној кугли налазили. Тек развојем ИКТ–а, који почиње изумом првих рачунара, а осамдесетих година широком употребом персоналних рачунара, наступа трећа информационо–технолошка фаза. Изумом интернета и развојем бежичних комуникационих модела, проток информација постаје готово тренутан и доступан свуда и сваком кориснику који поседује рачунар и има приступ некој од информационих мрежа. Паралелно са тиме, развијала се и обавештајна активност, којој је такво стање ствари погодовало. Питање квалитета информација које се нуде у медијима и могућности њихове провере представља додатни проблем, јер поузданост и тачност информација представља један од најважнијих приоритета обавештајних система.

Информација данас не представља само знање, већ и капитал, јер правовремена информација даје могућност њеном кориснику за боље и брже прилагођавање новонасталим тржишним условима, као и за стицање већег профита. Поред тога, доносиоцима државних одлука, лицима која управљају националним системима, потребна је права информација како би одлуке које доносе биле у складу са националним интересима те државе. Управо због тога велика се пажња посвећује овој области, а ТНК које послују у више земаља, широм планете Земље, оснивају сопствене службе преко којих долазе до информација од значаја за пословање пословног субјекта. „Поседовање информација даје предност у односу на друге. Оне су моћно средство које омогућава заузимање супериорног положаја, а у процесу одлучивања омогућавају доношење квалитетних одлука, лакше сналажење у несигурном свету, а тиме и једноставније остваривање циљева.“ (Петковић, 2009: 108-109)

Информација као ресурс има изузетан значај у готово свим областима људског деловања, у економији, медицини, астрономији, војној тактици и оперативци. Данас је свима јасно да је поседовање поузданих информација у реалном времену једна од суштинских предности у односу на конкурента, односно непријатеља. Исто тако, наводно заштићена информација, а доступна свима, нема готово никакву вредност. Управо због тога, информације је потребно заштитити и онемогућити неовлашћеним лицима

приступ без сагласности њиховог власника. Отицање битних информација из пословних система може да угрози њихово функционисање, доведе до великих губитака, чак и пропасти.

Првуловић сматра да није проблем само доћи до корисних сазнања и употребљивих података, него је још важније резултате њихове анализе адекватним мерама заштитити. Спречавање неовлашћеног приступа информацијама и њихове употребе у складу са интересима њихових поседника, даје поседницима шансу за пословни успех и развој шире заједнице. Да би се имао потпун ефекат у врло сложеној „међународној утакмици", није неопходно доћи само до употребљивих информација, што свакако није лако, већ их је потребно адекватним мерама заштитити, а затим употребити тако да за пословног субјекта постигну највећи ефекат у датим околностима. (Првуловић, 2010: 179-84)

Могло би се закључити да пренос, чување и заштита информација представљају основ за стабилан развој друштвене заједнице. У неким ситуацијама, претходно наведене радње утичу и на опстанак друштвене заједнице, чиме се бави теорија информација[24]. Њен задатак је да пружи теоријске и практичне оквире за синтезу система који обезбеђују ефикасност и расположивост информационих ресурса.

4.2. ПОСЛОВНЕ ИНФОРМАЦИЈЕ, ПОСЛОВНА И ДРЖАВНА ТАЈНА

Појам *пословних информација* је сложен и комплексан. Стога, ваљан обухват синтагматског појма *пословне информације* узима у обзир следећа одређења: тајну, теорије о заштити тајности, класификацију података, врсте и значај пословних информација (шема бр.2).

[24] Клод Шенон (Claude Shannon) је оснивач ове теорије. Године 1948. изненадио је тадашњу научну заједницу која се бавила телекомуникацијама, показавши да је грешку преноса информација могуће смањити произвољно за све брзине преноса испод капацитета канала. Шенон је у свом раду тражио одговор на два фундаментална питања теорије комуникација: *До које мере се неки скуп података може компромитовати?* и *Шта је крајња брзина комуницирања за задати комуникациони канал?* (Јаворовић и Биланџић, 2007: 57)

Шема бр.2: Врсте, класификација и начела пословних информација

Почеци, а самим тим и потреба за увођењем заштите тајности података, бележе се развојем оружаних снага, што значи да су се војна тајна и подаци који су је сачињавали, први нашли под мерама заштите безбедносних система. С обзиром да су интереси државе у савременом добу много шири и да поред војне обухватају и области економије, науке и политике, потребно је у свим овим областима одредити податке чијим би се „отицањем“ могла нанети несагледива штета држави која их поседује. У етимолошком смислу, термин „тајна“ представља нешто што се скрива и припада некој средини. Уколико тај термин посматрамо и у другим светским језицима донекле ћемо схватити значај и специфичност његовог одређења. У енглеском језику реч “secret“ представља тајну, док је у немачком говорном подручју та реч „die Gehaim“. Прва реч означава нешто „издвојити“ или „одвојити“, а друга

„припада уз дом“. Један од аутора који се тиме бавио јесте Еразмус (Erasmus, 1952) који наводи да тајна може да има два својства: материјално или формално.

А) Тајна у материјалном смислу

Тајна у материјалном смислу представља ону врсту тајне коју је држава или нека друга организациона јединица прогласила тајном законским актом или нормативно–правним прописом. Ипак, не можемо да се ограничимо само на податке који представљају државну тајну, јер поред података који су законом и другим прописом, општим актом, или одлуком надлежног органа проглашени војном, односно службеном тајном, постоје и подаци који нису формално проглашени тајном, а чије би одавање, проузроковало штетне последице по одбрану и безбедност државе. Стога је потребно направити разлику између онога што је проглашено тајном и онога што представља тајну по својој природи.

Б) Тајна у формалном смислу

Тајну у формалном смислу представљају сви подаци, чињенице, средства и поступци, који су неким прописом државног органа, наредбом војног органа, односно надлежног старешине војне јединице или установе, проглашени тајним подацима. (Ковачевић, 1986: 16-21) Поједини аутори се са овим не слажу, а између осталих и Ерасмус, који сматра да се у овим случајевима тајном проглашавају подаци који у неким моментима задржавају степен тајности, а интерес за њихово чување више није актуелан, тј. исти је безначајан. (Ерасмус, 1952)

Према Закону о заштити пословне тајне Републике Србије, пословном тајном се сматра било која информација која има комерцијалну вредност зато што није опште позната нити је доступна трећим лицима која би њеним коришћењем или саопштавањем могла остварити економску корист и која је од стране њеног држаоца заштићена одговарајућим мерама у складу са

законом, пословном политиком, уговорним обавезама или одговарајућим стандардима у циљу очувања њене тајности, а чије би саопштавање трећем лицу могло нанети штету држаоцу пословне тајне.

У ширем контексту, тајна подразумева сваки податак о једној држави (предузећу, државној институцији, државној организацији, синдикату, удружењу ветерана рата, научном институту, универзитету) који је од битне важности за ту државну целину, а чије би сазнање од стране неовлашћених лица могло да проузрокује конкретну штету, како за ту институцију, тако и за државу у целини. (Првуловић, 2010: 160-162)

Пословна тајна се дефинише као „чињенице у вези са пословањем привредне организације, посебно важне са гледишта пословања те организације или са гледишта привреде или заједнице у целини, а које могу бити познате само ограниченом кругу лица“. (Мала енциклопедија: 676)

Привредни закони, али и саме државне институције дефинишу шта то представља пословну тајну, а Кривичним законом и Законом о тајности података дефинисане су казне за њено неовлашћено одавање.

Ц) Теорија апсолутне тајности

Најједноставније објашњење ове теорије садржано је у тврдњи да се апсолутна тајност изједначава са нечим што је непознато. Да ли је нешто непознато само некоме кога посматрамо и (или) је непознато свима. Да би непознато заиста и добило облик тајне потребно је да се свесно скрива од непознатих лица која би доласком у њен посед, због различитих интереса, могла да проузрокују штету њеним носиоцима. То не значи да је тајна орочена на неодређено време нити да нешто што је тренутно јавно не може да, у одређеном моменту и под одређеним околностима, постане тајна. (Родић, 1965: 555)

Д) Теорија релативне тајности

Заступници ове теорије сматрају да тајну представљају они подаци који су доступни само одређеном броју људи. У том смислу ова теорија се назива и теоријом „затвореног круга“. Међутим, постоји и други угао гледања на ову теорију који произилази из законодавног оквира, а уводи појам *државне тајне*. Из наведеног угла државну тајну представљају подаци који не смеју да буду доступни другој држави. (Дурманов, 1942: 3)

Е) Класификација података

С обзиром да тајни подаци немају исту важност, они се класификују, а сваком од њих се одређује степен поверљивости, па су самим тим приступи, као и врста санкција уколико се учине доступним трећем лицу, различити. Законом о тајности података утврђена је скала поверљивости. У члану 14. утврђени су степени тајности и садржина података, а у члану 15. утврђено је означавање страних тајних података. Према овом закону, као тајни податак може се одредити податак од интереса за Републику Србију чијим би откривањем неовлашћеном лицу настала штета. Ови подаци односе се нарочито на: 1) националну безбедност Републике Србије, јавну безбедност, односно на одбрамбене, спољнополитичке, безбедносне и обавештајне послове органа јавне власти; 2) односе Републике Србије са другим државама, међународним организацијама и другим међународним субјектима; 3) системе, уређаје, пројекте, планове и структуре који су у вези са подацима из тач. 1) и 2); 4) научне, истраживачке, технолошке, економске и финансијске послове који су у вези са подацима из тач. 1) и 2).

Податак који се сматра тајним по наведеном закону може да има један од следећих степена тајности:

- „Државна тајна”, који се одређује ради спречавања настанка неотклоњиве тешке штете по интересе Републике Србије;
- „Строго поверљиво”, који се одређује ради спречавања настанка тешке штете по интересе Републике Србије;

- „Поверљиво”, који се одређује ради спречавања настанка штете по интересе Републике Србије;
- „Интерно”, који се одређује ради спречавања настанка штете за рад, односно обављање задатака и послова органа јавне власти који их је одредио.

Законом је утврђено да ће ближе критеријуме за одређивање степена тајности „Државна тајна” и „Строго поверљиво” одредити Влада, уз претходно прибављено мишљење Савета за националну безбедност. Ближе критеријуме за одређивање степена тајности „Поверљиво” и „Интерно” одређује Влада, на предлог надлежног министра, односно руководиоца органа јавне власти.

Овим Законом се уносе и бројне измене у област заштите тајних података. Поред скале поверљивости, новина су и дефиниције основних појмова, као и овлашћена лица за одређивање тајности података (Председник Народне скупштине, Председник Републике, Председник Владе, руководилац органа јавне власти, изабрани, постављени или именовани функционер органа јавне власти који је за одређивање тајних података овлашћен законом, односно прописом донесеним на основу закона или га је за то писмено овластио руководилац органа јавне власти, лице запослено у органу јавне власти које поседује писмено овлашћење руководиоца тог органа). Новину представља и начин означавања докумената који садрже тајне податке, начин означавања страних тајних података, временско ограничење тајности података, престанак тајности (утврђивањем датума, наступањем одређеног догађаја, истеком рока). Овим законом уведена је обавеза периодичне процене тајности, утврђен је начин за опозив тајности и промену степена и времена трајања. Прецизиране су опште мере заштите, посебне мере заштите, приступ тајним подацима, безбедносне провере, посебна овлашћења за приступ тајним подацима, поступак за издавање сертификата, контрола и надзор. Утврђене су надлежности Канцеларије Савета за националну безбедност и заштиту тајних података, начин размене података без закљученог међународног споразума и казнене одредбе.

Одредбама члана 86. Закона о тајности података утврђено је да је Канцеларија Савета за националну безбедност и заштиту тајних података у служби Владе са својством правног лица, у чијој су надлежности одређени послови спровођења и контроле примене овог закона и надзор над спровођењем закона. У складу са чланом 87. Канцеларија Савета извршава бројне послове у вези са тајним подацима: поступа по захтевима за издавање сертификата и дозвола; обезбеђује примену стандарда и прописа у области заштите тајних података; стара се о извршавању прихваћених међународних обавеза и закључених међународних споразума између Републике Србије и других држава, односно међународних органа и организација у области заштите тајних података и сарађује са одговарајућим органима страних држава и међународних организација; израђује и води Централни регистар страних тајних података; предлаже образац безбедносног упитника; предлаже образац препоруке, сертификата и дозволе; води евиденцију о издатим сертификатима, односно дозволама, као и евиденцију о одбијању издавања сертификата, односно дозвола; организује обуку корисника тајних података у складу са стандардима и прописима; предлаже Влади план заштите тајних података за ванредне и хитне случајеве; опозива тајност податка у складу са одредбама овог закона; после престанка органа јавне власти који немају правног следбеника, обавља послове који се односе на заштиту тајних података; сарађује са органима јавне власти у спровођењу овог закона у оквиру своје надлежности; обавља и друге послове који су предвиђени овим законом.

4.2.1. Појам и карактеристике пословних информација

Француски физичар и математичар Бријон (Louis-Marcel Brillouin) је дао следећу дефиницију информације: „Информација је функција односа између могућег одговора пре и после њеног пријема/спознаје.“ (http://www.zmne.hu/aarms/docs/Volume2/Issue1/pdf/02NOWA.pdf, 2016, 3. јул)

Шенон (Claude E. Shannon) је информацију математички дефинисао као негативну вредност логаритма вероватности догађаја (случајева), одређујући тако њен синтаксни аспект, који се односи на граматику или синтаксу описа, чувања и преноса порука. (http://worrydream.com/refs/Shannon%20-%20A%20Mathematical%20Theory%20of%20Communication.pdf, 2016, 3. јул)

Винер (Norbert Wiener) наводи да је информација назив за садржај који је размењен са спољашњим светом, тако да му се ми прилагодимо и да наше прилагођавање чини осетљивим на њега. Информација је информација, не материја или енергија. (http://www.sveiby.com/articles/Information.html, 2016, 3. јул)

Махлуп (Machlup) наводи да је информација упућена људском уму и да је од људског ума примљена. (Harmon et al., 1987: 206-227)

Дакле, постоје различите дефиниције информације које зависе од приступа, потреба и интереса аутора, односно подручја којим се аутор бави и сврси којој му дефиниција служи. Дигитални облик приказивања података и информација ствара могућност за њихову објективизацију, складиштење и обраду.

Пословне информације су све информације које су у функцији делатности пословног субјекта, односно све информације потребне за његово пословање и остваривање пословних циљева и интереса. Информација у неком тренутку не мора да има обележја пословне информације, али исто тако у неком другом тренутку то може да постане, што зависи од потреба пословног субјекта. Ако узмемо као пример интернет, као извор мноштва информација, проверених и непроверених, тачних и нетачних, увиђамо да неке од њих постају пословне оног тренутка када их физичко лице или пословни субјект употреби у циљу задовољења пословних потреба. Оне за тог пословног субјекта имају пословну вредност јер су му омогућиле да утиче на остваривање пословних резултата. У циљу бољег разумевања проблема, неопходно је увести две карактеристике пословних информација: релативност и релевантност. Релативност је објашњена кроз претходни пример, а релевантност се односи на проналажење не било какве информације, већ оне која за корисника постаје најкориснија и највреднија.

Поред ова два појма, са аспекта употребљивости, за корисника је од изузетне важности и поузданост информација. У том смислу сваки пословни субјект има за циљ да обезбеди поуздане информације на основу којих доноси квалитетне пословне одлуке. Са аспекта поузадности важно је да ли је информација проверена или непроверена. Уколико је непроверена то не значи да није тачна, већ да је мање поуздана од оне која је проверена из више извора. Извори података у том смислу могу да буду јавни или тајни. Јавни извори су доступни, не само корисницима пословних информација, већ и широј јавности. Један од највећих јавних извора података и информација је интернет. Међутим, то могу да буду и разни стручни семинари, предавања, изложбе, сајмови, стручна литература и слично. Са аспеката употребљивости пословних информација, за пословног корисника посебну важност и вредност имају информације до којих се долази искључиво пословно–обавештајном делатношћу (business inteligence). До таквих података се долази применом легалних, полулегалних, а понекад и илегалних метода, по принципу „циљ оправдава средство“.

Пре саме процене и провере поузданости, пословни субјект прикупља од извора податке и складишти све информације које могу на било који начин да помогну његовом функционисању и испуњавању пословног циља. Тек након њиховог складиштења и обраде, информација може да се употребљава, како би руководство доносило одлуке у складу са циљевима и интересима пословног субјекта.

4.2.2. Врсте пословних информација

Пословне информације могу се раврставати према различитим критеријумима. Најчешћа подела пословних информација је на унутрашње и спољне. Унутрашње информације су оне које већ постоје или су део неког пословног система. Самим тим, ова врста информација је доступна субјектима тог пословног система, а њена доступност са аспекта брзине, између осталог, зависи од квалитета самог информационог система у којем

је похрањена. Ради се о информацијама које се односе на кадрове, добављаче, набавку, финансијске извештаје, производни програм, развојне пројекте, улагања и слично. Подаци се унутар пословног субјекта селектују, разврставају и додељује им се степен тајности. То значи да многи од ових података не смеју да „дођу у руке“ конкурента, јер би њиховом експлоатацијом конкурент могао да представља претњу по пословање пословног субјекта. За разлику од унутрашњих, спољни подаци се налазе изван пословног субјекта, али могу да утичу на његово пословање. За долажење до оваквих врста информација примењују се различите методе, како легалне тако и нелегалне. Потребно је нагласити да подаци доступни широком кругу људи, као што су подаци на интернету, могу да буду неком пословном субјекту, у право време и на правом месту, од веће важности од података до којих се долази посебним методама.

Следећа класификација одређује информације као опште, стручне, функционалне и специјализоване или посебне информације. Опште информације се уопштено односе на све пословне субјекте, пословно активне на неком подручју, без обзира какву делатност обављају. Ради се о опште познатим информацијама до којих корисник долази из јавних извора, као што су медији, интернет, јавне институције и слично. Стручне информације се односе на стручне области и важне су само за пословне субјекте који се њима баве, као што су производња, трговина, разне услужне делатности и слично. Функционалне информације су оне које се односе искључиво на једну грану пословне делатности, као што је грађевина, те се у оквиру те гране врши анализа о развијености, тренутном стању, конкуренцији и другим параметрима који показују у ком се стању посматрана делатност налази. Ове информације обично користе стручни аналитичари. Они стручним анализама указују на мере надлежних државних институција, али и на мере удружења, савеза и комора које повезују пословне субјекте и које би требало спроводити да би се ситуација у некој пословној делатности променила. Специјализоване или посебне информације опредељују стратегију деловања неког пословног субјекта у његовом пословном амбијенту. Њихов задатак је да одговоре на питања снаге, могућности, интереса и циљеви пословања.

Пословне информације се могу поделити и у односу на њихово порекло, те у том смислу разликујемо сопствене и туђе. Сопствене информације односе се на пословање неког пословног субјекта и на њих он полаже неку врсту власничког права, али и обавезу да омогући истима приступ од стране контролних или инспекцијских органа. Туђе пословне информације доступне су пословном субјекту уз одобрење и услове које му одређује други пословни субјект у чијем су власништву. Овде се поставља питање пословне етике корисника таквих информација и обавезе да не буду злоупотребљене против пословног субјекта од којег су прибављене, већ да се користе искључиво у циљу побољшања сопственог пословања.

Последњом класификацијом прави се разлика између јавних и тајних информација. Јавне су оне информације које се о неком пословном субјекту могу пронаћи у јавним медијима или у базама података које су доступне широј јавности, па самим тим и конкуренту. Тајним информацијама сматрају се оне које пословни субјект, на основу Закона о тајности података, одређује за пословну тајну. Такви подаци се штите посебним мерама јер се њиховим отицањем може нанети штета пословном субјекту несагледивих размера. Када су у питању државне институције, заштитом информација које представљају државну тајну баве се специјализоване контраобавештајне службе, а њихово објављивање у јавности или омогућавање увида неовлашћеним лицима, може да изазове озбиљне проблеме када је у питању национална безбедност. Неке информације, без обзира што представљају пословну тајну за неког пословног субјекта, морају да се достављају државним институцијама, нпр. министарству финансија које на основу укупног државног буџета, корисницима додељује финансијска средства за текућу годину. Када су у питању приватни привредни субјекти, они имају обавезу достављања завршних рачуна где су садржане неке информације које би могле да представљају предмет интересовања конкурента или кроз евиденцију платног промета код пословних банака омогућују запосленима информације о финансијским трансакцијама, висини промета добара и услуга са другим пословним субјектима. Управо због тога постоје законом установљене обавезе чувања пословних тајни клијената од стране

запослених у државним и приватним институцијама, а који до таквих података долазе по природи посла којима се баве. Специфичност представљају безбедносно–обавештајне целине унутар државе, које изворне податке сачињене у облику примарних докумената могу да достављају искључиво органима који имају право контроле таквих институција. Тиме и лица запослена у контролним институцијама постају носиоци тајних информација са највишим степеном поверљивости и предмет интересовања страних служби које настоје да дођу до тих података. (Јаворовић и Биланџић, 2007: 121-124)

4.2.3. Значај пословних информација

Свака информација има своју улогу и може да се искористи у различите намене. Једна информација може неком пословном субјекту да представља основу за доношење најважнијих пословних одлука, док за другог не мора да има икакву важност. У питању су интереси и тренутак у којем информација има неку важност и могућност искоришћења. Самим тим, информације се не би могле делити на добре и лоше или на квалитетне и неквалитетне, јер оне су управо онакве каквим их начине они који их користе и употребљавају. Информације је неопходно стално проучавати уз примену развијених научних метода. Њихова примена је свестрана у различитим људским делатностима као што су привреда, култура, политика, безбедност, те је неопходна интердисциплинарност у њиховом проучавању, као и у њиховој примени.

Посматрајући са аспекта употребљивости и њиховог каснијег значаја, пословне информације би требало да задовоље неколико начела (према Protic, 2013: 133-150):

- *Правовременост* — да би пословни субјекат могао пословну информацију да експлоатише и да њеном спознајом постигне очекивани пословни резултат, она мора да буде обезбеђена у повољном тренутку. То је посебно важно у неким делатностима као

што је берзанско пословање. Не мање важно је поседовање правовремених информација од стране државних безбедносних служби које спроводе активности на заштити људских живота, као што је случај код противтерористичких акција. Начело правовремености је једно од основних начела и темељ успеха пословног субјекта.

- *Објективност* — да би информација имала вредност и важност за пословног субјекта она мора да буде посматрана непристрасним очима корисника. Ово је можда једно од најкомплекснијих начела, јер тешко је искључити животна искуства, образовање, окружење, пословни амбијент, као и трендове приликом доношења пословних одлука. Све то утиче на објективност доносиоца одлука, али и на објективност онога ко информацију прикупља и презентује кориснику. Због необјективности, пословне компаније су често трошиле много више финансијских средстава у борби против конкурента него што је то било потребно да би овладале тржиштем. Објективност исто тако, посебну важност има код доношења одлука војних старешина у ратним условима, па се дешавало да се недовољно оспособљена, опремљена и попуњена војна формација упути на задатак за који нема довољно потенцијала и капацитета, што за последицу има велике људске губитке и губитак територије.[25]
- *Тачност* — тачност информације у поступку доношења одлуке за пословног субјекта има посебну важност. Пословни субјект само на основу тачних информација може да доноси квалитетне одлуке, те се због тога овом начелу посвећује посебна пажња.
- *Провереност* — без обзира са коликом вероватноћом може да се тврди да је нека информација тачна, уколико не постоји могућност за проверу из других извора, она се узима са резервом, а у високоризичним активностима најчешће се одбацује и не утиче на ток доношења одлука. Информација која може да се провери из више извора, има за пословног субјекта већу важност. Понекад се пословни

[25] Напад Немачке на СССР у Другом светском рату.

субјекти у пословним активностима служе делатностима као што је пласирање дезинформација. Тиме конкуренте доводе у заблуду и изазивају доношење погрешних пословних одлука.

- *Потпуност* — пословна информација може да буде тачна и проверена, али ако није потпуна она нема одговарајућу важност за пословног субјекта и не обезбеђује му доношење квалитетних одлука. На пример, уколико безбедносне службе располажу са информацијом да ће се у неком простору догодити терористички напад, а да немају тачну информацију о времену напада, та информација јесте тачна али није потпуна. Дакле, да би информација била потпуна она мора да поседује све елементе и да буде тако „заокружена“ да доносиоцу одлука обезбеди недвосмислену предност у односу на конкурента и минималан пословни ризик.
- *Поузданост* — управо претходна два начела одређују начело поузданости јер није могуће да информација буде поуздана, а да при том не буде тачна. Исто тако не може да буде поуздана, а да не може да се провери из више извора, осим у случају када се ради о општепознатим и општеприхваћеним чињеницама.
- *Безбедност и заштићеност* — поседовати осетљиве пословне информације, а претходно их необезбедити и на тај начин омогућити их доступнима неовлашћеним лицима, представља основни задатак безбедносних субјеката. Пракса је показала да је људски фактор „најслабија карика“ у случају нежељеног отицања пословних информација из пословног система. То не значи да информације одлазе само планским деловањем човека и обавештајним деловањем у корист другог пословног субјекта, већ значи да исте могу да буду доступне другим субјектима захваљујући непажњи или слабијој безбедносној култури лица која са њима располажу, а запослена су у том пословном субјекту.

5. БЕЗБЕДНОСТ ПОСЛОВНИХ ИНФОРМАЦИЈА

Важност и значај пословних информација у савременим друштвеним односима проузроковао је непрекидан рат између пословних конкурената, супарничких држава, политичких противника, али и између пословних партнера, политичких сарадника и пријатељских држава. Обавештајне службе у циљу доласка до таквих информација примењују разне методе за прикупљање података, а безбедносне службе им се у томе супротстављају.

Посебан проблем представља безбедност ИКС која може да се одреди као стање и степен отпорности и заштићености ИКС и информационо–комуникационе делатности у односу на разне врсте претњи и угрожавања. Безбедан ИКС подразумева да се прикупљање, обрада, складиштење, чување, размена и коришћење података и информација, спроводи без сметњи. (Јаворовић и Биланџић, 2007: 307)

Најшири појам у контексту безбедности једне државе јесте појам *националне безбедности* који се различито схвата и тумачи. У најширем поимању под њим се подразумева опстанак државе или национални опстанак, односно одсудна одбрана ради очувања територијалног интегритета, политичке независности и државних институција. У великим и моћним државама под националном безбедношћу подразумева се заштита свих националних интереса, одсуство рата или његово успешно вођење и завршетак. Према другом схватању, под националном безбедношћу, заснованом на спољашњим чиниоцима подразумева се одсуство претњи, односно положај у међународној заједници који онемогућава угрожавање виталних интереса. (Мијалковски, 2009: 28-31)

5.1. УГРОЖАВАЊЕ ПОСЛОВНИХ ИНФОРМАЦИЈА

Заступљеност ИКТ–а у свакодневном животу савременог човека је досегла такав ниво да је готово незамисливо функционисање друштва без примене напредних технологија овог типа. Пракса је показала да напредне ИКТ–е поједностављују приватне и пословне обавезе човека, омогућавају бржу и лакшу комуникацију и податке чине доступним корисницима без обзира где се на Планети тог момента налазе. Приступ таквим подацима је тиме омогућен и појединим лицима која немају поштене намере када је у питању експлоатација осетљивих информација. Данас на појединим сајтовима интернета, случајно или намерно, могу да се пронађу званични војни приручници и упутства као што је упутство за израду експлозивних направа, оруђа или упутства за употребу хемијских агенаса у циљу израде оружја за масовно уништење. Такве информације погодују неким екстремистичким и терористичким организацијама у повоју, које још увек немају развијене механизме за обуку лица и довољно сазнања о тим областима. Данас постоји низ националних и међународних институција које се баве спречавањем и истрагама ове врсте криминала, који се најчешће назива високотехнолошким криминалом.

5.1.1. Појам угрожавања пословних информација

Да би се лакше схватио појам угрожавања пословних информација, неопходно је поћи од појма претње коју Путник дефинише на следећи начин: „Претња је, по природи, апстрактан концепт — она је нешто што има потенцијал да стави једну организацију, особу или друштво у ризичну ситуацију. Претња је могућност да се оствари нежељени догађај. Када се ова могућност актуализује, она престаје да буде претња и постаје догађај попут других. У тренутку када је претњу уочио надлежни ауторитет или менаџмент она постаје део ризика, те као таква предмет расподеле њиховог времена и

расположивих ресурса (људских, техничких, финансијских итд.) ради супротстављања“. (Путник, 2009: 62)

ИКС су данас основа за пословање великих пословних система, у којима менаџмент захваљујући квалитетним корисничким програмима, анализама, пресецима и проценама, долази до употребљивих информација на основу којих доноси стратешке одлуке. О значају информационих технологија сведоче активности надлежних државних органа који се односе на увођење е-управе, што представља једну од ставки Стратегије развоја информационог друштва у Републици Србији до 2020. године (http://www.gs.gov.rs/lat/strategije-vs.html, 2015, 12. април).

Данас је грађанима омогућено школовање употребом ИКТ, подизање докумената, заказивање прегледа у здравственим установама, комуникација са јавним службама и установама. С друге стране, захваљујући техничким достигнућима, лицима са штетним намерама, омогућено је лакше фалсификовање службених докумената и исправа, као и друге врсте манипулација када је у питању електронско пословање. Војни ИКС, системи државне управе, системи за контролу ваздушног и железничког саобраћаја, снабдевање гасом, водом, електроенергијом, врло су атрактивни уносни циљеви. Како се заштитити од тешко предвидљивих извршилаца напада као што су: незадовољни грађани, разочаран персонал, терористи, непријатељске државе или, пак, верски фанатици? Ако имамо на уму да им на располагању стоје сателитски линкови, савремени компјутери и велики избор разноврсних мета (компјутерски системи: аеродрома, болница, саобраћајне сигнализације, банака, нуклеарних погона и оружја) схватићемо колико решавање овог проблема представља велики изазов. (Ђорђевић, 2007)

Често се под информационим системима подразумевају само техничка средства (рачунари и системи преноса информација на даљину и сл.), међутим, потребно је уврстити и људе који их користе и опслужују, као и физички простор у којем се информације размењују и касније анализирају.

Недовољно дефинисана законска регулатива која се односи на заштиту информационих система је погодно тле за противзаконито деловање злонамерних организација и појединаца који својим деловањем

угрожавају поједине сегменте националне безбедности, али исто тако и личну безбедност грађана.

Извори угрожавања пословних информација се могу поделити у четири категорије (према Ђорђевић, 2007: 77):

1. Опасности по систем које настају као последица природних стихија, политичких немира и ратова, то јест као последица „више силе“,
2. Технички извори угрожавања, акциденти настали као последица неадекватног хардвера или квара на уређајима,
3. Угрожавање система од стране запослених као последица немара, нестручности или лоше организације и
4. Злонамерне активности од стране људи изван система или из редова запослених.

1. Угрожавање информационо–комуникационих система који настају као последица природних непогода и стихија је тешко предвидети, а самим тим супротстављање овом облику угрожавања је ослоњено искључиво на предузимање превентивних мера које обухватају квалитетну процену ризика у зависности од подручја на којем ИКС егзистира. У том смислу, процена ризика ИКС–а се знатно разликује у зависности од региона у којем пословни субјекат послује. Врсте елементарних непогода којима је могуће угрожавање се готово ни у чему не подударају. Јапан је, на пример, територија која је склона ерозијама и потресима, као и појавом цунамија великих степена разарања. Процена ризика угрожавања ИКС би се у случају ове земље односила на превентивну заштиту од облика угрожавања којима би Јапан могао да буде изложен у наредном периоду, а предвиђања могућих претњи се спроводе на основу егзактних показатеља.[26] За разлику од Јапана, Конго је земља у којој су климатски услови опредељујући када је у питању заштита ИКС–а. Екстремно високе температуре, суше, пешчане олује су климатски параметри који могу да

[26] Цунами који се 2011. године догодио у Јапану, изазван земљотресом јачине 8.9 степени по Рихтеровој скали, однео је око хиљаду живота. Због појаве цурења радиоактивних материја затворено је 11 нуклеарних електрана. (http://www.vesti-online.com/Vesti/Svet/122853/Japan-Zemljotres-podigao-cunami-, 2015, 7. мај)

утичу негативно на рад ИКС–а, а пажњу би требало усмерити управо на њих како би се заштита ИКС–а спроводила на највишем могућем нивоу. Конго је, за разлику од Јапана, држава у којој је политичка ситуација нестабилна и у којој сваког тренутка сукоби зарађених снага могу да доведу до грађанског рата ширих размера, што додатно утиче на стабилност и угроженост ИКС–а. Поред тога, економски развој државе утиче и на слабију примену превентивних мера којима би се штетне последице елементарних непогода смањиле на ниво за који би могло да се каже да је прихватљив или очекиван. Овим је делимично објашњен значај квалитетне безбедносне процене која представља синтезу свих претходних знања и искустава и стручну научну анализу предвиђања будућих догађаја, а којима би се ИКС могао довести у неповољну ситуацију по његове кориснике. Не треба заборавити на то да ИКС не постоји сам за себе, већ да је његова улога пренос и снабдевање подацима и информацијама корисника.

2. Технички извори угрожавања који настају као последица кварова на уређајима односе се пре свега на недостатке везане за технологију израде, квалитет материјала и на грешке конструктора приликом израде хардвера или програмера приликом израде софтвера. Финансијски терет у случајевима откривања оваквих недостатака пада на произвођача опреме, који неретко кориснику мора да плати све наступајуће трошкове као и трошкове због нарушавања угледа у јавности што се одражава на перспективу њеног пословања.

Технички извори угрожавања се најбрже отклањају, а последице по ИКС су тада минималне. Овде је важно напоменути да се не ради о намерним облицима угрожавања, како споља тако и изнутра, већ искључиво о грешкама човека или тима.

3. Угрожавање ИКС од стране запослених које настаје као последица немара и нестручности је питање којем се поклања посебна пажња у свим пословним системима. Едукација запослених и повећање безбедносне културе на потребан ниво, представља основ безбедносне заштите сваког система, па самим тим и ИКС–а. Данас запослени

међусобно комуницирају разменом електронске поште, као и употребом мобилних телефона и апликација које омогућавају комуникацију у реалном времену, при том не водећи рачуна која све документа размењују тим путем и колико је такав вид комуникације безбедан. ИКС унутар једног пословног субјекта је по правилу заштићен, међутим губитак преносне меморије, укључивање пословног рачунара на којем се налазе поверљива документа на интернет, представља један од најчешћих случајева који доводе до отицања тајних података, а резултат су ненамерног деловања. Исто тако, изношење података који представљају тајну за пословање пословног субјекта пред другим лицима, представља безбедносни ризик. Познато је да се подаци међу људима шире веома великом брзином и да поверљиви разговори између пријатеља немају очекивани степен конспиративности.

Перманентном едукацијом запослених, организовањем семинара и курсева унутар пословних субјеката, као и подизањем свести запослених о могућим последицама по безбедност ИКС–а које могу да наступе услед њихове непажње и нестручности, подиже се ниво заштите пословних информација унутар једног ИКС–а, а смањује се степен његовог угрожавања од стране неовлашћених лица. У циљу превазилажења уоченог проблема, неопходно је појачати и организационе услове ИКС–а који се пре свега односе на квалитет информационих система и активацију адекватног стручног надзора. Безбедносна процена би се у том случају односила на анализу запослених лица у привредном субјекту са аспекта нивоа приступа поверљивим подацима, на степен обучености и безбедносне културе запослених и на друге карактеристике као што су навике (изношење радних докумената и рад код куће, употреба преносних меморија). Законска регулатива се подједнако односи на санкционисање кривичних дела одавања службене тајне без обзира да ли је до исте дошло случајно или намерно, те стога овој категорији угрожавања пословних информација треба поклонити посебну пажњу.

4. Злонамерне активности људи запослених у систему или оних који су ван система — Један од најчешћих облика угрожавања пословних

информација овог типа представљају хакерски напади, који се реализују у циљу продора у ИКС, како би се дошло до података који су од стране њиховог власника проглашени за поверљиве или тајне. У том смислу, злонамерни носиоци таквих делатности употребом програма као што су вируси, црви, тројански коњи и слично и продором у забрањену зону, долазе до тајних података које касније користе за разне врсте уцена и превара.

Пиратерија као следећи облик врсте угрожавања пословних информација представља противзакониту активност, а односи се на илегално умножавање и продају програмских пакета (softwer) или преправљање програма без сагласности и допуштења аутора. Дакле, ради се о криминалној противзаконитој активности која је строго кажњива, а у себи има све елементе организованости, од производних до продајних активности носиоца такве делатности.

Једна од најизраженијих и најчешћих злонамерних активности јесте коришћење интернета за спровођење криминалних радњи као што су трговина људима, продаја дроге, вршење превара, обављање финансијских превара крађом идентитета и слично. Овај облик криминала се у литератури назива високотехнолошки или сајбер (енгл. cyber) криминал.

Један од међународних докумената који дефинише категорије сајбер криминала је Европска конвенција о сајбер криминалу (http://www.coe.int/sr_RS/web/conventions/, 2016, 3. јул). Карактеристична дела која могу да се доведу у контекст рада су:

- Дела против поверљивости, интегритета и доступности компјутерских података и система (незаконити приступ, пресретање, уплитање у податке или системе, коришћење уређаја, програма, лозинки);
- Дела везана за компјутере код којих су фалсификовање и крађе најтипичнији облици напада;
- Дела везана за кршење ауторских и сродних права обухватају репродуковање и дистрибуцију неауторизованих примерака дела компјутерским системима.

UNDOC-ова обимна студија о компјутерском криминалу (енгл. Comperhensive Study on Cybercrime) из 2013. године, четрнаест дела групише у три категорије (према https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, 2016, 3. јул):

- Дела против поверљивости, интегритета и доступности компјутерских података или система код којих је најзаступљенији незаконити приступ компјутерском систему; незаконити приступ, пресретање или стицање компјутерских података; незаконито ометање компјутерског система или компјутерских података; производња, дистрибуција или поседовање алата за злоупотребе рачунара и кршење приватности или мера за заштиту података;
- Дела везана за компјутере ради личне или финансијске користи или штете какви су превара или фалсификат; дела везана за идентитет; кршење ауторских права или права на жиг; слање или контролисање слања ”spam“ порука.
- Дела везана за компјутерске садржаје, а односе се на говор мржње, дистрибуцију или поседовање дечје порнографије или за подршку тероризму.

Класификација cyber криминала домаћих аутора Дракулића указује на следеће категорије (према Дракулић и Дракулић, 2005):

- Политички: cyber шпијунажа, хакинг, cyber саботажа, cyber тероризам, cyber ратовање;
- Економски: cyber преваре, хакинг, крађа интернет услуга и времена, пиратство софтвера, микрочипова и база података, cyber индустријска шпијунажа, преварне интернет акције (неиспоручивање производа, лажна презентација производа, лажна процена, надграђивање цене производа, удруживање ради постизања веће цене, трговина робом са црног тржишта, вишеструке личности);
- Производња и дистрибуција недозвољених и штетних садржаја: дечја порнографија, педофилија, ширење ставова верских секти, ширење

расистичких, нацистичких и сличних идеја и ставова, злоупотреба жена;

- Манипулација (трговина, дистрибуција и слично) забрањеним производима, супстанцама и робама: дрогом, људима и децом, људским органима, оружјем;
- Повреда cyber приватности: надгледање е–поште, spam, phishing, крађа идентитета, прислушкивање, снимање chat rooms[27], праћење е–конференција, приказивање и анализа cookies[28].

5.1.2. Облици и субјекти угрожавања пословних информација

Корисници пословних информација улажу планске и организоване напоре с циљем да их оптимално и ефикасно заштите од лица (појединаца) и колективитета који настоје и покушавају да их сазнају. Реч је о непрекидном, двостраном процесу који треба да резултује регистровањем чињеница, односно да да одговор на питања ко, како и зашто може да угрози пословне информације. Сазнате чињенице се користе за планирање и реализовање њихове заштите. Расположива сазнања указују на следеће карактеристичне облике и изворе угрожавања пословних информација (Јаворовић и Биланџић, 2007: 296):

А) Угрожавање пословних информација у сајбер простору

- Сајбер напади техничког типа
- Сајбер напади уз коришћење обмане
- Злоупотреба сајбер простора као средства масовне комуникације

[27] *Соба за чет* (енгл. chat — онлине интерактивна комуникација између сурфера) — Помоћу чета је могућа комуникација са људима који се налазе у истом chat room–у, с тим што је много уобичајенија комуникација дописивањем, тј. куцањем преко тастатуре, него директна комуникација говором, помоћу микрофона и слушалица. (http://bezbednostdecenanetu.weebly.com/105610771095108510801082-104810851077108810851077109 0-108710861112108410861074 1072.html, 2016, 3.јул).

[28] *Колачић* (енгл. Cookie) — метод који у софтверу служи за прикупљање информација о лицима која посећују неку Web локацију да не би посетилац морао да се региструје сваки пут приликом посете. (Тасић и Бауер, 2004)

- Субјекти претњи у сајбер простору

Б) Шпијунажа

- Корупција и поткупљивање као мотив за спровођење шпијунаже

Ц) Криминал у области интелектуалне својине

Д) Физички напади на ИКС

Е) Организациони услови као извор угрожавања (шема бр.3)

Шема бр.3:Облици угрожавања пословних информација

5.1.2.1. Угрожавање пословних информација у сајбер простору

Повезивање рачунара са серверима (рачунарима великог капацитета) на којима се чувају резервне копије података представља један од облика ризика у сајбер простору. У случају губитка података информације се могу реконструисати са резервних медијума чиме се обезбеђује ефикасност, економичност и поузданост рада пословног субјекта. Да би се повећала ефикасност запослених, врши се повезивање рачунара на интернет чиме се омогућује међусобна комуникација запослених са удаљених локација,

комуникација са другим компанијама и омогућује се пренос важних података и пословних информација. Међутим, потребно је имати у виду да овај процес може бити угрожен на различите начине. У том смислу пословни субјект предузима све мере како би открио, контролисао и, у што већој мери, ублажио утицај могућих ризика. Интернет пружа брз и прилично јефтин начин за обављање послова и пренос информација. Ипак, тај процес може бити поремећен на различите начине, тако што ће подаци бити украдени, измењени, уништени. У циљу анализе постављене теме са аспекта могућности отицања заштићених информација, потребно је извршити анализу ИКС у којима се рачунари повезују са серверима[29]. Конфигурисањем приступа интернету, омогућује се комуникација са другим рачунарима и пренос података у оба смера, што представља посебну претњу за сервере, посебно уколико нису заштићени одговарајућим рачунарским програмима. Узимајући у обзир да је интернет мрежа која наводно „нема власника“, иако је познато да су поједине државе и институције власници делова комуникационих канала, проблем отицања заштићених информација додатно долази до изражаја. (Цигурски, 2002: 117)

Да би се лакше разумело које су то најосетљивије тачке криминалног понашања корисника ИКС–а, потребно је нагласити да постоје следећи нивои рачунарских примена: прикупљање и пренос података, складиштење података, аутоматска обрада података, дијагностика стања и доношење одлука, управљање и контрола, истраживање и развој.

Информациони криминал представља противзаконито понашање група и појединаца чији су основни циљеви деловања везани за недозвољени приступ информацијама о појединцу, организацијама или институцијама. Потребно је нагласити да се понекад изједначавају појмови *информациони* и *компјутерски криминал*. Информациони криминал представља шири појам од компјутерског криминала. Компјутерски криминал подразумева да је компјутер средство којим је извршена противзаконита делатност

[29] У области информационих технологија сервер је рачунарски систем који пружа услуге другим рачунарским системима — клијентима. Комуникација између сервера и клијента одвија се преко рачунарске мреже.

прикупљања информација, што у случају информационог криминала не мора да буде случај. С обзиром на то да се у Републици Србији ова врста криминала у званичним институцијама дефинише као високотехнолошки, јасно је да су и извршиоци такве врсте криминалних активности образована и едукована лица из области ИКТ–а, па је самим тим доказивање и сузбијање ове врсте делатности сложен поступак. Код појединих аутора појављује се и термин *cyber криминал* (Дракулић и Дракулић, 2010).

Мотиви за извршење противзаконитог дела високотехнолошког криминала могу да буду:

- политички — деловање у циљу слабљења политичких противника и изазивања политичких промена (компромитација, уцена и сл.),
- економски — крађа идентитета, преваре у пословању, пиратерија, недозвољена трговина,
- производња и дистрибуција забрањеног садржаја (сатанизам, педофилија, екстремизам и шовинизам, верски фундаментализам, секте),
- психосоматска обољења (задовољавања болесних амбиција и потреба, психичка оптерећеност и фиксација на једну личност — најчешће јавну или на његову породицу и сл.).

У UNDOC студији Comperehensive Study Cybercrime из 2013. године се полази од од 14 дела Cyber криминала груписаних у 3 категорије:

- *дела против поверљивости, интегритета и доступности компјутерских података или система* код којих су најзаступљенији: незаконити приступ компјутерском систему; незаконити приступ, пресретање или стицање компјутерских података; незаконито ометање компјутерског система или компјутерских података; производња, дистрибуција или поседовање алата за злоупотребе рачунара и кршење приватности или мера за заштиту података.
- *дела везана за компјутере ради личне или финансијске користи или штете* какви су: превара или фалсификат; дела везана за индетитет; кршење ауторских права или права на жиг; слање или контролисање

слања spam порука; дела која проузрокују личну штету и тражење или „нега“ деце.

• *дела везана за компјутерске садржаје* односе се на: говор мржње; дистрибуцију и поседовање дечије порнографије или за подршку тероризму.

((Дракулић и Дракулић, 2010: 223).

Да би се смањио ризик потребно је идентификовати потенцијалне претње и рањиве тачке у ИКС-у. Претња по безбедност информација је свака активност која представља опасност за поверљивост, интегритет, или расположивост података. Слаба тачка је пропуст у заштити информација. Терминолошки, безбедност информација подразумева: поверљивост (обезбеђује да само овлашћено особље има приступ информацијама), интегритет (обезбеђује да само овлашћено особље модификује податке), расположивост (обезбеђује овлашћеном особљу приступ информацијама и системима кад год је то потребно).

Контрола ризика при употреби ИКТ–а постиже се утврђивањем и вредновањем ризика, откривањем извора претњи и рањивих тачака и предузимањем мера да се ризици потпуно отклоне или сведу на минимум. Ризик је изложеност губитку или могућем оштећењу. Када говоримо о безбедности информација, под ризиком подразумевамо могућност да спољни фактори угрозе податке, што би проузроковало губитак времена, новца и репутације. Претња се дефинише као свака активност која представља могућу опасност по информације. Слаба тачка одређена је као пропуст у заштити информација односно безбедности система, мреже, процесима и процедурама. (Кукрика, 2002: 81-82)

Унутрашње тачке упада представљају најчешће системи који нису у обезбеђеној просторији и којима није конфигурисана локална заштита. Спољашње тачке приступа представљају компоненте које повезују пословне субјекте са интернетом, апликације које се користе за комуникацију преко интернета и комуникациони протоколи. Мрежну структуру чине каблови, мрежни уређаји и мрежни сервиси који омогућавају повезивање рачунара. Ова структура омогућава и повезивање са интернетом и прикључивање

удаљених рачунара изван компаније. Тачке упада су места преко којих је могуће прикључење и продор у мрежну инфраструктуру и приступ информацијама. Спољашњи упад је могућ кроз везу са интернетом извођењем *DoS* напада или испробавањем корисниковог имена и лозинке који би омогућио пролаз кроз проверу аутентичности. Унутрашњи напад могао би потећи од неког запосленог који може да се повеже преко отвореног мрежног прикључка и покуша да приступи заједничким ресурсима који не захтевају лозинку. (Ruth & Hudson, 2004: 13)

Апликације које се користе за приступ интернету, такође могу представљати тачку упада. Спољашњи напад може се реализовати убацивањем вируса или паразитских програма преко *e*-поште. Отварањем ове поште, вирус може да зарази систем или да омогући нападачу контролу система. Напад изнутра могућ је преко помоћних програма оперативног система, који служе за повезивања са другим системима на интерној компанијској мрежи и који за приступ не захтевају корисничко име и лозинку. Могућа је и злоупотреба апликација као што је *web* претраживач за приступ поверљивим информацијама са ограниченом безбедношћу приступа. (Ruth & Hudson, 2004: 21)

Интернет и друштвене мреже који су рањиви и несигурни због огромног броја корисника, отворености и нерегуларности, идеално су скровиште криминалцима различитог типа, којима је потребно друштво, као што им је неопходна и „публика“. Лакоћа „вршљања“ сајбер простором даје им осећај моћи и неухватљивости. (Дракулић и Дракулић, 2005)

Путник прави следећу класификацију претњи у сајбер простору:

- Сајбер напади
    - Сајбер напади уз коришћење обмане (социјални инжењеринг и сајбер напади техничког типа и фишинг)
    - Сајбер напади техничког типа (напади помоћу малициозних програма — malwer, напади усмерени на опструкцију услуга — Denial of Service или Distributed Denial of Service)
- Злоупотреба сајбер простора као средства масовне комуникације
    - Информационо ратовање

- Пропаганда
- Психолошки рат
- Обавештајна делатност (Путник, 2009: 73).

5.1.2.1.1. Сајбер напади техничког типа

Врсте угрожавања у сајбер простору би се могле поделити у две категорије. Прву категорију представљају случајне или ненамерне грешке настале креирањем неког програмског пакета, које употребом од стране корисника обезбеђују неовлашћеним лицима приступ заштићеним информацијама. Други, чешћи облик угрожавања представља смишљено састављени програми за наношење штете у ИКС као што су malweri[30] (вируси, црви (енгл. worms), тројански коњи, споредна врата), рекламирање без сагласности корисника (енгл. adwer), ботови, отмичари, шпијуни (енгл. spyware) и слично. Најчешће се пажња усмерава ка претњама које долазе из окружења и сматрају се могућим, док оне које се јављају унутар система врло често бивају занемарене.

Вирус (енгл. virus) је било који програм који зарази извршне датотеке и при њиховом покретању преноси се на друге извршне датотеке и извршава неке штетне акције. Термин *вирус* у информатичком смислу је први употребио Фред Коен (Fred Cohen) у чланку објављеном 1984. године под насловом „Експерименти у рачунарским вирусима“.

Неки вируси, поред сопствене репродукције, садрже још две компоненте:

- Функцију активације која садржи основне критеријуме на основу којих вирус „одлучује“ да ли да изврши напад;
- Једну или више додатних функција које се састоје од редоследа инструкција за наношење штете систему у виду брисања датотека или

[30] Назив је добијен од речи *malicious* и *software.*

диска, приказивања нежељених порука на екрану итд. (Путник, 2009: 75 - 76)

Тројански коњ (енгл. trojan horse) представља злонамерни програм који се маскира као користан, а онда се прикачи на неки други користан програм и на тај начин нападачу шаље информације о корисничким лозинкама, банковним рачунима и другим подацима до којих нападач настоји да дође. У неким земљама, као што је САД и Аустралија, тројански коњи се користе и за потребе полиције, наравно уз одобрење суда, те се на тај начин прикупљају информације о потенцијалним извршиоцима кривичних дела из области високо-технолошког криминала. Ова врста програма се шири и ажурира инсталацијом комерцијалних оперативних система или преко даваоца интернет услуга. Даваоци интернет услуга су у обавези да на захтев надлежних државних служби безбедности, а уз сагласност суда, обезбеде надлежним органима приступ и инсталацију таквих врста података.

Црви (енгл. worms) су програми или кодови који користе сигурносне пропусте у програмима или у оперативном систему да би се ширили и извршавали путем мреже. Црв је самокопирајући рачунарски програм који користи мрежу за слање сопствених копија на остале рачунаре унутар неке мреже, без интервенције корисника. Чини штету на мрежи тако што је успорава. За дистрибуцију ове врсте програма најчешће се користи електронска пошта.

Споредна врата (енгл. backdoor) је програм који се најчешће у рачунару шири комбинацијом са тројанским коњем или црвом. Један од примера споредних врата представља *споредна рупа* који активира улаз у систем у који се инсталира, дајући могућност контроле система познаваоцу IP адресе. Споредна врата је дакле програм који омогућава комплетно заобилажење сигурносне процедуре у одређеном систему.

Следећи програми се употребљавају у активностима *неауторизованог праћења активности корисника*:

Adware је програм који без дозволе корисника приказује рекламе на његовом рачунару доносећи аутору приходе од сваке рекламе. Могу бити инсталирани на разне начине, а најчешће као тројанци или црви.

Spyware је злонамерни програм који скупља информације о кориснику и начину како користи рачунар. Дистрибуирају се као тројанци или црви. *Spyware* може да прати које „*web* сајтове" корисник посећује, електронску пошту коју шаље, или да бележи откуцане карактере на тастатури откривајући тако шифре или личне податке корисника. Сакупљени подаци се могу пренети до централног рачунара и злоупотребити. Врло често се налазе у саставу бесплатних програма, а најчешће бесплатних игара које се инсталацијом уносе у рачунар, и притом шаљу информације о коришћењу интернета неког корисника и слично.

Spam је нежељена пошта. Најчешће су у питању *spam* рекламне поруке чијим слањем спамери зарађују. Негативни ефекат је губитак радног времена на читање и брисање ових порука из inbox–а. Spam поруке су везане и за крађу идентитета јер се шаљу у име недужне особе или компаније.

Лишавање услуге (DoS) и *дистрибуирано лишавање услуге* (DDOS) су напади који имају циљ да онемогуће клијенте да користе рачунарске услуге, рачунарске мреже[31] и информационе ресурсе. Опструкција се реализује нападом на системе који омогућавају наведену услуге (нпр. сервер електронске поште). Напади се односе на део о доступности информација, а не на њихову поверљивост или садржај. Сајбер напади су усмерени на деструкцију, то јест лишавање услуга корисника тако што нападе извршавају на делове система који те услуге обезбеђују, као што су сервери. Такви напади могу да проузрокују озбиљне штете и последице по функционисање државног система, на последице које се односе на нарушавање имиџа националне државе, као и ширење страха међу њеним грађанима. Слична је

[31] Рачунарска мрежа је скуп рачунара повезаних одговарајућом комуникационом опремом. Она омогућава да рачунари у мрежи међусобно комуницирају, односно да размењују податке. На тај начин се омогућава да се одређени рачунарски ресурси (подаци, програми, рачунарско време, периферијски уређаји итд.), лоцирани на рачунарима повезаним у мрежу, ставе на располагање свим корисницима мреже. Главне компоненте рачунарске мреже су комуникациони медијум, комуникациони уређаји, комуникациони протоколи и командни софтвер. То се постиже нападом на системе који омогућују ову врсту услуга (сервер са ускладиштеним *web*-сајтовима или сервер електронске поште). Нападом је угрожена доступност информација, а не њихова поверљивост. Један од начина извођења напада је генерисање великог броја захтева у краткој јединици времена. Потенцјална последица је губитак времена потребног за оспособљавање система, што посредно може узроковати и економске последице. (Либрић, 2008)

ситуација и са појединим пословним субјектима, који трпе огромне економске губитке блокадом сајтова и сервера чији је задатак несметано обезбеђивање функционалности пословања. Сам начин напада изводи се тако што нападач успоставља у првој фази контролу над првим рачунаром који постаје „мастер“ напада. Преко овог рачунара инфицирају се други рачунари који се називају „зомбији“. Ефекат се постиже оног момента када зомби рачунар извршава сваку радњу коју нападач задаје неком врстом malwera, најчешће црвом, преко мастера, а да при том корисник није ни свестан шта се дешава. „Зомби рачунар се може испрограмирати тако да омогући отварање споредних врата унутар локалне мреже пословног субјекта, односно организације којој рачунар припада и на тај начин, депласира све примењене безбедносне мере организације.“ (Петковић, 2009: 293- 295)

Компаније у свету издвајају десетине милијарди долара за заштиту од програма као што су malweri који корисницима одузимају радно време и на тај начин смањују продуктивност рада тих компанија. Према речима Џона Стјуарта (John Stuart), шефа одељења за безбедност података у компанији *Cisco*, безбедност информација није више само борба против вируса и *spam*-а. Данас, покушај да се обезбеде послови, лични идентитет, па и саме државе, захтева већи ниво координације између страна које у прошлости нису заједно сарађивале онолико колико је било потребно. Да ли ће национална, лична безбедност, као и безбедност компанија бити на високом нивоу, зависиће само од сарадње и комуникације између ових страна. (Петковић, 2009).

5.1.2.1.2. Сајбер напади уз коришћење обмане

Неки од најизраженијих облика *сајбер напада уз коришћење обмане* су:

Мрежна крађа идентитета — Фишинг (енгл. Phishing) користи се за описивање илегалног прикупљања осетљивих информација обманом (бројеви кредитних картица, корисничка имена, лозинке, PIN кодови и

слично), при којој се нападач представља као неко вредан поверења и као неко ко има право и потребу за таквом врстом података (нпр. лажне поруке наводно послате из банке или друге финансијске организације). (Путник, 2009: 89) *Фишинг* поруке могуће је препознавати по томе што се у поруци траже лични подаци, инсистира се на хитности, линкови су лажирани, тело (body) електронске поруке је најчешће слика, пружају се нереална обећања и сл. Спровођење *Фишинг* напада врши се коришћењем различитих техника, маскирање URL адреса, пресретање комуникације, пропусти у *веб*-апликацијама, лажиране HTML email поруке. Заштита од *phishing* напада подразумева едукацију корисника, снажну аутентификацију корисника, обраћање пажње на сигурност при развоју web-апликација, сигурност email корисника, дигитални потпис порука електронске поште. (Путник, 2009: 85-86)

Термин *социјални* (*друштвени*) *инжењеринг* се употребљава у случају поступка заобилажења разних врста заштита, одавањем лозинки или других поверљивих информација које њихови власници свесно или несвесно одају нападачу. *Социјални инжењеринг* означава врсту напада при којој се нападач не служи информатичким техникама, већ путем комуникација наводи жртву да учини безбедносне пропусте и прекрши норме и процедуре, а да не примети да је изманипулисана. Нападачи користе разне технике које у великом броју случајева постају изузетно ефикасне. До изражаја долази вештина нападача да, у наизглед необавезном разговору, дођу до таквих информација које им обезбеђују пробијање постављених механизама заштите.

Социјални инжењеринг припада скупу напада на рачунарске системе, али и на системе у ширем смислу речи. Он се најједноставније може дефинисати као умеће навођења других особа да поступају према жељама нападача. Ради се о начину стицања информација и података до којих нападач легитимним путем не би могао доћи. Односи се и на прибављање бројева кредитних картица и PIN бројева у сврху *on-line* плаћања туђим картицама. При томе се не искоришћавају слабости и недостаци техничких система, већ се напад усмерава на најслабију карику целокупног ланца у

систему безбедности — на људски фактор. У суштини, ради се о психолошкој игри, у којој нападач покушава да злоупотреби неко од шест основних правила људског понашања: ауторитет, склоност, узвраћање, доследност, друштвена неоспорност, реткост. (Cialdini, 2009) Најчешће методе преваре које се користе у социјалном инжењерингу су уверавање (које се сматра најважнијим предусловом), лажно представљање, стварање одговарајуће ситуације, искоришћавање моралне одговорности, жеља за помагањем и коришћење старих веза из пословних контаката.

5.1.2.1.3. Злоупотреба сајбер простора као средства масовне комуникације

Један од најчешћих облика злоупотребе сајбер простора представља информационо ратовање. У циљу бољег разумевања овог појма, потребно је дефинисати и направити разлику између појмова као што је информационо ратовање, информатички рат, сајбер рат и мрежни рат. Информационо ратовање обухвата правне и дипломатске мере, пропаганду, психолошке кампање, политичке и културне субверзије, уплитање у локалне медије, активности на промоцији дисидентских и/или опозиционих покрета преко ИС. (Пуповац, 2001: 37)

„Информатички рат је само једна компонента информационог ратовања која се своди само на његов технички аспект, коришћење технике ради реализације циљева унутар информатичке структуре непријатеља. Разлика између информатичког и информационог ратовања је онај квалитет који се може обухватити појмом социјални инжењеринг, односно употреба информационе структуре за промену свести припадника нападнутог ентитета.“ (Ђорђевић, 2007: 83)

Информатичко ратовање може да се дефинише као „акције које се предузимају у циљу постизања информационе предности као подршке војној стратегији, деловањем на непријатељске информације и информационе системе, при томе штитећи своје информације и информационе системе.“ (Цигурски, 2002: 143)

Сајбер рат подразумева прикупљање информација о информационом систему непријатеља како би се његови ИС–и делимично или у потпуности елиминисали.

Мрежни рат представља сукобе ниског интензитета који значе намеру да се онемогући, оштети или промени оно што циљна популација зна о себи или мисли да зна о себи и свету у коме живи.

О важности информационог простора сведоче актуелне војне доктрине које информациони простор третирају као пети борбени амбијент, паралелно са копном, водом, ваздухом и космосом. (Цигурски, 2002: 141) Потребно је нагласити да информатички рат и информационо ратовање не подразумевају искључиво уништавање информационих система непријатеља него и заштиту сопствених информационих система, што укупној војној стратегији даје предност у решавању сукоба. Дакле информационо ратовање представља сегменат подршке свеукупној војној стратегији тако што спровођењем информационих активности слабе непријатеља, а сопственим снагама дају предност у домену спровођења војних активности, како у рату, тако и у миру. Инфомрациони рат се примењује и у сферама економије, политике и културе, чему је погодовао развој интернета. Као и физички, сајбер простор такође припада ономе ко га се први домогне. Како би стратегије успостављања контроле над интернетом биле успешне потребно је да се усвоје следеће максиме:

- загосподарити каналима за проток информација,
- емитовати у највећој могућој мери властите погледе и ставове са циљем њиховог наметања,
- непрекидно усавршавати методе и средства за обраду информација. (Путник, 2009: 97)

Следећу врсту злоупотребе сајбер простора представља *сајбер тероризам* и он се односи на пропаганду и психолошки рат. За сајбер тероризам погодно је деловање у областима као што су хемијска, прехрамбена, фармацеутска индустрија, водоснабдевање, нуклеарни програми, енергетска делатност. (Ђорђевић: 2007: 82-84) Циљеви сајбер терористе усмерени су на нарушавање безбедности живота и имовине

грађана као и основних субјеката који обезбеђују нормално функционисање друштва. Ефекти који се постижу спровођењем сајбер тероризма су ширење страха, панике и насиља. Предност у односу на класични тероризам је географска покривеност и могућност брзог деловања готово у свим деловима света.

Путем сајбер простора терористи теже да допру до три аудиторијума:

- постојећих и потенцијалних бораца и подржавалаца,
- међународног јавног мњења које није директно укључено у конфликт, али је заинтересовано за његове кључне елементе,
- непријатељске или противничке јавности. (Путник, 2009: 105)

Терористичке организације деловањем у различитим друштвеним делатностима могу да проузрокују штете великих размера, што може да угрози животе више стотина и хиљада људи. Хемијски акциденти, намерно изазвани, могу да проузрокују загађења у животној средини и да негативно утичу на безбедност грађана који насељавају таква подручја будући да изазивају штетне утицаје по здравље становништва и негативне импликација на квалитет и исправност пољопривредних производа који се користе у исхрани. Постигнути ефекти могу да буду краткорочни и дугорочни. Циљеви које терористичке организације настоје да постигну су брзи, краткорочни и ефикасни и иду ка томе да степен страха и незадовољства достигну максимум, како би утицај на опстанак владајуће структуре био што ефикаснији. Пласирање разних врста дезинформација о деловању терористичких група на територији неке државе, затим блокада и „рушење“ сајтова важнијих државних органа и управа, представља такође једну врсту cyber тероризма која у одређеној мери постиже ефекат страха и несигурности код грађана те националне државе или бар неког њеног дела. Трећи аспект cyber терористичког деловања у сајбер простору представља прикупљање и пласирање информација путем интернета о изради смртоносног оружја које ће у каснијој фази бити примењено у терористичке сврхе. На разним интернет порталима постоје читава упутства о начину израде експлозивних направа којима је могуће угрозити животе и безбедност

грађана циљане државе у већим размерама.[32] Овде се у суштини ради о потребној логистичкој подршци сајбер тероризму коју терористи спроводе путем интернета, како би се створили услови за извођење терористичког акта. Као и у претходним ситуацијама које се односе на шпијунажу или криминално деловање корисника информационих система, у спровођењу ове врсте недозвољене активности, терористима посао олакшавају лица која се налазе унутар система, а спремни су да, услед неких разлога (нпр. верски фундаментализам) или уцена на сарадњу, помажу таквим организацијама.

Терористичке организације користе сајбер простор такође за регрутовање и обуку потенцијалних трерориста путем интернета. Поједини web-сајтови и форуми приказују елементе обуке, снимке из актуелних сукоба, борилачке вештине и слично. Поред наведене намене, интернет се често користи за прикупљање новчаних фондова потребних за финансирање активности терористичких организација. Размена информација међу терористичким органзацијама и појединцима је такође развојем интернета једноставнија, теже се открива, а применом одговарајућих заштитних мера гарантује готово потпуну конспиративност. [33]

5.1.2.1.4. Субјекти претњи у сајбер простору

Хакерски напади представљају продор у ИС корисника са намером манипулисања и прибављања заштићених података и информација, пословних тајни и других поверљивих података.

„*Хакер* је особа која ствара изван стандардних техничких лимита, користећи сопствене вештине, са циљем да надмудри и креативно превазиђе ограничења која му се намећу, не само у пољима његових интересовања (која се могу сврстати под информационе технологије) већ и у свим осталим

[32] У Ослу (Норвешка), 2011. године извршен је напад на зграду Владе у којем је погинуло седморо људи, бомбом направљеном од вештачког ђубрива. Сличан напад се догодио 1995. године у Оклахоми у којем је страдало 168 жртава. (http://www.politika.rs/vesti/najnovije-vesti/Bomba-u-Oslu-napravljena-od-vestackog-djubriva-i-dizela.lt.html, 2016, 4. март)

[33] Пласирање скривених порука, мигрирање сајтова, паразитски сајтови.

аспектима живота.“ (Путник., 2009: 121) Хакери који искључиво за себе желе да остваре себичне интересе и на тај начин да дођу до новца и других врста користи, називају се *крекери*. Они нелегално користе информационе системе и наносе штету рачунарском систему жртве. У ову категорију се могу сврстати сви они чија се активност описује као декадентна, усмерена на ширење болесних идеја и погледа (националне, расне, верске и друге нетрепељивости и мржње), уцењивање, преваре, лажна обећања, трафикинг, дроге и на рушење друштвеног система и општеприхваћених вредности. *Хактивисти* се користе истим методама и техникама као и хакери, међутим циљеви које они спроводе односе се на привлачење пажње јавности на неки политички, социјални и проблем друге врсте. Нападом на „web сајт“, хактивисти мењају његов садржај, најчешће насловну страну, као доказ да су били присутни, а често га и блокирају. *Инсајдери*, у најширем смислу представљају злонамерне актере који дејствују прикривено унутар и против организације чији су део. Мотиви за спровођење злонамерне активности могу да буду: различит систем вредности у односу на радну организацију у којој су запослени, радозналост, освета, изнуда, уцена. Сајбер простор и ИКТ су постали окосница диверзификације криминалних дела и инструменти који криминалним организацијама омогућавају бољу оперативну ефикасност. Тежња за илегалним стицањем профита представља суштински мотив за профил сајбер криминалца у односу на профил хакера, који је мотивисан најчешће славом, забавом или злобом.

5.1.2.2. Шпијунажа

Према међународном праву, шпијуни су тајни агенти једне државе или међународне организације послати у иностранство у намери тајног прикупљања података у вези са војном, политичком или економском ситуацијом. Мада све државе „стално или повремено шаљу шпијуне у иностранство и мада се то не сматра погрешним, морално, политички или правно, такви агенти, разуме се, немају било какав признати статус према

међународном праву јер они не представљају агенте за одржавање њихових међусобних односа" (Ђорђевић, 1978: 54).

Шпијунажа би се могла поделити на следеће категорије[34]:

1. Политичка шпијунажа
2. Војна шпијунажа
3. Економска шпијунажа
4. Електронска шпијунажа

1. *Политичка шпијунажа* представља интересовање страних обавештајних служби „за рад државних органа и организација и њихових активности у области унутрашње и спољне политике (Ђорђевић, 1986: 975)". У том деловању посебна пажња посвећује се носиоцима јавних функција као што су шефови држава, председници влада, министри и друге високе државне личности.

2. *Војна шпијунажа* представља прикупљање обавештења и података о оружаним снагама постојећих или евентуалних противника, „као и о оружаним снагама других земаља било у циљу своје одбране или агресивних циљева" (Ђорђевић, 1986: 977). Изузетак је војна шпијунажа у условима рата коју међународно право не забрањује. Разлог таквог тумачења има утемељење у томе да шпијун ухваћен у делу не одговара због кршења правила међународног права и не може му накнадно бити суђено, осим ако је држављанин државе у којој је починио дело шпијунаже.

3. У свакодневном животу и у правној теорији *економска шпијунажа* се често назива привредном шпијунажом, док се у високо индустријски развијеним земљама често среће појам индустријска шпијунажа. Потребно је разјаснити разлике у терминима. Индустријска шпијунажа је типична карактеристика савремене шпијунаже, јер је индустрија производ и карактеристика савременог друштва. Уско је упућена на ону делатност чија је

[34] Могуће је разликовати неколико области у којима се развијају посебни модели тајних операција. То су: политичке акције, пропагандно-психолошке операције, економске мере и паравојно ангажовање. То значи да тајне акције укључују пружање политичких савета, финансијске помоћи појединцима, политичким странкама и лидерима, подршке појединим невладиним организацијама, синдикатима, пропагандне операције, школовање појединаца, економске мере, паравојно организовање са циљем рушења или подршке власти и атентате. (Richelson, 1995: 342).

позадина чисто комерцијалне природе. Индустријска шпијунажа се може посматрати као скупни појам који обухвата конгломерат деликата којем припадају крађа, утаја, превара, нелојална конкуренција, подмићивање, фалсификовање докумената и слично. Између термина економска и привредна се не могу направити јасне разлике. Индустријска шпијунажа може да представља само једно подручје и део економске шпијунаже, јер је по својим задацима усмерена на одређену, уску, специфичну и стручну делатност у области економске шпијунаже. Осим тога, економска шпијунажа, поред тог комерцијалног аспекта, укључује и аспект јавно–правне природе чија је делатност везана за посредно обарање влада, политичке притиске, изнуђивање одређених уступака од неке земље и слично. У вези свега наведеног, јасно је колико је тешко дати прецизну дефиницију економске шпијунаже. „Стога је једно шире одређење економске шпијунаже дефинисано као скуп радњи неког лица усмерених на поверљиве економске податке и писмена“ (Радовић, 2008). Субјекти којима се оне саопштавају, предају и одају су „стране државе, стране организације или лица којима служе починиоци дела шпијунаже” (Дракулић, 1996: 335).

4. *Електронска шпијунажа* усмерена је ка прикупљању података о противничким електронским средствима и системима свих техничких и електронских видова комуникација и веза, хватању и дешифровању порука и информација противника одасланих електромагнетним таласима, бежичним, а донекле и жичаним везама (телефонским, телеграфским, телепринтерским, радиом, рачунарским, телефаксом и другим везама) и усавршеним средствима за прислушкивање и разбијање кодова, снимању противничких територија и објеката од виталног интереса најсавременијим средствима са земље, из ваздуха и са морских пространстава, обезбеђењу тајности шифрованих порука сопствене земље, односно ка спречавању страних држава да дођу у посед виталних тајни и слично. (Мијалковић, 2013: 101) Ова врста шпијунаже користи се за прикупљање података у банкарству, посебно код инвестиционих банака, корпорација и војних система. Она припада савременим шпијунским активностима, као што је то случај и са сателитском шпијунажом, коју за сада спроводе искључиво најразвијеније земље света.

Управо државне обавештајне агенције имају значајну улогу у прикупљању података у савременим шпијунским делатностима, а један од најпознатијих сателитских система за прикупљање података основан од стране Националне безбедносне агенције САД–а назива се „Echelon“. „Echelon“ располаже са неколико хиљада пријемних станица распоређених у земљама потписницама споразума: САД, Велика Британија, Аустралија, Канада и Нови Зеланд.

Питање војно индустријског комплекса у пословним активностима и прикупљање података о производним потенцијалима земаља коришћењем метода пословне шпијунаже представља једну од кључних активности коју спроводе државе у циљу заштите сопствених пословних интереса. Трговина наоружањем и војном опремом представља један од кључних елемената за буџетски прилив развијених земаља, те су, самим тим, подаци, који утичу на правилно доношење одлука надлежних лица из државног апарата којима се побољшава конкурентска позиција домаћих индустријских и извозних капацитета на другим тржиштима, веома важни. Активности пословне шпијунаже се спроводе и у циљу заштите сопственог тржишта и других циљаних тржишта од конкурената који настоје да обезбеде пласман сопствених производа. Више пута је у историји забележено да су се између појединих земаља на директан и индиректан начин водили ратови како би се задржао примат у пословним активностима трговине наоружањем и војном опремом, а исто тако и експлоатацијом природних ресурса као што су гас, нафта и други необновљиви ресурси. Дакле, пословна шпијунажа се данас највише примењује у областима високих технологија, електронике, информатике, свемирских истраживања, ваздухопловства, индустрије наоружања и у другим елеменатима од важности за систем одбране. Паралелно са развојем науке и захтеви обавештајних организација су постали израженији и обухватнији. Развојем сателитске технологије, након Другог светског рата, најразвијеније земље света, а пре свега САД и тадашњи СССР, су започеле нову еру шпијунаже која се назива сателитска шпијунажа. Сателити су употребљавани у сврху локализације објеката, анализе терена, навигације, телекомуникација. Иако су високе технологије заступљене и у обавештајним активностима држава и даље је човек као извор информација

на првом месту. Информације добијене од човека представљају бољи основ за доношење квалитетних одлука. За прикупљање података користе се лица тренутно запослена и бивши запослени у привредним субјектима и институцијама које представљају предмет интересовања обавештајних агенција. Најчешће се ради о незадовољним лицима која су запослена унутар тих организација или лицима која су на неки начин искомпромитована и уцењена на сарадњу. Такође, мотив за уступање сазнања може да буде и материјална заинтересованост, као и вршење утицаја на послодавца у циљу остваривања других личних интереса као што је напредовање, решавање статуса чланова породице и других лица блиских даваоцу информација.

Бечка конвенција о дипломатским односима (http://www.ius.bg.ac.rs/prof/Materijali/milboj/Konvencija%20o%20diplomatskim%20odnosima.pdf, 2016, 2. јул), која је ступила на снагу 1964. године и Бечка конвенција о конзуларним односима (http://demo.paragraf.rs/combined/Old/t/t2003_08/t08_0075.htm, 2016, 2. јул) из 1961. године су међународни документи који третирају ова питања. Конвенцијом о дипломатским односима предвиђено је да је једна од основних функција дипломатског представништва обавештавање свим дозвољеним средствима о условима и развоју догађаја у држави у којој се акредитује и подношењу извештаја влади државе која акредитује. Дипломата, који не жели да изазове међународни инцидент, нужно мора да познаје законе државе акредитације, посебно у вези са одредбама кривичног закона који разматра кривична дела шпијунаже (Члан 41. Бечке конвенције о дипломатским односима). Исти члан обавезује дипломатског службеника да се не меша у унутрашње ствари државе акредитације. Члан 29. наводи да је личност дипломатског службеника неприкосновена и он не може бити хапшен и притваран од стране органа државе акредитације, док се у члану 31. изричито наводи да дипломатски службеник ужива имунитет од кривичног судства. Бечка конвенција о дипломатским односима предвиђа и заштиту дипломатских службеника и њихових просторија од специјализованих, пре свих контраобавештајних, служби државе у којој су акредитовани, неповредивост архиве дипломатске мисије, ма где се они налазили. Службена

преписка мисије је неповредива и односи се на све врсте преписки у оквиру функције дипломатске мисије. Држава у којој се акредитује дужна је да обезбеди несметану реализацију функција особљу дипломатске мисије, да им омогући комуникацију са државом која их је акредитовала и слободу кретања члановима дипломатске мисије уз ограду везану за подручја од значаја за националну безбедност.

Легалитет ратне шпијунаже био је успостављен још Хашким правилником из 1907. године (http://www.vs.rs/content/-attachments/CMO/Radni materijal za pripremu-MHP zbirka 2013 Srb Eng.pdf, 2016, 2 јул), који је прописао услове под којим се шпијунска делатност може примењивати између сукобљених страна, односно дефинисао појам шпијуна. Према овом правилнику, шпијун је само она особа која, делујући потајно или под лажним изговорима, прикупља или настоји да прикупи обавештења у оперативној зони једне зараћене стране, с намером да их саопшти противничкој страни. Зато се, према овој одредби, шпијунима не сматрају непрерушени војници који продру у оперативну зону непријатељске војске ради прикупљања обавештења и војна и невојна лица задужена да преносе пошиљке намењене њиховој или непријатељској војсци.

Допунски протокол I из 1977. године прихвата и проширује решења из Хашког правилника утврђујући да ниједан припадник оружаних снага у сукобу, ако падне под власт противничке стране док је ангажован у шпијунажи, нема право на статус ратног заробљеника, осим ако је у униформи својих оружаних снага. У овом другом случају, такво лице неће се сматрати да је ангажовано у шпијунажи. Протокол такође прописује да се неће сматрати припадником оружаних снага стране у сукобу који пребива на територији под окупацијом противника, ако прикупљање обавештења од војног значаја не врши лажно се представљајући, односно ако није ухваћен док се бавио шпијунажом.

Са аспекта ове анализе од значаја је поменути и Допунски протокол уз Женевску конвенцију о заштити грађанских лица за време рата (http://www.mfa.gov.rs/sr/images/stories/komisija/МКСК%20-%20Izvori%20MHP.pdf, 2015, 2. фебруар) из 1949. године, који представља

додатни напредак у кодификацији међународног ратног права. Наведени документ се, између осталог, бави и регулисањем питања „перфидног начина ратовања" који се забрањује. Под тим појмом се подразумевају следеће радње:

- лажно истицање симбола предаје или намере преговарања,
- симулирање болести или рањавања,
- претварање да је неко цивил и да има статус неборца и
- ношење лажних униформи, амблема или симбола, чиме лице узурпира право заштићеног статуса у ратним сукобима.

Појам пословна шпијунажа се појавио тек 80–их година прошлог века, а највећи допринос њеном научном утемељењу је дао Стеван Дедијер. Он је упозоравао још 70–их година прошлог века на важност обавештајне делатности за функционисање целокупног друштва, а не само државе. (Dedijer & Jéquier, 1987) Лидери пословних субјеката су схватили да је за доношење одлука у вези пословања потребно нешто више од интуиције и искуства. Пословна шпијунажа представља „комбинацију података, информација и знања у односу према пословном окружењу у којем компаније делују, комбинација која, ако делују на основу истих, компанијама омогућава стицање конкурентске предности или доношење битних одлука" (http://www.institute-for-competitive-intelligence.com/articles-general/the-language-of-businessintelligence, 2014, 3. мај).

Економска шпијунажа се често поистовећује са појмом пословне шпијунаже, иако је само њена врста. Она се односи на прикупљање података о привредним субјектима искључиво у циљу бољег позиционирања на тржишту и стварања већег профита. Индустријска шпијунажа, као најужи појам, подразумева такву врсту делатности која се односи на технички и технолошки развој и уже професионалне интересе одређених пословних субјеката. Дакле, индустријска шпијунажа представља „само једно подручје и део економске шпијунаже, јер је она по својим задацима усмерена само на одређену специфичну стручну делатност у области економије" (Петковић, 2009: 116).

Области које представљају предмет интересовања носиоца индустријске шпијунаже су: наука, техника, минералне сировине и свемирска истраживања. Прикупљени подаци из ових области дају предност сопственој држави на позиционирању њених компанија на иностраном тржишту. Размештај и капацитети минералних сировина, обновљивих и необновљивих енергетских ресурса, представљају један од кључних елемената интересовања обавештајних служби, посебно високо–развијених земаља. Технолошка открића представљају предмет истраживања јер су у директној вези са развојем свих врста индустрије, а резултат су исцрпљујућих и скупих вишегодишњих научних истраживања. Ако узмемо у обзир само истраживања у фармацији и медицини која се односе на проналаске лекова за лечење болести, онда може да се схвати колико новца је потребно да би започела њихова масовна производња. Доласком до информације о саставу таквих лекова и достигнутим истраживањима у вези спровођења тестирања на здравље људи и појаве које настају њиховом конзумацијом, ствара се значајна тржишна предност компаније која себи може да обезбеди такве информације, јер је на тај начин избегнуто да се у цену коштања укључи и цена истраживања, која се често мери и десетинама милиона евра. Научна истраживања из области свемирског развоја су и даље једна од најстрожије чуваних тајни најразвијенијих земаља света, пошто се достигнућа у овој области узимају као мерило свеукупног техничког и технолошког развоја.

Дакле, осим војне и политичке шпијунаже, у новије време све чешће се говори и о економској, пословној, индустријској и привредној шпијунажи. Фабрике, корпорације, концерни и удружења, било да су приватно или државно власништво, на свом подручју и у оквиру своје надлежности, оснивају своје службе за прикупљање података о производњи, плановима производње нових производа, ценама, наступима на домаћем и светском тржишту истоврсних привредних субјеката у својој и страним земљама. Чврста повезаност и међузависност привреде свих земаља у свету, као и конкуренција која стоји изнад свега тога, условили су и развој економске шпијунаже до невероватних размера. Економска шпијунажа, као нова економска дисциплина, иако негде занемарена, заузима значајно место у

односима међу државама и водећим транснационалним компанијама. Када се ради о економској шпијунажи неопходно је упозорити да се на њу не може гледати само са становишта националне безбедности, јер се често ради о шпијунажи међу домаћим привредним субјектима. Тако да у САД–у око 70 % обавештајне делатности против америчких фирми реализују друге америчке фирме, 23 % стране фирме, а само 7 % стране државне обавештајне службе. (Петковић, 2009)

Економска шпијунажа и класична шпијунажа (у литератури се наводи као „шпијунажа“) су идентичне активности осим у делу који се односи на подручје рада. Економска шпијунажа добија посебан значај након завршетка Другог светског рата и поделе света на два блока, на земље које су приступиле „НАТО савезу“ и земље потписнице „Варшавског уговора“. Између два супротстављена блока наступа време „хладног рата“ у којем обавештајне и контраобавештајне службе имају водећу улогу у заузимању примата у светској политици. Економска шпијунажа у то време није представљала посебан сегмент већ је била део војно–политичке шпијунаже, с тим да су се прикупљени подаци користили у циљу побољшања привредних капацитета сопствене националне државе. Распадом „Варшавског блока“ и окончањем биполарне поделе света, економска шпијунажа заузима централно место у стратегијама савремених држава. Значај економског развоја заузима важно место и у развоју осталих области као што је одбрана, индустрија, квалитет и степен међународне сарадње. Америчка служба FBI (енгл. *Federal Bureau of Investigation*) прави разлику између економске и индустријске шпијунаже, на тај начин што првом управља држава, а спроводе је обавештајне институције које, применом легалних и нелегалних метода, прикупљају тајне податке од значаја за конкурентску државу и користе их за јачање сопственог државног и приватног сектора, док индустријском шпијунажом управљају приватни пословни субјекти у циљу постизања пословне предности у односу на конкуренцију.

Предност над конкуренцијом у пословању се данас постиже захваљујући расположивости квалитетним индустријским, производним или финансијским информацијама до којих пословни субјект долази

ангажовањем сопствених обавештајних ресурса. Економска шпијунажа представља скуп добро планираних мера и активности у циљу прибављања поверљивих економских информација од значаја за пословну активност привредних субјеката и за заштиту економских интереса сопствене државе. Економска шпијунажа обухвата велики број поступака агресивног карактера чији је циљ угрожавање конкурента на светском тржишту применом легалних и нелегалних средстава, веома често неспојивих са етичким постулатима пословања. За разлику од обавештајне делатности, економска шпијунажа употребљава све расположиве методе, од медија до најсложенијих поступака, који се користе и у надметању са традиционалним савезницима.

У циљу прикупљања тајних података, користе се средства као што су запошљавање својих људи у конкурентским компанијама, ангажовање специјализованих агенција, коришћење дипломатских представника у иностраним земљама где компанија има пословне интересе. (Нешковић, 2013: 58)

Дакле, економска шпијунажа се спроводи и користи да привредном субјекту пружи конкурентску предност на тржишту. У основи она се спроводи и користи свакодневно. Људи прикупљају релевантне пословне информације, анализирају их у одређеном контексту и на тај начин их чине корисним у процесу доношења одлука. Такав прерађени производ — информација се онда користи у одлучивању, изради бољих планова или за неке друге сврхе. Познавање и разумевање конкурената и тржишта је неопходно на путу да се постане успешан привредни субјект. Познавање тржишта и конкуренције је посебно важно у процесу дугорочног стратегијског планирања. (Даничић и Стајић, 2008: 226-227)

С обзиром да у контраобавештајним структурама важи правило да је превентива најважнији чинилац успешног супротстављања обавештајној делатности, све службе тог карактера, биле оне државне или везане за пословање неке приватне компаније, највеће капацитете посвећују добијању информација које обезбеђују правовремено реаговање и спречавање настајања нежељеног безбедносног догађаја. С обзиром да такво ангажовање подразумева стручност пре свега лица које га спроводе, приватне компаније

често у својим саставима запошљавају бивше кадрове обавештајно–безбедносних служби којима су ове методе и технике познате, а база лица са којима одржавају контакте обезбеђује приступ и најосетљивијим врстама информација.

5.1.2.2.1. Корупција и поткупљивање као мотив за спровођење шпијунаже

Европски савет у свом извештају из 1994. године корупцију дефинише као понашање лица која на службеном или приватном положају злоупотребљавају своју дужност да би остварили зараду или добитак било које врсте. Приватни интереси се у овом случају стављају испред општих или јавних интереса, а најчешћи пример у којем се испољава је ненаменско трошење новчаних средстава пореских обавезника.

У пословним преговорима, а у циљу обезбеђења квалитетније позиције и остварења пословних циљева, учесници се често користе и нелегалним средствима и методама доласка до поверљивих информација, а једна од њих је поткупљивање корумпираних преговарача друге стране. Још је 1937. године, у енциклопедији *Свезнање*, корупција дефинисана као „кварење духа, обичаја, текста; у обичнијем смислу – систем потплаћивања при свршавању послова код јавних или приватних установа на штету тих установа“ (Првуловић, 2010: 224).

Иако је дефиниција, посматрајући то из угла модерног друштва, мањкава и непотпуна, она ипак осликава суштину ове појаве која данас представља један од најозбиљнијих проблема који утичу на тржишне токове у глобалним размерама. Од међународних институција које су прве озбиљније почеле да се баве овом незаконитом активношћу, издваја се ОЕЦД, која је још 1997. године усвојила Конвенцију против корупције. У њој дословце стоји да „компаније не смеју ни директно ни индиректно нудити, обећавати, давати и тражити мито или друге услуге како би договорили посао.“ (Првуловић, 2010: 224) Међутим, то је ипак остало само у домену теорије, а пракса показује нешто сасвим друго. Посебан проблем када је

корупција у питању представљају земље Источне Европе. Корупција у овим земљама је посебно дошла до изражаја приликом спровођења поступка приватизације државних предузећа и њиховог преласка у приватно власништво.

У циљу супротстављања корупцији, националне државе, све чешће користе термин „транспарентност“ који подразумева јавна тендерска и аукцијска надметања. Ипак улога безбедносног система у сузбијању, пресецању и отклањању корупције данас има највећу улогу. Тренутно у свету, а исто тако и код нас, најризичније области са аспекта корупције су: полиција, здравство, правосуђе и школство. (http://www.transparentnost.org.rs/index.php/sr/, 2015, 2. јун) Ипак, не треба се заваравати да корупција не постоји у високоразвијеним земљама и да је она присутна искључиво у земљама у развоју. Много је корупционашких афера потресло високоразвијене западне земље у којима су најодговорнији државни функционери били учесници догађаја, а новац као награду депоновали су управо у банкама земаља у којима је тајност улога један од основних постулата пословања. [35]

Данас се корупција испољава кроз разне облике, од примања новца у виду награде за учињено дело (уступање пословних информација неовлашћеним лицима) до куповине разних врста поклона мале и средње вредности. Посебан проблем и опасност по једно друштво представља корупција стимулисана од стране политичких странака које захваљујући донацијама локалних предузетника, истима омогућавају повољнији статус на тржишту, а у појединим случајевима монополистички положај. У неким мање развијеним државама, у којима је и даље изражена слабост институција и

[35] Корупционашка афера „AUGUSTA“, која се догодила 1995. године у Белгији, потврђује појаву корупције и у високоразвијеним земљама. Ради се о набавци 46 хеликоптера од стране италијанске фирме „AUGUSTA“ који су по карактеристикама били далеко слабији од немачких и француских хеликоптера „Пума“ и „Газела“. За наведену корупционашку аферу оптужен је Вили Клас, министар иностраних послова Белгије и генерални секретар НАТО-а. Надлежни суд је установио 1995. године да је фламанска Социјалистичка партија, коју је водио именовани, на рачун у швајцарској банци, као противуслугу добила новчана средства у висини од 1,7 милиона америчких долара. Међутим, исте године, исти суд је утврдио да је Клас 1988. године, за време док је обављао функцију министра привреде, обезбедио француској авиоиндустрији „DASO“ посао ремонта борбених авиона, за који је партија Класа добила 2 милиона долара. (Првуловић, 2010: 228-229).

недоследно спровођење законске регулативе, ТНК испољавају свој утицај тако што доводе на власт лица која уместо да спроводе политику од државног интереса спроводе је у складу са интересима компанија. За таква решења, која пре свега иду у корист ТНК, добијају награде у виду новчаних или других материјалних средстава.

5.1.2.3. Криминал у области интелектуалне својине

Један од најчешћих облика пословних тајни, а предмет су интереса лица и организација које би њиховом употребом могле да постигну жељени пословни или неки други ефекат, представљају економски патенти, заштићени знакови и индустријске тајне као облик пословних тајни. Поједина лица и пословне организације настоје да дођу до претходно наведених података користећи све методе на располагању, свесни да такви подаци представљају предност за боље и квалитетније позиционирање на тржишту. Тиме се ствара такозвана нелојална конкуренција, која крађом патента ствара копију производа, знатно јефтинијег од оригиналног. Разлог за то је избегавање издвајања новца за развој и других додатних трошкова који су понекад пресудни за одређивање висине цене неког производа. Крађа привредних патената и заштитних знакова је чест и присутан вид нелојалне конкуренције. „Производни изум, заштићен у патентном заводу друге земље, неовлаштено се копира и износи на тржиште у верно имитираној амбалажи, опремљен фалсификатима, жигова, грбова и знакова“. (Првуловић, 2010: 202) Овде се ради о копији оригиналног производа који се на тржиште пласира у форми оригинала. С друге стране, крађа патента у фази развоја омогућује лицу или организацији која до њега дође да оформи производ под својим именом и да на тај начин постане нелојална конкуренција њеном ствараоцу или аутору. У циљу борбе против таквих и сличних случајева на глобалном нивоу основана је Светска организација за заштиту интелектуалне својине. Наведена организација своју надлежност на спречавању наведених дела може да спроводи само међу државама потписницама конвенције. У циљу

бољег разумевања проблематике потребно је дефинисати неколико основних појмова.

Интелектуална својина подразумева индустријску својину (иновације, заштитни знакови) и ауторска права (литерарна, музичка, ликовна, филмска дела). Иако се подстицањем стварања иновација стимулише привредни раст тако што се подижу инвестиције у иновативну индустрију, као и ниво запошљавања, заштита интелектуалне својине је прихваћена међу државама на различит начин. (http://www.paragraf.rs/propisi/-zakon_o_autorskom_i_srodnim_pravima.html, http://www.paragraf.rs/propisi/zakon_o_patentima.html, 2015, 4. јун)

По дефиницији *патент,* представља исправу којом надлежни орган за регистрацију проналазака потврђује у корист одређене особе заштиту конкретног проналаска (Закона о патентима, Службени гласник Републике Србије, 99/2011, члан 2.).

Ауторско дело је оригинална духовна творевина аутора, изражена у одређеној форми, без обзира на његову уметничку, научну или другу вредност, његову намену, величину, садржину и начин испољавања, као и допуштеност јавног саопштавања његове садржине. *Ауторско право* је морално и својинско (власничко, наследно) право једног аутора на његово уметничко или литерарно дело (Закон о ауторским и сродним правима, Службени гласник Републике Србије, 104/2009, 99/2011, 119/2012, 29/2016, члан 2.).

Од међународних институција, које се тренутно баве питањима заштите патената, најзначајнији је Европски завод за патенте (енгл. *European Patent Office*) који обезбеђује државама потписницама заштиту од неовлашћеног коришћења заштићених патената (https://www.epo.org/index.html, 2015, 4. јун). На међународном плану 1883. године усвојена је Париска конвенција о заштити патената. Иницијатива за усвајање ове конвенције је потекла од индустријски најразвијенијих земаља, а иста дефинише да за коришћење технолошких открића и патената, корисник мора са власником патента да склопи уговор и финансијски му обезбеди надокнаду за коришћење. Највећа и у светским токовима

најистакнутија организација која се бави заштитом патената јесте Светска организација за интелектуалну својину (WIPO) са седиштем у Женеви. Од организација у Републици Србији, заштитом патената се бави Завод за интелектуалну својину Републике Србије (Првуловић, 2010: 245–246).

У циљу бољег разумевања ове проблематике, неопходно је дефинисати појам *индустријске тајне* као „чување пројеката и података о новом производу до тренутка његове јавне промоције, да би се појавио први и једини на тржишту и тим остварила предност над конкурентима“ (Првуловић, 2010: 204).

Други аспект овог проблема представља бесправно умножавање и продају заштићених производа (softwer, други производи) који су интелектуална својина или производи на које поједина лица полажу ауторска права. Крађа заштитних знакова и индустријских тајни представља један од видова борбе против нелојалне конкуренције у којој носилац такве активности копира заштићени производ и износи га на тржиште у верној и имитираној амбалажи. До података у овом случају долази се на различите начине, а један од њих је посета сајмова и изложби на којима се од носилаца пројекта, техничког и продајног особља као и овлашћеним и неовлашћеним фотографисањем настоји прикупити што више информација о производу. Познато је да на велике сајмове аутомобила Јапанци шаљу стручњаке и конструкторе који врше фотографисање, праве скице најновијих техничких и дизајнерских решења. Међутим, постоје и други начини доласка до података који представљају индустријску тајну као што је подмићивање службеника и конструктора у циљу откривања развојних планова и пројеката и прелазак у конкурентска предузећа. [36]

Пиратерија је врло изражена у видео и аудио индустрији, у копирању компјутерских програма. Процена је да је око 35 % програма инсталираних на личним и пословним компјутерима у свету пиратског порекла. Такви се програми најчешће користе у Кини, означена као земља која нелегалне

[36] Валтер Де Силва, чувени дизајнер аутомобила Алфа Ромео 156, 1999. године је прешао у супарничку компанију *Фолксваген*. Спортски имиџ који је захваљујући наведеном конструктору добио аутомобил Сеат постао је директна конкуренција у то време популарним аутомобилима Алфа 146 и Алфа 156. (Првуловић, 2010: 205)

програмске пакете користи у највећој мери. У том смислу све је присутнија и израженија борба у циљу заштите патената, како на међународном тако и на националном плану, која подразумева доношење квалитетних законских решења у циљу предузимања санкција према починиоцима и других мера које ће сузбијати наведену нелегалну активност. (Првуловић, 2010: 247-248)

5.1.2.4. Физички напади на информационо-комуникационе системе

Физички напади на информационе системе представљају један од најчешћих начина доласка до поверљивих информација које се примењују од стране неовлашћених лица и организација. Најчешћи облик спровођења ове недозвољене и законом забрањене активности представља крађа података и информација која може да буде унутрашња и спољна у зависности од тога ко је спроводи. [37]

У циљу спречавања и предузимања превентивних мера којима би се наведена активност спречила или бар у некој мери ублажила, надлежне државне институције појединих националних држава спровеле су истраживања. Истраживање Министарства трговине и индустрије Велике Британије спроведено 2004. године је указало да је већина упада и крађе поверљивих података спроведено од стране спољних чиниоца, а не унутрашњих (www.security–survey.gov.uk, 2016, 3. април).

Следећи начин доласка до поверљивих података и информација представља крађа информатичке опреме која подразумева физички приступ до рачунара или меморијских јединица на којима се чувају поверљиви подаци. Иако тешко изводљиво, многе компаније посебну пажњу поклањају заштити информација од стране програмских облика угрожавања, а притом заборављају важност сегмента физичко–техничког обезбеђења објекта.[38]

[37] Случај крађе тајних база података из државне лабораторије у Лос Анђелесу 2004. године (Јаворовић и Биланџић, 2007: 300).

[38] Случај крађе лап топ рачунара из компаније Hewlett – Packardна у којем су се налазили подаци 200.000 тадашњих и бивших запослених лица. (www.pcchip.hr/?cmd?=21&arh=1&solo_id=7470, 2014, 11. јун)

Такође, један од битних начина физичких напада на ИКС представља онеспособљавање информатичких центара, сервера и рачунарских јединица. Овај физички напад се најчешће спроводи изнутра, од стране лица запосленог у компанији или институцији која је предмет напада. ИКС који је предмет напада онеспособљава се тако да изазове најмањи могући степен сумње од стране лица запослених у безбедносном сектору компаније, а најчешће се симулира као грешка система настала из неких других разлога као што су напонске осцилације, прљавштина, дотрајалост опреме и слично. Губитком таквих информација, које не морају нужно да буду означене као поверљиве, компанија трпи огромну штету што утиче на њену конкурентност и могућност прилагођавања новим пословним изазовима. У тим ситуацијама, уништавају се делови информационог система који не могу да се регенеришу, тј. они делови на којима су ускладиштени подаци до којих није могуће доћи другим путем.

Подметањем пожара постиже се сличан ефекат као у претходном случају, с тим да је проузрокована штета много већа и да је активност могуће спровести како изнутра тако и споља. Пожаром се циљају делови компаније у којима се налазе најважнији делови информационог система, а цео случај се најчешће приказује као ненамеран, уклањају се трагови који могу да доведу до извршиоца, а као и у претходном случају извор настанка пожара се приказује као технички квар. С обзиром да је у случају пожара вештачењем тешко установити како је до истог дошло и утврдити одговорност запослених лица, овом сегменту заштите од пожара се унутар компанија и институција поклања посебна пажња.

На последњем месту је терористички напад на ИКС и његово уништење. У овом случају највећу опасност од оваквог акта имају државне институције које поседују информације о терористичкој организацији, њеним члановима и намерама о спровођењу неког терористичког акта. У том случају терористичке организације су спремне на спровођење активности којима би се таква институција у потпуности уништила, као и докази са којима располаже. О постојању доказа терористичка организација је обавештена од стране лица изнутра који из разних мотива вођама исте

пружају осетљиве информације. Мотив за сарадњу може да буде верски, идеолошки али и материјалне природе ако је у питању лице које живи под високим материјалним оптерећењем, материјалном задуженошћу и слично.

Када је у питању угрожавање из окружења, онда говоримо искључиво о догађајима који су узроковани вишом силом, где је делатност људи у потпуности искључена осим у делу превентивног деловања и правовременог предвиђања могућег тока догађаја. Поједине категорије које изазивају оштећења информационих система као што су прашина и влага могуће је елиминисати из окружења применом хигијенских и грађевинских мера како би се информатичка опрема заштитила од таквих видова угрожавања. Ово је посебно изражено с обзиром да ИКС базирају свој рад на врло осетљивој технологији која захтева посебне услове за несметано функционисање.

5.1.2.5. Пропусти у организационим условима као облик угрожавања информационо–комуникационих система

Неповољни организациони услови такође могу негативно да утичу на заштиту информација као и на заштиту целог ИКС–а. Углавном се ради о пропустима узрокованим нестручношћу руководећег кадра организације или институције и запослених задужених за спровођење активности заштите, а нису у довољној мери оспособљени за такву активност. Зато се као први услов угрожавања овог типа наводи слаба организација информационог система који не задовољава неопходне услове како би информација или податак био заштићен. Овај услов треба да успостави менаџмент пословног субјекта преко стручних органа који се баве информационим технологијама тако да обезбеди заштиту информација у највећој могућој мери и да успостави систем контроле којом би се превентивно утврдили евентуални пропусти запослених и на тај начин спречило ненамерно или намерно отицање информација. Нестручност кадра који се бави информационим технологијама је могуће превазићи едукацијом запослених или запошљавањем лица која могу да обезбеде захтевани ниво функционисања

ИКС–а. Потребно је напоменути да се од кадра који се бави ИКТ–ом захтева посебан степен поверења и поседовање највишег степена одобрења приступу подацима који за пословни субјект представља пословну тајну. Нестручност може у каснијој фази да доведе до лошег одржавања и изостанка квалитетног сервисирања техничке опреме, што такође може негативно да се одрази на степен заштићености информација. Међутим, проблем заштите информација није само проблем менаџмента и кадра запосленог у информационим технологијама, већ и сваког запосленог који треба да буде упознат са безбедносним процедурама ИКТ–а. У циљу тога, у оквиру пословног субјекта, потребно је вршити перманентну едукацију запослених јер њиховим лошим поступањем, штете по организацију или институцију могу да буду несагледиве. На послетку, потребно је истаћи да проблем некомпатибилних рачунарских система онемогућава нормалну комуникацију између два система и размену информација, те на тај начин цео систем излаже ризику неблаговременог реаговања и спречавања нежељеног догађаја. (Јаворовић и Биланџић, 2007: 304)

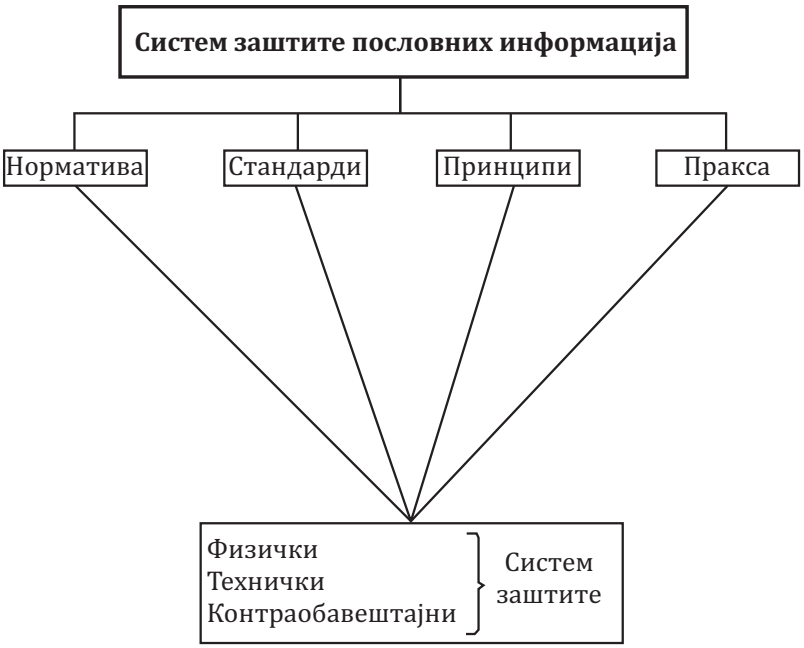
5.2. МЕРЕ И СИСТЕМИ ЗАШТИТЕ ПОСЛОВНИХ ИНФОРМАЦИЈА

Нагли развој ИКТ–а довео је до нових видова комуникације и размене података који се суштински разликују у односу на до тада разрађен традиционални систем размене. У циљу регулисања међусобних права и обавеза дошло је до усклађивања докумената, процедура, правила што је захтевало професионалан кадар, квалитетну организацију пословних процеса и примену савремених технологија. Заштита поверљивих информација у том смислу подразумева стандардизацију информационе безбедности, а савремени стандарди који се данас употребљавају односе се на генерисање, пријем и складиштење података, као и на ИКС–е. Активности у склопу информационе безбедности се реализују у циљу заштите информација, тако да обезбеде несметан и непрекидан рад ИКС–а, а да ризике и претње по ИКС–е сведе на минимум. Информација има смисла ако је

квалитетна и уколико није изложена било каквом облику деформације и губитка (без обзира да ли се ради о ненамерном или намерном угрожавању) и ако се налази код онога коме је намењена. Заштита и брига о информацијама је због тога приоритетан задатак сваког појединца, групе људи или заједнице уопште, те представља обавезу свих учесника у систему размене, а уједно подразумева минимум неопходних знања, професионализма и организованости.

Са злонамерним појединцима све чешће покушавају да се изборе национална права, међународне организације и асоцијације, као и приватни сектор и корисници. Циљ је да се ублаже негативне последице и смање губици који настају због вршења наведених криминалних активности. Последице су финансијски губици, губитак репутације, времена, угрожавање поверења корисника, потрошача, смањење продуктивности, осећај несигурности, угрожености и беспомоћности појединца, губитак породичних веза, нестабилност, конфликти, психолошки породични проблеми, комуникациони проблеми и сл. Посебан проблем је национална безбедност, здравље нације и други проблеми од суштинског значаја за функционисање националне заједнице. (Урошевић, 2014)

Узимајући у обзир претходно изнете чињенице, основано је закључити да је ефикасна заштита пословних информација нужна. У том смислу сваки субјект, посебно националне државе, улажу огромне напоре који се огледају у успостављању посебног система (шема бр.4).



Шема бр. 4: Систем заштите пословних информација

5.2.1. Стандарди у заштити пословних информација

Систем заштите информација укључује принципе, нормативе, праксу и стандарде. Принцип представља фундаменталну истину или законитост која се не доказује, а узима се као основа за извршавање рационалне активности. Неки од усвојених принципа који обезбеђују квалитетну заштиту информација су (према Грубор, 2010: 29):

- Принцип „никад сам“ спречава монополски положај и обавезује запошљавање најмање два лица за послове ауторизације права приступа, процесуирања осетљивих информација, тестирања и измена хардвера и софтвера, измене безбедносних процедура;
- „Ротација радних места“ обезбеђује да нико није незаменљив, а спроводи се у складу са бројем запослених који поседују одговарајуће стручне квалификације;
- „Раздвајање дужности“ обезбеђује да једно лице не може истовремено

обављати две или више од десет следећих парова функција ИКС–а: програмирање, обрада података, контрола квалитета ИКС–а, чување електронских медија, предаја поверљивих информација, издавање овлашћења, системско програмирање, администрација базе података, модификација система заштите, контрола овлашћења за приступ.

Нормативи треба да обезбеде шири оквир за имплементацију програма заштите и да пропишу санкције које сноси онај ко прекрши усвојене процедуре. Историјат правне заштите бележи четири основне фазе. Прва фаза имала је за циљ заштиту приватности, друга репресију економског криминалитета везаног за компјутере, трећа фаза осигурала је заштиту интелектуалне својине на пољу компјутерске технологије, док четврта фаза ставља акценат на хармонизацију досадашњих прописа ради што веће међународне компатибилности националних законодавстава. (Кукрика, 2002: 34)

Стандард заштите је усвојен и објављен документ који успоставља спецификацију и процедуре, дизајниране како би обезбедиле да документа, материјали, производи, методи или сервиси заштите, одговарају намени и конзистентно извршавају предвиђене функције. У пракси, стандард заштите садржи читав сет аранжмана за покривање што већег броја типичних безбедносних захтева за одржавање ризика на прихватљивом нивоу. Стандарди заштите обезбеђују препоруке за развој, имплементацију и одржавање система заштите и главни су алат за побољшање квалитета контрола заштите интегрисањем делова стандарда у пословне процесе, процену квалитета и избор контрола заштите, побољшање програма образовања, обуке и развоја свести о потреби заштите. Битни атрибути квалитета сваког стандарда су: документованост, расположивост, свеобухватност, да је издат од стране националног тела за стандардизацију, адекватан намени, рентабилан, добровољно прихваћен, усаглашен са законима и да обезбеђује индикаторе прогреса. (Грубор, 2010: 33)

Грубор наводи да општи модел стандарда заштите укључује следеће елементе:

- Терминологија — укључује листу дефиниција и појмова;

- Принципи — обезбеђују аксиоматска правила за израду упутства заштите;
- Методологија — обезбеђује поједностављен опис начина коришћења концепта, метода и техника као и њихових међусобних односа;
- Елементи стандарда — обезбеђују специфичне захтеве за дефинисану компоненту заштите;
- Упутство и додаци за примену — обезбеђују детаљан опис примене елемената стандарда у специфичним ситуацијама;
- Технике и алати — подржавају примену стандарда (Грубор и Милосављевић, 2010: 33).

Овом проблематиком се у Републици Србији бави Институт за стандардизацију Србије који, између осталог, доноси, развија, преиспитује, мења, допуњава и повлачи српске стандарде и сродне документе, обезбеђује усаглашеност српских стандарда и сродних докумената са европским и међународним стандардима и сродним документима у сарадњи са међународним организацијама које се баве стандардизацијом, прописује стандарде у одређеним областима. (http://www.iss.rs/la/button_4.html, 2016, 24. децембар)

Релевантна међународна тела која се баве стандардизацијом у области заштите информација су: ISO (енгл. International Organisation for Standardisation), BSI (енгл. British Standards Institute), BSI (нем. Bundesamt fuer Sicherheit in der Informationstechnik; German), IEC (енгл. International Elektrotehnical Commision), NIST (енгл. National Institutte for Standards and Technology; USA).

Стандарде заштите информација доноси Међународни технички комитет за стандардизацију ISO/IEC JTC1/SC27, формиран 1990. године и састоји се од следећих тела:

- Систем за управљање заштитом информација;
- Криптографски и други механизми заштите;
- Критеријуми за евалуацију заштите;
- Сервиси и контроле заштите;

- Технологије за заштиту приватности и управљање идентитетом.

Постоје бројни стандарди који се односе на различите области док је за поље информација, комуникација и безбедности информација усвојено шест стандарда. Ниједан од њих не покрива све области у којима је потребна заштита података, већ се међусобно допуњују и регулишу специфичност ИКС–а. У том смислу постоје следећи стандарди: ISO/IEC 15408 за интеграцију захтева за безбедност у софтверским процесима, спецификацију карактеристика производа и проверу испуњености захтева за информациону безбедност, ISO/IEC 113335 за управљање безбедношћу информационих технологија, ISO/IEC 17799 стандард за информациону безбедност који је еволуирао у стандарде ISO/IEC 27000 намењен за прављање система заштите информација и стандард NIST SP 800.

Грубор сматра да су основне предности стандардизације заштите ИКС:

- Смањење комплексности управљања системом заштите;
- Већа могућност избора и израда стандардне документације;
- Обезбеђење интероперабилности различитих система заштите;
- Формирање базе знања у области заштите;
- Незамењиви алат у процесима сертификације и акредитације система заштите;
- Обезбеђује осетљиве методе и дефинише најбољу праксу заштите. (Грубор и Милосављевић, 2010: 33)

Недостатак је у томе што не постоји општеприхваћен интегрални стандард за управљање заштитом који би дао одговор на питање како нешто урадити, а не само шта урадити. Један од најприхваћенијих стандарда, код нас и у свету, је стандард ISO/IEC 27k који се састоји од више појединачних стандарда. Ми ћемо се осврнути на три: ISO/IEC 27000, ISO/IEC 27001 и ISO/IEC 27002 који описују терминологију, начин увођења система за заштиту информација и сам систем заштите. Увођење система за управљање безбедносшћу реализује се применом PDCA циклуса који се састоји од четири фазе: планирај (plan), уради (do), провери (check), делуј (act).

Plan -План
Do- Уради
Check - Провери
Act - Побољшај

Слика бр. 5: PDCA циклус

(http://www.tehnologijahrane.com/enciklopedija/principi-upravljanja-kvalitetom-prema-iso-9001-standardu, 2016, 2. март)

Један од стандарда који има широку примену и у нашој земљи јесте SRPS ISO/IEC 27000:2014 коиј је усклађен са међународним стандардима. Њиме се заступају следећи елементи који гарантују безбедност ИКС–а:

- Поверљивост — обезбедити доступност информацијама искључиво особама које поседују ауторизацију за приступ. Подаци и информације се осталим лицима запосленим у неком систему омогућавају само до оног нивоа који обезбеђује извршавање редовних радних обавеза. За приступ осталим информацијама потребна је сагласност или одобрење надлежних лица која се баве заштитом информација у пословном субјекту.
- Интегритет — обезбедити да информација у целом процесу остане тачна и неизмењена, да задржи изворни облик и суштину онога што она представља или означава. Напади на ИКС се често односе на нарушавање интегритета информација, која услед измене власнику шаље погрешну поруку, те се он погрешно позиционира у односу на конкурента или противника.
- Доступност — обезбедити континуирани приступ информацијама од стране лица која поседују ауторизацију за приступ.

ISO 27000 је међународни стандард из велике *ISO* породице стандарда и требало би га схватити као светски и општеприхваћен стандард за систем управљања заштитом ИКТ, иако су се због огромног значаја заштите информатичких ресурса у међувремену појавили многи национални прописи

и стандарди са ограниченим дометом. Модел система управљања заштитом информатичких ресурса који подржава стандард *ISO* 27000 прилагођен је за организације свих типова и величина, као и деловању у различитим географским, културним и социјалним условима. Он омогућава ТНК да имплементирају јединствен систем за управљање заштитом информатичких ресурса на разним локацијама, елиминишући на тај начин потребу усаглашавања са националним законодавством и локалним стандардима. Овај модел се лако интегрише са системом за управљање квалитетом према захтевима стандарда *ISO* 9000:2000. Захтеви стандарда *ISO* 27000 представљају јасан редослед потеза које је потребно спровести да би се у организацији поставио систем заштите информација на одговарајући начин и детаљна упутства за интерпретацију поступка имплементације наведеног PDCA процеса. ISO 27000 стандард обезбеђује преглед и увид у фамилију ISO 27 к стандарда. Он прецизира терминологију, скраћенице и терминолошке неправилности. (Кукрика 2002)

ISO/IEC 27001 даје формалну спецификацију система управљања, односно захтеве за добијање лиценце за ISO/IEC 27k стандард. Да би се утврдило да ли организација испуњава предвиђене захтеве, она може бити проверавана у складу са стандардом који обезбеђује модел за успостављање, имплементацију, руковање, надзор, ревизију, одржавање и побољшање система за управљање информацијама. При увођењу стандарда ISO/IEC 27001 менаџмент треба да: 1. систематски процењује ризике по информациону безбедност; 2. осмисли свеобухватан пакет контрола информационе безбедности; 3. усвоји свеобухватан поступак управљања, како би осигурали континуитет у примени мера информационе безбедности. (http://www.iso.org/iso/home.html, 2016, 3. март)

ISO/IEC 27002 — стандард одређује опште принципе за планирање, имплементацију и побољшање система за управљање информацијама. Контролишу се и проверавају специфични захтеви за информациону безбедност, што се одређује проценом ризика. Стандард, такође, обезбеђује упутства за ефективно управљање безбедношћу информација у пракси и помоћ руководиоцима пословних субјеката у успостављању односа поверења

између организација. ISO/IEC 27002 се дели на 12 области: 1. процена ризика; 2. политика безбедности; 3. организовање система управљања безбедношћу информација; 4. управљање имовином — инвентар и класификација средстава везаних за информације; 5. људски ресурси (аспекти информационе безбедности који су одређени запошљавањем кадра, променом радног места или напуштањем организације); 6. физичко обезбеђење објеката у којима се налази ИТ — базирана технологија; 7. комуникације и оперативни менаџмент, то јест управљање контролама техничке безбедности рачунарских система и мрежа; 8. контрола и ограничење права приступа рачунарским мрежама, системима, апликацијама, функцијама и подацима; 9. обнављање, развој и одржавање информационих система уграђивањем безбедносних елемената и апликација; 10. управљање инцидентима везаним за информациону безбедност; 11. управљање пословним континуитетом и 12. усаглашеност политике информационе безбедности са стандардима и законима. (http://www.iso.org/iso/home.html, 2016, 8. март)

ISO/IEC 27004/5/6/7 — ова четири стандарда изведена су из претходна три, а нуде могућности за примену у реализацији захтева за информациону безбедност, обезбеђују метричке методе, тј. процену ефикасности имплементираног система за управљање информацијама (ISO/IEC 2700413), процену ризика (ISO/IEC 2700514), акредитацију организација које ће издавати лиценце (ISO/IEC 2700615) и ревизију система (ISO/IEC 2700716). (http://www.iso.org/iso/home.html, 2016, 8. март)

Размотрене чињенице, између осталог, указују на то да пословне информације у ИКС–у државе представљају својеврсан елемент њене критичне инфраструктуре који мора бити адекватно заштићен. Реч је о комплексном и изазовном задатку који реализују субјекти и снаге, условно разврстани у две групе: државне институције и привредни субјекти (шема бр.5).

Шема бр.5: Заштита пословних информација

5.2.2. Правни оквир у заштити тајности података

Рад са подацима у Републици Србији уређен је кроз следеће системске прописе: Закон о заштити података о личности као и Закон о тајности података. Поред ових, обрада података је уређена и Кривичним закоником као и прописима у области одбране, унутрашњих послова, Законима о службама безбедности и другим нормативним актима који регулишу ову област. С обзиром да Закон о тајности података није доживео потпуну примену у пракси и да је 2010. године донет по узору на тадашњи чешки закон о заштити тајности, потребно га је константно допуњавати и мењати поједине одредбе како би се усагласио са стварним потребама.

Реформа области заштите тајних података подразумева: 1) реформу националног система безбедности; 2) уставне и законске измене, кроз хармонизацију прописа са прописима и стандардима Европске уније у овој области; 3) едукацију и обуку кадрова који непосредно учествују у креирању и заштити тајних података; 4) евалуацију од стране међународних институција кроз успостављање процеса билатералне сарадње, али и оне у

вези са Европском унијом, НАТО и слично; 5) превођење практичних позитивних и негативних искустава у одговарајућу законску и подзаконску регулативу (Матић, 2009).

Иако су усвојене Уредбе које дефинишу проблематику информационе безбедности, неопходно је доношење законске регулативе која ће у складу са одлуком савета ЕУ 488 из 2013. године правно регулисати ову област. Одлука 488 се односи на безбедносна правила за заштиту тајности података. Њоме се регулишу размене података са трећим државама и међународним организацијама, оснивање институционалне инфраструктуре која ће применом посебних поступака и мера вршити послове информационе безбедности, формирање заједничке мреже националних органа за спровођење информационе безбедности и друге одреднице које је потребно испунити од стране земаља чланица ЕУ. Република Србија је 26.05.2011. године потписала са Европском Унијом Споразум о безбедносним процедурама за размену и заштиту тајних података. (Матић, 2009: 30)

Обавезе које проистичу из овог Споразума: (а) штити тајне податке које је доставила или разменила друга Страна према овом споразуму на начин који је бар једнак оном који за њих предвиђа Страна доставилац; (б) старају се да тајни подаци који се достављају или размењују према овом споразуму задрже ознаку тајности коју им је доделила Страна доставилац, да се не означе нижим степеном тајности или да им се не опозове тајност без претходне писмене сагласности Стране доставиоца. Страна прималац штити тајне податке, сходно одредбама њених прописа о тајности података или материјала који носе једнаку ознаку тајности; (в) не користе такве тајне податке за друге сврхе осим оних које је предвидела страна од које потичу подаци, односно због којих се такви подаци достављају или размењују; (г) не откривају те тајне податке трећим странама, или било којој институцији, односно органу ЕУ који нису у Споразуму наведени као надлежни органи, без претходне писмене сагласности Стране доставиоца; (д) не дозвољавају приступ тајним подацима физичким лицима, осим ако треба да буду упознати, ако су прошли одговарајућу безбедносну проверу и ако постоји одобрење односне Стране; (ђ) старају се о безбедносној заштити објеката у

којима се чувају тајни подаци које је доставила друга Страна, и (е) старају се да сва физичка лица која имају приступ тајним подацима буду упозната са обавезом заштите таквих података, у складу са важећим законима и прописима. (Службени гласник Републике Србије – Међународни уговори, 1/2012, Члан 5)

Године 2008. Влада Републике Србије и Организације Северноатлантског пакта у Бриселу су потписале Споразум о безбедности информација и кодекса о поступању, који је потврђен тек 2011. године. Њиме се установљавају најопштије обавезе страна потписница у вези са разменом и руковањем осетљивим, односно поверљивим подацима. Стране ће штитити и чувати информације и материјал који припадају другој страни; учинити све што је потребно да обезбеде да такве информације и материјал, уколико су поверљиви, задрже онај степен поверљивости који је одредила она страна од које те информације и материјал потичу, као и да ће чувати такве информације и материјал у складу са договореним заједничким стандардима; неће размењене информације и материјал користити у друге сврхе осим оних наведених у оквирима појединачних програма, као и одлука и резолуција који се на те програме односе; неће такве информације и материјал откривати трећој страни без сагласности стране од које потичу. Влада Републике Србије прихвата обавезу да сви њени држављани, који у току обављања службених дужности захтевају или могу имати приступ информацијама или материјалу размењеном у оквиру активности сарадње одобрених од стране Северноатлантског савета, буду подвргнути одговарајућој безбедносној провери пре него што им се одобри приступ таквим информацијама и материјалу. Пре размене било каквих поверљивих информација између Владе Републике Србије и НАТО, надлежна тела за безбедност ће међусобно утврдити да је страна прималац спремна да информације које добија заштити у складу са захтевима стране од које потичу. (Службени гласник Републике Србије – Међународни уговори, 1/2012, Чланови 1, 2. и 5)

Народна Скупштина Републике Србије је усвојила сет закона који се односе на заштиту тајности података и на законске последице које ће бити

предузимане према лицима која се не придржавају предвиђених законских постулата (табела бр. 3).

Табела бр. 3: Списак закона и кривичних дела који су везани за заштиту тајних података

Редни Број	Закони/Уредбе	Кривично дело/Казнене одредбе
1.	**Кривични закон**	<u>Кривична дела против безбедности рачунарских података:</u> *Члан 298. Оштећење рачунарских података и програма* *Члан 299. Рачунарске саботаже* *Члан 300. Прављење и уношење рачунарских вируса* *Члан 301. Рачунарска превара* *Члан 302. Спречавање и ограничавање приступа јавној рачунарској мрежи* *Члан 303. Неовлашћено коришћење рачунара или рачунарске мреже* *Члан 304. Прављење, набављање и давање другом средства за извршење кривичних дела против безбедности рачунарских података* *Члан 305. Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података* <u>Кривична дела против уставног уређења и безбедности Републике Србије:</u> *Члан 316. Одавање државне тајне* *Члан 320. Припремање дела против уставног уређења* <u>Кривична дела против слобода и права човека и грађанина:</u> *Члан 142. Повреда тајности писма и других пошиљки* *Члан 146. Неовлашћено прислушкивање и снимање* *Члан 146. Неовлашћено прикупљање личних података* *Члан 145. Неовлашћено објављивање и приказивање туђих списа, портрета и снимака.* <u>Кривична дела против човечности и других добара заштићених међународним правом:</u> *Члан 388. Трговина људима* *Члан 391. Тероризам* <u>Кривична дела против Војске Србије:</u> *Члан 415. Одавање војне тајне* <u>Кривична дела против интелектуалне својине: неовлашћено искоришћавање ауторског дела или предмета сродног права и повреда проналазачког права:</u> *Члан 201. Повреда проналазачког права* *Члан 199. Неовлашћено искоришћавање ауторског дела или предмета* <u>Кривична дела против привреде</u> *Члан 240. Одавање пословне тајне* *Члан 225. Фалсификовање и злоупотреба платних картица* *Члан 231. Прање новца*

		Кривична дела против животне средине *Члан 268. Повреда права на информисање о стању животне средине*
2.	**Закон о тајности података**	*Члан 98. Кривично дело* *Члан 99. Прекршајна одговорност одговорног лица у органу јавне власти*
3.	**Закон о заштити података о личности**	*Члан 57. (новчана казна)*
4.	**Закон о заштити пословне тајне**	*Члан 19. Привредни преступ*
5.	**Закон о информационој безбедности**	*Члан 30. и Члан 31. (новчана казна)*
6.	**Закон о агенцији за борбу против корупције**	*Члан 73. Правне последице осуде, Члан 74., Члан 75., Члан 76. (новчана казна)*
7.	Уредба о посебним мерама заштите тајних података у информационо-телекомуникационим системима	/
8.	Уредба о посебним мерама физичко-техничке заштите тајних података	/
9.	Уредба о посебним мерама надзора над поступањем са тајним подацима	/

Законом о тајности података (Службени гласник Републике Србије, 104/2009) уређује се јединствен систем одређивања и заштите тајних података који су од интереса за националну и јавну безбедност, одбрану, унутрашње и спољне послове Републике Србије, заштите страних тајних података, приступ тајним подацима и престанак њихове тајности, надлежност органа и надзор над спровођењем закона, као и одговорност за неизвршавање обавеза из закона и друга питања од значаја за заштиту тајности података.

Законом се регулише који подаци се могу одредити као тајни. То су подаци од интереса за Републику Србију чијим би откривањем неовлашћеном лицу настала штета, ако је потреба заштите интереса Републике Србије претежнија од интереса за слободан приступ информацијама од јавног значаја. Подаци се односе на: националну безбедност Републике Србије, јавну безбедност, односно на одбрамбене,

спољнополитичке, безбедносне и обавештајне послове органа јавне власти; односе Републике Србије са другим државама, међународним организацијама и другим међународним субјектима; системе, уређаје, пројекте, планове и структуре; научне, истраживачке, технолошке, економске и финансијске послове.

Законом се такође прописују *врсте мера заштите*. Одређено је да орган јавне власти примењује опште и посебне мере заштите у складу са законом и прописом донетим на основу закона, ради заштите тајних података који се налазе у његовом поседу. Опште мере заштите тајних података обухватају: одређивање степена тајности; процену претње за безбедност тајног податка; одређивање начина коришћења и поступања са тајним податком; одређивање одговорног лица за чување, коришћење, размену и друге радње обраде тајног податка; одређивање руковаоца тајним подацима, укључујући и његову безбедносну проверу у зависности од степена тајности податка; одређивање посебних зона, зграда и просторија намењених заштити тајних података и страних тајних података; надзор над поступањем са тајним податком; мере физичко–техничке заштите тајног податка, укључујући и уградњу и постављање техничких средстава заштите, утврђивање безбедносне зоне и заштиту ван безбедносне зоне; мере заштите информационо–телекомуникационих система; мере крипто–заштите; заштитни режим радних и формацијских места, у оквиру акта о унутрашњем уређењу и систематизацији радних места; утврђивање посебних програма образовања и обуке за потребе обављања послова заштите тајних података и страних тајних података.

За приступ и коришћење тајних података врши се *безбедносна провера* у зависности од степена тајности, и то: основна безбедносна провера, за податке означене степеном тајности "ИНТЕРНО" и "ПОВЕРЉИВО"; потпуна безбедносна провера, за податке означене степеном тајности "СТРОГО ПОВЕРЉИВО"; посебна безбедносна провера, за податке означене степеном тајности "ДРЖАВНА ТАЈНА". Безбедносном провером се врши процена безбедносног ризика, нарочито од приступа и коришћења тајних података. У оквиру безбедносне провере надлежни орган са аспекта безбедности оцењује

наводе у попуњеном безбедносном упитнику. Надлежни орган, у вези са наводима из безбедносног упитника, прикупља личне и друге податке од лица на које се ти подаци односе, од других органа јавне власти, организација и лица, из регистара, евиденција, датотека и збирки података које се воде на основу закона.

Законом о заштити података о личности (Службени гласник Републике Србије, 97/2008, 104/2009, др. Закон, 68/2012. одлука УС и 107/2012) уређују се услови за прикупљање и обраду података о личности, права лица и заштита права лица чији се подаци прикупљају и обрађују, ограничења заштите података о личности, поступак пред надлежним органом за заштиту података о личности, обезбеђење података, евиденција, изношење података из Републике Србије и надзор над извршавањем овог закона. Заштита података о личности обезбеђује се сваком физичком лицу, без обзира на држављанство и пребивалиште, расу, године живота, пол, језик, вероисповест, политичко и друго уверење, националну припадност, социјално порекло и статус, имовинско стање, рођење, образовање, друштвени положај или друга лична својства. Послове заштите података о личности обавља Повереник за информације од јавног значаја и заштиту података о личности.

Закон дефинише када обрада података о личности није дозвољена. Између осталих, наводе се следећи случајеви: када физичко лице није дало пристанак за обраду, ако се обрада врши без законског овлашћења; када се врши у сврху различиту од оне за коју је одређена, без обзира да ли се врши на основу пристанка лица или законског овлашћења за обраду без пристанка; кад сврха обраде није јасно одређена; када су број или врста података који се обрађују несразмерни сврси обраде; када је податак неистинит и непотпун, односно када није заснован на веродостојном извору или је застарео.

Изузеци се односе на обраду личних података без пристанка лица у случајевима када је обрада неопходна ради обављања послова из своје надлежности одређених законом или другим прописом у циљу остваривања интереса националне или јавне безбедности, одбране земље, спречавања,

откривања, истраге и гоњења за кривична дела, економских, односно финансијских интереса државе, заштите здравља и морала, заштите права и слобода и другог јавног интереса. У осталим случајевима потребан је писмени пристанак лица.

Законом о заштити пословне тајне (Службени гласник Републике Србије, 72/2011) уређује се правна заштита пословне тајне од свих радњи нелојалне конкуренције. Информацијама које се штите као пословна тајна у смислу закона сматрају се нарочито: финансијски, економски, пословни, научни, технички, технолошки производни подаци, студије, тестови, резултати истраживања, укључујући и формулу, цртеж, план, пројекат, прототип, код, модел, компилацију, програм, метод, технику, поступак, обавештење или упутство интерног карактера и слично, без обзира на који начин су сачувани или компилирани.

Изузетак се односи на информације које не представљају пословну тајну, а означене су као пословна тајна ради прикривања кривичног дела, прекорачења овлашћења, злоупотребе службеног положаја или другог незаконитог акта или поступања домаћег и страног физичког и правног лица.

У Закону о заштити пословне тајне је дефинисан појам *пословне тајне*. Пословном тајном сматра се било која информација која има комерцијалну вредност зато што није опште позната нити је доступна трећем лицу које би њеним коришћењем или саопштавањем могло да оствари економску корист, и која је од стране њеног држаоца заштићена одговарајућим мерама у складу са законом, пословном политиком, уговорним обавезама или одговарајућим стандардима у циљу очувања њене тајности, а чије би саопштавање трећем лицу могло нанети штету држаоцу пословне тајне. Прецизно је дефинисано који се подаци сматрају пословном тајном: неоткривени подаци о тестовима или други подаци чије стварање захтева одговарајући напор и трошкове, који се подносе државним органима ради добијања дозволе за стављање у промет лекова, односно медицинских средстава или пољопривредних хемијских производа који користе нова хемијска једињења, као и ради добијања аката којима се дозвољава стављање у промет биоцидних производа; други подаци

који су посебним законом, другим прописом или актом правног лица проглашени пословном тајном. Пословна тајна која садржи податак од интереса за Републику Србију сматра се тајним податком и штити се по одредбама закона којим се уређује тајност података.

Такође, законом се прецизира да се радња предузета у оквиру индустријских или комерцијалних активности, а која за последицу има откривање, прибављање, односно коришћење информације које представљају пословну тајну, без сагласности држаоца пословне тајне и на начин супротан закону и добрим пословним обичајима, сматра делом нелојалне конкуренције. Под начином супротним добрим пословним обичајима, у смислу овог закона, подразумева се свака радња предузета у циљу утакмице на тржишту којом се наноси или се може нанети штета конкуренту или другом физичком, односно правном лицу, а нарочито: повреда уговорних одредаба о чувању пословне тајне; злоупотреба пословног поверења; индустријска или комерцијална шпијунажа; превара; навођење; прибављање информације која представља пословну тајну од стране трећих лица која знају или су била дужна да знају да та информација представља пословну тајну и да је прибављена од лица у чијем је законитом поседу.

Прибављање информација од стране трећег лица које поседује заштићене информације представља један од најзаступљенијих начина доласка до поверљивих података како у привредним активностима (know how), тако и оним које се односе на државну управу.

Законом о информационој безбедности (Службени гласник Републике Србије, 6/16) уређују се мере заштите од безбедносних ризика у ИКС–у, одговорности правних лица приликом управљања и коришћења ИКС–а и одређују се надлежни органи за спровођење мера заштите, координацију између чинилаца заштите и праћење правилне примене прописаних мера заштите. У циљу остваривања сарадње и усклађеног обављања послова у функцији унапређења информационе безбедности, као и иницирања и праћења превентивних и других активности у области информационе безбедности, основано је Тело за координацију послова

информационе безбедности, као координационо тело Владе, у чији састав улазе представници министарстава надлежних за послове информационе безбедности, одбране, унутрашњих послова, спољних послова, правде, представници служби безбедности, Канцеларије Савета за националну безбедност и заштиту тајних података, Генералног секретаријата Владе, Управе за заједничке послове републичких органа и Националног ЦЕРТ-а (Национални центар за превенцију безбедносних ризика у ИКТ системима).

Законом су одређени ИКТ системи од посебног значаја, тачније они који се користе: у обављању послова у органима јавне власти; за обраду података који се, у складу са законом који уређује заштиту података о личности, сматрају нарочито осетљивим подацима о личности; у обављању делатности од општег интереса и то у областима: производње, преноса и дистрибуције електричне енергије, производње и прераде угља, истраживања, производње, прераде, транспорта и дистрибуције нафте и природног и течног гаса, промета нафте и нафтних деривата; железничког, поштанског и ваздушног саобраћаја, електронске комуникације, издавања службеног гласила Републике Србије, управљања нуклеарним објектима, коришћења, управљања, заштите и унапређивања добара од општег интереса (воде, путеви, минералне сировине, шуме, пловне реке, језера, обале, бање, дивљач, заштићена подручја), производње, промета и превоза наоружања и војне опреме, управљања отпадом, комуналних делатности, послова финансијских институција, здравствене заштите, услуга информационог друштва намењене другим пружаоцима услуга информационог друштва у циљу омогућавања пружања њихових услуга.

Оператор ИКТ система од посебног значаја одговара за безбедност ИКТ система и предузимање мера за његову заштиту. Мерама заштите ИКТ система обезбеђује се превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима. Неке од мера заштите ИКТ система су: постизање безбедности рада на даљину и употребе мобилних уређаја; обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду

оспособљена за посао који раде и разумеју своју одговорност; заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система; класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком; ограничење приступа подацима и средствима за обраду података; одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа; предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности односно интегритета података; физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему; заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем; заштита података и средства за обраду података од злонамерног софтвера; заштита од губитка података; заштита података у комуникационим мрежама укључујући уређаје и водове; превенција и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама.

Оператор ИКТ система од посебног значаја самостално или уз ангажовање спољних експерата врши проверу усклађености примењених мера ИКТ система са актом и о томе сачињава извештај. Оператор ИКТ система од посебног значаја може поверити активности у вези са ИКТ системом трећем лицу, када је обавезан да уреди однос са тим лицем на начин који обезбеђује предузимање мера заштите тог ИКТ система у складу са законом. Оператори ИКТ система од посебног значаја обавезни су да обавесте Надлежни орган о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности. Ако је инцидент везан за извршење кривичних дела која се гоне по службеној дужности, Надлежни орган, односно орган коме се упућују обавештења о инцидентима, обавештава надлежно јавно тужилаштво, односно министарство надлежно за унутрашње послове. Ако је инцидент повезан са нарушавањем права на заштиту података о личности, Надлежни орган,

односно орган коме се упућују обавештења о инцидентима и самостални оператор ИКТ система, о томе обавештавају и Повереника за информације од јавног значаја и заштиту података о личности.

Улога Националног центра за превенцију безбедносних ризика у ИКТ системима (Национални ЦЕРТ) је да обавља послове координације превенције и заштите од безбедносних ризика у ИКТ системима у Републици Србији на националном нивоу. Посебан центар за превенцију безбедносних ризика у ИКТ системима (Посебан ЦЕРТ) обавља послове превенције и заштите од безбедносних ризика у ИКТ системима у оквиру одређеног правног лица, групе правних лица, области пословања и слично. Центар за безбедност ИКТ система у републичким органима (ЦЕРТ републичких органа) обавља послове који се односе на заштиту од инцидената у ИКТ системима републичких органа, изузев ИКТ система самосталних оператора.

Законом се уређује да је министарство надлежно за послове одбране одговорно за послове информационе безбедности који се односе на одобравање криптографских производа, дистрибуцију криптоматеријала и заштиту од компромитујућег електромагнетног зрачења.

У циљу превазилажења уочених проблема везаних за слабости законске регулативе која се односи на заштиту тајних података, Влада Републике Србије усвојила је у јулу 2011. године ***Уредбу о посебним мерама заштите тајних података у информационо–телекомуникационим системима*** (Службени гласник Републике Србије, 53/2011) која дефинише обавезе Органа јавне власти, односно правног лица које по основу уговорног односа пружа услуге органу јавне власти. Уредбом је прописан низ техничких и организационих мера заштите, чијим предузимањем би тајни подаци, који настају, чувају се и преносе у информационо–телекомуникационим системима, били сачувани од компромитовања и не би били доступни неовлашћеним лицима. Употреба информационо–телекомуникационог система условљена је израдом анализе ризика. У изради анализе ризика укључени су плански, организациони и временски фактори. Уредба о посебним мерама заштите тајних података инсистира на употреби техничких стандарда ИСО 17999 и ИСО 27001.

Ова уредба дефинише посебне мере заштите тајних података у информационо–телекомуникационим системима које могу бити техничке и организационе, а предузимају се у циљу спречавања случајних грешака, неправилног и недозвољеног прикупљања, чувања, обраде, коришћења, оштећења, уништења, као и фалсификовања и злоупотребе тајних података. Посебне мере заштите тајних података у систему односе се на: објекат у коме је смештен систем (опрема, документи, програмска подршка и мрежа); простор, просторије, односно безбедносне зоне у којима се обрађују тајни подаци у систему; овлашћена лица за управљање безбедношћу система; све учеснике у раду система; коришћење система за потребе рада са тајним подацима; режим рада система; заштиту тајних података приликом обраде и чувања у систему; заштиту од ризика компромитујућег електромагнетног зрачења, као и инсталирање уређаја за чување тајних података.

Техничке мере из ове уредбе се нарочито односе на: физичку заштиту објеката, простора, просторије, односно безбедносне зоне у којима се обрађују тајни подаци у систему, као и средстава и докумената из система; противпожарну заштиту; обезбеђивање и заштиту опреме (избор одговарајуће и поуздане опреме, обезбеђивање опреме током њеног рада, редовно сервисирање и снабдевање резервним деловима) и докумената при њиховом коришћењу и чувању; заштиту програмске подршке (у фази пројектовања, развоја и коришћења програмског система); заштиту мреже (приликом пројектовања и рада).

Организационе мере ове уредбе нарочито се односе на: организацију технологије рада у систему при пројектовању (израда прелиминарне студије о развоју којом се утврђује степен тајности података који се обрађују у систему и степен тајности самог система, идејног пројекта, главног пројекта, извођачког пројекта и увођења пројектованих решења) и при оперативном раду система (планирање рада и вођење евиденција о извршавању свих поступака у раду система и кретању документације); утврђивање поступака у случају ванредних околности; остале услове за успешно функционисање система (контрола приликом заснивања радног односа, утврђивање послова и задатака учесника у раду система, стручна обука запослених и друго).

Услови које систем мора да испуњава се односе на: заштиту од неауторизованог приступа, која подразумева идентификовање и поуздано гарантовање идентитета (аутентикација) лица која имају приступ систему; контролу и вођење евиденције о приступу систему; континуирано бележење (аутоматизовано, ручно или комбиновано) о безбедносном стању система (безбедносни запис), активностима система, као и изменама постојећег стања система; проучавање безбедносних записа од стране овлашћених лица; одређивање овлашћења корисницима у вези са безбедношћу система; одређивање овлашћења корисницима у вези са коришћењем система; обезбеђивање безбедног начина означавања степена тајности; идентификацију корисника који врши измене, штампање, преснимавање или брисање тајног документа; бележење измене, штампање, преснимавање или брисање тајног податка од стране корисника; заштиту важних техничких и програмских елемената, системских могућности и функционалности система; обезбеђење резервних архива тајних података, за случај губитка постојећих архива, као и вођење евиденција о приступу архивама.

Уредба о посебним мерама физичко–техничке заштите тајних података донета је на основу Закона о тајности података (Службени гласник Републике Србије, 104/09) и члана 42. став 1. Закона о Влади (Службени гласник Републике Србије, 55/05, 71/05 — исправка, 101/05, 65/08, 16/11).

Уредбом се уређује да се тајни податак чува, користи и обрађује у просторији, односно простору који је одређен као административна или безбедносна зона и има одговарајућу безбедносно–техничку опрему, односно одговарајућа средства техничке заштите. Поред посебних мера предвиђених овом уредбом, на чување, коришћење и обраду страног тајног податка се примењују и посебне мере предвиђене међународним споразумом.

Истом је такође дефинисано да се просторије у којима се чувају, користе, обрађују и уништавају тајни подаци обезбеђују противпровалним и противпожарним системом. Просторија је, по правилу, опремљена: једним од безбедносних механизама на улазним вратима, са могућношћу евиденције података о уласку у простор (приступним читачем кодова, картица, тастатуре и слично или биометријским системом), како би се приступ таквим

просторијама могао ограничити, надзирати и евидентирати; опремом за безбедно чување предмета и докумената; енергетским прикључком на непрекидно и алтернативно (агрегатско) напајање; сигурносним механичким системом за закључавање са ограниченим бројем кључева, без могућности умножавања или томе одговарајућим одвојеним аутоматизованим и мануелним решењима.

Простор око просторија у којима се чувају, користе, обрађују или уништавају тајни подаци, као и пут до њих, по правилу, се обезбеђују видео–надзором.

Уредба посебним мерама надзора над поступањем са тајним подацима (Службени гласник Републике Србије, 90/2011) је донета на основу Закона о тајности података (Службени гласник Републике Србије, 104/09) и Закона о Влади (Службени гласник Републике Србије, 55/05, 71/05 — исправка, 101/07, 65/08, 16/11).

Посебне мере надзора обухватају непосредан увид, одговарајуће провере и разматрање поднетих извештаја у вези са спровођењем свих мера заштите тајних података или једне, односно одређених мера заштите тајних података које се спроводе у оквиру унутрашње контроле органа јавне власти. Руководилац органа јавне власти, у складу са законом, врши унутрашњу контролу у органу јавне власти непосредно или преко овлашћеног лица, односно преко унутрашње организационе јединице у органу јавне власти.

Унутрашња контрола проверава спровођење мера заштите тајних података, а нарочито у односу на: одређивање степена тајности податка; означавање докумената и омота докумената; посебну просторију за пријем тајних података; евидентирање, чување и депоновање тајних података; означавање ормара и каса у којима се чувају и депонују тајни подаци; начин коришћења и приступа тајном податку, вођење евиденције корисника и евиденције о приступу тајном податку, као и чување тих евиденција; начин вршења умножавања, превођења и израде извода из тајних података; паковање и достављање тајних података унутар и ван безбедносне зоне; поступак уништавања тајних података; евиденцију улаза и излаза лица и возила, коришћење безбедносних пропусница и посебних безбедносних

пропусница, функционисање физичког и електронског система за обезбеђење објекта и простора; поседовање, евиденцију и чување сертификата за приступ тајним подацима; пријем, обраду, пренос, чување, архивирање и уништавање тајних података у електронској форми; чување крипто кључева; чување уговора који садрже тајне податке; начин заштите тајних података страних правних и физичких лица.

У међувремену, од ступања на снагу Закона о тајности података, донети су и следећи подзаконски акти: Уредба о обрасцима безбедносних упитника (Службени гласник, 30/10), Уредба о садржини, облику и начину достављања сертификата за приступ тајним подацима (Службени гласник, 54/10), Уредба о одређивању послова безбедносне заштите одређених лица и објеката (Службени гласник, 72/10), Уредба о увећању плате државних службеника и намештеника који обављају послове у вези са заштитом тајних података у Канцеларији Савета за националну безбедност и заштиту тајних података и Министарству правде (Службени гласник, 79/10), Уредба о садржини, облику и начину вођења евиденција за приступ тајним подацима (Службени гласник, 89/10), Уредба о начину и поступку означавања тајности података, односно докумената (Службени гласник, 8/11), Уредба о ближим критеријумима за одређивање степена тајности „Државна тајна" и „Строго поверљиво" (Службени гласник, 46/13), три Уредбе о ближим критеријумима за одређивање степена тајности „Поверљиво" и „Интерно" у Безбедносно–информативној агенцији (Службени гласник, 70/13), Канцеларији Савета за националну безбедност и заштиту тајних података (Службени гласник, 86/13) и Министарству унутрашњих послова (Службени гласник, 105/13), Уредба о посебним мерама заштите тајних података које се односе на утврђивање испуњености организационих и техничких услова по основу уговорног односа (Службени гласник, 63/13) и Правилник о службеној легитимацији и начину рада лица овлашћених за вршење надзора над спровођењем закона (Службени гласник, 85/13).

Законом о агенцији за борбу против корупције (Службени гласник Републике Србије, 97/2008, 53/2010) уређују се оснивање, правни положај, надлежност, организација и начин рада Агенције за борбу против корупције,

правила у вези са спречавањем сукоба интереса при вршењу јавних функција и пријављивањем имовине лица која врше јавне функције, поступак и одлучивање у случају повреде овог закона, увођење планова интегритета, као и друга питања од значаја за рад Агенције. *Корупција* је овим законом одређена као однос који се заснива злоупотребом службеног, односно друштвеног положаја или утицаја, у јавном или приватном сектору, у циљу стицања личне користи или користи за другога; *функционер* је свако изабрано, постављено или именовано лице у органе Републике Србије, аутономне покрајине, јединице локалне самоуправе и органе јавних предузећа и привредних друштава, установа и других организација чији је оснивач, односно члан Република Србија, аутономна покрајина, јединица локалне самоуправе и друго лице које бира Народна скупштина; *јавна функција* је функција у органима Републике Србије, аутономне покрајине, јединице локалне самоуправе, органима јавних предузећа и привредних друштава, установа и других организација, чији је оснивач, односно члан Република Србија, аутономна покрајина, јединица локалне самоуправе, као и функција других лица које бира Народна скупштина, а подразумева овлашћења руковођења, одлучивања, односно доношења општих или појединачних аката; *повезано лице* је супружник или ванбрачни партнер функционера, крвни сродник функционера у правој линији, односно у побочној линији закључно са другим степеном сродства, усвојитељ или усвојеник функционера, као и свако друго правно или физичко лице које се према другим основама и околностима може оправдано сматрати интересно повезаним са функционером; *приватни интерес* је било каква корист или погодност за функционера или повезано лице; *сукоб интереса* је ситуација у којој функционер има приватни интерес који утиче, може да утиче или изгледа као да утиче на поступање функционера у вршењу јавне функције односно службене дужности, на начин који угрожава јавни интерес; *поклон* је новац, ствар, право и услуга извршена без одговарајуће накнаде и свака друга корист која је дата функционеру или повезаном лицу у вези с вршењем јавне функције; *протоколарни поклон* је поклон који функционер прими од стране државе, њеног органа или организације, међународне организације или

страног правног лица, приликом службене посете или у другим сличним приликама.

Агенција надзире спровођење Националне стратегије за борбу против корупције, Акционог плана за примену Националне стратегије за борбу против корупције и секторских акционих планова; покреће поступак и изриче мере због повреде овог закона; решава о сукобу интереса; обавља послове у складу са законом којим је уређено финансирање политичких странака, односно политичких субјеката; даје мишљења и упутства за спровођење овог закона; даје иницијативе за измену и доношење прописа у области борбе против корупције; даје мишљења у вези са применом Стратегије, Акционог плана и секторских акционих планова; прати и обавља послове који се односе на организовање координације рада државних органа у борби против корупције; води регистар функционера; води регистар имовине и прихода функционера; пружа стручну помоћ у области борбе против корупције; сарађује са другим државним органима у припреми прописа у области борбе против корупције; даје смернице за израду планова интегритета у јавном и приватном сектору; сарађује са научним организацијама и организацијама цивилног друштва у спровођењу активности превенције корупције; уводи и спроводи програме обуке о корупцији, у складу са овим законом; води посебне евиденције у складу са овим законом; поступа по представкама правних и физичких лица; поступа по пријавама државних службеника, односно запослених у органима Републике Србије, аутономне покрајине, јединице локалне самоуправе и органима јавних предузећа, установа и других организација чији је оснивач Република Србија, аутономна покрајина или јединица локалне самоуправе, односно органима привредних друштава чији је оснивач, односно члан Република Србија, аутономна покрајина или јединица локалне самоуправе и запослених у државним органима и организацијама; организује истраживања, прати и анализира статистичке и друге податке о стању корупције; у сарадњи са надлежним државним органима прати међународну сарадњу у области борбе против корупције; обавља и друге послове одређене законом.

Кривичним законником (Службени гласник Републике Србије, 8572005, 88/2005 – ИСПР. 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014) су посебно обухваћена *кривична дела против безбедности рачунарских података*. Кривична дела против безбедности рачунарских података су скуп кривичних дела где се као објекат и као средство за извршење кривичног дела јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови продукти у материјалном и електронском облику. Кривични законик препознаје следећа дела ове врсте:

Чланом 298. *Оштећење рачунарских података и програма* дефинисане су кривичне радње као што су неовлашћено брисање, измена, оштећење, прикривање рачунарских података или програма и сл. Предвиђена је новчана казна или казна затвора до једне године за учиниоца.

Члан 299. *Рачунарске саботаже* је кривично дело које се односи на исте радње као у претходном кривичном делу с тим што се ради о ометању поступака електронске обраде и преноса података који су од значаја за државне органе, јавне службе, установе, предузећа или друге субјекте. Предвиђена је казна затвора у трајању од шест месеци до пет година.

Члан 300. се односи на *Прављење и уношење рачунарских вируса.* Делом је одређена забрана намерног уношења рачунарског вируса у туђ рачунар или рачунарску мрежу. Предвиђена је новчана казна или казна затвором до шест месеци за починиоца.

Члан 301. *Рачунарска превара* односи се на радње уношења нетачних података или пропусте приликом уношења тачнних података и прикривања или лажног приказивања података чиме се утиче на резултат електронске обраде и преноса података. Да би дело било учињено неопходна је намера учниоца да себи или другом прибави противправну имовинску корист и тиме некоме проузрокује имовинску штету. Предвиђена је новчана казна или казна затвором до три године за учиниоца.

Члан 302. *Спречавање и ограничавање приступа јавној рачунарској мрежи* односи се на неовлашћено спречавање или ометање приступа јавној рачунарској мрежи. Учинилац ће се казнити новчаном казном или затвором

до једне године. Ако дело учини службено лице у вршењу службе, казниће се затвором до три године.

Члан 303. *Неовлашћено коришћење рачунара или рачунарске мреже* инкриминише неовлашћено коришћење рачунарских услуга или рачунарских мрежа у намери прибављања противправне имовинске користи. Починилац ће се казнити новчаном казном или затвором до три месеца.

Члан 304. *Прављење, набављање и давање другом средства за извршење кривичних дела против безбедности рачунарских података* забрањује поседовање, прављење, набављање, продају или уступање другом на употребу рачунара, рачунарских система, рачунарских података и програма ради извршења кривичног дела. Предвиђена је казна затвором у трајању од шест месеци до три године.

Члан 305. *Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података* забрањује кршење мера заштите у смислу неовлашћеног укључивања у рачунар или рачунарску мрежу или неовлашћеног приступа електронској обради података. Предвиђена је новчана казна или казна затвором до шест месеци.

Кривични законик такође дефинише *кривична дела против уставног уређења и безбедности Републике Србије,* а посебно интересантно са аспекта заштите информације је дело шпијунаже. Прецизно је одређено кривично дело *Шпијунаже*: „Ко тајне војне, економске или службене податке или документе саопшти, преда или учини доступним страној држави, страној организацији или лицу које им служи, казниће се затвором од три до петнаест година. Ко за страну државу или организацију ствара обавештајну службу у Србији или њом руководи, казниће се затвором од пет до петнаест година. Ко ступи у страну обавештајну службу, прикупља за њу податке или на други начин помаже њен рад, казниће се затвором од једне до десет година. Ко прибавља тајне податке или документе у намери да их саопшти или преда страној држави, страној организацији или лицу које им служи, казниће се затвором од једне до осам година.

Члан 316. се односи на *Одавање државне тајне*, односно на неовлашћено саопштавање, предају или чињење доступним података или

докумената непозваном лицу, који су неком поверени или до којих је на други начин дошао, а који представљају државну тајну. Предвиђена је мера казне затвором у трајању од једне до десет година. Посебно су наведени чланови који дефинишу наведено дело у ратном стању и који указују на то да је дело учињено из нехата. У складу са тим, санкције су у првом случају оштрије, а у другом блаже у односу на основни облик кривичног дела. Изузеће представљају подаци или документи који су управљени на тешке повреде основних права човека, или на угрожавање уставног уређења и безбедности Србије, као и подаци или документи који за циљ имају прикривање учињеног кривичног дела за које се по закону може изрећи затвор од пет година или тежа казна. У члану 5. дефинисан је појам државне тајне којом се сматрају подаци или документи, који су законом, другим прописом или одлуком надлежног органа донесених на основу закона, проглашени државном тајном и чије би одавање проузроковало или би могло да проузрокује штетне последице за безбедност, одбрану или за политичке, војне или економске интересе Србије.

Члан 320. се односи на кривично дело *Припремање дела против уставног уређења*. Припремање подразумева набављање или оспособљавање средстава за извршење кривичног дела, отклањање препрека за извршење кривичног дела, договарање, планирање или организовање са другим ради извршења кривичног дела или друге радње којима се стварају услови за непосредно извршење кривичног дела. Став 3. инкримише радњу пребацивања на територију Србије лица или оружја, експлозива, отрова, опреме, муниције или других материјала ради извршења једног или више кривичних дела. Предвиђена је казна затвора од две до десет година.

Кривичним законом су одређена кривична *дела против слобода и права човека и грађанина.*

Члан 142. се односи на *Повреду тајности писма и других пошиљки,* којим се одређује забрана отварања, повреде тајности и неовлашћеног задржавања туђег писма, телеграма или пошиљке. Посебно је наглешена повреда тајности електронске поште или другог средства за

телекомуникацију. Предвиђена је новчана казна или затвор до две године. Уколико је извршилац службено лице у вршењу службе, казна се пооштрава.

Члан 146. *Неовлашћено прислушкивање и снимање* се односи на забрану да се подаци о личности, који се прикупљају, обрађују и користе, неовлашћено прибаве, саопште другом или употребе у сврху за коју нису намењени. Предвиђена је новчана казна или казна затвором до једне године. Ако дело учини службено лице у вршењу службе казниће се затвором до три године.

Члан 146. се односи на *Неовлашћено прикупљање личних података*. Овим чланом је забрањено личне податке, који се прикупљају, обрађују и користе на основу закона, неовлашћено прибављати, саопштити другом или употребити у сврху за коју нису намењени. Предвиђена је новчана казна или казна затвором до једне године за учиниоца.

Чланом 145. је инкриминисано *Неовлашћено објављивање и приказивање туђих списа, портрета и снимака*. Збрањено је објављивање, приказивање списа, портрета, фотографије, филма или фонограма личног карактера без пристанка лица које је спис саставило или на кога се спис односи, односно без пристанка лица које је приказано на портрету, фотографији или филму и чији је глас снимљен на фонограму. У ставу 3. захтева се пристанак другог лица чиме се осетно задре у лични живот тог лица.

Посебно поглавље се односи на *кривична дела против човечности и других добара заштићених међународним правом.*

Члан 388. се односи на *Трговину људима*. У члану су дефинисане радње које подразумевају извршење дела: врбовање, превожење, пребацивање, предаја, продаја, куповина, посредовање у продаји, сакривање или држање другог лица, а у циљу експлоатације његовог рада, принудног рада, вршења кривичних дела, проституције или друге врсте сексуалне експлоатације, просјачења, употребе у порнографске сврхе, успостављања ропског или њему сличног односа, ради одузимања органа или дела тела или ради коришћења у оружаним сукобима. За учиниоца је предвиђена казна затвора од три до дванаест година. Подразумева се да је починилац применио силу, претњу или

неки други начин извршења описан у члану, осим у случајевима када је дело учињено према малолетном лицу. У том случају казна затвора не може бити мања од пет година. Уколико је дело учињено од стране организоване криминалне групе казна не може бити мања од десет година затвора. Пристанак „жртве“ не утиче на постојање кривилног дела, што је одређено у тачки 10.

У члану 391. одређено је кривично дело *Тероризам*. Дело се односи на намеру да се озбиљно застраши становништво, или да се принуди Србија, страна држава или међународна организација да нешто учини или не учини, или да се озбиљно угрозе или повреде основне уставне, политичке, економске или друштвене структуре Србије, стране државе или међународне организације. Између осталог у ставу 3. је одређено да се радња односи на уништење државног или јавног објекта, саобраћајног система, инфраструктуре, укључујући и информационе системе, непокретне платформе у епиконтиненталном појасу[39], опште добро или приватну имовину на начин који може да угрози животе људи или да проузрокује знатну штету за привреду.

Кривичним закоником, такође су дефинисана *кривична дела против Војске Србије.*

Члан 415. *Одавање војне тајне* је дефинисано на следећи начин: „Ко неовлашћено другом саопшти, преда или на други начин учини доступним податке који представљају војну тајну или прибавља такве податке у намери да их преда непозваном лицу, казниће се затвором од шест месеци до пет година.“ У овом члану је одређено који се подаци сматрају војном тајном и наглашено да се ради о тајним подацима који би могли да проузрокују штетне последице за Војску Србије, одбрану и безбедност земље. Такође, прецизирани су изузеци када се нешто не сматра војном тајном.

[39] Право, појас који обухвата морско дно и простор испод тога дна (до дубине на којој је могуће искоришћавање природних богатстава), а налази се ван територијалног мора обалне државе. (према http://www.hrleksikon.info/definicija/epikontinentalni-pojas.html, 2016, 3. јун)

Кривичним законником обухваћена су и *кривична дела против интелектуалне својине: неовлашћено искоришћавање ауторског дела или предмета сродног права и повреда проналазачког права.*

Члан 201. *Повреда проналазачког права* се односи на радње неовлашћене производње, увоза, извоза, понуде ради стављања у промет, складиштења или коришћења у привредном промету производа или поступака заштићених патентом. Предиђена је новчана казна или казна затвором до три године.

Чланом 199. *Неовлашћеног искоришћавања ауторског дела или предмета сродног права* су обухваћене радње неовлашћеног објављивања, снимања, умножавања, или на други начин јавног саопштавања у целини или делимично ауторског дела, интерпретације, фонограма, видеограма, емисије, рачунарског програма или базе података. Предвиђена је казна затвором до три године.

Кривичним законником су одређена, такође, *кривична дела против привреде.*

Члан 240. *Одавање пословне тајне* подразумева забрану неовлашћеног саопштавања, предаје или на други начин чињења доступним података који представљају пословну тајну. Такође се сматра недозвољеним прибављање таквих података у намери да се предају непозваном лицу. Предвиђена је казна затвором од шест месеци до пет година.

Члан 225. се односи на кривично дело *Фалсификовања и злоупотребе платних картица* и инкриминише радњу израде лажних платних картица или преиначавање правих платних картица са намером употребе. Предвиђена је казна затвора од шест месеци до пет година и новчана казна. Отежавајућа околност може да буде у висини прибављене противправне имовинске користи.

Члан 231. *Прање новца* се односи на радњу прикривања или лажног приказивања незаконитог порекла имовине. Посебно је наведено лажно приказивање чињеница о имовини са знањем да та имовина потиче од кривичног дела. Предвиђена је казна затвором од шест месеци до пет година и новчана казна.

Кривична дела против животне средине су посебно обрађена у Глави 24 Кривичног законика Републике Србије.

Повреда права на информисање о стању животне средине (Члан 268) дефинише дело на следећи начин: Ко противно прописима ускрати податке или пружи неистините податке о стању животне средине и појавама који су неопходни за процену опасности по животну средину и предузимање мера заштите живота и здравља људи, казниће се новчаном казном или затвором до једне године.

На основу анализе претходно издвојених кривичних дела, и њиховог законског одређења, могу се извести следећи закључци. Закон о изменама и допунама Кривичног законика Републике Србије, из децембра 2012. године, је донео ширење кривично–правне репресије, посебно, у погледу терористичких кривичних дела. Повећан је број кривичних дела тероризма и запрећено је високим казнама у складу са препорукама референтних међународних организација и тела. Појачана репресија и рана инкриминација вероватно представљају последицу ескалације терористичких аката широм света. Посебно је интересантно што неке припремне радње законодавац подиже на ранг радње извршења. Такође, радња подстрекавања се прописује као посебно кривично дело.

Проналазаштво се примарно штити патентним правом које је дефинисано у Закону о патентима. Међутим, правна заштита која је обезбеђена наведеним правом није у неким случајевима довољна, па је оправдана кривичнопроцесна интервенција коју обезбеђује Кривични законик. Кривичнопроцесном интервенцијом су посебно обезбеђени одређени аспекти проналазачког права. Важно је напоменути да се сви облици кривичног дела Повреде проналазачког права могу учинити само са умишљајем.

У кривично законодавство Републике Србије, кривично дело Прање новца је уведено први пут 2001. године. Незаконито порекло имовине подразумева да имовина (покретне и непокретне ствари, новац, имовинско право) потиче од вршења кривичног дела. Сви облици кривичног дела Прање

новца се такође могу извршити искључиво са умишљајем. Код трећег облика наведеног дела, чија је радња стицање, држање или коришћење имовине, знање о пореклу имовине треба да постоји у тренутку њеног пријема. Дакле, кривично дело не постоји уколико се до сазнања дошло у време када се имовина већ користи.

Кривично дело Одавања пословне тајне се извршава и самим чином прибављања података који представљају пословну тајну, иако није извршена њихова предаја другом лицу. Службеном тајном се сматрају подаци или документи који су законом, другим прописом или одлуком надлежног органа проглашени пословном тајном, а чије је одавање проузроковало или би могло проузроковати штетне последице за предузеће или други субјект привредног пословања. Извршилац наведеног кривичног дела не мора нужно да буде овлашћено лице које располаже подацима који представљају пословну тајну, већ и свако друго лице које је до пословне тајне дошло на било који начин, па и на противправан. Недовољно јасан може бити сегмент који се односи на нехатни облик кривичног дела, пошто није довољно прецизно дефинисан у случајевима када пословне тајне нису довољно обезбеђене и чувају се на начин којим се неовлашћеном лицу омогућава њихова спознаја.

Кривично дело *Повреда права на информисање о стању животне средине* се може извршити чињењем или нечињењем. У првом случају ради се о ускраћивању података о стању животне средине, а у другом о саопштавању неистинитих података који се односе на стање животне средине. Право на информисање се може ограничити у случајевима када би информације о стању животне средине негативно утицале на међународне односе, одбрану земље, безбедност итд.

Кривична дела против безбедности рачунарских података су први пут уведена у кривично законодавтсво Републике Србије 2003. године. Поред Кривичног законика, значај за сузбијање наведене врсте криминалитета има Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала (Службени гласник Републике Србије, 61/05, 104/09). Кривично дело *Рачунарска саботажа* се односи на податке од значаја за државне органе, јавне службе, установе и привредне субјекте.

Стојановић сматра да би у формулацију кривичног дела требало унети термин „од значаја за делатност“, како би се разграничило кривично дело *Рачунарске саботаже* од кривичног дела *Оштећење рачунарских података и програма* (Стојановић, 2007: 874). *Рачунарска превара* је кривично дело које се односи на случајеве када је радња извршења утицала на исход или резултат електронске обраде и преноса података. Уколико до тога није дошло, наведено дело ће се квалификовати као покушај који не подразумева законске санкције.

Кривична дела против уставног уређења и безбедности Републике Србије се такође неформално називају и политичким кривичним делима. Стога, посебно је значајно пронаћи праву меру између кривичнопроцесне заштите државе и угрожавања слободе и права грађана. Реална опасност постоји и у смислу да се кривично право у овој области злоупотребљава од стране политичких елита које су на власти прогањањем политичких противника. Кажњавање за припремне радње се може оправдати побољшањем превенције у делу реаговања у раној фази остваривања кривичног дела, али у исто време ствара могућност за евентуалне злоупотребе од стране носиоца власти. Природа свих кривичних дела против уставног уређења и безбедности Републике Србије подразумева да су учињена са умишљајем, осим дела *Одавање државне тајне* које може да има и нехатни облик. Кривично дело *Шпијунаже*, по Кривичном законику Републике Србије постоји иако је исто учињено на штету неке друге државе, а не искључиво Републике Србије. Посебан облик наведеног кривичног дела постоји у ситуацији када неко ствара обавештајну службу у држави и руководи њоме, а то чини за потребе друге државе или организације. Други облик се састоји у ступању у страну обавештајну службу, прикупљању података за њене потребе, с тим да прикупљени подаци не морају нужно да буду тајни. Трећи облик подразумава прикупљање података за другу државу или организацију са намером да се предају тој држави или организацији. Дакле, овај облик је превентивног карактера у односу на претходна два. Припремне радње за основни облик кривичног дела *Шпијунаже* су такође кажњиве. Кривично дело *Одавање државне тајне* се разликује од дела

Шпијунаже пре свега у елементу иностраности, који код првог кривичног дела не постоји.

Кривична дела против Војске Србије нису издвојена у односу на остала кривична дела посебним кривичним правом Републике Србије. Специфичности кривичних дела против Војске Србије се односе на извршиоце који могу бити војна лица, али и остали грађани уколико су дела учињена за време ратног стања.

Кривична дела против уставног уређења и безбедности у законодавству Сједињених Америчких Држава (САД)

Посебан императив у погледу стварања кривичноправних услова за успешно супротстављање страним обавештајним службама су перманентно праћење искустава контраобавештајних и безбедносних служби широм света, промене у кривичноправној регулативи која се односи на шпијунску делатност, као и промене у кривичнопроцесним законским решењима у вези са предвиђањем истражних радњи и техника на њиховом доказивању и сузбијању. У том смислу ћемо размотрити како су наведена кривична дела дефинисана у законодавству Сједињених Америчких Држава, Републике Немачке и Републике Хрватске. С обзиром на тенденције Р.Србије усмерене на приступању ЕУ, у даљем тексту ће се анализирати правна регулатива која третира наведена кривична дела у законодавству Р. Немачке и Р. Хрватске, као најмалаће чланице ЕУ. С обзиром на измене Закона о кривичном поступку из 2013. године и увођења тзв. „Тужилачке истраге“ која подразумева посебну улогу тужилаштва током вођења преткривичног поступка, а која је својствена англосаксонским државама, у даљем тексту ће се анализирати правна регулатива која третира кривична дела шпијунаже дефинисана у законодавству САД.

Закон о шпијунажи и цензури Сједињених Америчких Држава (https://www.fas.org/sgp/library/edgar.pdf, 2016, 1. јул) је за разлику од Кривичног законика Републике Србије кривично дело шпијунаже квалитетније разарадио, а кривичне санкције су знатно оштрије у односу на

домаћи закон. Овим законом одређено је да агент (шпијун) може бити оптужен и осуђен на максималну казну до десет година затвора и новчану казну до 5.000 USD, иако није учинио кривично дело шпијунаже, али је пропустио да се региструје код Државног секретара за регистрацију агента стране службе. Овим су изузети акредитовани дипломатски и конзуларни службеници, чији статус је регулисан Бечким конвенцијама о дипломатској и конзуларној служби. *Поверљива информација* је дефинисана као информација владиних агенција која је из разлога националне безбедности посебно пројектована, а чије је ширење забрањено. У тренутку прекршаја, информација мора бити посебно пројектована као поверљива и оптужени мора имати специфичне намере да би омогућио ту врсту информација неовлашћеној особи или страној влади, свестан да ће издаја или употреба такве информације бити штетна по безбедност или интерес САД–а.

Закон је подељен у Секције, а само неке од њих ће се разматрати, тачније само оне које могу да се доведу у контекст рада.

У Секцији *Прикупљања, преношења или губитка одбрамбених информација* наведени су објекти и покретне ствари значајне за националну безбедност које треба заштитити, а чије би поседовање могло да обезбеди предност страној држави. Предвиђени су случајеви и начини који би могли да проузрокују да одбрамбене информације дођу у посед стране државе. Наведен је списак објеката и покретних ствари као што су: истраживачке лабораторије и средства и материјали које истраживачи користе. Одговорност према заштићеним информацијама је такође дефинисана у овој Секцији, па је самим тим одређено кажњавање непажње код губитка, крађе, нестанка, оштећења или уништења, неврaћања документа на место које је одређено и пропуштања да се хитно извести претпостављени. За сва дела предвиђена је казна до 10.000 USD или до десет година затвора, а могуће је изрећи и обе казне, у зависности од висине штете.

Секција *Прикупљање, испоручивање одбрамбених информација* се односи на достављање података страним владама или оружаним снагама, као и на спровођење активности како би се остварио циљ усмерен на наношење штете или прибављања користи страној држави. Јасно је

дефинисано коме и о чему/коме се не сме пренети информација. За учиниоца овог дела предвиђена је смртна казна, доживотна казна затвора или казна затвора на извесно време.

Секција *Фотографисање, скицирање и објављивање фотографија безбедносних објеката* се односи на заштиту војних, поморских и сличних објеката, инсталација и опреме за фотографисање, скицирање и објављивање, без претходно добијеног одобрења од надлежне команде. Председник САД–а може прогласити неки објекат од виталне важности чиме забрањује претходне активности без одобрења одговарајуће војне команде. Фотографије или скице морају бити поднете претпостављеној команди због цензуре или других мера које се у овом случају сматрају непоходнима.

Секција *Информације које се односе на криптографску и комуникациону присмотру* је донета у циљу заштите поверљивих информација у области криптографије и комуникацијског надзора. Под комуникацијским надзором се подразумевају све процедуре и методе коришћене за пресретање информација. Дефиниција криптографског система подразумева све методе тајног писања и све електронске или механичке уређаје или методе који су коришћени у сврху откривања или прикривања садржаја, његовог значаја или самог значења комуникације.

Кривична дела против уставног уређења и безбедности у законодавству СР Немачке

Кривични закон СР Немачке (https://www.gesetze-im-internet.de/bundesrecht/stgb/gesamt.pdf, 2016, 1. јул), у првом поглављу које носи назив *Издаја мира, велеиздаја, угрожавање демократске правне државе*, врши поделу кривичних дела на унутрашња и спољна угрожавања безбедности државе. У другом поглављу, под називом *Издаја земље и угрожавање њене спољне безбедности*, обрађена је и проблематика шпијунаже. У првом члану овог поглавља дефинисана је *државна тајна* коју представљају чињенице, предмети или судске одлуке доступне само ограниченом броју људи који се морају тајити пред иностраним партнерима

да би се отклонила опасност по спољну безбедност државе. Законом је одређено и шта не може да буде државна тајна, те је прописано, на пример, да државне тајне нису чињенице које се негативно рефлектују на слободно демократско уређење и да њиховим несаопштавањем уговорним партнерима СР Немачка чини преступе о међународно уговорена ограничења у наоружању.

Кривично дело *Издаје земље* у кривичном законодавству представља саопштавање државне тајне страној сили или неком од њених посредника, дозвољавање да она доспе у посед неке стране силе или неком од њених посредника, јавно саопштавање државне тајне да би се нанела штета матичној држави или удовољило некој страној сили. Санкција за наведено кривично дело је казна затвора од најмање годину дана. Тежи облик наступа када починилац злоупотреби своју одговорну улогу чувања државне тајне или када својим делом доведе у опасност спољну безбедност СР Немачке. У нарочито тешким случајевима починилац се кажњава доживотним затвором или казном затвора не мањом од пет година. У односу на Републику Србију казнене одредбе су знатно оштрије за исто дело.

Кривично дело *Објављивања државне тајне* је описано као дело у којем је извршилац онај ко дозволи да, државна тајна која се чува од стране неке државне службе или по њеном налогу, доспе до неовлашћеног лица и тиме доведе у опасност спољну безбедност земље. Предвиђена казна за ову врсту кривичног дела је шест месеци до пет година затвора.

Прикупљање података који представљају државну тајну подразумева извршење радње прикупљања тајних података са намером да се предају неовлашћеном лицу. За наведено кривично дело предвиђена је казна затвора од једне до десет година. Наведено дело припада категорији дела у покушају, чиме је наглашена строгост у примени законских одредби које се односе на област шпијунаже. Упоређујући висину казне за наведено кривично дело са висином казне за учињено кривично дело *Шпијунаже* у Кривичном закону Републике Србије, може се приметити да су висине казни идентичне, иако се у кривичном делу *Прикупљања података* ради само о радњама које претходе покушају извршења дела *Шпијунаже*.

Кривични закон, предвиђа кажњивост нехатног кривичног дела *Предаје државне тајне*. Нехатна радња се састоји из јавног објављивања или чињења доступним државне тајне коју чува надлежни државни орган, при чему се, из нехата, доведе у опасност спољна безбедност државе. Ова врста кривичног дела санкционише се казном затвора до пет година или новчаном казном. Предвиђен је и блажи облик нехата, према коме се третира онај који непозваном лицу непромишљено учини доступном државну тајну, те на тај начин доведе у опасност спољњу безбедност Савезне Републике Немачке. Починилац ће се казнити затворском казном у трајању до три године или новчаном казном.

Кривично дело *Против државне шпијунаже* је прописано за она лица која за страну силу обављају делатност која је усмерена на откривање или саопштавање државних тајни. Ово је основни облик кривичног дела и не мора нужно да обухвати опис радње кривичних дела прикупљања државних тајни, већ се таква лица могу ангажовати на прикупљању других података који нису обухваћени овим кривичним делима, као што је распитивање о личностима које су у контакту са државним тајнама и слично. Други облик наведеног кривичног дела односи се на акт извршиоца спремног да открије и саопшти државну тајну страној сили или њеном представнику, уколико то кривично дело није обухваћено описом кривичних дела издаје земље и предаје државне тајне. Дакле, овде се ради о кажњивости свесног покушаја да се изврши кривично дело шпијунаже. За оба облика кривичног дела су предвиђене идентичне санкције и то казна затвора до пет година или новчана казна. У нарочито тешким случајевима предвиђена је казна затвора од једне до десет година. Починилац кривичног дела се не кажњава уколико је био присиљен на такво понашање од стране силе или њеног представника и уколико добровољно одустане од радње и надлежном државном органу саопшти све што зна о тим радњама.

Кривично дело *Шпијунаже по службеној дужности* подразумева радњу извршења коју немачки држављанин чини против своје државе за тајну службу неке друге силе, обављајући шпијунску делатност која је усмерена на саопштавање или слање података, предмета или информација. Посебан

облик кривичног дела подразумева активности које се односе на изражавање могућности како би се учиниле радње из основног облика. Оба облика кривичног дела санкционишу се казном затвора до пет година или новчаном казном. Тежи облик наведеног кривичног дела подразумева да је починилац саопштио или послао податке, предмете или информације које чува неки надлежни орган, тако што је злоупотребио службени положај који га обавезује на чување таквих тајни или да је делом изазвао тешке штетне последице за СР Немачку. Санкција за тежи облик наведеног кривичног дела је казна затвора од једне до десет година.

Кривични законик предвиђа могућност изрицања специјалних заштитних мера суда за починиоце кривичних дела шпијунаже који су осуђени за кривично дело које подразумева предумишљај и на затворску казну не мању од шест месеци. У таквим случајевима суд има могућност да прогласи починиоца неспособним за обављање јавне службе и да му ускрати право да учествује на јавним изборима, као изборни кандидат и гласач. Овим му се онемогућују уставна права по законодавству Републике Србије и основна људска права да бира и да буде биран, што такође наглашава изричитост Кривичног закона СР Немачке када су у питању кривична дела усмерена против уставног поретка.

У поглављу *Кривична дела против одбране земље* инкриминисани су деликти *Војне шпијунаже* и њима сродна дела. Овде је дефинисано и кривично дело пропаганде против система одбране СР Немачке. Опис радње кривичног дела подразумева свесно и намерно ширење неистинитих и грубо искривљених тврдњи у циљу ометања делатности система одбране и спречавања у обављању задатака одбране замље. Санкција је казна затвора од пет година или новчана казна.

Саботажа на средствима за одбрану подразумева неовлашћено уништавање, оштећење, мењање, чињење неупотребљивим, одстрањивање средства, установа или уређаја који у потпуности или претежно служе одбрани земље и заштити цивилног становништва од ратних опасности, те се тиме угрожава безбедност, борбена готовост снага или се доводе у питање животи људи. Поред овог основног облика кривичног дела, предвиђен је и

посебан облик који подразумева свесну производњу или испоруку предмета или сировина са грешком, чиме се доприноси изазивању опасности по становништво. Наведена кривична дела санкционисана су истоветно, затворском казном од три месеца до пет година.

Кривични деликт рада за обавештајну службу која угрожава националну безбедност подразумева извршење дела изван подручја важења овог закона, а односи се на установе, партије и друга удружења и њихове чланове који прикупљају обавештења о стварима везаним за одбрану земље, врше обавештајну делатност која за предмет има ствари везане за одбрану земље или врбују друге за такву делатност и подржавају активности против безбедности СР Немачке или борбене готовости њених трупа. Из описа радње кривичног дела се изузима делатност усмерена на информисање јавности у оквиру уобичајеног извештавања путем штампе или других електронских медија. Наведено кривично дело, као што може да се види, налази се на граници задирања у основна људска права и слободе, а могући проблеми су избегнути изузећем.

Кривично дело *Снимања опасног по безбедност* подразумева снимање или описивање војних средстава, војних објеката, уређаја или активности и предају истих другоме, чиме се свесно угрожава безбедност или борбена готовост трупа. Учинилац се ослобађа одговорности уколико је извршилац имао дозволу за снимање издату од надлежног органа. За ову врсту кривичног дела су прописане казна затвора до пет година или новчана казна. Посебна врста овог кривичног дела подразумева фотографисање или снимање, из авиона или друге летелице, територије или предмета на подручју важења овог закона и предају тих фотографија другом, чиме се свесно угрожава безбедност СР Немачке или борбена готовост њених трупа. За ову врсту кривичног дела прописана је казна затвора до две године или новчана казна.

Врбовање за службу у туђој војсци је дело које постоји у случајевима када неко лице у корист неке стране силе врбује немачког држављанина за службу у војној или сличној организацији или га приведе њеним официрима.

За ово кривично дело предвиђена је затворска казна у трајању од три месеца до пет година.

Кривична дела против уставног уређења и безбедности Републике Хрватске

Године 2013. наступиле су измене у кривичноправној области Републике Хрватске. (http://www.zakon.hr/z/98/Kazneni-zakon, 2016, 1. јул)

У четрнаестој глави дефинисана су кривична дела против приватности, која поред личне приватности, обухватају одредбе везане за пословни простор и пословна документа. Кажњава се дело неовлашћеног уласка у дом или туђи пословни простор или ограђени простор са максималном казном од једне године затвора. Уколико наведено дело изврши овлашћено службено лице казна је до три године затвора. Одредба закона предвиђа неповредивост писама или других личних и пословних пошиљки, а запрећена казна је до годину дана затвора. У односу на Републику Србију санкције за наведено кривично дело су ригорозније. У Републици Србији је за исто дело прописана новчана казна или алетрнативна казна затвора до две године. Кривични закон (Казнени закон) инкриминише и неовлашћено прислушкивање, тонско и визуелно снимање, а запрећена казна је до три године затвора. Уколико је дело извршило службено лице током обављања дужности биће кажњено затвором од шест месеци до пет година. За дела неовлашћеног тонског и видео снимања запрећена казна је затвор до једне године, уз обавезно одузимање снимака и средстава којима је снимано.

Наведена дела су анализирана, с обзиром на то да обавештајне службе примењују радње које она описују. Опис дела је врло сличан са делима у Републици Србији, али су законске санкције оштрије.

Глава двадесет четврта Кривичног закона Републике Хрватске се бави кривичним делима против привреде. Члан 262. инкриминише О*давање и неовлашћено прибављање пословне тајне*, односно индустријску шпијунажу. Радња кривичног дела се односи на саопштавање пословних тајни, предавање докумената или њихово чињење доступним неовлашћеном лицу.

Ово кривично дело има два облика, одавање и прибављање пословне тајне. Одавање пословне тајне чини лице које неовлашћено саопшти, преда или на други начин учини доступним поверљиве податке из области економске делатности. С друге стране, особа која прикупља податке у намери да их преда непозваном лицу извршила је кривично дело прибављања пословне тајне. Санкција за наведено кривично дело је казна затвора до три године. У случају да починилац себи или другоме делом причини имовинску корист или нанесе знатну штету предузећу, кажњава се затвором од шест месеци до пет година.

Евидентно је да Кривични закон Републике Хрватске за разлику од Кривичног закона Републике Србије није дефинисао појам *пословне тајне*, већ то препушта пословним субјектима. Исто тако, у Кривичном закону Републике Хрватске није предвиђено одавање пословних тајни страних субјеката другим страним субјектима.

Глава тридесет друга дефинише кривична дела против државе. Тако се члановима закона предвиђају кривична дела *Помагања непријатељу* и *Подривање војне и одбрамбене моћи државе.* Кажњава се политичка и економска сарадња са непријатељем државе током оружаног сукоба и предвиђа се казна затвора од једне до десет година. Посебан члан подразумева дело чињења неупотребљивим или предаје у руке непријатељу одбрамбених постројења, објеката, положаја, наоружања или других војних и одбрамбених средства, предаја трупа непријатељу или на други начин ометање и довођење у опасност војне и одбрамбене моћи Републике Хрватске. Предвиђена санкција је затворска казна од једне до десет година.

У посебној глави разматрају се кривична дела против Републике Хрватске као што су велеиздаја, признавање окупације и капитулације, спречавање борбе против непријатеља, одавање тајних података и шпијунажа.

Кривично дело *Шпијунаже* је описано готово идентично као у Кривичном закону Републике Србије, изузев чињенице да се наводи експлицитно да су извршиоцу поверени тајни подаци или је до њих дошао на противправан начин. Став два прописује кажњавање и за саму припрему

кривичног дела, који се истиче у акту прикупљања тајних података. У том случају нужно је утврдити и намеру да се они доставе страној обавештајној служби. За ово дело је предвиђена казна затвора од шест месеци до пет година. У овом сегменту се може увидети сличност са Кривичним законом СР Немачке. Став три инкриминише рад за страну обавештајну службу и предвиђа се казна од једне до десет година затвора. Став четири се односи на чињење кривичног дела у току рата или оружаног сукоба у коме учествује Република Хрватска. Законодавац истиче чињеницу да Хрватска не мора бити у рату да би њене оружане снаге учествовале у оружаном сукобу будући да је чланица НАТО–а и Европске уније, па се могу ангажовати у борбеним мисијама у мултинационалним операцијама које предводе наведене међународне организације.

Кривични закон Републике Хрватске у сегменту који се бави кривичним делима против оружаних снага, разматра и кривична дела *Неовлашћеног уласка у војне објекте и израду скица или цртежа војних објеката и борбених средстава*.

Кривично законодавство Републике Србије у области кривичноправне заштите од кривичних дела шпијунаже усаглашено је са међународним конвенцијама и актима које је Србија ратификовала. Може се констатовати да је и на плану кривичнопроцесне регулативе која регулише примену посебних истражних мера у супротстављању шпијунажи Србија наведену област уредила у складу са савременим законодавним решењима других држава. То подразумева прилагодљивост модерним методама деловања страних обавештајних служби не ограничавајући права и слободе грађана, посебно имајући у виду потребу за превентивним и репресивним деловањем против потенцијалних извршица кривичних дела која угрожавају безбедност и националне интересе Републике Србије.

Упоредном анализом кривичноправне законске регулативе Сједињених Америчких Држава, Савезне Републике Немачке и Републике Хрватске, можемо закључити да је кривично законодавство Републике Србије потпуно савремено дефинисало материју кривичног дела шпијунаже,

као и да су предвиђени њени модерни појавни облици. За очекивати је да ће у току процеса преговора за пријем у чланство у ЕУ могу очекивати нови захтеви за корекцију кривичноправне регулативе у појединим областима које регулишу наведену материју.

Такође, потребно је истаћи да законска регулатива сама по себи не може реализовати неопходну превентиву функцију нити је гарант за ефикасно репресивно деловање државног апарата на спречавању и сузбијању кривичних дела шпијунаже и других тешких кривичних дела против уставног уређења Републике Србије. Међутим, успостављен актуелни правни ситем Републике Србије пружа реалне основе за откривање и доказивање наведених кривичних дела и ствара могућност додатног успостављања ефикасних криминалистичких и правних института и метода у правним прописима.

5.2.3. Мере заштите тајних података у ИКС

Мере заштите тајних података се деле на опште и посебне. Неке од општих мера заштите пословних информација су:

- одређивање степена тајности;
- процена претње за безбедност тајног податка (на основу значаја тајног податка за националну безбедност врши се безбедносна процена која обухвата: ситуацију у непосредном окружењу — макро и микро локација, безбедносне ризике и претње, мере безбедносне заштите);
- одређивање начина коришћења и поступања са тајним податком (безбедносне процедуре);
- одређивање одговорног лица за чување, коришћење, размену и друге радње обраде тајног податка;
- одређивање руковаоца тајним подацима, укључујући и његову безбедносну проверу у зависности од степена тајности податка;
- одређивање посебних зона, зграда и просторија намењених заштити

тајних података и страних тајних података;

- надзор над поступањем са тајним податком.

Посебне мере заштите би се могле поделити на следеће категорије:

Мере физичко–техничке заштите тајног податка — укључују уградњу и постављање техничких средстава заштите, утврђивање безбедносне зоне и заштиту ван безбедносне зоне (Систем физичко–техничког обезбеђења обухвата низ нормативних, оперативних, информативних и образовно–едукативних радњи и мера којима се, између осталог, успоставља: организација вршења послова физичко–техничког обезбеђења; функционисање службе и система физичко–техничког обезбеђења; кадровски састав службе физичко–техничког обезбеђења; опремљеност потребним средствима и опремом, обучавање и стручно оспособљавање радника физичко–техничког обезбеђења за рад).

Физичко обезбеђење представља обезбеђивање: објеката, имовине и ствари у транспорту од уништавања, оштећења, крађе и других облика штетног деловања, као и обезбеђивање лица од угрожавања њиховог живота, физичког и психичког интегритета, приватности и личних права, те других облика угрожавања њихове личне сигурности. Техничко обезбеђење (у смислу искључиво техничког, али и комбинованог физичко–техничког обезбеђивања) је обезбеђивање објекта и имовине, ствари у транспорту и лица техничким средствима и уређајима, у складу са правним прописима и прописаним стандардима.

Мере које се предузимају на заштити ИКС–а требало би да омогуће да мрежна инфраструктура буде физички безбедна: постављање физичко–техничког обезбеђења (чувари, сензори, аларми, видео надзор итд.), идентификационе картице за особље, резервни извор напајања електричном енергијом, укопавање мрежних каблова (или уградња у зидове), закључавање разводних ормара и просторије са серверима и строга контрола кључева (број копија, примопредаја, овлашћене особе итд.), облагање опреме заштитним кућиштима, печаћење просторија и кућишта, одржавање система заштите од пожара и друго. Од логичког обезбеђења се очекује да спречи

нападе са даљине на инфраструктуру, односно уређаје конфигурације. (Ruth & Hudson, 2004: 138)

Мере заштите информационо–телекомуникационих система — обзиром на комплексност и начин реализације противзаконитих послова прања новца, која се најчешће спроводи применом савремених ИКТ, безбедносне службе посебну пажњу посвећују *заштити рачунарских података.* Слаба тачка у безбедности оваквих информација је слабост мреже, система или процеса који има највише шанси да буде угрожен, што подразумева изградњу квалитетног система одбране ИКТ. Исти обухвата обезбеђивање мрежне инфраструктуре, комуникационих протокола, сервера, апликација и система датотека, као и проверу идентитета корисника. Нападач у процесу угрожавања ИКС–а у овом случају треба да прође неколико фаза одбране, а то су: систем за проверу аутентичности корисника, безбедност комуникационих протокола, безбедност апликација и безбедност датотека.

Џигурски истиче значај пројектовања сигурносних механизама за ИКС. Пројектовање садржи идентификацију свих објеката који треба да буду заштићени, дефинисање што више могућих претњи, одређивање колико су претње вероватне, имплементацију адекватног сигурносног система. (Џигурски, 2002: 138) Обезбеђивање мрежне инфраструктуре се врши смањивањем броја приступних тачака и стављањем мрежне баријере у приступној тачки. Избор комуникационог протокола је такође важан детаљ у систему одбране. За електронску трговину потребно је инсталирати обезбеђен протокол за пренос хипертекста (*Hypertext Transfer Protocol Secure*, HTTPS), који користи слој безбедних логичких прикључака за заштиту комуникација. Апликације преко којих се приступа Интернету, требало би да имају најсвежије безбедносне исправке. У читавом систему компаније пожељно је инсталирати неки од система за проверу аутентичности, ради потврде да корисник који покушава да приступи ресурсима има таква овлашћења. Врло важно је да се у случају инцидента, односно ванредног догађаја, унутар система могу пронаћи и одговарајући записи о томе шта се тачно догодило. Ови записи могу омогућити реконструкцију догађаја и

поправку слабих тачака у систему. Приступ пословним рачунарима је потребно ограничити до нивоа редовног функционисања запосленог лица, али никако више од тога. У систему заштите потребно је предвидети могућност за појаву инцидентних ситуација, када је потенцијалне ризике пожељно свести на минимум. Најсложенији за решавање су инциденти који су настали деловањем самих запослених. Мотиви за напад на систем изнутра могу бити различити. Један од њих је незадовољство запослених због отпуштања или премештаја на друго радно место. За доказивање учињених напада на систем, потребно је обезбедити одговарајуће доказе који могу бити валидни и у судском поступку. Истрага и вештачење записа на рачунару може бити од пресудног значаја у правном поступку против неког од запослених. Због тога се морају сачувати одговарајући записи који могу представљати доказни материјал. Џигурски објашњава да се посебна филозофија заштите користи у случају корисничког нивоа. На претходним нивоима се користила математика као научна дисциплина која обезбеђује заштиту. На корисничком нивоу се углавном користе организација рада и психологија. Сигурносна политика представља скуп правила и упутстава за понашање корисника система у циљу избегавања неизвесности у поступцима које предузима корисник, који могу довести до нарушавања сигурности. Индивидуални корисник сам за себе усваја сигурносну политику, док администратори система усвајају сигурносну политику за цео систем и она је знатно комплекснија јер треба да обухвати и понашање свих који имају везе са системом. (Џигурски, 2002: 137–138)

Приликом пројектовања ланца надзора мора се водити рачуна о одредбама националног законодавства, иако је интерес послодавца да строго контролише рад запослених укључујући надзор рачунара, е–поште и контролу телефонских разговора. Међутим, законске норме и прописи који регулишу приватност могу представљати битан ограничавајући фактор за овакве безбедносне системе. Безбедносни разлози захтевају да се посебна пажња посвети употреби заменљивих медијума за чување података (магнетне траке, *CD/RW/DVD-ROM*, дискови, флеш картице, паметне картице итд.). Безбедносни проблем представља чињеница да ови уређаји

омогућавају копирање података са сервера и њихово уклањање без могућности филтрирања или проверавања помоћу мрежног пролаза. Магнетна трака је традиционални меморијски медијум за чување резервних копија и архивирање података. Ови подаци се на тракама могу заштитити лозинкама и шифровањем, а саме траке морају се чувати у режиму појачане физичко–техничке заштите. *CD*, екстерни дискова, флеш картица својом ниском ценом, капацитетом, поузданошћу постали су популарни и незаменљиви у употреби. Велики безбедносни проблем представља могућност њихове злоупотребе. Њихова величина и облик постају готово непремостива препрека у систему обезбеђења, нарочито ако злоупотребу врше сами запослени.

Мере крипто–заштите[40] — криптографија представља шифровање и дешифровање података ради обезбеђења поверљивости података, интегритета, провере идентитета и непорицања. Шифровање (енгл. encryption) је метод који омогућава да се код отвореног текста сакрије његов садржај, односно да се текст трансформише у нечитљив и неразумљив садржај (шифрат). Шифрат за који није познат кључ зове се криптограм. Шифровање се користи да би се обезбедило да нико, осим корисника коме је порука намењена не може да сазна њен садржај. Поступак који омогућава да се од шифрата добије оригинални отворен текст назива се дешифровање (енгл. decryption). Криптографија је наука која се бави проучавањем и проналажењем метода за шифровање и дешифровање података у циљу њихове заштите. Криптоанализа је наука о „разбијању“ шифара. (Ђокић, 2008) Механизам трансформације података треба да задовољава два услова: криптоанализа треба да буде неисплатива, било временски, било економски; трансформација и реверзна трансформација треба да буду што мање захтевне за овлашћене кориснике. Шифровање података могуће је коришћењем одговарајућег криптосистема (енкрипције). Према начину употребе кључева криптографски алгоритми се могу поделити у две групе:

[40] „Основу сигурности података на Интернету, и уопште на рачунарским мрежама представља њихово трансформисање у облик који нападачу не пружа ни једну информацију о садржају.“ (Џигурски, 2002: 132)

алгоритми који користе симетричне кључеве, односно симетрични алгоритми, који користе један кључ и за шифровање и за дешифровање и алгоритми који користе асиметричне кључеве, асиметрични алгоритми, где постоје два кључа (јавни кључ и приватни кључ). Тајност се обезбеђује тако што нико не може открити за неко разумно време ни садржај података ни приватни кључ. Корисник генерише по одређеном алгоритму два кључа. Један проглашава за приватни и познат је само њему, а други јавни кључ дистрибуира осталим корисницима. Комуникација се одвија тако да особа А поруку шифрује јавним кључем особе Б и од тада је једино особа Б у стању да ту поруку дешифрује приватним кључем. Добра пракса је да се кључеви временом замењују). (Ђорђевић, 2007: 111-119)

Заштитни режим радних и формацијских места — регулисан је у оквиру акта о унутрашњем уређењу и систематизацији радних места.

Утврђивање посебних програма образовања и обуке — за потребе обављања послова заштите тајних података и страних тајних података.

6. ОБАВЕШТАЈНЕ АКТИВНОСТИ У САВРЕМЕНОМ СВЕТУ

Савремени свет се данас суочава са новим и све сложенијим видовима претњи на које није могуће лако одговорити. Потреба за обавештајним деловањем је данас израженија више него икад у готово свим људским делатностима, посебно у политици, привреди и одбрани. Глобализација и развој комуникационо–информационих технологија учинио је да савремени међународни односи буду много динамичнији и међусобно зависни. Како у унутрашњим тако и у спољним пословима једне националне државе догађаји се дешавају убрзано са знатно већим степеном неизвесности и тежим могућностима предвиђања, што представља један од основних задатака обавештајних институција. Превелика количина информација са којима се лидери пословних субјеката данас суочавају нимало не олакшава решавање проблема, већ га додатно компликује у смислу одвајања битног од небитног, важног од мање важног. Да би у гомили информација одвојили оне које заслужују пажњу лидера и које ће им омогућити доношење квалитетних одлука, обавештајне институције прикупљене информације анализирају, систематизују и претварају у „знање“. Дакле, предвидети будућност, што је из угла обичног човека сложен и немогућ задатак, представља основ и суштину делатности обавештајне службе. Систематизацијом претходних искустава, знања, студија случајева и научних истраживања у областима у којима обавештајне службе делују, стварају се услови за доношење закључака о могућем исходу посматраног догађаја, који свакако не може бити непогрешив јер зависи од много фактора.

6.1. ОБАВЕШТАЈНИ РАД У НОВОМ ОКРУЖЕЊУ

За појам „обавештајно“ не постоји универзална дефиниција која би га у потпуности објаснила, па се самим тим користе дефиниције више аутора. Тако Адамс наводи да појам обавештајно (intelligence) подразумева „прикупљање или дистрибуцију информација, посебно тајних информација; информација о противнику или потенцијалном противнику“ (Adams, 1995: 27). У Војном лексикону обавештајна делатност представља „активност обавештајних и војнообавештајних служби, институција и органа за потребе државног, политичког или војног руководства. Обухвата планирање, прикупљање, проверавање, анализу, селекцију и достављање обрађених података на коришћење. Представља непрекидан процес којим се руководству обезбеђују подаци о другим државама, њиховим оружаним снагама и другим чињеницама значајним за вођење текуће и дугорочне политике и припрему и вођење рата“ (Војни лексикон, 1981: 336).

У Француској се обавештајна делатност посматра као скуп активности чији је циљ да највишим државним властима, дипломатији, оружаним снагама и снагама унутрашње безбедности остваре аутономну могућност разумевања и предвиђања развоја у стратегијском окружењу, што је основа за доношење одлука и акција. (Défense et Sécurité nationale Le Livre Blanc, 2008: 133)

Дефиницију обавештајне делатности дао је и Мајкл Ворнер (Michael Warner) који наводи да је „обавештајна делатност тајна државна активност усмерена ка разумевању и утицању на стране ентитете“ (Warner, 2002: 21). Своју дефиницију Ворнер базира на пет кључних елемената: 1) обавештајна делатност користи тајне изворе и начине прикупљања података; 2) реализују је државни службеници за потребе државног руководства; 3) усмерена је на стране субјекте; 4) омогућава доносиоцима одлука разумевање и 5) утицај на стране ентитете на такав начин да се не могу директно повезати са матичном државом.

Из дефиниција се може видети да обавештајна делатност не подразумева само располагање са информацијама о неком лицу или о неком

догађају, већ и саму организацију, пут доласка до неке информације која се од стране њеног власника штити посебним мерама. Она подразумева неколико корака: планирање, прикупљање информација, анализу и дистрибуцију. Уколико информација до које се дође обавештајним деловањем није пажљиво анализирана и правилно искоришћена у доношењу пословних одлука, онда се не може говорити о обавештајном деловању већ искључиво о пуком прикупљању информација које може да спроводи било ко и за било чије потребе. Обавештајна делатност, за разлику од тога, подразумева организовану активност стручно–специјализованих институција и организација које пажљиво планирају своје активности, анализирају добијена сазнања и доносе закључке које презентују надлежном руководству, које на основу тих информација доноси одлуке. Прикупљене информације се сврставају у категорије и додељују се стручно надлежним државним ресорима. У том смислу обавештајну делатност је могуће спроводити у областима политике, одбране и привреде, у зависности од карактера информација на коју се обавештајна делатност односи. Ради тога у оквиру сваке од наведених делатности постоје развијена обавештајна тела која се баве прикупљањем података и информација о лицима и догађајима који су предмет интересовања руководства једне националне државе. Дакле, обавештајна делатност је пажљиво планирана и осмишљена активност којом се остварују прецизно утврђени циљеви. На врху управљачког тела налазе се највиши државни органи који дају општа усмерења, која се спроводе од стране оперативних делова обавештајног система. Највиши државни органи су укључени у део обавештајних активности формулисања општег државног интереса, а њих планирају и спроводе обавештајне службе једне државе, свака у свом ресору. Управљачке структуре обавештајне службе, а на основу постављених општих циљева и интереса, планирају, координирају своје активности и започињу са прикупљањем података.

Подаци се прикупљају (Johnson, 2007) из отворених извора (енгл. *Open source intelligence* — OSINT), свима доступних, а најчешће се ради о подацима и информацијама које немају посебну оперативну вредност већ служе за проверу и допуну већ прикупљених сазнања другим методама. Прикупљање

тајних података врши се посредством људских извора (енгл. *Human intelligence* — HUMINT) или контролом средстава везе (енгл. *Signal intelligence* — SIGNIT).

Сама активност прикупљања података се спроводи у четири фазе (Dearth & Goodden, 1989).

Најважнија фаза представља *прикупљање података* које може да буде опште и конкретно. Опште прикупљање података и информација се односи на све запослене у оквиру неког пословног субјекта. Овде се ради о прикупљању јавних информација општег карактера које су доступне широј јавности, а до њих се долази вршећи редовне пословне обавезе. Конкретно прикупљање података је сложеније и спроводе га посебно обучена лица (професионалци) јер захтева стручност, обученост и темељно планирање и координацију унутар више структура пословног субјекта. У циљу бољег разумевања овде је потребно направити категоризацију података: јавни подаци (свима доступни), приватни (лични подаци), тајни подаци. Иако је пословно–обавештајна активност углавном усмерена на прикупљање података применом етичких и легалних метода, често се, због високих захтева менаџмента неке организације и пословних интереса пословног субјекта, прибегава прикупљању података применом неетичких метода, а понекад и нелегалних средстава. Тиме пословно–обавештајна делатност прелази у противзакониту активност и представља пословну шпијунажу.

Следећу фазу чини *анализа прикупљених података*. Анализом се подаци обрађују, систематизују, одвајају тачне информације од нетачних и доносе се закључци са одређеном дозом поузданости о неком догађају или појави.

Подаци прикупљени у првој фази су необрађени, то јест „сирови подаци“, тако да је у фази анализе потребно одвојити тачне од нетачних, проверене од непроверених или делимично проверених, као и битне од небитних информација. Методе које се примењују у овој фази обавештајног рада су анализа, синтеза, компарација, индукција, дедукција, процена и друге.

Последња фаза овог циклуса представља достављање информација крајњем кориснику, тј. *дистрибуција података*. Ова фаза се не завршава у

моменту достављања информација јер менаџмент врло често тражи допуну сазнања и на тај начин из фазе дистрибуције надлежну организациону јединицу за обавештајне послове враћа у фазу прикупљања података и фазу њихове поновне анализе узимајући у обзир нове чињенице из окружења и слично. Дистрибуција представља фазу обавештајне активности у којој се крајњи производ обавештајног рада представља кориснику, руководству пословног субјекта. На основу представљеног производа руководство доноси пословне одлуке. У зависности у којој мери је наведени производ утицао на доношење одлуке код руководства организације и какви су пословни ефекти тиме постигнути, вреднује се рад обавештајне организације на оперативном нивоу као и у сегменту способности њеног менаџмента.

Поједини амерички аутори наглашавају потребу интердисциплинарости у изучавању феномена обавештајне делатности. Научници, историчари, психолози и лекари су имали важну улогу у стварању обавештајне парадигме. Они који се баве овом парадигмом, за разлику од већине других подухвата у друштвеним наукама, деле опште мишљење о методологији, подацима, питањима која захтевају решење и проблемима који остају да се реше. Већина се бави истраживањима обавештајног циклуса: постављање обавештајних захтева, прикупљање података, анализа података, и дистрибуција. Алкесандер Џорџ (Alexander George), на пример, наводи да обавештајни неуспех може да се јави у било ком тренутку у обавештајном циклусу, ако професионалци који се баве обавештајном делатношћу и политичари не одговоре на било које од шест питања: (1) идентификују непријатеља (ко?); (2) процене вероватноћу напада (да ли?); (3) утврде врсту акције (шта?); (4) одреде локацију напада (где?); (5) процене време акције (када?); (6) одреде мотив (зашто?). Аутор покушава да одговори на питање зашто се јављају пропусти у обавештајној делатности и да развије најбољу праксу. (Johnson, 2007: 32)

„Обавештајна“ делатност више није искључиво поверена држави и њеним институцијама већ се у наведене активности укључују и организације из приватног сектора тако да би се могло рећи да обавештајна делатност није више привилегија влада националних држава већ и других организација као

што су привредне, еколошке и друге. О њиховој успешности, могућностима и способностима сведочи улога коју имају организације за корпоративну заштиту унутар привредних организација, а односе се на заштиту информација и позитивну улогу у пословању једне привредне организације. У циљу правовременог располагања информацијама између појединих пословних субјеката води се прави рат, који се у стручној литератури назива „рат за информације“. Да би дошли до информација пословни субјекти често ангажују специјализоване агенције које се баве таквом активношћу, а основане су од стране бивших припадника обавештајно–безбедносних служби којима су познате методе и средства прикупљања података. Обавештајне информације пажљиво анализиране и претворене у конкретна знања дају предност неком пословном субјекту у тржишној утакмици и омогућавају му боље и квалитетније позиционирање у пословним активностима. У настојањима да дођу до што квалитетнијих података, поједине обавештајне агенције или целине пословних субјеката примењују легалне и нелегалне методе прикупљања података. Државни обавештајни и контраобавештајни апарат такође прибегава прикупљању података и информација на такав начин, посебно у условима повећане угрожености њене националне безбедности (Петковић, 2009: 195-202).

Такође, пословно обавештајна делатност поред офанзивне компоненте (обавештајна активност — прикупљање информација) поседује и дефанзивну компоненту (енгл. Counterintelligence — контраобавештајна) која има за циљ да онемогући отицање информација које су означене као пословна тајна.

6.2. МЕТОДЕ И СРЕДСТВА ОБАВЕШТАЈНОГ РАДА

Прикупљање података је фаза обавештајног циклуса која се пажљиво планира и спроводи од стране посебно обучених и стручних лица, применом метода које се деле на легалне и нелегалне. Пре свега неопходно је дефинисати пословне циљеве сопственог пословног субјекта и приоритете за стицање сазнања, а све у циљу квалитетнијег пословног деловања. Бернар

(Bernhardt) дефинише четири кључне обавештајне тачке које чине основу за одређивање обавештајних приоритета (према Bernhardt, 2003: 28–36):

- стратегијско пословно одлучивање (енгл. decision topics);
- кључни конкуренти, добављачи и клијенти (енгл. key player topics);
- рано упозорење везано за могуће претње и рано уочавање пословних могућности (енгл. early warning);
- пословне–противобавештајне тачке (енгл. counterintelligence topics).

Биланџић наводи да пословни субјект мора дефинисати који су то конкретни подаци — категорије података који представљају интерес пословног субјекта. Наведени аутор их дели на три категорије (према Јаворовић и Биланџић, 2007: 243-244).

- Подаци о окружењу у којем делује пословни субјекат — ради се о подацима који се односе на глобално окружење, а који утичу на пословање пословног субјекта. У том смислу прикупљају се подаци о политичким и привредним догађајима у свету, региону или у држави са којом пословни субјект сарађује. Поред тога, ова категорија подразумева прикупљање података у областима права, науке, технологије и у другим областима које могу да утичу на пословну сарадњу између пословних субјеката.
- Подаци који се односе на тржиште — наведена категорија се односи, пре свега, на пословне субјекте којима је у пословању примаран профит. Истраживање се односи на то где се одвијају пословне активности, пословне могућности, где и како пласирати сопствене производе, ко су садашњи, а ко потенцијални потрошачи наших производа. За разлику од истраживања тржишта, обавештајне службе које делују у оквиру националних држава истражују амбијент у којем се обавештајна активност спроводи. У контексту истраживања амбијента истражују се потенцијални објекти угрожавања и носиоци недозвољених активности, као и њихова интересовања.
- Подаци који се односе на конкуренцију — подаци о конкуренцији подразумевају податке о пословној стратегији конкуренције,

финансијским условима деловања, развоју нових производа и услуга, начинима дистрибуције, пословним партнерима, кадровима. Поред тога, прикупљају се подаци о потрошачима који конзумирају конкурентске производе, њиховим животним навикама, потребама и жељама.

Сапсфорд (Sapsford) и Џап (Jupp) у свом раду обрађују следеће методе прикупљања података (према Sapsford & Jupp, 2006):

- Посматрање;
- Постављање питања;
- Претраживање мрежа;
- Коришћење докумената.

Постављање питања се по овим ауторима, на пример, реализује кроз следеће активности: непосредни интервју (face to face), телефонски интервју, поштански упитници и друге методе.

Методе прикупљања података у најопштијем смислу се могу поделити на: прикупљање података кроз разговор, прикупљање података кроз планско усмеравање лица, прикупљање података преко јавних, свима доступних извора. Најважније легалне методе којима се обавештајне службе и институције служе у прикупљању информација су (према Првуловић, 2010: 163–176):

- *Слање упита институцијама и привредним субјектима са којима пословни субјект остварује пословну сарадњу*. Упити се шаљу на више адреса и обухватају пажљиво одабрана и конципирана питања која представљају предмет интересовања онога ко упите шаље. Из добијених одговора извлаче се закључци о сферама које представљају пословну тајну за њеног корисника. Исто тако, врше се претпоставке шта то за власника информација представља сиву, а шта црну зону, као и области у којима спроводи активности мањег или већег интензитета. Предност ове методе прикупљања података је могућност деловања са дистанце и понављања истих питања из упитника већем броју интересантних организација. Приликом ових активности избегава се двосмисленост или погрешно схватање лица од кога се информација добија, јер писани текст може да анализира више лица одједном и да се на основу њихових спознаја врше заједничке синтезе и

закључци који се користе у даљим активностима. Уколико одговор на захтев садржи графиконе, табеле и друге врсте графичких приказа, то знатно олакшава доношење закључака и припрему извештаја за дистрибуцију до крајњих корисника. Недостатак ове методе је немогућност проширивања сазнања кроз постављање додатних питања која појашњавају неки догађај или захтев, као и стављање у контекст понашања даваоца информација приликом давања одговара, што може да укаже на његову искреност и на поузданост податка. Ова метода прикупљања сазнања се најчешће користи у привредним пословним активностима, као и у активностима дипломатско конзуларних представника, а у циљу промоције и унапређења економских активности сопствене земље са земљом домаћина. Даваоц информација је у овом случају много обазривији и опрезнији, јер је свестан да је пружање информација у писаном облику обавезујуће по њега и да се рачуна на њихову поузданост. На основу претходних разматрања, могло би се закључити да је овај облик прикупљања података најједноставнији, али у исто време и најмање ефикасан што свакако не би требало да буде реметилачки фактор у даљем спровођењу таквих активности, посебно ако се има у виду да подаци прикупљени на овај начин могу да служе за допуну претходно добијених сазнања или за њихову потврду.

- *Заказани оперативни разговор* представља један од чешћих облика прикупљања података од саговорника за кога се претпоставља да их поседује или да до њих може да дође личним ангажовањем. Заказани разговор се најчешће води са непознатим лицем, а заказује се било непосредно било преко посредника, тако што се лицу саопштава, делимично саопштава или уопште не саопштава повод вођења разговора. Када се ради о овлаштеним службеним лицима државних институција, почетни проблеми око могућег одбијања се превазилазе обавезом грађана да се одазову позиву и отклањањем сумње да је повод за разговор фингиран, а да су разлози потпуно другог садржаја. У току таквих разговора се код саговорника гради што је могуће виши степен поверења, заподевањем заједничких тема за које обе стране показују одређени степен интересовања. Разговори се воде углавном на местима на којима то саговорнику највише одговарају, неретко у

пословним просторијама саговорника или на јавним местима на којима је отежано записивање добијеног садржаја. Од примаоца информација се очекује да поседује висок степен концентрације и изражену способност меморисања садржаја из разговора, као и да непосредно по завршетку разговора начини забелешку како би се избегла могућност заборављања. Кроз разговор се истражују интересовања, животне навике, склоности саговорника и слично како би се лакше успоставио следећи контакт. Вештина лица које води разговор у овом делу долази до потпуног изражаја, као и могућност адаптације саговорнику. Такви разговори морају бити пажљиво осмишљени и планирани и ни у ком случају иницијативу не сме да преузме саговорник јер се у том случају може довести у питање крајњи циљ. Ова техника се често користи у раду обавештајно–безбедносних служби, мада је присутна и у дипломатским активностима. Дипломатско–конзуларни представници заказују разговоре са лицима — представницима институција или привредних субјеката који имају пословни потенцијал за почетак или наставак пословне сарадње. Овај метод је врло користан, даје жељене резултате, ствара услове за примену других метода за прикупљање података и у највећој мери зависи од способности лица које води заказани разговор.

- *Пословни сусрет* је разговор до којег припадник обавештајних структура долази случајно, изненада и неприпремљено. У овом случају је потребно истаћи пожељне особине лица које води овакве врсте разговора: сналажљивост и адаптација у новонасталим ситуацијама, способност брзог размишљања и преусмеравања тока разговора у жељеном правцу. Случајан сусрет може да буде добар основ за наставак контаката са интересантним лицем. Важно је да се саговорник заинтересује за предложену тему и да његов утисак буде повољан како би се створили неопходни услови за наставак контаката. С друге стране, случајан сусрет и не мора да буде „случајан“ што се реализује планским додиром лица које води разговор у контакт са „метом“, а да цела ситуација делује за „мету“ потпуно коинцидентна. У том смислу, неопходно је познавати навике „мете“, места по којима се креће, интересовања као и друге појединости из приватног и пословног живота које би олакшале комуникацију, посебно у почетном делу

када је стицање поверења најважније. Оног момента када такав сусрет прерасте у прикупљање информација више не говоримо о пословном сусрету већ о оперативном разговору који има све елементе заказаног разговора, осим што није заказан.

- *Пословни ручак* представља методу која у суштини не одступа у много чему од методе *заказаног оперативног разговора*, с тим што је евидентна разлика у стварном поводу контакта. Код *заказаног оперативног разговора* саговорник је свестан да ће бити предмет истраживања лица које води разговор, док код овог метода то не мора да буде случај, осим у дипломатским круговима када је позив на ручак еквивалентан позиву на прикупљање података. Повољне основе ове методе прикупљања података представља амбијент у којем се разговор води — најчешће у скупоценим ресторанима где се саговорнику обезбеђује потпуно уживање у понудама ресторана. Опуштеност и отменост амбијента изазивају код саговорника појачан осећај вредности и обезбеђују лакше продирање у сфере интересовања. Недостатак ове врсте комуникације представља то што се води на јавном месту и тиме пружа могућност конкуренту или другим непозваним лицима да идентификују лица са којима је заказан састанак и да изврше утицај на њих у смислу прихватања сарадње. Сваки следећи сусрет би могао да буде катастрофалан за припадника обавештајног сектора пошто би информације које прикупља биле прецизно дозиране и пласиране од конкурентске обавештајне организације. Такви подаци би сопствени менаџмент довели у заблуду, а крајњи резултат би могао да проузрокује несагледиве последице за пословну организацију.
- *Пословном вечером* као методом прикупљања података делимично се превазилази проблем уочен у методи *пословног ручка*. Најефективнији облик пословне вечере је онај који се организује за породицу потенцијалне мете, на којој поред гостију присуствује искључиво породица домаћина. Реализацијом ове методе прикупљања података избегава се јавно излагање саговорника, а у приснијем амбијенту стварају се и услови за обавештајно деловање и на чланове породице. Често су се најважнији пословни подаци прикупљали управо преко супруге „оперативне мете“ која поседује информације о неком

догађају, а није довољно оспособљена да исте задржи у тајности. Важна је и улога супруге лица који прикупља информације, јер понекад од њених способности зависи оперативни успех целог догађаја. Пословна вечера дакле представља виши степен односа између лица које прикупља информације и носиоца тајних података, јер се подразумева да су лица досегла близак ниво комуникације и да се у будуће сусрете укључују и чланови породице обе стране. Ови односи могу да имају добре и лоше стране посматрано из угла обавештајног и контраобавештајног наступа. У ситуацијама када се пословна вечера организује за већи број лица присна комуникација губи на значају, пре свега због велике концентрације других лица која се на вечери налазе управо из истог разлога. У таквим ситуацијама циљ је да се успостави што више контаката са што је могуће већим бројем учесника догађаја у којима се процењују потенцијални извори података и лица са којима би се могли наставити будући сусрети. Веома је важно имати на уму да ниједна озбиљна информација не може да буде прикупљена ако је сарадња између два лица искључиво једносмерна, то јест ако у том разговору саговорнику немамо шта да понудимо, што је најчешће друга информација која представља предмет његовог интересовања. Шта „дати“ саговорнику представља задатак не само лица које води разговор већ и целог оперативног тима који је укључен у реализацију пословно–обавештајне активности.

- *Пријем* представља догађај који се организује од стране државних институција, мултинационалних компанија и других пословних субјеката приликом прославе државних празника, јубилеја, важних историјских датума, отварања нових радних јединица и слично. Карактеришу га велико бројно стање и скуп веће групе лица која на такве догађаје долазе из разних разлога, од обавештајног деловања до личних разлога чије би додатно појашњавање било сувишно. Пријем је углавном формалан и неискрен догађај који од учесника захтева висок ниво срдачности, расположења и учтивости, а све то у циљу остављања што јачег утиска на скуп и на лица која представљају предмет интересовања. Разговори су кратки, површни, без постављања сувишних питања, а најчешће су уопштени и потпуно небитни како за једну, тако и за другу страну. Понекад се и у таквим разговорима прикупљају

подаци и информације које потврђују претходну слику о неком лицу или догађају, што им даје одређену дозу корисности. Суштина ове методе прикупљања података представља могућност селекције и избора оперативно интересантних лица према којима би се у неком наредном периоду могао реализовати обавештајни наступ.

- *Протоколарна посета* пословном субјекту отвара могућност за прикупљање података, а примењује се најчешће у индустријским гранама. У саставу делегација које обављају ову врсту посета, укључују се лица обучена за прикупљање података који се реализују вођењем разговора са стручним особљем. У таквим разговорима настоји се да се прикупи што више информација о техничким решењима појединих производних склопова, производним капацитетима, тржишним условима за пласман производа, добављачима и купцима. Забележени су случајеви да су приликом протоколарних посета од стране обучених лица вршена тајна снимања и фотографисања интересантних производних решења која су касније примењивана и на сопственим производима. Такви случајеви су забележени и у војној индустрији.
- *Посета сајмовима, митинзима и изложбама* представља начин прикупљања података који обезбеђује присуство више пословних субјеката на једном месту. Прикупљају се прецизна сазнања о изложеним производима и услугама, који за јавност представљају најновија достигнућа тог пословног субјекта. Представници излагача су спремни да откривају техничке карактеристике неког производа, као и друге појединости са којима су упознати или за чије саопштавање имају сагласност менаџмента компаније. Иако је сајам јавна манифестација, вешт прикупљач информација може да прикупи и друге податке који су везани за пословање пословног субјекта, а односе се, на пример, на примања запослених, радно време, поштовање безбедносних процедура и остало што би могло да утиче на побољшање властитог положаја у пословном окружењу. У том смислу, врло су ефикасне посете војно–индустријског комплекса аеро–митинзима на којима високо развијене земље настоје да промовишу највећа достигнућа у области производње борбених авиона. Фотографисањем, разговорима са летачким и

инжењерским особљем, тежи се прикупљању што прецизнијих сазнања о ваздухоплову, података о његовим борбеним могућностима као и других техничких решења и унапређења. Лице које прикупља информације најчешће није у саставу званичних делегација, јер се у тим случајевима са лицима која пружају информације врши безбедносна припрема која прецизира шта сме, а шта не сме да се говори о ваздухоплову.

- *Претрага „web сајтова“* оперативно интересантних привредних субјеката и њихових конкурената, такође представља легалну методу прикупљања података, све док лице које прикупља информације не примени информатичке методе уласка у забрањену, такозвану сиву зону власника или корисника информација. Иако се ради о претрагама свима доступних сајтова, сазнања прикупљена на тај начин понекад служе за допуну прикупљених сазнања другим методама или за повезивање различитих догађаја.

Најчешће нелегалне или нелегитимне методе прикупљања података које се користе у оперативном раду су:

- *Плаћање посредника за прибављање информација* представља једну од најчешћих техника прикупљања података. Припрема за ову делатност подразумева селекцију лица из окружења која располажу информацијама интересантним за сопствени пословни субјект. Друга фаза је избор лица која би услед различитих разлога била спремна да достављају информације, с тим да је материјални фактор опредељујући у већини случајева. Следи стварање поверења и осећаја сигурности да неће бити откривена нити на било који начин бити злоупотребљена. Четврта фаза подразумева добро осмишљен и разрађен поступак примопредаје информација како би се посредник у потпуности заштитио, а супротној страни онемогућило његово откривање. Контрола посредника и стална едукација као и усмеравање представљају један од кључних фактора успеха пословно–обавештајног система. Подаци који се на овај начин обезбеђују морају бити од високог значаја, тачни и проверљиви. У зависности од важности информација, одређује се и висина материјалне награде за посредника. Дакле, у питању је класична трговина у којој посредник долази до информације у писаној или другој форми, предаје

је наручиоцу и за наведену активност добија одговарајући новац или другу врсту материјалне сатисфакције.

- *Поткупљивање државних функционера* или руководиоца мултинационалних компанија представља методу која у потпуности улази у такозвану црну или недозвољену зону прикупљања информација. Овом техником се прикупљају информације са највишег нивоа и имају недвосмислено највећу вредност, како за њиховог власника, тако и за онога ко покушава да их прибави. Ради се најповерљивијим подацима и информацијама од стратегијског и оперативног значаја, а прибављају се од лица која прихвате договорени облик сарадње. У међународној литератури таква лица се најчешће називају „кртице“ и то је термин усвојен и у домаћој стручној литератури. Ангажовати таква лица за своје потребе, тј. за потребе сопственог пословног субјекта, представља један од најтежих задатака лица из пословно–обавештајног система. Сама припрема и реализација ангажовања је сложена, дуга, осетљива и подразумева брижљиво планирање највишег тела обавештајног система. У том смислу, изучавају се навике потенцијалних извора података, њихов социјални и материјални статус, однос према основним људским вредностима као и према савременим друштвеним токовима. Сам чин ангажовања кртице се најчешће реализује у иностранству како би се избегло привлачење пажње служби безбедности земље домаћина. Мотив за прихватање пословног ангажмана најчешће је материјалне природе, међутим неретко се користе компромитација лица и уцена на сарадњу, чиме се такво лице присиљава да без своје воље прикупља осетљиве, строго поверљиве информације. Обавештајна делатност је строго санкционисана по законима земље домаћина и за то су прописане најстроже затворске казне, што од лица које планира и спроводи такву делатност захтева максималну професионалност и опрезност у обавештајном раду. У случају пословне шпијунаже неовлашћено уступање података из подруча пословања компаније је такође забрањено и санкционисано, како законским тако и нормативним актима тог пословног субјекта.
- *Разговор са отпуштеним или пребеглим кадровима пословног субјекта* представља методу прикупљања података мање рискантном у односу на

претходни метод будући да је могућност откривања саговорника искључена, осим у случајевима у којима је исти обавезан на чување пословних тајни. У појединим државним институцијама и компанијама запослена лица потписују писани документат који их обавезује на чување тајни и у случајевима када својевољно или услед отпуштања напусте тај пословни субјект или државну институцију. Према таквим лицима се, по потреби, примењују контраобавештајне мере служби безбедности и иста се налазе у одговарајућим документима као носиоци пословних тајни. Управо због тога, обавештајни систем предузима све мере како би разговор са таквим лицима организовао уз поштовање свих безбедносних процедура. Недостатак ове методе је неискреност саговорника, који, незадовољан својим статусом, износи једним делом тачне, а другим нетачне податке о пословном систему у којем је некад радио, кат–кад због пренаглашених емоција, а кат–кад ради причињавања што веће штете бившем послодавцу. Дакле, мотив за пристанак на сарадњу је материјалне природе, али и осветољубивост.

- *Откуп докумената* представља такође врло рискантну методу прикупљања информација. Њоме се подразумева да је лице које је пристало на пословну сарадњу, небитно из којих разлога и побуда, способно да изврши задатак, као и да поседује објективне и субјективне карактеристике за извршење повереног му задатка. Објективне карактеристике се односе на његов положај у друштву и пословном субјекту или институцији у којој се подаци налазе, док се субјективне карактеристике односе на његове личне способности као што су интелектуални ниво, оријентација у времену и простору, комуникативност и сл. Све набројане особине су потребне да би се такав задатак квалитетно извршио и да би тражени документат стигао у руке наручиоца, руководиоца пословно–обавештајног система, а преко њега до менаџмента компаније или државног руководства. Данас се често воде полемике о томе да се неки документи и разни подаци означени као „строго поверљиво", државна или пословна тајна налазе на интернету и да су тиме свима доступни, што јесте делимично тачно. Ипак, не треба заборавити на чињеницу да је за доношење најсложенијих одлука и даље потребно да такве информације буду обезбеђене у писаној форми са оригиналним потписом и

печатом циљане компаније или државне институције и да буду саопштене директно од носиоца тајних података („жив језик“). Сви остали подаци који се налазе у електронским и писаним медијима се сматрају делимично провереним, с обзиром на то да се понекад намерно пласирају како би се противник навео на погрешне закључке.

- *Разменом података са сродним службама* се обезбеђују подаци и информације које употпуњују претходно прикупљена сазнања другим методама. Сазнања добијена на тај начин се користе у циљу ажурирања безбедносних докумената стратегијског нивоа, међутим неретко се у билатералној сарадњи, у контакту са припадницима других пословно–обавештајних система прикупе и врло употребљиви оперативни подаци. У обавештајном и контраобавештајном раду понекад је потребно, да би мозаик био у потпуности сложен и попуњен, располагати информацијама до којих се долази на потпуно случајан и непланиран начин. Такви подаци за даваоца информација немају готово никакву вредност јер их сматра општепознатима, док за онога који их прикупља могу да представљају последњу коцкицу којом ће употпунити мозаик. У том контексту, контакти са припадницима других служби, размена пословних информација, заједничка едукација, учешће у заједничким активностима могу да дају оперативно интересантне резултате.

6.3. МЕТОДЕ АНАЛИЗА ПОТАДАКА И БЕЗБЕДНОСНА ПРОЦЕНА

Прикупљене податке пословно обавештајни субјект обрађује применом познатих метода и техника и тиме почиње анализа података која представља следећу фазу оперативног рада. Анализа поред тога што треба да одговори зашто је и у којој мери нека информација важна за пословни субјект, треба такође да одговори и на питање каква је пројекција будућих кретања догађаја на које се та информација односи. У анализи је садржано више информација о неком догађају које га ближе одређују, а поред

објективности и прогнозе будућих кретања, анализа би требала да понуди алтернативна решења као и да буде правовремена. Развојем ИКТ аналитичка делатност у пословно обавештајном систему је постала знатно употребљивија и систематичнија. Употребом наменских програмских апликација, аналитичка делатност је постала једноставнија, а за пословни менаџмент корисниј у процесу доношења одлука. Употребом графикона, хистограма и табеларним прегледима олакшава се увид у обрађене податке и врши се паралелна анализа добијених резултата, чиме се процес доношења одлука скраћује и квалитативно унапређује. Како би се сваки проблем сагледао из најширих углова и тиме створили услови за подношење квалитетног аналитичког извештаја, у саставу аналитичких тимова је неопходно ангажовање искуснијих кадрова из најразличитијих друштвених делатности. У овој фази рада се сублимирају, не само сазнања прикупљена непосредним обавештајним деловањем из скоријег временског периода, већ и сва остала сазнања која је аналитички тим до тада стекао, искуствено или едукацијом. Управо због тога је важно да аналитички тим буде састављен од људи различитог образовања, различитих животних искустава као и социјалног статуса. У обавештајно–пословној делатности се најчешће користе следеће врсте обавештајних анализа:

- *Складиштење података* (енгл. Data warehouse) — Инмон (Inmon) наводи да је „складиште података врста базе података унутар које су подаци сложени према функционалном подручју, садржајно непромењени након похрањивања, те конзистентно односно на доследан начин приказани" (Inmon, 2005: 9-10). Подаци у тој бази података су груписани по функционалним целинама (нпр. набавка) и приликом постављања упита од стране корисника програмског пакета, тај податак или више њих који се односе на захтевани упит, се аутоматски издвајају из базе података и користе за његове потребе. Ова врста аналитичке обраде представља најједноставнији облик анализе података јер захтева селекцију или разврставање и похрањивање, тј. складиштење. Подаци похрањени на овај начин се уз помоћ одговарајућих програмских апликација, као што је нпр. „Microsoft access", међусобно повезују по разним упитима и на тај начин се

обезбеђује њихова квалитетнија експлоатација. Број упита не треба да буде превелик јер би се тиме превише умањио опсег потенцијалних резултата. Најкомплекснија фаза ове врсте анализе података представља постављање квалитетних упита који треба да одговоре на захтеве менаџмента пословног субјекта. (Kimball & Ross, 2011)

- *Квалитет података* (енгл. Data quality) — према Јаворовићу и Биланџићу (2007: 248) представља фазу аналитичког процеса која подразумева да се прикупљени подаци похрањени у одговарајуће базе или складишта, обраде у смислу да се изврши селекција битних од небитних података, да се степенују по важности и да се врши перманентна процена њихове употребљивости. На тај начин се избегава беспотребно гомилање непотребних података који су некад имали, а сада немају употребну вредност, чиме се база растерећује, а кориснику података се такви подаци не презентују. Иако ова врста анализе података делује једноставно и не превише захтевно, врло је комплексна и сложена. Захтева пажљиву процену сваког податка и степеновање у зависности од његове вредности. У неким организацијама и институцијама се подаци, како би се избегло отицање тајних података, степенују највишим степеном тајности, што беспотребно оптерећује систем и његове кориснике, нарочито ако имамо на уму да се такви подаци штите посебним контраобавештајним мерама. Тачно је да један податак у неком моменту може да буде од изузетне важности за пословни субјект, а да већ следећи дан, сат, па чак и минут нема никакву употребну вредност. Стога је неопходно перманентно ажурирати прикупљена сазнања и процењивати њихову вредност, јер је то важно како за корисника тако и за конкуренцију која настоји да до таквих података дође. Да би се тајни подаци у потпуности заштитили, потребно је константно имати на уму врсте и облике угрожавања пословних информација, затим методе и технике прикупљања података путем којих конкурентски пословно обавештајни апарат настоји да дође до њих. Мере заштите се планирају у складу са наведеним елементима и константно се ажурирају у односу на актуелну безбедносну ситуацију. Документ којим су обухваћена сва претходно

прикупљена селектирана и актуелна сазнања о неком догађају или делатности назива се безбедносна процена.

- *Копање података* (енгл. Data mining) — представља аналитички метод који подразумева извлачење скривених података у актуелним и старим базама како би се на основу упоредне анализе извршила пројекција будућих кретања пословања пословног субјекта. Ради се углавном о скривеним подацима до којих се долази употребом аналитичких програма специјализованих за ову врсту аналитичког метода која подразумева да се подаци прикупљају аутоматизовано. (Јаворовић и Биланџић, 2007: 249)
- *„On – line аналитичка обрада"* (енгл. Online Analytical Processing — OLAP) — представља анализу која не врши верификацију хипотетичких узорака и релација како би се предвидело будуће понашање. „Копање" за разлику од ове аналитичке методе открива узорке и релације, а у циљу реализације исте намене.
- *„SWOT анализа"* (енгл. Strenghts, weaknesses, opportunities, threats analysis) — представља аналитички метод обраде података врло примењив у различитим друштвеним областима, од привреде, одбране, индустрије, политике итд. У питању је квалитативни аналитички метод који је први открио и дефинисао Кен Ендрју (Ken Andrews) у свом раду „The concept of corporate strategy" (1971). Ова метода се састоји у анализи унутрашњих и спољних фактора који утичу на пословање пословног субјекта. Фактори из унутрашњег окружења су способности (strenghts — S) и слабости (weaknesses — W), а фактори из спољњег окружења су могућности (opportunities — O) и претње (threats — T). Сваки од њих се посебно разрађује до најситинијих делова, а неке од њих ћемо навести:

Способности: финансијски капитал са којим пословни субјект располаже, технолошка опремљеност и оспособљеност, инфраструктурна покривеност, едукативна оспособљеност кадрова, образовање и прилагодљивост савременим условима менаџмента пословног субјекта, производни капацитети, развијеност маркетиншког сектора и сектора продаје, позиционираност на тржишту, иновативне способности.

Слабости: недовољно и непотпуно дефинисана стратегија деловања пословног субјекта, недовољна образованост запослених кадрова, недостатак вештина у пословним преговорима, лоша диверзификација производа, недовољна маркетиншка активност, застарео производни погон, застарео концепт производа, недовољна покривеност ИТ технологијама и другим средствима савремене комуникације.

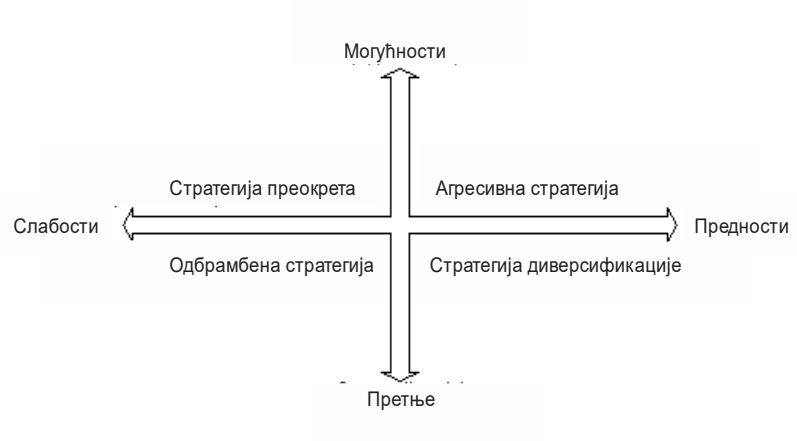
Могућности: слабости конкурента или противника, отварање нових тржишта и недовољна спремност конкурента да се прилагоди новонасталим тржишним променама, послован однос заснован на бази историјских пријатељских односа, приступање чланству у међународним организацијама и пласирање производа по повлашћеним условима, отварање представништава, деташмана, конзулата и других представништава као и производних капацитета у земљи домаћина, слаба монетарна политика конкурента.

Претње: улазак надмоћније конкуренције на тржиште, усвајање нових царинских стопа и прелевмана[41] од стране земље увоза, улазак извознице у организације и институције којима се ограничава пословање са другим пословним субјектима, незадовољство сопствених кадрова висином примања и условима рада, незадовољство купаца и потрошача квалитетом робе и услуга, демографске промене, захтеви за поштовањем нове законске регулативе и нова стандардизација.

[41] Посебна такса која се уводи да би се изједначиле цене увозне робе са ценама домаће робе. (http://www.kombeg.org.rs/Komora/udruzenja/UdruzenjeTrgovine.aspx?veza=3539, 2016, 13. фебруар)

Слика бр. 6: SWOT матрица
(http://www.businessstudynotes.com/wp-content/uploads/2015/10/What-is-SWOT-Analysis1.png, 2016, 13. Фебруар)

На основу анализе наведених елемената пословни субјект доноси одлуку о изабраној стратегији, а опције су приказане на слици:



Слика бр. 7: SWOT стратегије
(http://infosys3.elfak.ni.ac.rs/nastava/PrintOnePage.jsp?page=UUIS_predavanja_6, 2016, 13. фебруар)

SO стратегија је потенцијално најуспешнија, пошто пословни субјект њеном применом максимално користи своје предности и шансе будући да себе доводи у позицију да бира кораке које ће спроводити у следећим пословним активностима уместо да реагује на новонасталу ситуацију.

WO стратегија се примењује у ситуацијама када пословни субјект поседује повољне шансе за реализацију пословног циља, свестан својих слабости које настоји да отклони како би пословни ефекат подигао на највиши степен. У питању је развојна стратегија.

ST стратегија се примењује у ситуацијама када пословни субјект поседује способности за извршење задатка које настоји да одржи или унапреди у односу на спољње опасности које му прете и угрожавају пословну активност. Дакле, циљ је максимизовати сопствене способности како би се потенцијалне претње свеле на прихватљив ниво.

WT стратегија представља одбрамбени облик стратегије када је привредни субјект свестан сопствених слабости са којима се суочава и покушава да их минимизира еквивалентно претњама којима је изложен од стране спољних утицаја. (Pickton & Wright, 1998: 101-109)

- *Анализа сценарија* (енгл. Scenario analysis) је најпре почела да се примењује у војној терминологији и за потребе војних операција. Ова техника омогућава да се на основу описа постојећег стања изврши прогноза будућег алтернативног развоја ситуације. У војној терминологији се често користи термин „рано упозорење“ што одређује о каквом се аналитичком методу ради. На основу предвиђања могућег тока нежељеног догађаја израђују се планови којима се спречавају штетне последице по пословни субјект. Овај аналитички метод почео се примењивати у привреди 60–их година, а подразумева примену неколико фаза (према Heijden van der, 1997): идентификација кључних догађаја из окружења који одређују будуће догађаје (политички, економски и сл.); идентификација појединачних догађаја који одређују будуће догађаје са тежиштем на идентификацији неизбежних догађаја; идентификација кључних догађаја који утичу на безбедност пословног субјекта и степеновање таквих догађаја у складу са потенцијалним степеном угрожавања; развој оквирних планова могућих сценарија догађаја; процена импликација сваког сценарија — најчешће се врши избор три највероватнија могућа сценарија од којих се изабере један, надзор након примене изабраног сценарија, допуна најновијим подацима и прилагођавање новим условима.
- *Стратегијски систем раног упозорења* (енгл. Strategic early warning system — SEWS) има за циљ да идентификује појаве и ситуације које могу да делују на интересе пословног субјекта у што је могуће ранијој фази. Менаџмент у том случају мора да располаже са правим информацијама у

право време јер је једино тако могуће отклонити опасност у највећој могућој мери. За разлику од претходног аналитичког метода, стратегијски систем раног упозорења обухвата следеће фазе (према Bernhardt, 2003): идентификација кључних обавештајних тачака; развој могућих догађаја; идентификација и прављење листе индикатора које је потребно надзирати; израда планова за надзор и прикупљање података. Дакле, овде је тежиште на дефинисању тачних индикатора који указују да је безбедносна ситуација усмерена према пословном субјекту промењена и да ће пословни субјект, с великим степеном вероватноће, бити угрожен. Како ниједан аналитички метод није непогрешив, претходно поменуто никако не умањује његов значај.

- *GAP анализа* (енгл. Gap — празнина, јаз) представља квалитативну анализу у чијем је средишту потрошач и задовољавање његових потреба (Јаворовић и Биланџић, 2007: 257). Суштина је да се добије одговор на питање да ли одређени производ задовољава потребе тржишта (каквог је квалитета, каква му је употребљивост и примењивост, задовољство потрошача производом, разлози куповине и постпродајне услуге и анализе).
- *PEST анализа* (енгл. Political, Economic, Sociokultural, Technological) се бави разумевањем окружења пословног субјекта чиме се стиче увид у пословне могућности, а претње се настоје минимизовати. Тиме се избегава предузимање погрешних корака у пословању и олакшава доношење квалитетних пословних одлука. Наведени аналитички метод подразумева анализу следећих елемената:

А) унутрашње окружење — финансијски капитал, кадрови, опремљеност ИТ технологијама, приходи запослених;

Б) спољно микроокружење — конкуренти, добављачи, купци, потрошачи, дистрибуција, производња;

Ц) спољно макроокружење — политички, економски, социолошки, технолошки фактори који представљају тежишни елемент за успешно разумевање PEST анализе. Политичким факторима се сматрају: законска регулатива земље домаћина са којом се реализује пословна активност, правне норме које регулишу права и обавезе настале из радног односа,

будући прописи, стабилност државних институција и доследност спровођења прописаних законских норми, лобирање, ратови и етнички сукоби, етика пословања, чланство у регионалним и међународним организацијама. Под економским факторима се подразумева: трендови у светској економији, тржишни циклуси, стопа незапослености, друштвени бруто производ, монетарна политика, стабилност домаће валуте, висина инфлације, економска политика Владе, пореска политика, сезонска кретања и сл. Социокултурним (друштвеним) факторима се сматрају: демографска структура становништва, степен образовања, религијска структура, слободно време, полна структура и заступљеност у друштвено политичком животу, животни век, однос према животној средини, имиџ производа, животни трендови, реклама и публицитет, медијска права, информисаност. Технолошки фактори треба да одговоре на питање да ли примена напредних технологија омогућава иновације у пословању и да ли и у ком обиму утиче на квалитет производа, његову дистрибуцију или комуникацију са клијентима.

За разлику од SWOT анализе, PEST анализира тржиште или већи број тржишта и њихове пословне могућности. SWOT анализа се односи на пословну јединицу или пословну идеју. Под њима подразумевамо елементе као што су: застарелост производних капацитета, механизми куповине, интелектуални капитал, глобална комуникација. (Гонан Божац, 2008: 19–34)

У склопу даљег разматрања безбедног пословања пословног субјекта и превенције нежељених догађаја исти врши процену безбедности штићеног објекта. О томе колики степен заштите ће бити примењен зависи од његовог значаја и степена угрожености. Проценом су обухваћени сви познати фактори који утичу или могу да утичу на безбедност пословног субјекта. На основу постојећег стања и прикупљених сазнања о објекту и његовом окружењу, прогнозирају се будући токови кретања догађаја који могу да утичу на његову безбедност, безбедност информација које се у њему чувају као и безбедност запослених лица. У изради процене безбедности битно је придржавати се неколико основних принципа: објективности, прецизности и проверљивости како би се стекла објективна слика о достигнутом степену безбедности пословног субјекта.

Сама реализација процене спроводи се кроз неколико фаза. У првој фази, на основу расположивих информација и сазнања, анализира се постојеће стање неком од претходно наведених метода. То подразумева прикупљање података о простору на којем се пословни субјект налази, објектима са којима располаже, материјалним и техничким средствима у употреби и осталим подацима од значаја за процену безбедности. Подаци морају бити прецизни, јасни и објективни. То подразумева детаљан обилазак објекта, уочавање најситнијих детаља који могу да утичу на његову безбедност као што је стање жичане ограде, важећи и алтернативни улази у круг објекта, прозори и врата којима се може приступити објекту, квалитет кровног покривача и други фактори који омогућавају физички приступ од стране неовлашћених лица. Следећа фаза представља прикупљање података о запосленима (образовна структура, социјални статус, материјални статус, криминалне склоности, склоност ка девијантном понашању и пороцима, везе са сумњивим лицима на територији и у конкурентским пословним субјектима). Ниво проверавања зависи од функције на којој се проверавано лице налази. Следећа фаза представља дефинисање безбедносних процедура запослених код пословног субјекта које подразумевају: поступање са документима, рад на рачунару, руковање новцем и другим материјалним средствима, протокол приликом успостављања пословних контаката са странцима, долазак и одлазак са радног места, употреба приватних рачунара и преносних меморија за службене потребе). У наредној фази се поновно врши детаљна анализа свих прикупљених података у циљу прецизног дефинисања критичних тачака које је потребно заштитити применом мера безбедносне заштите. Безбедносна процена је континуиран процес који се стално мења и допуњује новим сазнањима од значаја за пословну активност пословног субјекта.

У циљу израде квалитетне безбедносне процене потребно је обухватити више фактора који у већој или мањој мери утичу на безбедност пословног субјекта (према Д.Т.):

- Макролокација — безбедносна ситуација на територији на којој се пословни субјект налази и на којој исти спроводи своју пословну активност;

- Микролокација — непосредна локација привредног субјекта и његова околина;
- Објекти којима пословни субјект располаже са свим њиховим карактеристикама и специфичностима;
- Просторије и објекти од посебног значаја;
- Распоред инсталација унутар и у непосредној околини објекта (водовод, грејање, електрична енергија, гас);
- Запослена лица (број, образовна структура, социјални статус, национална структура итд);
- Протокол са странкама;
- Протокол са страним партнерима;
- Процедуре у вези чувања докумената;
- Руковање новцем и другим драгоценостима;
- Пријем робе и потрошног материјала;
- Стање у служби физичко–техничке заштите (попуњеност, кадровска структура, оспособљеност за обављање дужности);
- Поступак у ванредним ситуацијама (пожар, поплава, земљотрес, терористички напад).

6.4. ОБЛАСТИ ОБАВЕШТАЈНОГ РАДА

Односи у савременом свету су изузетно сложени у свим областима људског живота, па самим тим и у пословним активностима. Нови односи захтевају потпуно редефинисање обавештајне делатности и организационе промене обавештајних институција, које у најсложенијим условима морају да пруже подршку процесу одлучивања. Проблем савременог света је непостојање међународних механизама и институција које човеку и пословном субјекту гарантују апсолутну безбедност у њиховом окружењу. Дакле, апсолутна безбедност и идеални услови не постоје ни у једној јединој сфери људске делатности (политичкој, привредној, одбрамбеној, друштвеној)

што наглашава додатну потребу развоја обавештајних институција. Ако се притом узме у обзир наглашена динамика и убрзане промене са којима се свет данас суочава, може да се схвати значај обавештајних институција у процесу доношења пословних одлука пословног менаџмента и државног руководства.

6.4.1. Политика и одбрана

„Стратегија преживљавања и економске експанзије малог народа (државе) се не може приписати величини њене оружане силе, бројности популације и величини територије, већ савршеној организованости њених обавештајно–безбедносних служби, као базе економских, дипломатских и војних активности.“ (Петковић, 2009: 87)

Почеци шпијунаже, као што је већ наведено, јављају се појавом војне шпијунаже. Војна шпијунажа је облик обавештајне делатности који је претеча свих других облика обавештајног рада, тј. други облици шпијунаже су били подређени потребама војне шпијунаже. Задаци војне шпијунаже су били војни производни капацитети и технолошка достигнућа у области одбране.

Држава је стајала иза свих облика шпијунаже и организовала је рад обавештајне службе тако што је покривала све области интересовања. Тек педесетих година прошлог века, долази до раздвајања војне шпијунаже од пословне шпијунаже која више није ексклузивни апарат руководства националних држава, већ постаје и апарат менаџмента пословних компанија. Пословне компаније оснивају специјализоване институције које се баве пословном обавештајном делатношћу и пословном шпијунажом као облицима свеукупне обавештајне делатности.

Војна индустрија данас представља један од основних привредних потенцијала развоја највећих светских држава. Могућност једне земље у производњи оружја не састоји се у томе шта она тренутно производи, коју врсту оружја и у којим количинама, већ у томе колико је њена индустрија способна да се преоријентише на ратну производњу. На тај начин се кроз

мирнодопску производњу оцењује и снага те земље, односно снага њене привреде и индустрије за производњу, утврђују њене људске, материјалне и техничке резерве, сировинска база и зависност у производњи од других земаља.

Извоз наоружања и војне опреме је уносан бизнис и чинилац посебно са аспекта попуне буџета националних држава. У том смислу, високо развијене државе воде непрекидну борбу око развоја софистицираног оружја и оруђа стратешког и тактичког нивоа, применом најновијих научних достигнућа и најсавременијих технологија, које постају предмет интересовања противникових обавештајних служби. Прибављањем развојних планова и најсавременијих техничких решења обавештајним деловањем, смањују се реални трошкови увођења новог производа на тржиште и омогућавају конкурентској страни продају по нижим ценама коштања или стварање већег профита у односу на војну индустрију која га је иновирала и развијала годинама уназад трошећи огромна новчана средства на разне врсте научних истраживања.

Раздвојити систем одбране од политичког система националне државе је врло тешко и непотребно, посебно због чињенице да одбрана представља сегмент политичког система државе. Обавештајне службе често у свом раду користе појединце из политике како би дошли до поузданих података о одбрамбеним потенцијалима националне државе или о војно–индустријским капацитетима. Неретко се догађа да припадници обавештајно–безбедносних служби постану извори података супарничкој страни чиме озбиљно угрожавају систем одбране матичне државе. Такви случајеви померају обавештајни рад из области одбране у област политике које се међусобно преплићу, а међу њима је тешко повући прецизну границу раздвајања. Подаци прикупљени на тај начин користе се у сврху процене политичке ситуације у држави, степена поштовања људских права у тим државама, поштовања законских обавеза и норми, стања медија, а све у циљу да би се извршила њена дестабилизација од стране непријатеља и створили услови за изградњу система који у сваком делу може да буде рањив по свим елементима. Подаци који се том приликом прикупљају ангажовањем

обавештајних служби пажљиво се проучавају, анализирају и достављају руководећим структурама које доносе кључне одлуке важне са аспекта безбедности сопствене националне државе и за наступ према другим државама за које сматрају да могу да угрозе њихове националне интересе. Сведоци смо догађаја да су поједине државе богате природним потенцијалима биле означене као потенцијални извори угрожавања безбедности највећих светских сила и свеукупног мира у свету, што је био повод за њихову војну интервенцију, насилну смену постојећег владајућег режима и довођење власти која ће поштовати „демократичност“ и међународна права и обавезе које се односе на употребу силе у случају рата. Такве војне интервенције се пажљиво планирају, обавештајне службе прикупљају податке који треба да обезбеде гаранцију да ће интервенција бити реализована са минималним или прихватљивим губицима. Дакле, обавештајни рад у области политике је најшири облик обавештајног деловања који се спроводи кроз легалне институције као што су дипломатско–конзуларна представништва националних држава и кроз рад обавештајних служби које, ангажовањем извора података у државама за које испоље интересовање и коришћењем јавних података, креирају политику ка тој држави, региону и целокупну међународну политику.

6.4.2. Привреда

Преплитање и прожимање политике, одбране и привреде националних држава је видљиво у дисциплини економске дипломатије која се кроз своје деловање користи готово идентичним методама и техникама прикупљања података као и класичне обавештајне службе. Циљ њиховог деловања је заштита националних интереса у међународним економским односима. Функције економског дипломате су веома важне и дају одговор на питање зашто је економска дипломатија значајна за свеукупан економски развој једне националне државе. Оне су представљене на следећи начин (према Првуловић, 2010: 15–18):

- Обезбеђење најповољнијих услова у трговини и другим формама економског повезивања и сарадње са страним државама и њиховим привредним субјектима;
- Утицај на успостављање мера стимулисања извоза домаћих роба и контрола промета капитала у склопу укупних развојних циљева и стратегије економског наступа земље у иностранству;
- Систематска анализа прилика на међународном тржишту и економским односима, анализа економског положаја и карактеристика страних земаља, њихових компаративних предности и могућности, као и конјуктурних тенденција на међународној економској сцени;
- Успостављање и неговање економских и пословних контаката са пословним и предузетничким круговима и надлежним ресорима земље пријема;
- Вођење билатералних и мултилатералних економских (трговинских, пословних, технолошких и др.) преговора;
- Припрема, учешће у изради и конципирање економских конвенција и споразума у међународној (билатералној и мултилатералној) економској сарадњи;
- Учешће у статусу експерта у раду међународних економских и других институција и организација;
- Стварање повољних пословних прилика за наступ привредних субјеката сопствене земље у иностранству.

Раичевић економску дипломатију дефинише на следећи начин: „Економска дипломатија обухвата коришћење дипломатских механизама и метода, у садејству са стратешким, спољноекономским циљевима и инструментима њихове операционализације од стране државе, у билатералним или мултилатералним токовима међународне економске сарадње, као и на домаћем привредном простору, а у циљу активног подржавања развоја националне економије и обезбеђивања спољноекономских интереса, позиционирања и непосредне подршке матичним привредним субјектима у међународном пословању (што обухвата

постизање политичких и других циљева у оквиру спољнополитичке стратегије конкретне државе на одређеним географским и политичким просторима или уопште у свету)“. (Првуловић, 2010: 18)

Евидентна је веза привреде једне земље и спољнополитичких интереса који се спроводе кроз активност економске дипломатије. Свакако да ће подаци прикупљени радом економског дипломате, а не односе се на економију, привреду или индустрију, бити искоришћени од стране руководства те државе у свеукупним спољнотрговинским активностима биле оне политичког, војног или привредног карактера.

Привредни развој и усвајање законских и других нормативних стандарда којима се стичу услови за приступање међународним организацијама као што је ЕУ, приступ новим тржиштима и развој производних и тржишних капацитета, представљају основ за анализу степена безбедности националних држава које имају амбиције да уђу у ЕУ. Унутрашња безбедност представља најважнији задатак Влада свих држава, што је могуће постићи искључиво развојем привреде, социјалне и монетарне политике. Приступ међународним организацијама гарантује чланицама већи степен спољне и унутрашње безбедности, али исто тако, с обзиром на либералност прекограничних процедура, ствара услове за лакше повезивање и кретање организованих криминалних група које се баве трговином наркотицима, трговином људима, као и терористичких организација. Задатак националних Влада је да дефинишу колико ће држава у таквим интеграционим процесима имати користи, а колико штете и у складу са тим да донесу одлуке и да примењују мере како би се усаглашени циљеви спровели у што краћем временском року.

Суштина успеха привредних субјеката, а самим тим спровођења пословно–обавештајне делатности и економске шпијунаже као њеног сегмента, састоји се у остваривању профита. Управо у неопходности да се задрже стечене конкурентске предности (и евентуално стекну нове) у дужем временском периоду, почива потреба и оправдање за стратегијским приступом у управљању привредним субјектима. Имајући ту чињеницу у

виду, сваки привредни субјект требало би да води континуирану борбу за побољшање конкурентске стратегије.

Према мишљењу М. Е. Портера (M. E. Porter) постоје три основне стратегијске опције, односно три генеричке конкурентске стратегије које привредни субјект може изабрати како би се изборио за своју стратегијску конкурентност:

- Стратегија вођства у трошковима (енгл. overallcostleadership),
- Стратегија диференцирања *(*енгл. differentiation) и
- Стратегија фокусирања (енгл. focus).

Привредни субјект који конкурише на глобалном нивоу може да се одлучи за ону стратегију која му највише одговара, правећи сопствену комбинацију основних стратегијских опција. Тако одређене активности може обављати у једној земљи, тј. у централи, а друге активности може обављати са нижим или вишим степеном координације. Такође, првобитно успостављена стратегија се може мењати у правцу који одговара. Различитости у међународној стратегији у односу на стратегију фокусирану на домаћу привреду, утичу и на разлике у прикупљању и анализи информација преко ИКС, што значи да ИКС једне компаније која послује и конкурише на глобалном плану треба да буде прилагођен одређеној географској дистрибуцији својих активности. Он би требало да буде, да се тако изразимо, подршка активностима глобално присутног предузећа. (Радун, 2008)

У погледу дефинисања основних конститутивних елемената конкурентске стратегије у теорији менаџмента постоје дилеме и разилажења, те се може говорити о три модела конкурентске стратегије:

- Први правац ослања се на теорије конкурентске стратегије које су изведене из привредне, гранске организације;
- Други правац мишљења чини скуп теорија фокусираних на специфичне ресурсе и компетенције којима је привредни субјект опремљен.

- Трећи теоријски приступ, који се постепено искристалисао у последњој деценији прошлог века, полазећи од непотпуности оба теоријска правца, указује на нужност синтетичког обухвата.

У складу са тим, обавештајни ресурси конкурентских привредних субјеката, који се ангажују на прикупљању осетљивих информација, такође су у обавези да прилагођавају сопствене стратегије новонасталим условима и окружењу, што чини сложен и непрекидан процес узрочно–последичних веза и поступака.

Велика Британија је прва држава која је у 19. веку почела да спроводи обавештајне активности у привреди. До тада је класична шпијунажа, која се слободно може назвати војном будући да се у највећем проценту користила у војне сврхе, била на индиректан начин коришћена и за прикупљање података о привредним активностима једне државе или конкурентског привредног субјекта. Методе и технике које су употребљиване за прикупљање информација значајних за развој сопствене привредне делатности биле су идентичне онима које су коришћене у класичним обавештајним активностима. Такве информације су најчешће биле „нус производ“ класичног обавештајног деловања усмереног на прикупљање података о намерама и активностима непријатеља. (Петковић, 2009)

У циљу бољег позиционирања на тржишту и квалитетнијег одлучивања, поједине земље у оквиру државних институција развијају своје обавештајно–безбедносне активности. Тако је у Јапану формиран JETRO (енгл. *Japan External Trade Organization*) који делује у оквиру Министарства за спољну трговину и индустрију. У САД–у су такве активности поверене организацији под називом NEC (енгл. *National economic concil*). (Петковић, 2009: 195) Иако су активности владиних агенција усмерене на побољшање положаја домаћих компанија на светском тржишту и њиховој заштити на домаћем, све је присутније оснивање таквих и сличних агенција које своје активности спроводе у оквиру самих компанија. У сарадњи са државним службама, земље домаћина такве агенције сузбијају, пресецају и превентивно делују на криминалне активности лица запослених у компанији и друге недозвољене активности које гарантују заштиту тајности података. Данас је

тешко одвојити зависност унутрашње безбедности државе од привредне, финансијске и других врста безбедности. Такође, све је теже направити јасну дистанцу између унутрашње безбедности националних држава и међународне безбедности, посебно у условима када је криминал премашио државне границе и када све више употребљавамо термине *међународна трговина наркотицима*, *међународни тероризам* и *међународна трговина људима.*

Предмет интересовања нису отворене и „сиве“ информације до којих се може доћи легалним или полулегалним методама прикупљања података, већ тајне информације које се прикупљају нелегалним методама, као што је инфилтрација припадника или лица блиских њима у пословну организацију, куповином информација или продором у забрањену зону путем интернет мрежа. Такве информације се штите контраобавештајним ресурсима компаније која представља мету, а многе од тих активности су забрањене од стране државе домаћина и у неким случајевима имају обележја кривичног дела шпијунаже.

Шири појмови од *економске* и *индустријске шпијунаже* су *пословна шпијунажа* и *пословно–обавештајна делатност* и њих је потребно додатно објаснити ради лакшег разумевања проблема. Озбиљнији развој пословно обавештајне делатности и пословне шпијунаже јавља се после Другог светског рата, када долази до јачања привредних активности у светским размерама. У почетку се за обавештајне активности у привреди усваја појам ”competetive intelligence“ који се дефинише као обавештајна делатност, односно процес прикупљања података легалним средствима (из јавних — отворених извора) обраде тих података, те израде анализа које служе при доношењу одлука у пословним субјектима везано за укупну тржишну конкуренцију, конкретне конкуренте на тржишту као и конкурентност пословног субјекта који спроводи пословну активност. (Combs & Moorhead, 1993) Каханер (Kahaner) сматра да је „competetive intelligence” системски програм за прикупљање и анализу информација о активностима конкурената и општим пословним развојним смеровима, који се спроводи да би се остварили циљеви властите компаније. Он даље објашњава да суштина

„competetive intelligence" нису саме информације него обавештајна активност са анализама и закључцима на основу којих се доносе одлуке. Аутори се слажу у томе да основни циљеви ове делатности могу бити подељени у следеће категорије (према Kahaner, 1996: 16–21):

- Открити претње усмерене према пословном субјекту од стране конкурента;
- Елиминисати или бар ублажити потенцијална изненађења која прете од конкурената;
- Смањити време потребно за реакцију;
- Тражити нове погодности за развој сопственог пословног субјекта.

Крајем осамдесетих година поједини аутори као што су Драјзнер (Dresner) и Дедијер (Dedijer) уводе појам „business intelligence" који је шири и свеобухватнији од појма „competetive intelligence". Биланџић наводи да је „business intelligence" (пословно–обавештајна делатност) обавештајна активност у пословном свету коју планирају, организују и спроводе пословни субјекти, при чему та активност подразумева процес легалног прикупљања јавних и свима доступних података етичким средствима, њихову анализу и претварање у готове пословно–обавештајне анализе (знање) ради пружања подршке вођама пословног субјекта, са циљем доношења и реализације што квалитетнијих пословних одлука усмерених ка очувању постојеће позиције пословног субјекта у пословном окружењу, избегавања било каквих претњи и утицања на укупан квалитативан напредак пословног субјекта. (Јаворовић и Биланџић, 2007: 205)

Обавештајна делатност не мора да буде нужно забрањена. Међутим, шпијунажа представља строго илегалну делатност, без обзира ко је покреће, организује, финансира или спроводи. Шпијунажа се спроводи у различитим друштвеним областима као што је привреда, политика и одбрана. Често се шпијунажа спроводи у склопу укупне обавештајне делатности обавештајно–безбедносних служби једне националне државе, а подаци се уступају државним институцијама надлежним за привредну активност те државе.

Из наведеног се може закључити да је тешко направити стриктну поделу између набројаних врста шпијунаже и обавештајног интересовања јер се добијени резултати шпијунских активности међусобно преплићу, па је, самим тим, поље делатности обавештајних служби много шире и обухватније.[42]

Основна разлика између пословно–обавештајне делатности и пословне шпијунаже односи се на јавност и на легитимитет. Док је пословно–обавештајна делатност јавна и легална, пословна шпијунажа је тајна и нелегална. Иако државне обавештајне институције у свом раду примењују нелегалне активности и баве се шпијунажом не могу се сматрати нелегалним и противзаконитим, пошто су оне основане од стране надлежних државних институција и своје активности спроводе у складу са одредбама националног законодавства. Међутим, предмет њиховог интересовања су тајни подаци који се од стране других националних држава или институција штите законским мерама.

Могло би се рећи да пословна шпијунажа и пословно–обавештајна делатност представљају финансијски рентабилне делатности јер позитивно утичу на буџетске приходе националне државе. Обавештајна делатност у циљу доласка до иновација представља уштеду за матичну државу, јер се тиме избегава плаћање лиценце земљи домаћина, а уз то избегавају се и трошкови развојних пројеката, маркетиншких активности, као и трошкови портфолиа. У том смислу, а у циљу спровођења пословне шпијунаже, обавештајне службе и посебне целине привредних субјеката, прикупљају сазнања која се односе на цене коштања неког производа, висину зарада запослених, посебно стручни кадар, на потенцијале домаћег тржишта и потражњу за одређеним производима. Све те активности се спроводе у циљу преузимања тржишта и пласирања конкурентских производа, као и евентуалног покретања производње коришћењем искустава и сазнања добијених обавештајним деловањем.

[42] Према проценама ЦИА у демократским државама се релативно мало информација налази у статусу тајних података, док у недемократским државама тајне информације чине између 10 и 20 % укупног броја информација. (Вукадиновић, 1994: 205)

7. КОНТРАОБАВЕШТАЈНА ЗАШТИТА ПОСЛОВНИХ ИНФОРМАЦИЈА

Заштита пословних субјеката, посебно ИКС–а које они употребљавају, захтева стратешки приступ проблему, посебно због чињенице да су део тих система данас државне установе, агенције и службе које представљају критичну инфраструктуру једне државе. При томе, треба имати у виду да ИКС не чине само технички уређаји који се користе у обради и преносу података, већ и људи који га користе као и простор и време у којем се информације обрађују и анализирају. Незаштићен или слабо заштићен ИКС постаје могућа мета разних интересних сфера, од деструктивних организација и појединаца до страних обавештајних служби које настоје доћи до тајних информација. Критична инфраструктура је различито дефинисана и одређена у свету.

„Критична инфраструктура и основни ресурси су појам који се односи на широк опсег различитих средстава и имовине који су неопходни за свакодневно функционисање друштвених, економских, политичких и културних система у Сједињеним Америчким Државама. Било какав прекид у елементима критичне инфраструктуре представља озбиљну претњу за правилно функционисање ових система и може довести до оштећења имовине, људских жртава и значајних економских губитака.” (Murray, 2012) У ЕУ „критична инфраструктура представља имовину, систем или његов део који се налази на територији земље чланице и који је неопходан за одржавање кључних друштвених функција, здравства, безбедности, сигурности, економског или социјалног благостања, а чије би ометање или

уништење имало значајан утицај на земљу чланицу" (Council Directive 2008/114/EC of 8 Decembar 2008, 345-375).

Европска комисија дефинише следеће области критичне инфраструктуре: енергија, информационе и комуникационе технологије, вода, храна, финансије, грађанске власти, јавни и правни поредак и сигурност, саобраћај, хемијска и нуклеарна постројења, космос и научно истраживање.

Недовољно регулисан правни оквир у коришћењу и пласирању информација путем интернета доводи до ефекта потпуне дезоријентације у информатичком простору. Просечног пословног корисника мреже обиље информација и дезинформација доводи у заблуду и може да представља потенцијалну претњу по безбедност компаније, али и по његову личну безбедност. Са друге стране, безбедност пословања је угрожена стављањем профита у центар пословног интереса, а недовољним вођењем рачуна о повратним спрегама производа и услуга на безбедност пословних субјеката. Дефинисани проблеми намећу потребу изградње организационих целина које се баве заштитом грађана, заједница и националних интереса, супротстављајући се злонамерним утицајима појединаца и група, и подизањем њихове безбедности на потребан ниво.

У домену све интензивније употребе услуга интернета, многа права се међусобно сукобљавају и ограничавају. На пример, право на слободу изражавања ограничава могућност да се примени право на заштиту од недозвољених и штетних садржаја. Разлози ограничавања који се најчешће истичу у националним правима и бројним међународним актима могу се груписати у четири категорије (према Дракулић и Дракулић, 2010):

1. јавни поредак, национална безбедност, информациона сигурност;
2. економска сигурност;
3. вођење судских поступака (кривичних, прекршајних);
4. сигурност и заштита права појединаца (заштита одређених категорија, нарочито деце и малолетника, заштита угледа и људског достојанства, поштовање интелектуалне својине, поштовање других облика својине и сл).

Заштита података представља скуп међусобно повезаних активности, метода, техника и норми, којима се обезбеђује приватност, сигурност, поверљивост и интегритет података од свих опасности које им прете. Сигурност треба да обезбеди податке од њиховог случајног и намерног откривања неовлашћеним корисницима или заштиту од неовлашћеног мењања, брисања и коришћења од стране неовлашћених корисника. Поверљивост подразумева да се подаци не смеју открити од стране неауторизованих појединаца и других ентитета или у неовлашћеним процесима. Расположивост подразумева да само одређени корисник може доћи до одређених података без баријера и ограничења. Интегритет се односи на изворе и тачност и подразумева забрану неауторизованог мењања података и њиховог уништавања. (Урошевић, 2014: 95)

7.1. ЗАШТИТА ПРАВА НА ПРИВАТНОСТ ПОЈЕДИНЦА

Нагли развој ИКТ у пословној и личној употреби је довео до одређених проблема који се односе на приватност појединца. Из тог разлога је потребно јасно и прецизно утврдити правила која дефинишу приступ индивидуалној сфери информација и на тај начин заштитити појединца од дефинисаних облика угрожавања. Такође је неопходно перманентно усвајати и допуњавати казнене одредбе којима се обезбеђује поштовање прописаних правила и процедура које се односе на заштиту приватности грађана.

Приватност, у најширем смислу, представља могућност и право појединца или групе да се осами и да не приказује одређене податке о себи. Приватност се појављује као вишезначна категорија: као право појединца и као приватност корисника. Приватност корисника обухвата: информације за укључивање одређеног терминала у систем, приватност говора, приватност података, приватност корисникове локације, приватност корисникове идентификације, приватност посебних начина укључивања и приватност његових финансијских трансакција. (Дракулић, 1996: 57)

Интернет је данас препун сајтова на којима се захтева остављање личних података у циљу наводних анкетних истраживања и маркетиншких промоција о неком производу или некој услужној делатности. Такви подаци, без знања и одобрења лица која у наведеним активностима учествују, могу да буду злоупотребљени и објављени без њихове сагласности, што пружа могућност њиховог угрожавања од стране злонамерних лица и организација.

Развојем науке и технике, нарочито ИКТ–а, приватност добија нову димензију. Аутори препознају нови концепт приватности — информациону приватност, коју посматрају као право појединца да контролише који подаци о њему могу постати доступни другима, коме и на који начин. Право на информациону приватност обухвата (према Дракулић, 1996: 64–65):

- Право на обавештеност, то јест, право појединца да буде упознат који се подаци о њему прикупљају, обрађују и чувају, за које сврхе и од стране кога се користе;
- Право на одговарајуће коришћење података;
- Право приступа и увида (право контроле);
- Право исправке;
- Право на правна средства.

Хипотетички би се могло рећи да основну меру заштите спроводи сам појединац тако што не попуњава анкете у којима се захтевају лични подаци, осим у случају проверених и познатих сајтова. Међутим, природа интернета и глобалних информационих система је таква да се без знања и сагласности неког субјекта могу о њему прикупљати значајни подаци. Сходно томе, изложеност личних и пословних података треба да се сведе на најмању могућу меру. (Ђорђевић, 2007: 151)

Један од актуелних проблема са којима се срећу грађани Републике Србије је употреба биометријских система у издавању личних докумената. Сведоци смо наговештаја да ће се на биометријским медијима чувати лични подаци који се односе, између осталог, и на медицинску документацију, навике, склоности и остали подаци који би у погрешним рукама могли да угрозе безбедност појединаца. Таква настојања свакако имају оправдање у научним круговима јер су утемељена на искуствима која доказују колико је

важно располагати правим информацијама у право време, посебно у ситуацијама у којима је угрожен људски живот или у ситуацијама које захтевају доношење брзих одлука. Међутим, такве информације морају бити заштићене највишим мерилима заштите података о личности, јер би могле да буду злоупотребљене, а крајњи ефекат и резултати контрапродуктивни. Подаци сублимирани на овај начин постају део информационог система, у поменутом случају информационог система здравствене заштите, што подразумева примену општих и посебних мера заштите.

У том смислу потребно је извршити идентификацију информатичких средстава које је потребно заштитити, а то подразумева (према Ђорђевић, 2007: 152):

- опис потребних карактеристика безбедносне архитектуре информационог система;
- идентификација облика угрожавања и опасности по информације;
- рангирање опасности по значају и могућој штети коју може да изазове;
- пројектовање решења којима се ризик и последице своде на минимум;
- спецификација имплементационих препорука.

Конвенција о заштити људских права и основних слобода (енгл. Convention of protection of human rights and fundamental freedoms) је документ Савета Европе који дефинише заштиту приватности. Чланови који се директно односе на заштиту приватности гласе:

- „Свако има право на поштовање свог приватног и породичног живота, дома и преписке“;
- „Јавне власти неће се мешати у вршење овога права сем ако то није у складу са законом и неопходно у демократском друштву у интересу националне безбедности, јавне безбедности или економске добробити земље, ради спречавања нереда или криминала, заштите здравља или морала или ради заштите права и слобода других.“ (http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm, 2016, 17. фебруар).

Прописима на нивоу ЕУ земље чланице су обавезне на давање гаранција у вези са поверљивошћу електронског саобраћаја (телефонских разговора, факсова, СМС/ММС порука, е–поште — речју, приватне и пословне комуникације свих облика). Посебно је потенцирана забрана надзора и снимања електронског саобраћаја од стране трећег лица без сагласности корисника на којег се то односи или без судског налога за надзор. Поменутим прописима се, такође забрањује, остављање било каквих записа на уређају корисника у циљу прикупљања информација о његовим активностима. Санкционише се ширење вируса, убацивање трагова о WEB активностима у корисников компјутер и остале злонамерне активности које нарушавају приватност корисникових телекомуникационих система и мрежних ресурса. (http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm, 2016, 18. фебруар)

У Декларацији о слободи комуникација на Интернету (енгл. Declaration on freedom of communication on the Internet; http://portal.unesco.org/ci/en/files/25147/11861368651Declaration-Inf(2003)007.pdf/Declaration-Inf(2003)007.pdf, 2016, 2. јул) из 2003. године дефинисано је седам принципа:

1. правила о Интернет садржајима;
2. саморегулација и корегулација;
3. одсуство претходне државне контроле;
4. уклањање баријера за учествовање појединаца у информационом друштву;
5. слобода пружања услуга путем интернета;
6. ограничена одговорност пружалаца услуга према интернет садржајима који су доступни њиховим корисницима;
7. анонимност.

„Европско право мора истовремено подробније да дефинише примену нових правних принципа, почев од анонимности, отворености и слободе, наднационалности, недискриминације и транспарентности и неутралности, до правног плурализма и суверености ’компјутера и мрежа’ уместо суверености државе“. (Дракулић и Дракулић, 2010)

Када се говори о врстама активности на мрежи као што су посете web сајтовима, обављање е–трансакција и друге врсте обављања пословних и приватних активности коришћењем мреже, оне морају бити посебно заштићене, а подаци који у таквим активностима настају, не смеју бити употребљени без сагласности власника. Безбедносне службе своје активности спроводе у циљу контраобавештајне заштите националних држава, државних институција и лица на руководећим државним функцијама, чиме се на посредан начин врши и контраобавештајна заштита појединаца или грађана. Дакле, контраобавештајна заштита појединаца или личности се спроводи искључиво у случају лица на највишим државним функцијама, као што су председник државе, председник Владе и специфичне државне функције за које, на основу безбедносне процене, постоје индиције да су предмет угрожавања од стране злонамерних организација или појединаца.

Закон о заштити података о личности (Службени гласник Републике Србије, 97/2008, 104/2009, др. закон, 68/2012 — одлука УС 107/2012) прописује да послове заштите података о личности обавља Повереник за информације од јавног значаја и заштиту података о личности, као самосталан државни орган, независан у вршењу своје надлежности. Циљ овог закона је да, у вези са обрадом података о личности, сваком физичком лицу обезбеди остваривање и заштиту права на приватност и осталих права и слобода. Законом су дефинисани нарочито осетљиви подаци. То су подаци који се односе на националну припадност, расу, пол, језик, вероисповест, припадност политичкој странци, синдикално чланство, здравствено стање, примање социјалне помоћи, жртву насиља, осуду за кривично дело и сексуални живот и могу се обрађивати на основу слободно датог пристанка лица, осим када законом није дозвољена обрада ни уз пристанак. Изузетак су подаци који се односе на припадност политичкој странци, здравствено стање и примање социјалне помоћи, који се могу обрађивати без пристанка лица, само ако је то законом прописано.

Лице, по наведеном закону, има право да од руковаоца захтева исправку, допуну, ажурирање, брисање података, као и прекид и привремену

обуставу обраде. Лице има право (*чл.22. Права лица поводом извршеног увида*) на брисање података уколико је:

- сврха обраде неодређена или није јасно одређена;
- сврха обраде измењена, а нису испуњени услови за обраду за ту измењену сврху;
- сврха обраде остварена, односно подаци више нису потребни за остваривање сврхе;
- начин обраде недозвољен;
- установљено да податак спада у број и врсту података чија је обрада несразмерна сврси;
- је податак нетачан, а не може се путем исправке заменити тачним;
- податак обрађиван без пристанка или овлашћења заснованог на закону и у другим случајевима када се обрада не може вршити у складу са одредбама овог закона. Лице има право на прекид и привремену обуставу обраде, ако је оспорило тачност, потпуност и ажурност података, као и право да се ти подаци означе као оспорени, док се не утврди њихова тачност, потпуност и ажурност.

Подносилац захтева за остваривање права у вези са обрадом може изјавити жалбу Поверенику (*чл. 38 Право на жалбу*):

- против одлуке руковаоца којом је одбијен или одбачен захтев;
- када руковалац не одлучи о захтеву у прописаном року;
- ако руковалац не стави на увид податак, односно не изда копију податка или то не учини у року и на начин прописан законом;
- ако руковалац услови издавање копије података уплатом накнаде која превазилази износ нужних трошкова израде копије;
- ако руковалац, супротно закону, отежава или онемогућава остваривање права.

Надлежности Повереника за заштиту информација од посебног значаја по Закону о заштити података о личности (*чл. 44 Надлежности*) су да:

- надзире спровођење заштите података;
- одлучује по жалби у случају прописаним законом;

- води Централни регистар;
- надзире и дозвољава изношење података из Републике Србије;
- указује на уочене злоупотребе приликом прикупљања података;
- саставља листу држава и међународних организација које имају одговарајуће уређену заштиту података;
- даје мишљење у вези са успостављањем нових збирки података, односно у случају увођења нове информационе технологије у обради података;
- даје мишљење, у случају када постоји сумња да ли се неки скуп података сматра збирком података у смислу овог закона;
- даје мишљење Влади у поступку доношења акта о начину архивирања и о мерама заштите нарочито осетљивих података;
- прати примену мера за заштиту података и предлаже побољшање тих мера;
- даје предлоге и препоруке за унапређење заштите података;
- даје претходно мишљење да ли одређени начин обраде представља специфичан ризик за права и слободе грађанина;
- прати уређење заштите података у другим земљама;
- сарађује са органима надлежним за надзор над заштитом података у другим земљама;
- одређује начин даљег поступања са подацима када је руковалац престао да постоји, осим ако је прописано друкчије.

Повереник може имати заменика за заштиту података о личности. Извештај који подноси Народној скупштини, Повереник доставља Председнику Републике Србије.

7.2. ЗАШТИТА ПОСЛОВНИХ ИНТЕРЕСА

Заштита пословних информација је данас задатак државних институција и службби, као и посебних организационих целина пословног

субјекта. Државне службе, обавештајне и контраобавештајне, на тај начин штите и националне интересе јер је пословање компанија уско повезано и са интересима националних држава, посебно у делу који се односи на буџетско финансирање и на повећање стопе запослености. Заштита пословних информација се у том смислу односи на све пословне процесе, без обзира да ли се ради о истраживачким пројектима, производним процесима или кадровским решењима. Носиоци пословних информација су лица запослена у пословном субјекту и информације похрањене у ИКС–у. У складу са тим организациона целина задужена за контраобавештајну заштиту (корпоративну безбедност) предузима мере којима спречава отицање података означених као пословна тајна и других информација које су од значаја за пословање пословног субјекта. Конкуренти доласком до таквих информација стичу предност на тржишту, обезбеђују сопственом пословном субјекту предност у односу на друге пословне субјекте и обезбеђују пословни успех који може да буде краткорочан или дугорочан, што зависи од квалитета обезбеђених информација. Досадашња концепција заштите пословних информација била је усмерена најчешће на успоставу механизма заштите информационе безбедности, што се показало погрешним. Истраживања у овој области су показала да су за 70 % случајева отицања тајних података (пословних тајни) одговорни запослени унутар система, инсајдери који свесно и намерно достављају информације заинтересованој страни, мотивисани најчешће материјалним разлозима или разним врстама притисака и уцена. (http://social-engineer.org/wiki/-archives/PenetrationTesters/Pentest-Winkler.html, 2016, 18. фебруар)

Савременим пословним организацијама потребан је поуздан нормативно–оперативни систем заштите који гарантује адекватан ниво безбедности лица, имовине и пословања. То посебно важи за све субјекте у привредној и ванпривредној области пословања, колективе који обухватају готово све сегменте рада, велике техничко–технолошке системе и за јавне привредне субјекте од виталног значаја за функционисање државе и друштва у целини. Најчешће радње и мере у заштити лица и објеката су: мере физичке и техничке заштите; мере заштите од пожара и хаварија; мере

противдиверзионе заштите; мере противприслушне заштите; као и мере санитарно–техничке, биолошке, хемијске и здравствене заштите.

Винклер (Winkler) анализу контраобавештајних активности пословних субјеката посматра кроз четири аспекта:

1) *Технички* — треба да обезбеди поверљивост и расположивост информатичких система и мрежа као и осталих техничких система са којима располаже пословни субјект;

2) *Бихевиористички приступ* — анализира губитак информација посредством нетехничких средстава, а носиоци таквих активности могу бити запослени унутар пословног субјекта, али и остала лица са којима основни субјект остварује разне облике пословне сарадње, као што су књиговодствене услуге, заједничка производња, франшизинг, заступање у продаји. Проблем се решава тако што се запосленим лицима онемогућава приступ свим информацијама, већ искључиво оном делу који се доноси на његову функцију унутар пословног субјекта. Управо тај сегмент омогућава да се отицање поверљивих информација сведе на ограничен број лица, чиме се и откривање евентуалног починиоца олакшава и пресеца недозвољена активност;

3) *Физички аспект* — анализира могућности за неовлашћен приступ пословним информацијама од стране неовлашћених лица и евентуалну крађу техничких и информатичких средстава у којима су информације похрањене. Мере које се предузимају у циљу спречавања овог облика угрожавања односе се на контролисано кретање унутар пословног субјекта и спречавање неовлашћеног уласка неовлашћених лица;

4) *Персонални аспект* — подразумева вршење безбедносних провера приликом запошљавања лица у пословни субјект, затим вршење безбедносних провера за приступ информацијама различитог степена поверљивости, као и остваривање контаката са лицима која су прекинула запослење у пословном субјекту без обзира на разлоге. (Winkler, 1996)

Дакле, задатак корпоративне, односно контраобавештајне структуре пословног субјекта, јесте да заштити информације пословног субјекта и спречи њихово откривање неовлашћеним лицима, те на тај начин омогући

висок ниво безбедности пословног субјекта. Заштита пословних информација се врши од нелегалних активности конкуренције, али и од легалних активности које могу да проузрокују штету пословном субјекту. Ризике и претње је потребно свести на минимум, а могућности и шансе максимално искористити. Програм заштите информација има три основне функције: успоставити контролу приступа информацијама, омогућити индивидуални приступ уз претходну идентификацију, имати механизме којима се у сваком тренутку може установити ко је, када, како и на који начин приступио поверљивим информацијама. (Јаворовић и Биланџић, 2007: 268)

Процес коорпоративне, односно контраобавештајне заштите пословног субјекта обухвата неколико фаза: прва фаза представља категоризацију пословних информација, која се, како наводе Ковачић (Kovacich) и Бони (Boni), дели на: поверљиве; за интерну употребу; приватне информације пословног субјекта; осетљиве информације; информације о власништву; пословне тајне (Boni, 2000: 150). Следећа фаза је успостављање заштитних безбедносних механизама који штите пословни субјект од напада споља и изнутра. Механизми и мере које се у том смислу доносе не треба да буду наметнуте у смислу да оптерећују запослене и стварају непотребно незадовољство и нелагодност у обављању свакодневних радних обавеза. Једноставно речено, оне треба да буду део усвојене и прихваћене безбедносне културе запослених у пословном субјекту. Последња фаза је анализа успостављених механизама и њихова перманентна корекција у складу са актуелном пословном ситуацијом.

Да би менаџмент пословног субјекта био правовремено обавештен у вези угрожавања пословних информација и да би на време могао да спроведе мере којима би се таква активност у потпуности спречила или бар ублажила, неопходно је дефинисати индикаторе нарушавања безбедности пословног субјекта који су променљиви, па је, самим тим, потребна њихова перманентна анализа и допуњавање. Бернар (Bernhardt) издваја следеће индикаторе који указују да је пословни субјект „мета“ обавештајних активности других пословних субјеката, а то су (према Bernhardt, 2003: 91–92):

- конкуренти поседују информације које представљају пословну тајну пословног субјекта;
- устаљени обиласци и посете пословног субјекта;
- долазак непозваних лица најчешће техничке струке, која наводно отклањају техничке кварове;
- континуиран неуспех на тендерским надметањима, лансирање сличних производа на тржиште од стране конкурента;
- прелазак стручног особља код конкурента;
- сумњиво понашање запослених појединаца;
- откривање техничких уређаја за прикупљање података.

Посебан проблем са аспекта заштите информација представља „on–line“ повезивање организационих целина унутар једне компаније које могу да буду дислоциране и на више континената. Информације које представљају пословну тајну се, у неким случајевима, размењују путем класичног интернета, чиме се ствара могућност отицања тајних података. Међутим, коришћење интернета, као што је то случај код е-продаје, је неизбежан и представља основно средство за такву врсту пословања. Мрежу је у том случају потребно заштитити посебним мерама криптозаштите као и приступ рачунарима и серверима на којима се чувају осетљиви подаци. Приступ рачунарима се ограничава ауторизацијом приступа, чиме се утврђује идентитет корисника. Ауторизација трансакције може да се спроведе преко помоћног канала или помоћу лозинке, што представља слабији вид заштите. Битно је да се процес ауторизације може спровести у сваком тренутку и без прекида.

Ђорђевић наводи да би при конципирању правила о е–пословању требало да се води рачуна о следећим принципима (Ђорђевић, 2007: 150):

- странке међусобно одређују уговорне односе у складу са потребама и проценама;
- правила се постављају начелно, без залажења у технолошка питања, јер би се тиме спутавао даљи развој е–пословања;
- правила се мењају само у случајевима када постају препрека даљем

развоју праксе;

- стварање услова за укључивање технолошки застарелих предузећа у е–пословање.

Поред наведених мера заштите пословних система, неопходно је перманентно повећање безбедносне културе запослених, кроз едукацију, организовање стручних курсева и семинара. Безбедносна култура корисника ИКС представља први степен заштите.

7.3. ЗАШТИТА НАЦИОНАЛНИХ ИНТЕРЕСА

Систем националне безбедности Републике Србије (Стратегија националне безбедности Републике Србије; http://www.kombeg.org.rs/Slike/CeBezbednost/statika/Strategija%20nacionalne%20bezbednosti%20Republike%20Srbije.pdf) у ширем смислу чине највиши органи законодавне, извршне и судске власти:

1. Народна Скупштина Републике Србије;
2. Председник Републике Србије;
3. Савет за националну безбедност;
4. Влада Републике Србије;
5. Судови и тужилаштва.

У ужем смислу, систем националне безбедности чине:

1. Систем одбране;
2. Министарство унутрашњих послова;
3. Безбедносно–обавештајни систем;
4. Привремени органи и координациона тела.

Систем одбране представља јединствену, структурно уређену целину снага и субјеката одбране чији је основни циљ заштита интереса Републике Србије од оружаног угрожавања споља. Војска Србије је основни субјект система одбране.

Снаге *Министарства унутрашњих послова* су део система националне безбедности чији је циљ заштита националних интереса у домену унутрашње

безбедности. Полиција је основна снага Министарства унутрашњих послова. Обавља послове заштите живота, личне и имовинске безбедности грађана, обезбеђења државне границе, борбе против тероризма и оружаног угрожавања изнутра и друге послове у складу са законом.

Безбедносно–обавештајни систем је функционално обједињен подсистем националне безбедности Републике Србије који чине Безбедносно–информативна агенција, Војнобезбедносна агенција и Војнообавештајна агенција. Послове усклађивања рада служби безбедности обавља Биро за координацију. Послове из области националне безбедности обављају и органи државне управе, институције надлежне за правосуђе, образовање и научну делатност и заштиту животне средине, Заштитник грађана, органи јединица локалне самоуправе, субјекти из области приватног обезбеђења, организације цивилног друштва, медији, правна лица и грађани који доприносе остваривању циљева националне безбедности.

Народна скупштина Републике Србије остварује свој утицај на све делове система националне безбедности уставотворном и законодавном делатношћу. Народна скупштина одлучује о рату и миру, доноси законе и друге опште акте у области националне безбедности и надзире рад Владе и других органа одговорних Народној скупштини, у складу са Уставом и законом. Преко Одбора за одбрану и безбедност, остварује надзор и демократску и цивилну контролу над системом националне безбедности.

Председник Републике Србије председава Саветом за националну безбедност и командује Војском Србије, у складу са Уставом и законом. Председник Републике указује на одређена питања и проблеме из домена националне безбедности, покреће њихово решавање и доноси акте из своје надлежности.

Влада усмерава и усклађује рад органа државне управе у домену националне безбедности, у складу са Уставом и законом. Влада предлаже и реализује политику националне безбедности, усмерава и усклађује функционисање система националне безбедности, обезбеђује материјална и финансијска средства за потребе система националне безбедности, управља делатношћу државних органа, органа државне управе, установа и правних

лица у области остваривања националне безбедности, у складу са Уставом и законом, и обезбеђује реализацију међународних уговора и споразума у области националне безбедности.

Најзначајнију улогу у спровођењу мера безбедносне и контраобавештајне заштите националних интереса има безбедносно–обавештајни систем националне државе. Руковођење безбедносно–обавештајним системом остварује се преко руководећих тела: Савета за националну безбедност и Бироа за координацију рада служби безбедности. *Савет за националну безбедност* је руководећи државни орган који усмерава и усклађује рад служби безбедности. Чланови Савета су: председник Републике, председник Владе, министар одбране, министар унутрашњих послова, министар спољних послова, министар правде, начелник Генералштаба Војске Србије и директори служби безбедности. Савет се дакле бави разматрањем основних питања која се односе на заштиту виталних интереса Републике Србије од свих врста угрожавајућих делатности и предлаже надлежним државним органима мере за унапређење националне безбедности. Поред тога Савет се бави питањем сарадње између националних безбедносних снага и институција са другим државним органима и институцијама којима одбрана и безбедност није примаран задатак. Савет такође разматра сарадњу надлежних државних органа са органима и службама безбедности страних држава и међународних организација. За вршење стручних и административних послова за потребе Савета за националну безбедност надлежна је Канцеларија Савета за националну безбедност. Задаци Канцеларије су: сазивање и припрема седница Савета, стручни послови у вези са праћењем спровођења смерница и Закључака Савета, послови административно–техничке подршке Бироу за координацију рада служби безбедности и чување и стављање на увид члановима Савета извештаја и других акта Савета. *Биро за координацију рада службе безбедности* утврђује задатке који се извршавају оперативним усклађивањем делатности служби безбедности и других државних органа и с тим у вези координира њихове активности, утврђује начин оперативног усклађивања у појединим случајевима, оснива мешовите радне групе за

оперативне задатке који се извршавају оперативним усклађивањем делатности и утврђује њихове задатке, анализира резултате оперативног усклађивања и о томе по потреби извештава. У раду Бироа за координацију служби безбедности могу по позиву да учествују: представници Министарства спољних послова, директор полиције и начелници управа полиције, Републички јавни тужилац, директор Управе царина и руководиоци других државних органа, организација и институција. (Закон о основама уређења служби безбедности, Службени Гласник Републике Србије 116/2007, 72/2012) Рад служби безбедности је под надзором *Народне скупштине Републике Србије* преко Одбора за контролу служби безбедности. Одбор је надлежан да: надзире уставност и законитост рада служби безбедности, надзире усклађеност рада служби безбедности са Стратегијом националне безбедности, стратегијом одбране и безбедносно–обавештајном политиком Републике Србије, надзире поштовање политичке идеолошке и интересне неутралности у раду служби безбедности, надзире законитост примене посебних поступака и мера за тајно прикупљање података, надзире законитост трошења буџетских и других средстава за рад, разматра и усваја извештаје.

Према Закону о основама уређења служби безбедности Републике Србије, службе безбедности Републике Србије су: Безбедносно–информативна агенција (БИА), Војнобезбедносна агенција (ВБА) и Војнообавештајна агенција (ВОА). ВБА и ВОА су органи управе у саставу министарства одбране Републике Србије.

ВБА је орган управе министарства одбране Републике Србије, односно ресорна војна контраобавештајна служба која обавља контраобавештајну заштиту Војске Србије и министарства одбране Републике Србије. Законом су дефинисани следећи послови које ВБА обавља: безбедносна заштита снага, објеката, средстава и активности; безбедносна заштита тајних података; персонална безбедност; индустријска безбедност; безбедносна заштита информационо–телекомуникационих система и криптозаштите; безбедносна заштита других субјеката система одбране; остали послови и задаци безбедносне заштите. У оквиру контраобавештајне заштите, ВБА: открива,

прати и онемогућава обавештајно деловање, субверзивне и друге активности страних држава, страних организација, група или лица усмерених против министарства одбране и Војске Србије; открива, прати и онемогућава унутрашњи и међународни тероризам, екстремизам и друге облике организованог насиља усмерених против министарства одбране и Војске Србије; открива, истражује и прикупља доказе за кривична дела против уставног уређења и безбедности Републике Србије, кривична дела против човечности и других добара заштићених међународним правом, кривична дела организованог криминала, кривично дело прање новца, као и кривична дела корупције (злоупотреба службеног положаја, трговина утицајем, примање мита и давање мита) и ако нису резултат деловања организоване криминалне групе, унутар министарства одбране и Војске Србије; открива, истражује и прикупља доказе за кривична дела којима се угрожавају тајни подаци и кривична дела против безбедности рачунарских података, прописана Кривичним закоником, законом којим се уређује тајност података, као и другим законима када су наведена кривична дела усмерена против министарства одбране и Војске Србије; планира, организује и спроводи контраобавештајну заштиту лица, објеката, активности и тајних података Министарства одбране и Војске Србије; прикупља, анализира, обрађује и процењује контраобавештајне податке из своје надлежности; обавља и друге контраобавештајне послове и задатке.

ВОА је орган управе министарства одбране. Војнообавештајна агенција остварује своју улогу прикупљањем и коришћењем првенствено обавештајних информација о војним могућностима страних држава које јесу или могу да буду носиоци угрожавања безбедности Републике Србије. Имајући у виду вишеструку испреплетеност војне сфере и других сфера међународних субјеката (страних држава), ВОА, између осталог, прикупља и обавештајне информације војно–политичког, војно–економског, научно–технолошког и сличног карактера, односно информације које утичу на војне могућности страних држава. У оквиру своје надлежности ВОА: прикупља и проверава податке и информације, обрађује их, анализира, процењује и доставља надлежним органима; сарађује и размењује

информације и податке са службама, организацијама и институцијама Републике Србије које се баве безбедносно–обавештајним пословима, као и са службама других земаља и организација у складу са утврђеном безбедносно–обавештајном политиком, међународним уговорима и преузетим обавезама; подзаконским актима и штити их од неовлашћеног откривања, давања, коришћења, губитка или уништавања; организује безбедносну заштиту објеката министарства одбране и Војске Србије у иностранству и лица која су од стране министарства одбране и Војске Србије службено упућена у иностранство; прибавља, развија и користи информационе системе, системе веза и системе за пренос података, као и средства за заштиту информација.

ВБА и ВОА су дужне да тачно, истинито и потпуно пруже обавештења о прикупљеним подацима о личности и о подацима од јавног значаја, у складу са прописима којима се уређује област заштите података о личности, област слободног приступа информацијама од јавног значаја и одредбама овог закона. Право на обавештење и увид у податке ограничава се у складу са прописима којима се уређују област слободног приступа информацијама од јавног значаја, тајност података, заштита података о личности и одредбама овог закона.

БИА је централна безбедносна служба Републике Србије која предузимањем обавештајних, контраобавештајних и безбедносних мера штити националну безбедност од носиоца шпијунско–субверзивних делатности. Организациона је целина Владе Републике Србије. Агенција у обављању послова из своје надлежности примењује одговарајуће оперативне методе, мере и радње, као и одговарајућа оперативно–техничка средства којима се обезбеђује прикупљање података и обавештења ради отклањања и спречавања делатности усмерених на подривање или рушење Уставом утврђеног поретка Републике Србије, угрожавање безбедности у земљи и, у вези са тим, предузима друге потребне мере и радње на основу закона и прописа донетих у складу са законом. Агенција предузима мере на откривању праћењу, документовању, спречавању, сузбијању и пресецању делатности организација и лица усмерених на вршење организованог криминала и

кривичних дела са елементом иностраности, унутрашњег и међународног тероризма и најтежих облика кривичних дела против човечности и међународног права и против Уставом утврђеног поретка и безбедности Републике, примењују овлашћења утврђена законом и другим прописима које примењују овлашћена службена лица и радници на одређеним дужностима министарства надлежног за унутрашње послове, у складу са прописима о унутрашњим пословима.

Основна улога контраобавештајног деловања од стране контраобавештајних служби јесте заштита државних и других врста тајни (службена, војна, пословна), државних и друштвених субјеката, органа и институција од спољних носилаца обавештајне делатности, које таква сазнања могу да употребе на разне начине ради угрожавања безбедности виталних вредности и интереса, односно националне безбедности. (Мијалковски, 2012: 148–155) Безбедносне службе спроводе своје активности тако што у складу са безбедносном проценом прикупљају податке о намерама и плановима непријатеља и у складу са ситуацијом правовремено откривају, прате и онемогућавају непријатеља у намери да дође до пословних информација. За разлику од обавештајне службе, контраобавештајна служба делује на територији матичне државе док обавештајне службе своје активности спроводе на територији других држава. У циљу контраобавештајне заштите тајних података, безбедносне службе одређују опште и посебне мере, безбедносне ризике[43] и проблеме[44] којима се постиже виши степен заштите пословних информација.

[43] Неажурна упутства којима су дефинисане мере заштите у поступању са тајним подацима, неусаглашеност са законским и подзаконским прописима, неажурне евиденције у вези са израдом, обрадом, умножавањем и дистрибуцијом тајних података, непостојање или невалидност сертификата за приступ тајним подацима, неспровођење дефинисаних мера заштите у раду с тајним подацима, непримењивање мера заштите рачунара на којима се обрађују тајни подаци, неадекватни услови за чување архивског материјала, уништавање докумената и радних материјала без вођења евиденције, неспровођење процедура у криптообради и нарушавање мера криптозаштите, изостанак контрола спровођења процедура у раду са тајним подацима.

[44] Непостојање упутстава којима су дефинисане мере заштите у поступању са тајним подацима, непостојање евиденција у вези са израдом, обрадом, умножавањем и дистрибуцијом тајних података, неконтролисано изношење тајних података из пословног субјекта, кршење прописаних мера заштите у транспорту, непрописна употреба интернета за слање и пријем података, пропусти у чувању и архивирању докумената.

8. ДИМЕНЗИЈЕ ЉУДСКЕ БЕЗБЕДНОСТИ КАО ОКВИР ЗА АНАЛИЗУ УТИЦАЈА КОМПРОМИТАЦИЈЕ ИНФОРМАЦИЈА НА СТАЊЕ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ — са осврtом на Републику Србију

Концепт људске безбедности представља наставак дуге борбе за права радника, родну равноправност, права мањинских група. Наведени концепт представља покушај да се отклоне главни недостаци непостојећих институционалних механизама у области безбедности. Концепт људске безбедности би се могао одредити као покушај да се подизањем нивоа квалитета живота грађана утиче на ниво њихове безбедности.

Конструисање индикатора подразумева операционализацију концепта. Индикатори се деле на објективне и субјективне. Објективни индикатори су ослобођени утицаја личних оцена, засновани су на чињеницама, док су субјективни фактори засновани на субјективној перцепцији индивидуе. Индикатори се могу односити на комплетну популацију или на ризичне групе. Уколико се односе на ризичне групе са аспекта нарушавања безбедности, стављају се у контекст превенције. Уколико се индикатори поставе лоше могу довести до неразумевања и неспоразума, односно до поједностављеног тумачења и доношења погрешних одлука. Потребно их је посматрати као полазну тачку за иницирање дискусије и привлачење интересовања јавности. Индикатор је дакле квантитативна или квалитативна мера која произлази из скупа података добијених посматрањем појава. Они служе за процену кретања, интензитета и промена кроз време. Исто тако служе за постављање циљева политике, скретање пажње на одређени проблем, мониторинг и компарацију. (Дулић и сар., 2010: 67)

У раду је примењен предлог за мерење људске безбедности који се заснива на Извештајима о људском развоју Уједињених нација, а индикатори људске безбедности су преузети од проф. Дулић (Дулић и сар., 2004: 315–330) који су такође усклађени са индикаторима наведеног Извештаја.

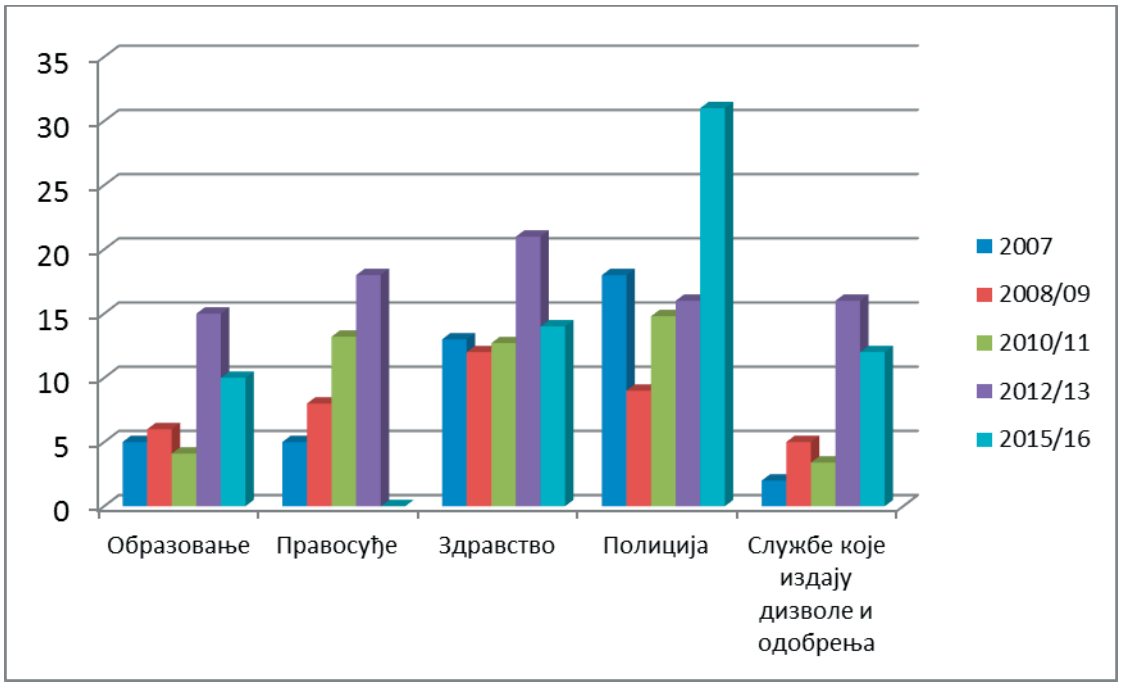
Корупција је феномен који снажно утиче на стање безбедности у оквиру свих седам димензија људске безбедности, посебно у делу који се односи на компромитацију пословних информација која за последицу има нарушавање квалитета живота грађана Републике Србије и напослетку националне безбедности Републике Србије. Невладина организација *Транспарентност Србија* је извршила истраживање у вези корупције у Републици Србији и представила резултате Глобалног барометра корупције 2015/16 за нашу земљу који указују на следеће закључке: (http://www.transparentnost.org.rs/images/dokumenti_uz_vesti/GCB_2016.pdf, 2016, 25. новембар):

- У Србији се годишње догоди најмање 374.000 неоткривених случајева подмићивања ради добијања услуга јавног сектора или заштите од кажњавања. Годишње, због примања и давања мита, надлежни органи поднесу 220 кривичних пријава, а за злоупотребу службеног положаја око 3.000, што је стотину пута мање од броја случајева ситне корупције на које указује ово истраживање. Према мишљењу наведене организације и на основу истраживања, долази се до закључка да мере које предузимају државни органи, кроз периодичне акције хапшења и примену стратегија и акционих планова нису донеле битан напредак. До тог циља се може доћи једино ако тужилаштво предузме уверљиве истраге свих пријављених сумњи на корупцију и обавести јавност о исходу и ако потенцијални узбуњивачи и сведоци корупције буду сигурни да неће претрпети штету.
- Истраживање непосредног искуства грађана са корупцијом (случајеви када су грађани дали мито, такозвана „ситна корупција“) било је фокусирано на осам сектора (односно институција): саобраћајна полиција, јавно здравство, образовни систем (у две категорије), судови — грађанске парнице, јавне службе које издају службене исправе (нпр.

пасош, изводи из службених евиденција, укњижење), службе надлежне за накнаде за незапослене и за друге накнаде у оквиру социјалног осигурања.

- Укупно је 68 % испитаника имало контакт са неком од посматраних институција — сектора, а од тог броја 22 % њих (или чланова домаћинства) је дало мито макар једном у последњих годину дана. Када се ови проценти пренесу на укупан број домаћинстава у Србији (попис из 2011), долази се до минималног броја од 374.205 случајева ситне корупције на годишњем нивоу, док је стварни вероватно значајно већи.
- Према последњим доступним подацима (2014) за кривично дело злоупотребе службеног положаја било је пријављено 3014 људи, за примање мита 142, за давање мита 84, трговину утицајем 33, а за злоупотребе у вези са јавном набавком 79. У истој години су због корупције оптужене 1044 особе. То значи да мање од 1 % кривичних дела корупције икада буде пријављено, а да је број оптужених и кажњених далеко мањи.
- С обзиром на то да са њима велики број грађана долази у контакт, највише случајева подмићивања је регистровано у односу на саобраћајну полицију и здравствене службе. Здравство узима 14 % подмићивања посматрајући проценте у односу на остале секторе, што је боље него стање из сличног истраживања из 2012. године, али и даље лошије него у барометрима из ранијег периода.
- Резултати који се односе на проценат грађана спремних да пријаве корупцију не дају разлог за оптимизам. Трећина грађана сматра да и „обични људи“ могу да допринесу борби против корупције, а приближно исти број сматра моралном обавезом да пријави корупцију чији је сведок. Међутим, пре четири године број грађана спремних да пријаве корупцију је био знатно виши (58 %). Свега 21 % грађана сматра да је пријављивање корупције „друштвено прихваћено“, што не делује обећавајуће за узбуњиваче.

На графикону бр. 7 су приказани подаци заступљености корупције у државним институцијама.



Графикон бр. 7: Корупција — степен подмићивања по секторима[45] (http://www.transparentnost.org.rs/images/dokumenti_uz_vesti/GCB_2016.pdf)

Из графикона бр. 7 се може уочити да је тренд развоја корупције у области здравства од 2007. године био у благом порасту. Последња истраживања у овој области указују на закључак да је 20015/16. године овај тренд у благом опадању, за разлику од других државних органа, као што је случај са полицијом и правосуђем где је тренд позитиван.

8.1. ЕКОНОМСКА И ЛИЧНА БЕЗБЕДНОСТ

Грађани Републике Србије имају осећај економске несигурности, пре свега, због транзиционих процеса којима се држава суочава, а најчешће се

[45] Глобални барометар корупције је највеће светско истраживање о искуствима грађана са корупцијом, перцепцијом грађана о корумпираности појединих институција и њиховој спремности да се укључе у борбу против корупције. У Србији је теренски део истраживања спроведен у периоду од 26. новембра 2015. до 22. фебруара 2016. на националном узорку од 1508 испитаника који репрезентује целокупно становништво (централна Србија и Војводина). Истраживање је спроведено CAPI методом „лицем у лице".

односе на проблеме буџетског дефицита, монетарне стабилности, висине јавног дуга и нестабилности појединих институција система. Да би се анализирала тренутна економска безбедност грађана Републике Србије, неопходно је дефинисати који су индикатори у директној вези са овом димензијом људске безбедности. У поглављу ће бити анализирани следећи индикатори који се односе на економску безбедност: кретање запослености и незапослености, структура запослених по сектору делатности, структура запослених и незапослених према школској спреми, висина примања по секторима, проценат привредних субјеката и становништва са приступом интернету и индекси трошкова живота. На основу изабраних индикатора дефинисаће се подиндикатори који указују на проблеме нарушавања економске безбедности становништва и студије случајева које потврђују везу између нарушавања економске безбедности и дефинисаних подиндикатора.

Заступљеност информационо–комуникационих технологија у индустријској производњи и укупној привреди једне државе представља показатељ њеног свеукупног економског, индустријског, али и технолошког развоја. Савремени концепт у модерној индустријској производњи подразумева употребу ИКТ у свим сегментима производње, што може да утиче негативно на њену безбедност и могућност опструкције од стране злонамерних лица и организација. Дакле, степен достигнућа примене ИКТ у индустријској производњи, односно у целокупним привредним активностима је индикатор који директно утиче на економску безбедност државе, а самим тим и њених грађана. Један од најосетљивијих сегмената употребе ИКС–а у пословању представља употреба интернета од стране привредних субјеката.

Употреба интернета у 2016. години од стране привредних субјеката је изузетно висока, 99.8 %, што представља повољну околност за отицање тајних података путем ИКС–а.[46]

У табели бр. 4 истакнут је проценат употребе интернета и WEB сајтова који пословни субјекти користе у свом пословању.

[46] Методологија подразумева анализу регистрованих предузећа на територији Републике Србије која имају десет и више запослених.

Табела бр. 4: Пословни субјекти који користе интернет и WEB сајтове у свом пословању у периоду од 2011. до 2015. године

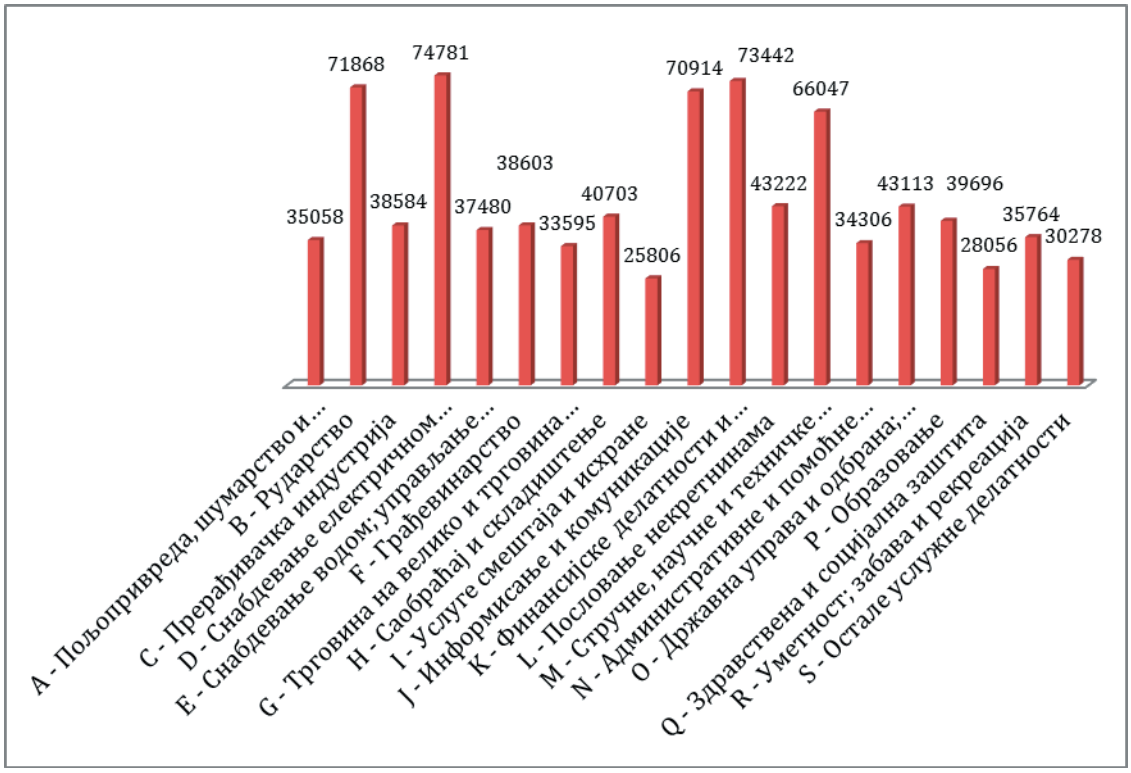
					%
	РЕПУБЛИКА СРБИЈА [1]				
	2011	**2012**	**2013**	**2014**	**2015**
Пословни субјекти који користе интернет и WEB сајт у свом пословању					
Интернет	97.2	97.7	99.6	100.0	99.1
WEB сајт	67.6	73.8	73.8	74.0	75.2

Извор података: Републички завод за статистику Републике Србије

[1] Од 1999. без података за АП Косово и Метохија

Из табеле бр. 4 је евидентно да је у посматраном периоду (2011—2015) приметан пораст употребе ИКТ–а у привредним субјектима, то јест, тренд употребе ИКТ–а у привредним субјектима је у порасту. Повезивање пословних рачунара у мрежу, што уједно представља и прикључење удаљених рачунара изван пословног субјекта и њихово повезивање са интернетом, представља повољну околност за отицање тајних података. Отицање пословних информација може да доведе до губитка позиције пословног субјекта на тржишту или да га у потпуности истисне из „тржишне утакмице“.

Стабилан извор прихода грађана утиче позитивно на школовање, планирање породице или уређење животног простора, што свакако утиче и на њихову економску сигурност. Компромитација информација о висини прихода државних службеника, њиховим склоностима и слабостима, као и слабостима државног система у смислу јавних финансија, би могла да се реализује кроз инвестиције конкурента у делатности у којима је могуће постићи већи пословни успех. Ако се ради о транснационалним компанијама, онда би конкурентска активност могла у крајности да утиче на целокупну привредну активност једне државе. (Графикон бр. 1)

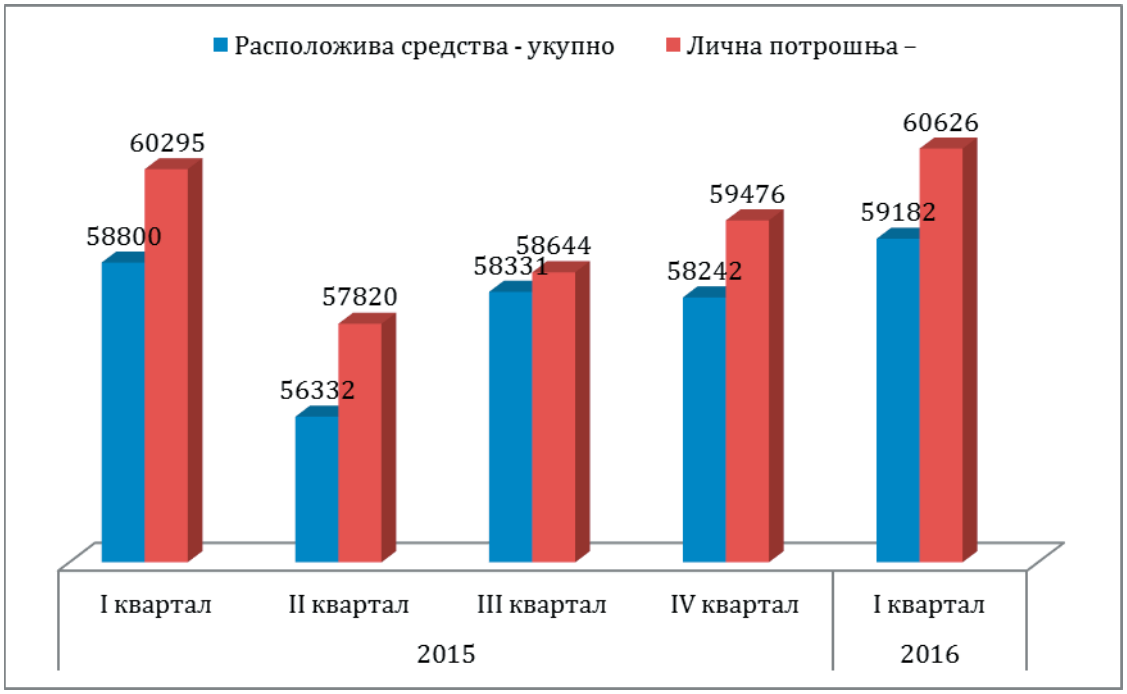


Графикон бр. 1: Просечне зараде запослених по секторима у јануару 2016. године[47]
(Извор: Републички завод за статистикуРепублике Србије)

Просечна нето зарада је у јануару 2016. године износила 45.332 динара, просечна зарада у државној управи и одбрани где је обавезно социјално осигурање износи 43.113 динара, мања је за 5 %, а плата у пословима административним и помоћним услужним делатностима износи 34.306 динара, што значи да је мања од посматраног просека за 24 %.

У графикону бр. 2 је приказана месечна потрошња становништва у временском периоду 2015—I квартал 2016. године.

[47] Подаци о просечним зарадама по запосленом добијају се на основу Месечног статистичког истраживања о запосленима и о зарадама запослених код правних лица и на основу података Министарства финансија (Пореска управа) за запослене код предузетника. Подаци о зарадама запослених код предузетника укључују се у обрачун просечних зарада од јануара 2009. године.



Графикон бр. 2: Месечна потрошња становништва у временском периоду 2015—I квартал 2016. године[48] (Републички завод за статистику Републике Србије)

Узимајући у обзир податке из претходна два графикона који се односе на примања запослених у државној управи и на административним пословима и просечну месечну потрошњу становништва видимо да су примања лица на наведеним пословима мања од месечне потрошње по домаћинству, што представља један од могућих индикатора нарушавања економске безбедности грађана.

Просечна потрошачка корпа за месец јануар 2016. године износила 67.277,45 динара и већа је од просечне потрошачке корпе из претходног месеца за 0,57 % или 387,4 динара (http://mtt.gov.rs/download/potrosacka-korpa/KUPOVNA%20MOC%20-%20JANUAR%202015.pdf, 2016, 10. мај). Узимајући у обзир претходно сазнање, висину просечних примања и просечне потрошачке корпе, евидентно је да висина примања посматране

[48] Највећи удео у личној потрошњи домаћинстава, у првом кварталу 2016. године, чине издаци за храну и безалкохолна пића — 34,6 % и становање, воду, електричну енергију, гас и остала горива — 17,3 %. Следе издаци за транспорт — 9,4 %, за остале личне предмете и остале услуге — 5,8 %, за одећу и обућу — 5,5 %, за комуникације — 5,2 %, за опрему за стан и текуће одржавање — 4,5 %, за здравље — 4,4 %, за алкохолна пића и дуван — 4,3 %, за рекреацију и културу — 4,2 % и 4,8 % чине издаци за остале групе личне потрошње.

категорије лица не покрива основне животне потребе, што такође потврђује претходно изнету претпоставку о могућем предузимању незаконитих активности запослених у државној, јавној управи и административним пословима, у виду примања мита и злоупотребе службеног положаја. Поред тога, наведена категорија лица, у циљу обезбеђивања додатних прихода којима подмирију основне потребе, прибегава додатним пословима и прековременом раду, што у неким случајевима представља сукоб интереса и узрокује друге неправилности које подлежу санкцијама.

Проблем незапослености постаје посебно изражен после 2000. године, а резултат је пре свега привредне транзиције. Смањивање броја запослених у државном и јавном сектору, као и приватизација и отпуштање радника неперспективних друштвених предузећа, подигла је степен незапослености на изузетно висок ниво. Неизвесност и несигурност запослених доприносе стварању повољне климе за чињење коруптивних дела, како би се у случају останка без запослења, створили додатни приходи за егзистенцију. То свакако није једини и најважнији мотив за коруптивно деловање, али је параметар који треба узимати у обзир приликом анализа.

UNDOC (енгл. *United Nation Office on Drugs and Crimes*) је институција која је 2011. године спровела истраживања заступљености и појавама корупције у Републици Србији. По резултатима ове институције, а на основу мишљења грађана Србије, корупција заузима треће место међу најзначајнијим проблемима са којима се Србија суочава, после незапослености, сиромаштва и ниског животног стандарда. Запажања о општој распрострањености корупције у државном сектору говоре искуства 6 % новозапослених државних службеника који су, у току три године истраживања, себи обезбедили посао уз помоћ мита. Корупција је заступљенија од осталих облика криминала, као што су крађа личне имовине, провале, крађе. Један од облика корупције који се појављује у истраживању јесте давање и примање мита. Мито се може употребити у разним облицима и контекстима, међутим истраживање показује да нису сви сектори државне администрације у Србији погођени корупцијом у истој мери. На основу искустава грађана који су давали мито (најмање једном у

току дванаест месеци пре спровођења истраживања), од запослених у државном сектору у Републици Србији, најчешће су мито примали лекари (55 % грађана са скоријим искуством са корупцијом дало је мито лекарима), затим полицајци (39 %), медицинске сестре (26 %) и службеници катастра (16 %). Остали државни службеници примају мањи проценат мита: од службеника за социјалну заштиту (1 %), до општинских службеника (10 %). Иако је тенденција удела запослених у државном сектору код земаља у транзицији последњих неколико година у опадању, удео запослених у државном сектору у Србији креће се и даље око 20 %. С обзиром на величину и значај државне администрације, сектори/агенције запошљавају нове раднике у редовној динамици. Процес запошљавања је обично регулисан тако да би се обезбедила транспарентност, а новозапослени се бирају на основу критеријума као што су компетентност и искуство. Међутим, резултати ове анкете показују да се и неки други фактори појављују као основ запошљавања, као што су непотизам, пријатељство, мито и слично. У већини земаља, запослење у државном сектору се обично сматра примамљивим, не само због природе самог посла већ и због предности које су типичне за државну администрацију, као што су сигурност радног места, друштвени статус и повољна плата. У том смислу, Србија није изузетак и, на основу резултата ове анкете, око 16 % грађана или чланова њихових домаћинстава пријавило се за радно место у државном сектору током три године које су претходиле истраживању, од којих је 23 % добило посао. (Корупција у Србији искуство грађана, UNDOC, 2011; https://www.unodc.org/documents/dataandanalysis/statistics/corruption/Korupcija u Srbiji - Iskustva gradjana withcover.pdf, 2016, 10. мај)

Према истраживању агенције „MEDIUM GALLUP“ и UNDP, 2005, 2010. и 2013. године, када су упитани о личном искуству са корупцијом, скоро трећина грађана Србије, 27 %, признало је да је последњих годину дана било у прилици да дâ или је дало мито. Подмићивањем се није служило 61 % грађана. Висина примања нема везе са спремношћу на подмићивање, али су му зато склонији високо и више образовани грађани, 33 %, док је за митом посегло 23% нешколованих. Проучаван је и утицај места становања на

корупцију. Показало се да су јој склонији људи у градовима (30 %) од оних са села (23 %) што је и логично јер је у граду више администрације и већа је конкуренција. Овакво истраживање је спроведено у 64 земље, на 60.000 људи. Резултати су показали да у богатим, стабилним земљама корупција не представља проблем. Што су институције проходније, мање је подмићивања. Сваки десети грађанин света је имао непосредно искуство са корупцијом, показало је Галупово истраживање. Она је најзаступљенија у Камеруну (50 %), мање од пет процената је има у Аустрији, Канади, Данској, Финској, Француској, Немачкој, Америци и Шпанији. На нашем нивоу, по истраживањима наведене агенције, од 20 до 30 %, заступљена је још у Албанији, Боливији, Чешкој, Еквадору, Румунији и Русији. Од наших суседа Хрватска и Македонија се најбоље котирају, 5—10 %. У њиховој групи су и Бугарска, Естонија, Турска, Јужна Кореја и Аргентина. Четрдесет процената испитаника сматра да је због малих плата за већину запослених у јавном сектору, узимање мита једини начин преживљавања. (http://www.novosti.rs/395.html:167431-Mito-kao-u-svetu, 2016, 11. мај)

Међународна асоцијација *Gallup International* такође је спровела истраживања, 2007. године у 61 земљи, а 2008. у 46 земаља. У Србији је то истраживање реализовала агенција *THC Medium Glalup*, на узорку од 1005 пунолетних грађана. Тада је утврђено да 33 % испитаника види свој посао као сигуран, да се 47 % суочава са могућношћу губитка посла, док 19 % не зна или није одговорило на ово питање. Према истраживању обављеном следеће 2008. године, 46 % испитаника види свој посао као несигуран, а исто толико испитаника сматра сигурним своје радно место (готово исто као претходне године), док је битно смањен број оних који нису одговорили на питање или су рекли да не знају (8 %). Године 2007. Србија је била на другом месту на светској листи земаља у којима је несигурност радног места висока. Крајем 2009. године, иста истраживачка агенција је на узорку од 438 запослених забележила да своје радно место 60 % испитаника види као несигурно. Узимајући у обзир претходне проценте (47 % — 46 % — 60 %) можемо закључити да грађани Србије страхују од веома велике несигурности запослења и, сходно томе, од велике егзистенцијалне неизвесности. Податке

о перцепцији несигурности радног места и изложености отпуштању увек треба гледати у релацији са малим могућностима за ново запошљавање. Радну несигурност много повећавају разни облици такозване флексибилизације радног односа, то јест разни облици запошљавања који посао чине на неки начин привременим. Управо у овом контексту треба посматрати покушаје примене норми карактеристичних за такозвану флексигурност. Наиме, у појединим западним земљама, у радно законодавство, унете су норме које поједностављују и олакшавају отпуштање радника, уз истовремено поједностављивање и олакшавање процедура запошљавања радника. Међутим, то је могуће само у земљама у којима има довољно радних места да се незапослени радници могу без дугог чекања поново запослити. Без обзира на неолиберални концепт о раду и раднику као роби, треба имати у виду да радна места никад и нигде нису била ни сигурна ни трајна. Уосталом, „радно место“ је само у робовласничком систему било трајно и сигурно, барем онолико колико је живот роба био трајан и сигуран. Када је радно место мање трајно и све мање сигурно, разумљива је и морално оправдана, тежња радника и радничких организација да радна места учине трајнијим и сигурнијим. Када сигурно радно место постаје реткост која је на великој цени, у земљама са високим степеном корупције, корупција је уобичајен и „нормалан“ одговор. У том контексту унеколико је разумљиво, али не и морално оправдано, настојање радника да готово масовно, путем подмићивања и других коруптивних процедура, учине своје радно место сигурнијим (Вујовић и сар., 2013).

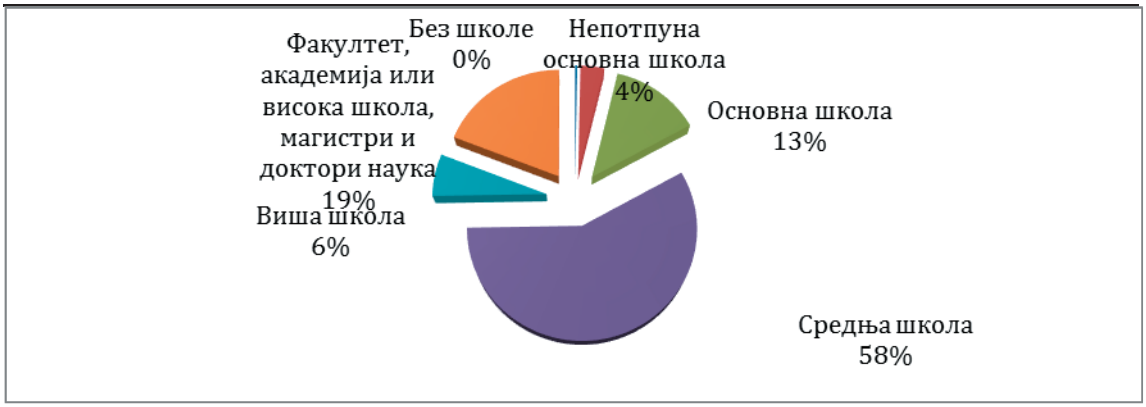
У табели бр. 5 дат је приказ радне активности становништва, а на графикону бр. 3 проценат запосленог становништва по стручној спреми у Републици Србији.

Табела бр. 5: Радна активност становништва старог 15 и више година према школској спреми у другом кварталу 2015. године

	2015/II квартал				
	Укупно	**Активно становн.**	**Запослена лица**	**Незапослена лица**	**Неактивно становн.**
Радна активност становништва старог 15 и више година према школској спреми					
РЕПУБЛИКА СРБИЈА [1]					
Укупно	6071726	3123204	2565712	557492	2948522
Без школе	109336	8911	8474	437	100425
Непотпуна основна школа	493307	96686	88869	7817	396622
Основна школа	1240343	407305	339021	68284	833038
Средња школа	3112674	1840272	1480959	359313	1272402
Виша школа	341577	186002	158043	27959	155575
Факултет, академија или висока школа, магистри и доктори наука	774489	584028	490346	93682	190461

Извор података: Републички завод за статистику Републике Србије

[1] Од 1999. без података за АП Косово и Метохија



Графикон бр. 3: Проценат запосленог становништва по стручној спреми у односу на укупан број радно активног становништва изнад 15 година старости у другом кварталу 2015. године (Републички завод за статистику Републике Србије)

Из табеле бр. 5 и графикона бр. 3 види се да је код категорије високообразованих грађана значајна разлика између запосленог и незапосленог становништва (19 %) у односу нпр. на средњеобразовано становништво код којег тај проценат износи 58 %. Наведени проценти делимично потврђују могуће проблеме добијене резултатима преходних

истраживања који указују да су подмићивању у циљу обезбеђења запослења склонији грађани вишег образовног нивоа.

Улазак иностраних трговинских ланаца на домаће тржиште, представља такође потенцијални проблем који може да има негативне импликације по економску безбедност грађана. Мотивисани стицањем профита, али и националним интересима држава из којих долазе, такви трговински ланци врше промоцију својих националних производа и форсирају њихову продају како би подстакли извозни потенцијал сопствене државе. Маркетиншком активношћу повећавају продају „својих“ производа нудећи их по повољнијим ценама или истицањем на најприступачнијим местима за купце. Квалитет производа се често замагљује добром маркетиншком промоцијом, а под велом економског и привредног развоја, највећи губитници постају државни буџет и грађани који купују такве производе. Ако при том узмемо у обзир да ТНК најчешће заступају интересе држава из којих долазе и да један од циљева ових компанија може да буде и долазак до информација које за државу домаћина представљају пословну или другу врсте тајне, можемо закључити колико неконтролисан и монополистички положај таквих компанија може да буде опасан по економски статус државе и њених грађана. Поједине транснационалне компаније су у процесу приватизације преузеле већ добро развијене тржишне потенцијале. Доласком до информација које представљају државну и пословну тајну, необновљиви енергетски ресурси су за неколико година експлоатисани до нивоа који је пре тога пројектован од стране државе за неколико деценија. Стављање профита у центар интереса, грађане су оставили без запослења, а државу без природних ресурса, што ће осетити тек генерације које долазе. (Ђурић и Јегеш, 2011)

Један од примера неповољног одражавања економских реформи националних држава у транзицији на економску безбедност грађана запослених у друштвеном сектору предвиђеном приватизационим програмима, представља процес приватизације спроведен у државама у окружењу и у Републици Србији. Поједине фабрике су приватизоване под потпуно неповољним условима, а у самом процесу запослени су остали без

посла, без новчане надокнаде и без правих програма запошљавања. Таква предузећа су врло брзо одлазила у стечај, а радници су завршавали на улицама са врло малим изгледом за поновно заснивање радног односа.

На основу спроведеног истраживања 2010. године (истраживање вршено за период 2001. до 2009. године), искуства у погледу ефеката извршених приватизација и реструктурирања су различита и крећу се у широком распону од неповољних до повољних ефеката (Стошић, Брњас, дедеић, 2010):

Значајан број приватизација у посматраном временском периоду је био потуно неуспешан. Агенција за приватизацију је у поступку контроле (која траје 1-2 године за аукцијску и до пет година за тендерску приватизацију) раскинула уговоре са око 25% до тада приватизованих предузећа. Повод за раскид говора су често били штрајкови, који су ескалирали крајем 2009., а посебно почетком 2010. године. Основни узроци раскида уговора су били неплаћање уговорене цене (и/или инвестиционог програма) и необезбеђење континуитета производње и исплата зарада запосленим. После тога, већина ових предузећа се дошла у још тежи финансијски и пословни положај, са врло слабим изгледима на опоравак. Бројни нови власници, мада су испунили обавезе предвиђене уговором о купопродаји, нису били у стању и/или нису били заинтересовани да обезбеде нормално функционисање купљених предузећа, с обзиром да је приватизација, у не малом броју случајева, била мотивисана стицањем имовине, а не растом обима пословања. Такође, бројни нови власници, не ретко потпуно без искуства у пословању купљеним предузећима, нису били у стању да унапреде њихово пословање. У оваквим ситуацијама, текуће пословање је било угрожено или је пак долазило до гашења доскорашње производне активности. Искуства у погледу извршених приватизација у појединим местима Србији су изразито неповољна, јер је дошло до гашења производне активности у готово свим приватизованим предузећима. У појединим приватизованим предузећима дошло је до одређених, углавном оперативних промена усмерених превасходно ка рационализацији броја запослених. Активности су углавном биле усмерене на отпуштању вишка

запослених, а без посла су остајали најчешће мање квалификовани и административни радници. Захваљујући томе смањени су укупни трошкови пословања и повећана је продуктивност. Повећање конкурентности, базирано искључиво на смањењу запослености и нижим издвајањима за трошкове радне снаге, не може бити једина дугорочна стратегија за остваривање вишег нивоа конкурентности. Промене у појединим, посебно великим "стратешким" предузећима, у првом реду су биле усмерене ка превазилажењу финансијских тешкоћа, а пре свега велике задужености и неликвидности. Тек након финансијске консолидације, која је захтевала значајна средства и време, могу се очекивати већа улагања у модернизацију и осавремењавање производње. У многим од ових предузећа ниво конкурентности је још увек низак. У области реструктурирања предузећа (око 70 некада великих и/или значајних друштвених предузећа) остварени су углавном скромни резултати, мада је управо оздрављење ових предузећа од кључне важности за динамизирање привредне активности, посебно у појединим градовима, регионима (у којима су ова предузећа носиоци привредне активности), а и на нивоу земље у целини. Основни стратегијски правци приватизације кроз реструктурирање су били: а) финансијско реструктурирање (пре свега отпуст, па и отпис дугова, првенствено према држави и јавним предузећима у државном власништву), б) реструктурирање радне снаге – смањивање вишкова запослених (заснивано углавном на тзв. пасивним мерама политике запошљавања, у којима су отпремнине и новчане накнаде финансиране од стране државе, били главни инструмент решавања проблема вишкова лица и ц) организационо реструктурирање (првенствено фрагментација предузећа и појединачна продаја делова предузећа или имовине, заједно са запосленима, те издвајање „non – core" делатности у самостална предузећа). У одређеном броју предузећа (пре свега оних приватизованих од стране „правих" иностраних инвеститора) дошло је до значајнијих унапређења, који се огледају у комплетној промени "анатомије и физиологије" пословања аналогно светским стандардима. Значајно је унапређен и иновиран пословни портфолио, извршена су улагања у модернизацију производне технологије, пословање се заснива на маркетинг

концепту, а ова предузећа све више оријентишу ка извозу, пре свега на околна, али и друга страна тржишта. Нажалост, број таквих предузећа није није велик.

Проблем нетачног извештавања у области рачуноводства такође представља проблем који је потребно анализирати кроз димензију економске безбедности. Једна од основних потреба задовољења информационих потреба пословног субјекта јесте одговарајући информациони систем и његови подсистеми. Рачуноводствени информациони систем, на пример, садржи информације у рачуноводству. Корисници финансијских извештаја у којима су похрањене рачуноводствене информације могу да буду: инвеститори, повериоци, пословни партнери, државне институције. У складу са финансијским извештавањем, које би по правилу требало да буде усаглашено са важећом законском и професионалном регулативом, менаџмент доноси одговарајуће одлуке. Међутим, неретко рачуноводствене манипулације, случајне или намерне, кориснике извештаја доводе у заблуду.

За разлику од грешака, активности које се предузимају с намером да финансијски извештаји буду нетачно интерпретирани називају се преварама, а базирају се, на следећим елементима:

- лажном приказивању значајних чињеница;
- свести починиоца о томе да је представљање лажно или испољавање потпуне немарности на истим;
- лице које добија информацију сматра је као поуздану и ослања се на њу приликом доношења одлуке;
- појави значајне финансијске штете која настаје захваљујући наведеном, а сносе је корисници информација (Шкорић Јовановић, 2009: 14).

Један од најпознатијих светских примера финансијских превара представља случај америчке компаније „Енрон“. Године 2001. „Енрон“ је била седма компанија по снази у САД. Наведена компанија је приказивала приходе које су остваривале њене целине за посебне намене, а обавезе тих целина су исказиване ванбилансно. Компанија је тако преценила своја потраживања за

1.2 милијарду долара, а све то у циљу обмане инвеститора. Као додатни проблем који је ишао у прилог лажном финансијском извештавању, представљала је међусобна зависност менаџера и ревизора, што је противно ревизорским кодексима. (Капаравловић, 2011: 163).

Посебан проблем са аспекта економске безбедности заједнице и њених грађана представља високотехнолошки криминал, који за разлику од осталих врста криминала подразумева употребу рачунара као средства којим се чини кривично дело. Употреба платних картица у интернет куповини, злоупотреба личних података на интернету, су само неке области интересовања лица која се баве овом врстом криминала, а у директној су вези са личном безбедношћу људи. Повећање степена употребе савремених ИКТ–а у пословању привредних субјеката је параметар који директно утиче на стање личне безбедности грађана. Глобални виртуелни свет интернета постао је погодно место за вршење пословних активности и за обављање приватних комуникација, а самим тим постаје предмет интересовања криминалних организација које компромитацијом информација настоје да дођу до додатног профита. Са проширеним границама деловања и различитим појавним облицима, високотехнолошки криминал данас поставља нове изазове којима се угрожавају грађани, колективна безбедност, као и економска стабилност националних држава.

У Републици Србији, у 2015. години, по подацима Републичког завода за статистику Републике Србије, 63.8 % домаћинстава поседује интернет прикључак. Проценат домаћинстава који је користио рачунаре и интернет у претходном периоду је приказан на табели бр. 6.

					%
	РЕПУБЛИКА СРБИЈА [1]				
	2011	2012	2013	2014	2015
Домаћинства која користе рачунаре и интернет					
Рачунари	52.1	55.2	59.9	63.2	64.4
Интернет	41.2	47.5	55.8	62.8	63.8

Извор података: Републички завод за статистику Републике Србије

[1] Од 1999. без података за АП Косово и Метохија

Табела бр. 6: Домаћинства која поседују рачунаре и интернет прикључак у временском периоду од 2011. до 2015. године[49]

Из података приказаних у табели бр. 6 може се извести закључак да је тренд употребе рачунара и интернета у домаћинствима у порасту, што посебно долази код изражаја приликом трговине путем интернета.

Данас, у свету расте број корисника платних картица у трговини путем интернета што утиче повољно на могућност њиховог угрожавања, компромитовања и касније злоупотребе од стране криминалних организација које се баве високотехнолошким криминалом. Тиме себи обезбеђују противправну имовинску, али и друге врсте користи. Прибављање личних података о власнику електронске картице криминалне групе постижу на један од описаних начина у претходним поглављима, а за злоупотребу су им потребни подаци о броју картице, року важности и CCV2 (Card Verification Value2) број који се налази на полеђини картице.[50]

С обзиром на распрострањеност и тренд развоја Интернет превара, за

[49] Проценат домаћинстава са најмање једним чланом старости од 16 до 74 године која имају приступ Интернету од куће.

[50] „Кардерски форуми постали су веома популарни као место и начин за размену знања и вештина потребних за вршење ових кривичних дела, као и за продају података о платним картицама који су на овај начин прибављени. Специјализовани форуми повезују кардере и купце, једне са другима. Они прво купују тест податке, испробају их да виде да ли функционишу како треба и, уколико су задовољни, купују већу количину података ради вршења кривичних дела. Ови подаци се касније користе за преваре везане за класичне видове злоупотреба као што су скидање новчаних износа на банкоматима помоћу лажних платних картица или куповина робе, као и за све друге видове превара типа „card not present“ на Интернету.“ (http://www.kpa.edu.rs/cms/data/akademija/nbp/NBP_2010_2.pdf, 2016, 10. мај)

очекивати је да у наредном периоду јачају везе између високотехнолошког, организованог и привредног криминала. Транснационални организовани криминал у области злоупотребе платних картица имаће експанзију у наведеном виртуелном окружењу. Такође се очекује појачан обим прања новца и злоупотребе платних картица преко „Off shore“ компанија које подржавају онлајн банкарске сервисе и виртуелна казина који су на граници са илегалним активностима.

У области високотехнолошког криминала у Републици Србији, 2014. године, откривено је 780 кривичних дела што је за 8,8 % мање у односу на 2013. годину када је откривено 855 кривичних дела. Преовлађујући облик овог криминала чине фалсификовања и злоупотребе платних картица. У 2014. години откривено је 481 кривично дело овог типа, док је 2013. године откривено 605 кривичних дела.

(http://www.mup.gov.rs/cms_lat/sadrzaj.nsf/informator.h, 2016, 10. мај)

Неки од подиндикатора[51] који указују на проблеме у сфери економске безбедности су:

- *богаћење лица на руководећим позицијама несразмерно новчаним примањима*

  Неквалитетним избором кадрова на руководећим местима у свим областима друштвеног живота стварају се услови за стављање личних интереса наведених лица у примаран план у односу на интересе од општег добра, као и услови за остале врсте злоупотреба у привредним и другим сферама пословања. Несразмерно трошење новчаних средстава лица на одговорним државним функцијама и специфичним административним пословима у односу на регистрована лична новчана примања, посебно осветљава наведени проблем, а надлежним службама указује на могуће злоупотребе наведених лица у склопу спровођења њихове пословне праксе. Злоупореба службеног

[51] Индикатори су преузети из књиге *Индикатори људске безбедности у Србији — извештај за 2004. годину* (Дулић и сар., 2005), а подиндикатори су лично дело аутора дисертације и покушај да се кроз њихово дефинисање превентивна активност надлежних институција у области економске безбедности грађана подигне на виши ниво.

положаја би се могла спровести кроз уступање поверљивих информација заинтересованим субјектима, које би кроз предузимање даљих поступака и мера остварили нелегалну зараду.[52]

- *повећање броја запослених у јавном сектору поред мера о забрани запошљавања*

  Наведени подиндикатор указује на могућност пораста броја случајева примања и давања мита, трговине утицаја као и богаћења лица на одговорним дужностима у државној управи, која учествују у раду комисија за доношење одлука о поступцима запошљавања. Несразмерно потребама, повећање броја запослених у државном сектору представља додатно оптерећење за државни буџет, а уз то ствара могућност за касније злоупотребе у виду пружања противуслуга за обезбеђивање запослења. Уступање информација о кандидатима који су аплицирали за одређено радно место, пре свега о њиховим слабостима и недостацима који могу да определе послодавца на избор приликом запослења, представља један од модела злоупотребе службеног положаја наведених лица. Прикривање стварних информација о другим кандидатима као и промена услова конкурса како би се прилагодили особинама жељеног кандидата, такође представља један од облика злоупотребе.
- *пораст броја случајева додатног рада од стране лица запослених на административним пословима*

[52] Године 2013. припадници МУП–а Републике Србије су у Панчеву извршили хапшење извршног директора блока прераде Рафинерије нафте Панчево и директора дирекције за стратегију и инвестиције блока прераде наведене компаније. Осумњичени су да су починили кривично дело примање мита приликом спровођења тендера за набавку. Један од наведених директора је као председник комисије за набавку уступио неовлашћеним лицима податке који представљају пословну тајну о висини одобреног новца који Рафинерија планира да издвоји у наредном периоду и о понуђеним ценама других понуђача који су учествовали на тендеру. За противуслугу су захтевали новчана средства, а осумњичени су за примање мита у износу од 303.000 евра. (*Новости*, 2013, 13. новембар).

Подиндикатор указује на недовољна примања запослених на одговорним државним пословима и немогућност задовољавања основних животних потреба које се огледају у додатном радном ангажовању. Таква радна активност се често сукобљава са интересима сталног радног места наведених лица или представља домен обавеза запослених које проистичу из редовног радног односа, а наплаћују се као додатне услуге. Наведена лица понекад прибегавају уступању поверљивих информација пословног субјекта заинтересованим странама које им врше надокнаду за противуслугу. Противуслуга може бити у материјалној форми, али и у другим врстама награђивања, протежирања итд.

- *пораст међудржавних инцидената у међународном пословању*
  Неквалитетном провером компанија, лица и дестинација са којима пословни субјект послује може да изазове озбиљан међународни инцидент који сопствену националну државу може да доведе у незавидан положај. То је посебно изражено и осетљиво у случајевима издавања извозних дозвола, приликом извоза наоружања и војне опреме. Поред тога што извозне дозволе могу да буду омогућене одређеном кругу пословних субјеката, чиме се врши њихово протежирање, оне могу да садрже скривене и нетачне информације о земљи увозници, како би се прикрила стварна дестинација извоза наоружања и војне опреме. Један од могућих инцидената у међудржавним односима, који би могао да доведе до озбиљних последица по статус земље извознице у међународним размерама, може да се изазове уколико наоружање и војна опрема, предвиђени за извоз, доспеју у посед милитантних група или држава које се налазе у супарничком односу са неком од признатих међународних организација.
- *пад активности пословног субјекта изазван губљењем пословних партнера*

Један од ресурса пословних субјеката који се штити посебним мерама безбедносне заштите представља знање (know how) запослених. Заштита се нормативно спроводи кроз потписивање низа међусобних уговора и других обавезујућих докумената, који регулишу однос две стране. Практично спровођење заштите се реализује кроз рад надлежних служби или организација које се баве безбедносном заштитом пословног субјекта, тако што се према носиоцима заштићених података спроводе одговарајуће превентивне мере.

- *пораст извозних привредних активности пословних субјеката регистрованих у Републици Србији са пословним субјектима у земљама захваћеним ратом*

  Подиндикатор указује на могуће сумњиве везе лица и привредних субјеката у земљи са лицима и привредним субјектима у иностранству, посебно са земљама захваћеним ратом, економским санкцијама и другим међународним интервенцијама. Одлуком признатих и референтних међународних институција, наведене земље се налазе под одређеним типом санкција које им умањују простор за пословне активности и забрањују неке од специфичних производа и услуга. Прикривањем информација у пословним документима о врстама, садржају или карактеристикама стварних производа који представљају резултат спољнотрговинског пословања, стварају се услови за њихово пласирање на жељену извозну дестинацију, чиме се заобилазе међународне санкције и друге врста забрана.

- *повећан број случајева отицања тајних података пословног субјекта и грађана сразмеран повећаној употреби ИКТ–а*

  Развој ИКТ–а је проузроковао и њихову повећану употребу, како у области пословања, тако и у свакодневним интересовањима и активностима грађана. Свест да се подаци налазе сигурно похрањени у рачунару и да као такви не могу да дођу у посед

неовлашћених лица представља само привидну сигурност корисника, која укључивањем рачунара у друштвене мреже може врло брзо да се доведе у дилему.[53]

На основу размотрених чињеница може се констатовати да наглашено коришћење ИКТ–а са једне стране знатно доприноси унапређењу економске безбедности грађана, а са друге стране условљава је, посебно када је реч о личној безбедности. Наиме, човекова приватност је вишеструко „нападнута“, будући да информације које сам о себи даје или се налазе у информационом систему, могу да дођу у посед непозваних лица. Такође, неквалитетним чувањем пословних информација матичних привредних субјеката, оне могу доћи у посед конкурената чиме се угрожава његов пословни успех. У случају масовне небезбедности пословних информација, такво стање ће у великој мери негативно утицати и на националну безбедност државе. Феномен корупције, повезан са осећајем несигурности постојећих и обезбеђењем нових радних места од стране грађана, а у циљу постизања минималног степена сопствене економске сигурности, представља снажан параметар достигнутог степена економске безбедности једне националне државе.

8.2. БЕЗБЕДНОСТ ИСХРАНЕ И БЕЗБЕДНОСТ ЗДРАВЉА

Избор врсте намирница које се користе у исхрани, учесталост и заступљеност оброка током дана и начин припреме хране, тј. навике у исхрани зависе од више различитих фактора као што су култура и обичаји,

[53] Текстуална база са подацима о личности 5.190.396 грађана Србије, уз више од 4.000 финансијских докумената (укупно преко 19 гигабајта садржаја), била је седам дана јавно доступна на званичном сајту Агенције за приватизацију Србије. Подаци потичу из евиденције носилаца права бесплатних акција коју води Агенција за приватизацију. Објављени су подаци који се односе на имена, презимена, средње име, јединствени матични број грађана и њихов статус у евиденцији носилаца права на бесплатне акције. У погрешним рукама ови подаци могу да доведу до масовне крађе идентитета грађана. О компромитацији података прво је обавештен Повереник за информације од јавног значаја и заштиту података о личности. Процена је да је ово највећи безбедносни пропуст у сфери заштите информационих система и приватности грађана који се десио у последње време у Републици Србији. (*Новости*, 2014, 15. децембар).

утицај породице и социјалног окружења, расположивост и доступност намирница. Навике у исхрани значајно доприносе ризику за настанак прекомерне ухрањености и гојазности, а сем тога, подаци о навикама у исхрани имају велики значај за процену нутритивних фактора ризика за настанак различитих здравствених поремећаја.

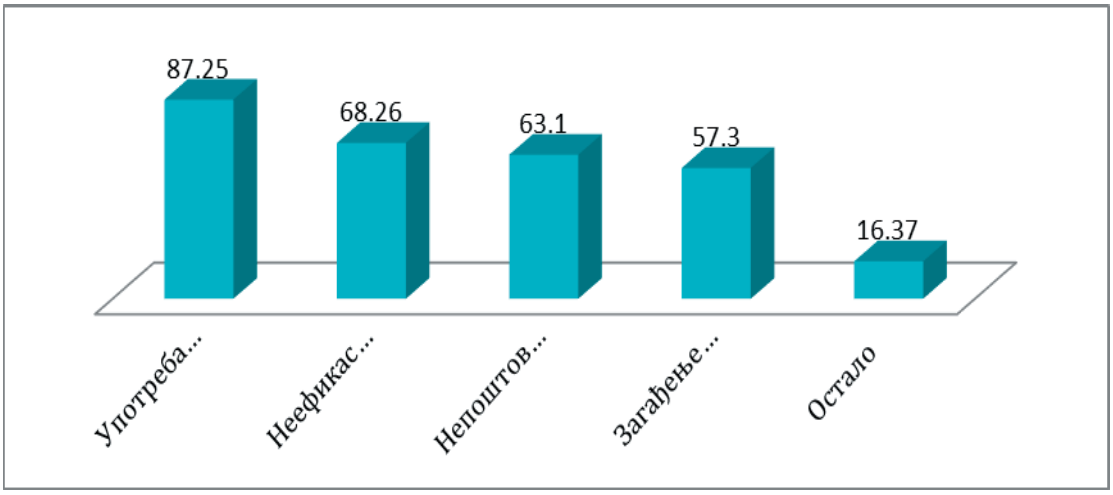
Посебан проблем са аспекта здравља представља неадекватна структура животних намирница, као и њихова физичко–хемијска и микробиолошка исправност. Под изговором заштите производа, поједини произвођачи хране не дозвољавају јавности увид у садржај супстанци који тај производ сачињавају. То свакако аутоматски не имплицира да је тај производ здравствено неисправан, али у времену када профит представља један од највиших циљева пословних субјеката и када важи максима „циљ оправдава сва средства", с правом се можемо запитати да ли је то што конзумирамо одговарајућег квалитета. Дакле, прикривање пословних информација о некој врсти намирница може негативно да се одрази на здравље грађана који егзистирају на одређеном простору, а дугорочно гледано, узимајући у обзир проритете државе у вези праћења и евалуације здравтсвеног стања популације, и на националну безбедност државе.

У даљим разматрањима, анализирани су следећи индикатори који се односе на безбедност исхране и безбедност здравља: микробиолошка исправност животних намирница, фактори који утичу на небезбедност хране, производња хране, навике грађана Републике Србије везаних за исхрану, законска регулатива која се односи на безбедност хране, фактори који утичу на небезбедност здравља и проблеми употребе ИКТ–а у здравству.

На територији Републике Србије је у мрежи института и завода у 2012. години контроли микробиолошке исправности подвргнуто 4502 узорка предмета опште употребе, од чега 2470 узорака домаћег порекла (54,86 %) и 2032 узорака из увоза (45,14 %). Од укупног броја микробиолошки контролисаних узорака, неисправно је било 58 узорака (1,29 %), од чега је 35 узорака потицало из домаће производње (1,41 %) и 23 узорка из увоза (1,13 %). Највећи проценат микробиолошке неисправности утврђен је у следећим групама предмета опште употребе: посуђе и прибор за животне намирнице

(3,63 %), осталим предметима опште употребе (1,76 %) и средствима за одржавање личне хигијене, негу и улепшавање лица и тела (1,49 %). Међу предметима опште употребе који су потицали из увоза, највећи проценат микробиолошки неисправних узорака утврђен је у средствима за одржавање личне хигијене, негу и улепшавање лица и тела (1,84 %). (http://www.batut.org.rs/download/izvestaji/higijena/Zdravstvena%20ispravnost%20predmeta%20opste%20upotrebe%202012.pdf, 2016, 9. мај)

На основу истраживања спроведеног у Републици Србији, од стране стручног тима на челу са проф. Дулић 2008. године (Дулић и сар., 2010: 114)[54], установљено је да испитивани грађани рангирају следеће факторе (три фактора са листе понуђених) који највише утичу на небезбедност хране на следећи начин: употреба недозвољених средстава у производњи хране (87,25 %), неефикасна контрола хране од стране инспекцијских органа (68,26 %), непоштовање стандарда од стране произвођача (63,10 %), загађење земљишта (57,30 %) и друго (16.37%), што је и приказано на графикону бр. 4.



Графикон бр. 4: Фактори који утичу негативно на безбедност хране у 2008. години

Употреба ИКТ–а у здравству, али и у производњи хране је посебно осетљива са аспекта нарушавања људске безбедности и посебно безбедносно

[54] Коришћени су подаци из 2008. године, с обзиром да каснија истраживања, од стране аутора који се баве питањима људске безбедности у Републици Србији, нису вршена. Приказани подаци треба да створе могућност за новија истраживања и паралалне анализе утицаја феномена корупције на безбедност здравственог система у односу на остале системе друштва.

интерсантна због могуће саботаже у делу дозирања прехрамбених компонената у производњи или увозу небезбедних производа.

Један од усвојених стандарда у производњи хране представља „Анализа опасности и критичне контролне тачке" (енгл. *Hazard Analysis and Critical Control Points* — HACCP; http://www.fda.gov/downloads/Food/GuidanceRegulation/HACCP/UCM077957.pdf, 2016, 9. мај). HACCP представља системски превентивни приступ којим се осигурава безбедност хране. Програм се бави превентивним мерама у производњи и промету хране које је потребно предузимати како би се ризик по здравље корисника свео на прихватљиву меру. HACCP програм разматра више следећих фактора, тј. тачака у производњи хране:

Фактори примарне производње се односе на мере које је потребно предузимати од стране произвођача, а односе се на прекомерну употребу пестицида, ђубрива и ветеринарских средстава у производњи инпута и сировина који се користе у даљој производњи. У савременој производњи пољопривредно прехрамбених производа делови овог процеса су аутоматизовани, што значи да компромитацијом информација у овој фази производње може да се утиче на састав хемијских материја, које у одређеним комбинацијама могу да изазивају штетне последице по људско здравље током касније употребе таквих производа у исхрани.

Објекти за производњу треба да омогуће максималне услове за производњу и прераду прехрамбених производа у смислу успостављања контролних механизама којима се врши аутоматска регулација температуре, влажности и других параметара од значаја за несметан производни процес. Изложеност појединих прехрамбених производа вишим температурним опсезима у односу на предвиђене, може да проузрокује микробиолошку неисправност примарних производа, који се преносе у касније фазе производње и такви долазе до крајњег корисника. У циљу елиминације претходно уочених могућих проблема, HACCP програм захтева да се управљање процесом производње реализује кроз успостављање контролних механизама. Одређују се критичне фазе у вези спречавања микробиолошке контаминације, физичке и хемисјке контаминације, проблема који могу бити

последица лошег управљања временским циклусима и температурним опсезима.

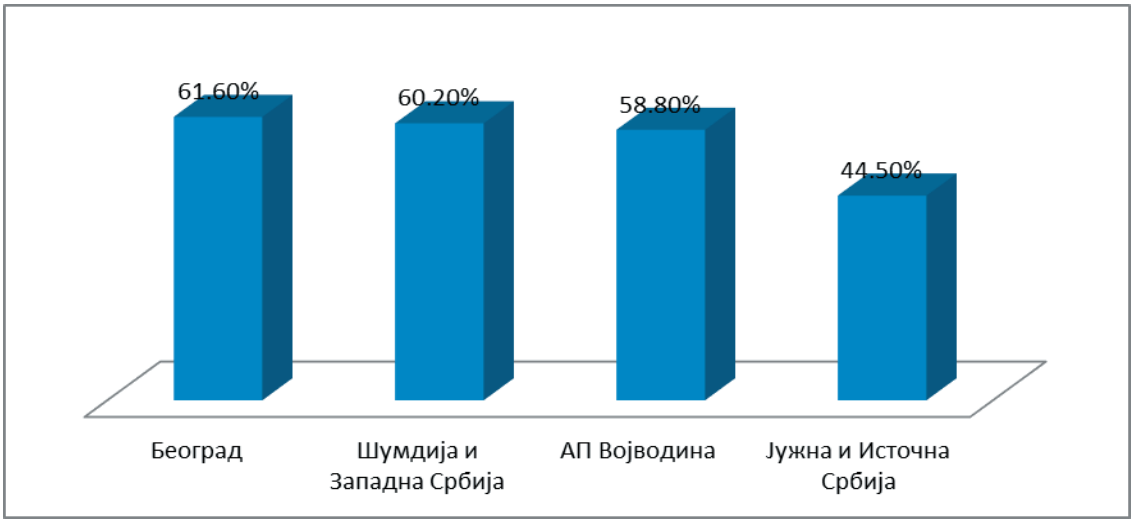
Следећи фактор могућег утицаја на безбедност хране у примени HACCP стандарда јесте *информација о производу* која би требало да буде прецизна и тачна у циљу спречавања нарушавања здравља корисника производа, али и ради правилног управљања залихама од стране произвођача. Нетачна информација о производу, као што су рокови употребе и хемијски састав, може да изазове озбиљне последице по безбедност здравља грађана. Поједини привредни субјекти прибегавају таквим поступцима, као што је враћање у продају залиха којима истиче законски рок употребе, како би избегли финансијске губитке. Посебан проблем представља увоз производа са истичућим роковима трајања, који се касније пакују у нову амбалажу и улазе у промет са информацијама о производу које не одговарају стварном стању.

Институт за јавно здравље Србије је спровео 2013. године истраживање приликом којег се дошло до следећих података везаних за навике грађана Републике Србије у вези здраве исхране (http://www.batut.org.rs/download/publikacije/IstrazivanjeZdravljaStanovnistvaRS2013.pdf, 2016, 9. мај):

- Конзумација воћа и поврћа, производа од велике важности са аспекта здраве исхране, је умерена и повезана је са материјалним стањем домаћинства — 41.1 % најсиромашнијих становника Србије свакодневно конзумира воће, док то чини 48.8 % чланова најимућнијих грађана. Слично, поврће свакодневно конзумира 52.8 % особа које припадају најсиромашнијем слоју и 60.1 % особа које припадају најбогатијем слоју становништва. Чак 54.4 % одраслих становника нередовно или никада не конзумира воће, док 42.9 % становника нередовно или никада не конзумира поврће. О свом здрављу при избору начина исхране не размишља 19.7 % одраслих становника Србије. Проценат оваквог становништва нешто је већи у популацији мушкараца (26.3 %), у Војводини (23.8 %), у руралним типовима насеља (22.7 %), као и међу становницима најнижег

образовног профила (23.6 %). Начин исхране из здравствених разлога променило је 49.1 % грађана у претходној години, при чему су становници урбаних насеља то чинили нешто учесталије у поређењу са становницима руралних насеља (50.9 % наспрам 46.5 %), као и жене у поређењу са мушкарцима (53.1 % наспрам 44.4 %).

- У погледу навика везаних за исхрану, поређење података прикупљених у 2006. и 2013. години открива да је проценат становника који свакодневно доручкује остао непромењен. У 2013. години свакодневна конзумација млека и млечних производа је учесталија у поређењу са 2006. годином (51.7 % наспрам 43.4 %), док је удео становништва које за припрему хране користи животињске масти мањи (25.9 % наспрам 33.6 %). Такође, нешто је мање становника који никада не размишљају о свом здрављу при избору начина исхране (19.7 % наспрам 21.3 %). Са друге стране, удео становништва који конзумира интегралне врсте хлеба значајно је мањи у 2013. години (8.2 % наспрам 14.3 % у 2006. години).
- Међу одраслим особама у Србији које су свесне да сопственим понашањем, у смислу недостатка физичке активности, недостатка воћа и поврћа у исхрани и пушењем, ризикују да оболе од болести срца и крвних судова, чак је 91 % њих који практикују непожељна понашања. Слично, међу особама које су свесне да ризикују да оболе од плућних болести постоји 71.4 % пушача, односно особа са факторима ризика за обољевање од плућних болести.
- Исправно мишљење о утицају фактора ризика на здравље има 56.7 % одраслих становника Србије — у питању су становници који су свесни да њихова понашања у вези са исхраном, физичком активношћу, пушењем, конзумирањем алкохола, и ризичним друштвеним активностима имају велики утицај на здравље. Свест о утицају ових фактора поседује 61.6 % одраслих становника Београда, 60.2 % становника Шумадије и Западне Србије, 58.8 % становника Војводине и 44.5 % становника Јужне и Источне Србије, као што је приказано на графикону бр. 5.



Графикон бр. 5: Свест о утицају фактора ризика на здравље одраслих становника Републике Србије

- Становници градова су у нешто већој мери свесни утицаја наведених фактора на здравље (59.4 %) наспрам становника руралних средина (52.7 %), док су женске особе (59 %) у нешто већој мери свесне од мушких (54.3 %). У поређењу са 2006. годином, проценат одраслог становништва Србије које има исправно мишљење о утицају различитих фактора ризика на здравље се повећао (са 49.1 % из 2006. години на 56.7 % у 2013. години).
- Медијске поруке у вези са здрављем прати 47.4 % одраслог становништва. Ово чешће чине жене (55.6 %) наспрам мушкараца (38.5 %), особе високог образовног профила (55.2 %) наспрам особа ниског образовног профила (43.1 %), као и становници урбаних насеља (49.2 %) наспрам становника руралних насеља (44.6 %). Поређење података из 2006. и 2013. године открива да се повећао удео особа у популацији одраслих становника Србије који прати медијске поруке у вези са здрављем (са 31.3 % на 47.4 %).

Прикупљени подаци и анализа Института за јавно здравље указују на позитиван тренд исхране становништва Републике Србије у посматраном периоду. Позитиван тренд је посебно изражен код високообразованог становништва у односу на остале образовне категорије и код становника

градова у односу на становнике руралних средина. Женска популација је свеснија о утицају фактора ризика на здравље у односу на мушку популацију и у већем проценту прати медијске поруке у вези са здрављем у односу на мушку популацију. Медијске поруке у вези здравља чешће прате особе високог у односу на особе нижег образовног профила и становници урбаних насеља у односу на рурална.

Навике у исхрани представљају један од параметара које је потребно узети у разматрање приликом извођења студија и закључака о степену оболелих, чија је болест узрокована неадекватном конзумацијом хране и пића. Узимајући у обзир чињеницу да неадкеватан унос хране и пића није нужно узрокован немаром грађана, већ да исти може бити последица необавештености или погрешне информисаности грађана о квалитету прехрамбених производа, може се донети закључак да је исправно мишљење о утицају фактора ризика на здравље један од најважнијих индикатора у овој области.

Законом о безбедности хране (Службени гласник Републике Србије, 41/2009) уређени су општи услови за безбедност хране и хране за животиње, обавезе и одговорности субјеката у пословању храном и храном за животиње, систем брзог обавештавања и узбуњивања, хитне мере и управљање кризним ситуацијама, хигијена и квалитет хране и хране за животиње. Циљ овог закона је да обезбеди висок ниво заштите живота и здравља људи и заштиту интереса потрошача, укључујући начело поштења и савесности у промету храном, узимајући у обзир када је то могуће заштиту здравља и добробити животиња, као и здравља биља и заштите животне средине.

- Овај закон прецизира да су субјекти у пословању храном дужни да потрошачу обезбеде информације које дају могућност избора производа на начин који неће да доведе потрошача у заблуду у погледу састава, својстава и намене производа. У супротном, уколико постоји било каква информација о неисправности намирница надлежно министарство је у обавези да обавести јавност о природи ризика по здравље грађана.

- Послове органа државне управе, у области безбедности хране, у фази примарне производње, врше: хране животињског порекла — ветеринарска инспекција, хране биљног порекла — фитосанитарна инспекција; у фази производње, прераде и промета на велико, и то: хране животињског порекла — ветеринарска инспекција, хране биљног порекла и безалкохолних пића — пољопривредна инспекција, мешовите хране — ветеринарска и пољопривредна инспекција, у фази увоза и провоза, и то: хране животињског порекла — гранична ветеринарска инспекција, хране биљног порекла — фитосанитарна инспекција, мешовите хране — гранична ветеринарска и фитосанитарна инспекција; у фази извоза, и то: хране животињског порекла — ветеринарска инспекција, хране биљног порекла — фитосанитарна инспекција, мешовите хране — ветеринарска и пољопривредна инспекција, вина и алкохолних пића — пољопривредна инспекција. Контролу генетски модификоване хране у свим фазама производње, прераде и промета врши фитосанитарна инспекција, а генетски модификоване хране за животиње ветеринарска инспекција.
- За послове лабораторијског испитивања и њима повезане стручне послове у ланцу хране оснива се Дирекција за националне референтне лабораторије, као орган управе у саставу Министарства пољопривреде и заштите животне средине.
- За прво стављање у промет нове хране, генетски модификоване хране и генетски модификоване хране за животиње на територији Републике Србије, субјект у пословању храном, односно храном за животиње мора имати дозволу, у складу са одредбама овог закона и посебних прописа.
- Министарство надлежно за послове здравља, Стручни савет, Националне референтне лабораторије и лабораторије у области безбедности хране и хране за животиње дужни су да воде евиденције, спискове и базе података, усклађене и повезане са

информационим системом Министарства, и у обавези су да их чувају и ажурирају.

- Министарство осигурава усклађивање и повезивање информационог система, са другим информационим системима Министарства, министарства надлежног за послове здравља, као и са међународним информационим системима у области безбедности хране и хране за животиње.

Безбедност здравља

Иако је безбедност здравља у директној корелацији са безбедношћу исхране то не значи аутоматски да је за анализу стања људске безбедности довољна анализа исхране становништва. Квалитет здравственог система са аспекта превентивне и примарне здравствене заштите представља такође битан чинилац безбедности здравља становништва. Посебно осетљив сегмент здравства из области лечења у сфери заштите ИКС–а представља припрема и производња лекова. Саботажа у овом сегменту може негативно да се одрази по здравље пацијената, а у крајњим границама и да доведе до смртних случајева.

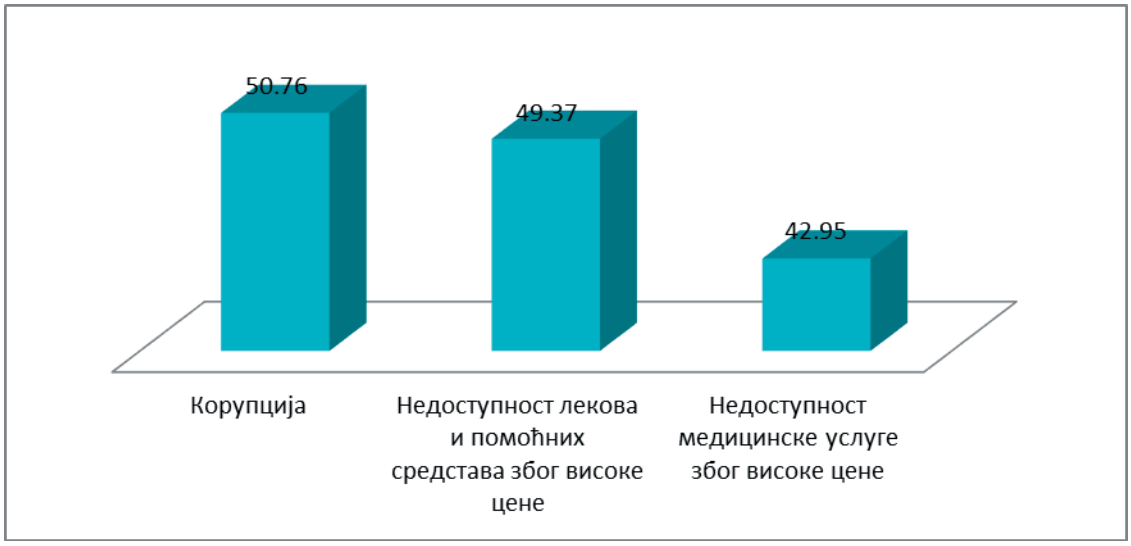
Отежано функционисање здравственог система Републике Србије је последица дотрајале опреме, празних фондова и корупције. Грађани су погођени сиромаштвом, неједнакошћу у погледу приступа здравственим услугама, неуједначеношћу квалитетом пружених услуга, слабостима финансирања здравства и недефинисаном улогом приватних здравствених установа. Здравље представља димензију људске безбедности која заузима прво место на ранг–листи аспеката сигурности грађана Србије. (Дулић и сар.,. 2010: 129)

Истраживање наведене групе аутора такође је показало да на смањење осећаја безбедности здравља утичу: корупција, недоступност лекова и помоћних средстава и недоступност медицинских услуга због високих цена. Спровођењем здравствених програма који би обухватили осетљиве категорије становништва суочених у највећој мери са претходно

дефинисаним проблемима унапредио би се здравствени систем, а самим тим и здравље становника Републике Србије. Програм би такође требао да обухвати категорије лица која немају услове за финансирање здравствених услуга, тако што би им се обезбедило лечење из посебно оформљених здравствених фондова. Потребно је такође ускладити односе између државне и приватне здравствене праксе, чиме би се проширили капацитети пружања здравствених услуга и растеретио државни здравствени систем. Последњу, али свакако не најмање важну меру унапређења здравственог система, представља формирање здравственог информационог система који је у неким здравственим установама започео са радом, али још увек у неформалном облику као помоћно средство за лакше обављање делатности. Јединствен информациони систем би омогућио ефикасније праћење и вршење анализа здравствених проблема са којима се становништво суочава, али би у исто време и омогућио увид у реалне потребе становништва за лековима и другим средствима лечења. Такве анализе би омогућиле надлежним лицима у министарству здравља увид у проблеме сегмената здравственог осигурања који захтевају највећу пажњу. Јединствен здравствени информациони систем би омогућио лакше праћење пацијената у вези лечења, прецизније одређење у вези набавке лекова и осталих потрошних средстава као и јасније прецизирање визије развоја и унапређења здравства Републике Србије у наредном периоду.

На основу већ поменутог истраживања, спроведеног од стране стручног тима на челу са проф. Дулић из 2008. године (Дулић и сар., 2010: 111)[55], установљено је да следећи фактори утичу негативно на безбедност здравља: корупција (50.76 %), недоступност лекова и помоћних средстава због високе цене (49.37 %) и недоступност медицинске услуге због високе цене (42.95 %), што је приказано на графикону бр. 6.

[55] Подаци из 2008. године су узимани у обзир из већ објашњених разлога (види: фуснота 53, 302).



Графикон бр. 6: Фактори који утичу негативно на безбедност здравља у 2008. години

Подиндикатори који указују на безбедносне проблеме у области безбедности исхране и здравља су:

- *појава прехрамбених производа на тржишту који у свом саставу садрже ГМО*

  Као могући узрок испољавања наведеног подиндикатора може да буде недовољно уређена законска регулатива у вези забране производње, увоза, извоза и продаје генетски модификоване хране. Међутим, корумпираност надлежних државних органа који би требало да спроводе одлуке Владе и законске мере којима се забрањује употреба наведених производа, ствара могућност да ГМО ипак дођу до крајњег потрошача. Омогућавање одређеним лобијским групама да спроведу своје циљеве везане за улазак на нова тржишта пласирањем генетски модификоване хране, такође је једна од злупотреба коју је могуће спровести од стране лица на одговорним државним позицијама. Наведена активност се може спровести кроз прикривање информација о декларацији производа, која не садржи одредбе о ГМО садржајима у структури проивода. Такође, израда лажне документације која се односи на здравствено безбедан производ, а не производ који је предмет

увоза један је вид манипулације и компромитације информација од стране надлежних лица. Слаб квалитет рада надлежних стручних и инспекцијских служби такође негативно утиче на појаву забрањених производа на домаћем тржишту, а за последицу, у крајњем случају, ствара неповољно здравствено стање нације.[56]

- *повећање броја оболелих болестима узрокованим конзумирањем хране и пића сумњивог порекла*

  Статистички посматрано повећање броја оболелих у једном региону или држави је узроковано разним факторима који, између осталог, могу да се тичу неправилне исхране и конзумације пића непозантог порекла и састава. Надлежне инспекцијске службе, услед корумпираности или неквалитетног рада, могу да проузрокују проблеме који се директно рефлектују на здравље грађана. Свесним прикривањем чињеница и информација о исправности неког прехрамбеног производа, омогућава се његово стављање у промет и долазак до крајњег потрошача. [57]

---

[56] Кинеске власти су отпустиле три званичника који су дозволили и спроводили контроверзни истраживачки пројекат финансиран од стране САД–а који је укључивао тестирање златног пиринча на деци школског узраста. Званичници су кажњени због „кршења релевантних прописа, научне етике и академског интегритета". Кинеска истрага начина на који је спроведено истраживање такође је изнела доказе који су у супротности са изнетим тврдњама о томе колико је златног пиринча дато деци да једу, у документу о истраживању који је објављен у *Америчком журналу клиничке исхране* (енгл. *The American Journal of Clinical Nutrition*). Један истраживач из Кинеске академије наука је прокоментарисао: „Или су истраживачи сада лагали о овоме или су лагали у свом раду. У сваком случају то је озбиљан прекршај." Претходно, у 2012. је дошло до повлачења студије коју су обавили истраживачи из центра *Danforth* који подржава компанија *Monsanto*, који су тврдили да су пронашли начин да се путем генетског инжењеринга појача протеински садржај касаве. До повлачења је дошло „након што истраживачи нису успели да пронађу било који податак који би потврдио тврдње изнете у раду". Такође је било вести о томе да су истраживачи који проучавају БТ токсине који су употребљени у ГМ усевима користили лажне слике у читавом низу објављених радова. (http://www.nature.com/news/china-sacks-officials-over-golden-rice-controversy-1.11998, 2016, 7. мај)

[57] Стручњаци с Универзитета Рочестер, који се баве истраживањем утицаја хемикалија на људску репродукцију, тврде да је проблем што већина пестицида који се данас широко користе у свету није одговарајуће тестирана. Тако су британски научници утврдили, пре неколико година, да многи пестициди који су се дотад сматрали безопасним лоше утичу на мушке хормоне. Тестови су показали да 30 од 37 тестираних пестицида блокира деловање

На основу резултата претходних истраживања може се констатовати да наглашено коришћење ИКТ–а знатно доприноси унапређењу безбедности исхране и здравља грађана, а са друге стране је условљава, посебно када је реч о безбедној производњи хране. Развој ИКТ је позитивно утицао и на област здравствене заштите, али је и довео у питање безбедност овог система који је у новим условима постао порознији и склон појави разних врста малверзација и других недозвољених активности. Подаци, нпр. здравствени картони осигураника у електронском облику, могу постати лако доступни разним интересним сферама и злонамерним групама који такве податке могу на најразличитије начине да злоупотребљавају. У том смислу би могли постати критични подаци о донорству, јер располагање таквим информацијама може криминалним круговима који се баве трговином људским органима отворити низ могућности да, изазивањем „случајних" несрећних догађаја и слично, дођу до жељеног органа и продају га примаоцу. Такође, подаци о историји болести појединаца могу да се злоупотребе тако што ће бити, без његове сагласности, презентовани другим лицима и здравственим установама које ће их употребити за додатно стицање

мушких хормона. Србија, према потрошњи хемикалија, спада у водеће европске земље и док Министарство пољопривреде стално понавља да је воће и поврће безбедно, представници мултинационалних компанија за производњу пестицида истичу да се 70 % пољопривредних производа у Србији и даље прска пестицидима сумњивог квалитета. Лимун, поморанџа и мандарина из Турске и спанаћ су били најотровнији, али су штетне хемикалије у недозвољеној количини откривене и у грожђу, шљивама, пасуљу, као и у малинама, паприкама и краставцима. Највише пестицида садржи кора јабуке, а следе целер, чери парадајз и краставци, док их је најмање у луку и кукурузу. Више од 50 % обрадиве површине у Србији третира се средствима за заштиту биља. То се чини на основу минималне документације, према закону о заштити биља из 1998. године. Ове хемикалије се у тлу задржавају две деценије, а најгори је DDT који изазива рак и неплодност и који је у другим земљама одавно забрањен. Познато је да и бројни „легални" пестициди узрокују хронични умор, канцер, али и разарају ендокрини систем. Чак 45 % произведене исхране у Србији потенцијално је опасно. Поједини пестициди могу да се користе само у Србији где се региструју с минимумом документације, али не у ЕУ чије земље имају много строжу процедуру. Руска служба за контролу пољопривредних производа „Росељхознадзор" открила је, приликом једне од контрола, да око 60 тона јабука из Србије садржи превисок ниво пестицида. Иначе, Русија је 2009. увезла 145 тона српских јабука с превисоком количином пестицида, а 2011. око 77 тона. Зато је увоз јабука из Србије смањен више од 2,5 пута у односу на 2012. годину. Русија је претходних година била највећи купац јабука из Србије, на то тржиште ишло је 90—95 % укупног извоза овог воћа. (http://www.vesti-online.com/Vesti/Tema-dana/503434/Koliko-je-hrana-zatrovana-pesticidima-1-Veseli-trovaci-na-srpskim-njivama, 2016, 7. мај)

профита, а кроз понуду здравствених услуга које уочени здравствени проблем могу да реше. Дакле, подаци о лечењу и други персонални подаци се морају заштитити посебним мерама безбедносне заштите, а за случајно или намерно одавање података надлежни лекари и остала лица запослена у медицинским установама морају да буду кривично и стручно санкционисани. Узимајући у обзир значај фармацеутске индустрије у Републици Србији, да је тржиште презасићено лековима разних фармацеутских произвођача, да је стављање лекова на такозване позитивне листе континуиран процес, те да је степен корупције у здравственом систему изузетно висок на шта указују подаци из претходних истраживања, могуће је извести закључке о потенцијалним облицима угрожавања здравственог система националне државе. Корупција је феномен који код свих седам димензија представља један од најизраженијих облика угрожавања безбедности људи, а посебно место и негативну улогу заузима у безбедности здравља као концепта људске безбедности.

8.3. ПОЛИТИЧКА БЕЗБЕДНОСТ И БЕЗБЕДНОСТ ЗАЈЕДНИЦЕ

Република Србија се још увек суочава са изазовима транзиције што, између осталог, захтева реформу правосуђа, полиције, јавне управе. Један од приоритета демократизације друштва и успеха реформи јесте задобијање поверења грађана у извршне органе власти, што се између осталог постиже анализом утицаја политичког система на стање људске безбедности кроз квалитетније информисање грађана о раду власти, спречавањем сукоба интереса извршних органа власти, смањењем корупције јавних и државних органа, унапређивањем области људских права. Неки од индикатора који ће се истраживати у поглављу су: равномерност у медијском представљању политичких странака током предизборне кампање, процена степена корумпираности правосудних органа, процена ефикасности спроведених реформи правосуђа, степен поверења грађана у правосудне органе, ставови грађана о корумпираности у јавној и државној управи, однос полиције и

органа локалне самоуправе, процена раширености корупције у полицији, степен поверења грађана у полицију, учешће малолетничког криминала у укупном криминалитету и однос укупног броја извршених кривичних дела у односу на број оптужених и осуђених.

8.3.1 . Утицај политичких структура на медије

Посебну улогу са аспекта безбедности заједнице има могућност злоупотребе медијских сервиса у циљу „пласирања“ дезинформација грађанима и ширења панике, што представља посебан проблем у специфичним ситуацијама, као што је нпр. проглашење ванредне ситуације. Слобода медија утиче на стање политичке безбедности, али и на безбедност заједнице. Поред броја, важан је квалитет медија и власничка структура медија са аспекта могућег монополског утицаја на јавну медијску слику. Објективни истраживачи стања у медијској сфери морали би да спроведу истраживања на терену, радећи упитнике и интервјуе, користећи остале инструменте, а све у циљу сагледавања ставова грађана и новинара о следећим питањима:

- степену слободе штампе,
- утицају власти на уређивачку политику медија,
- постојању контроле над дистрибуцијом штампаних медија,
- степену корупције у медијима и њеном утицају на рад медија,
- процени могућности несметаног извештавања,
- ставовима новинара о постојању политичких притисака на рад медија,
- ставовима новинара о постојању аутоцензуре,
- степену поверења грађана у објективност медија, у зависности од врсте медија. (Ђорђевић, 2013: 137)

Влада Републике Србије је отпочела спровођење Медијске стратегије (2011) и побољшање правног оквира за функционисање медија по стандардима ЕУ. У августу 2014. године је донет Закон о јавном информисању и медијима, Закон о електронским медијима и Закон о јавним

медијским сервисима што представља значајан напредак у овој области. Међутим, поред доношења наведених закона потребно је приказати максималан степен политичке воље и опредељености за имплементацију наведених прописа.

Савет за борбу против корупције је идентификовао и издвојио пет системских проблема који годинама паралишу систем јавног информисања у Републици Србији, а то су: нетранспарентност медијског власништва; нетранспарентност финансирања, економски утицај кроз буџет, пореске олакшице и друге индиректне облике финансирања јавним новцем; проблеми приватизације медија и неизвестан статус јавних сервиса; цензура и аутоцензура; таблоидизација. Савет за борбу против корупције истиче да су спорост у спровођењу медијских реформи, недовољно развијена регулатива и зависност од јавних и приватних извора финансирања довели до тога да у периоду 2011—2014. године медији не остварују улогу која им припада у демократском друштву. Медијски садржаји најчешће нису резултат слободног, објективног или истраживачког новинарства. Због економске зависности и спреге са политичком и економском елитом као и неформалним центрима моћи, већина медија не врши функцију повећања опште информисаности грађана. У претходном Извештају који је сачињен 2011. године Савет је указивао на проблеме недовољно транспарентне власничке структуре медија у Републици Србији. Тада је јавности саопштено да је у посматраном периоду 2008—2010, од 30 најзначајнијих присутних медија, било чак 18 медија чији прави власници нису познати. Савет је указао да је од 11 националних емитера њих 9 са нетранспарентним власништвом. „Такво стање је крајње забрињавајуће уколико се има у виду да је медијским законима у Србији, међународним препорукама и конвенцијама, утврђена потреба транспарентности власништва као услова за успостављање плурализма медија и спречавање недозвољене медијске концентрације.“ (http://www.paragraf.rs/propisi/strategija razvoja sistema javnog informisanja u republici srbiji do 2016, 2016, 10. мај)

Један од проблема у овој области представља податак да су код већине медија компаније регистроване у иностранству, те је готово немогуће

сазнати њихову стварну власничку структуру. Стварни власници су најчешће сакривени иза низа компанија регистрованих на удаљеним "рајским" дестинацијама, где се адвокатске и консултантске фирме јављају као власници у име и за рачун својих клијената. Као могући разлози за оснивање оваквих компанија наводи се пре свега тајност података како о власништву тако и о пословању. Разлози за евентуално тајно пословање су жеља власника да буде скривен од очију јавности, евентуалне пореске олакшице или пореске утаје, прибављање новца за финансирање медијске делатности из нетранспарентних извора и стварање тајних фондова. Ове компаније су најчешће регистроване на адресама адвокатских и консултантских кућа које осим власничке преузимају и дневно оперативне послове за своје клијенте.

Савет за борбу против корупције је на основу спроведеног истраживања закључио да је део штампаних и електронских медија у Србији са већинским друштвеним, односно државним капиталом, под директном контролом политичких странака. Политичке странке медије користе како би очували привилегије власти и обезбедили себи повлашћени положај у изборним кампањама. Зависност јавних медија од новца из јавних извора финансирања је један од облика неформалног утицаја. Други начин директног политичког утицаја на неприватизоване медије манифестује се кроз њихове органе управљања, као што су уредници, директори и чланови управног или надзорног одбора привредног субјекта издавача, односно емитера. Агенција наводи да и у случајевима када се спроводе, јавни конкурси су симулирани и њихов исход је унапред познат. У органима управљања неприватизованих јавних медија не седе новинари или стручна лица већ експоненти политичких странака. (http://www.paragraf.rs/propisi/strategija razvoja sistema javnog informisanja u republici srbiji do 2016, 2016, 10. мај)

Процес приватизације медија се свесно одуговлачио годинама уназад, а исти је у претходном периоду предмет регулације Закона о приватизацији 2002. године, затим Закона о радиодифузији, Закона о јавном информисању.

Препорука Савета за борбу против корупције је да у поступку приватизације медија надлежни државни органи посебну пажњу усмере на

испитивање порекла новца потенцијалних купаца и на транспарентност поступка.

Један од најдиректнијих облика политичке контроле медија у Србији заступљен је током изборних кампања и то кроз време које политичке странке закупе у електронским медијима и кроз огласни простор у штампаним медијима. Највећи део трошкова током изборне кампање 2014. политичке странке су усмеравале на оглашавање на ТВ станицама, што није био случај 2016. Према истраживању Транспарентности Србија, 187 странака су на парламентарне и београдске изборе потрошиле преко 10 милиона евра, што је веома слично са подацима који се односе на изборе из 2012. године. (http://www.transparentnost.org.rs/index.php?option=com_content&view=category&id=39&Itemid=51&lang=sr, 2016, 10. мај)

Министарство надлежно за послове информисања би у циљу отклањања уочених проблема требало да успостави ефикасне механизме мониторинга и надзора над функционисањем система финансирања и суфинансирања медијских пројеката у Републици Србији из буџетских и јавних извора. Такође је потребно успоставити мониторинг и надзор над реализацијом пореских олакшица, донација, буџетских дотација и других облика директне или индиректне државне помоћи која представља могући извор утицаја на медијску независност. Потребно је инсистирати и на транспарентности процеса приватизације медија у Републици Србији и приступ информацијама од јавног значаја.

Агенција за борбу против корупције требало би да на основу извештаја Савета преиспита по службеној дужности да ли постоје разлози за покретање поступка, односно да ли сви функционери у органима управљања медија са државним капиталом поштују прописе који уређују конфликт интереса, укључујући и законске обавезе функционера који су уједно и власници приватних медија. (http://www.antikorupcijasavet.gov.rs/Storage/Global/Documents/izvestaji/izvestaj%20mediji%2026%2002.pdf, 2016, 10. мај)

Нови концепт безбедности подразумева разматрање безбедности локалних заједница, која по неким питањима може да одступа од степена националне безбедности. Специфичности локалне заједнице представљају

ниво привредних активности једног региона, ниво културне и образовне развијености, традиционалне обичаје и друго. Неки од индикатора које је потребно анализирати у контексту овог сегмента дисертације су: анализа рада полиције у одређеној локалној заједници, имајући у виду степен корупције, успех на расветљавању кривичних дела почињених од стране пунолетних лица и кривичних дела почињених од стране малолетних лица по локалитету и осуђена физичка лица према врстама кривичних дела по локалитету.

На основу индикатора и њихове анализе потребно је дефинисати подиндикаторе који указују на проблеме нарушавања безбедности заједнице, а правилним одабиром студија случајева потврдила би се веза између подиндикатора и стања безбедности локалне заједнице. Безбедност заједнице и лична безбедност грађана су у директној корелацији. Анализа стања личне безбендости подразумева анализу неколико фактора од којих је најбитнији криминал са свим његовим појавним облицима, пре свега корупција државних тела.

8.3.2. Корупција и компромитација информација у полицији

МУП Републике Србије је у претходном периоду покренуо активности на успостављању партнерства и усклађивања сопствених активности са активностима других друштвених тела и грађана, а све у циљу креирања безбедне заједнице. Циљ ове кампање је превенција криминалних догађаја на одређеној територији и подизање степена поверења грађана у полицију. Развој информационо–комуникационих технологија је између осталог позитивно утицао на рад полицијских структура у локалним заједницама. Грађани су приступом интернет порталима полицијских станица и управа, могли да се информишу о актуелним дешавањима у свом месту пребивалишта, као и да пријављују уочене неправилности које су у супротности са законодавним системом Републике Србије. Квалитетно и правовремено информисање заједнице о безбедносним догађајима,

ризицима и могућим претњама утицало би и на подизање степена безбедности њених грађана, посебно млађе популације. У исто време, квалитет сарадње грађана са полицијом представља основ за њен успешан рад на превентивном плану деловања. Репресивне мере је потребно свести на минимум захваљујући превентивним мерама, које ће се предузимати против лица већ познатих полицији као потенцијални учиниоци кривичних дела.

Као и у другим државним системима, корупција није заобишла ни систем полиције. Успех у борби против корупције у претходном периоду је унапређен усвајањем законодавног оквира који је заокружен доношењем Закона о јавним набавкама, новог текста Закона о одузимању имовине проистекле из кривичног дела, као и пре тога донетом Закону о изменама и допунама Кривичног законика РС (којим су раздвојене функције одговорног и службеног лица). У примени је и Национална стратегија за борбу против корупције у Републици Србији за период од 2013. до 2018. године, којом су прецизиране активности Министарства унутрашњих послова. Корупција је у раду органа државне управе, аутономне покрајине и локалне самоуправе откривана у неколико видова. У најчистијем виду, *кроз примање и давање мита* (Инспекторат за рад у Министарству рада, запошљавања и социјалне политике); *присвајање новца намењеног исплати физичким лицима или чему другом* (Градска управа града Јагодина; Унија послодаваца Србије); затим у виду *незаконитих исплата запосленима* уз редовна примања (Општина Бабушница); као и у виду *злоупотреба приликом расписивања јавних огласа за давање пољопривредног земљишта у закуп*, а са циљем прибављања користи физичким лицима (СО Ћуприја). Поред тога, можемо поменути и *незаконито признавање права на доделу стамбених просторија* (ухапшени председник и генерални секретар Привредне коморе Београд), као и *незаконито омогућавање извоза психоактивних супстанци* (пријављена начелница Одељења за опојне дроге и прекурсоре у Министарству здравља РС). (http://www.mup.gov.rs/cms_lat/sadrzaj.nsf/informator.html, 2016, 11. мај)

На основу спроведеног истраживања о корупцији у полицији[58], из угла перцепције грађана, дошло се до следећих резултата:

- За више од две трећине грађана корупција у полицији је распрострањена. У истраживањима јавног мњења полиција се увек нађе у првих пет најкорумпиранијих институција. Такво је и тренутно стање, а поред полиције корумпиране су и следеће институције: здравство, царина, судство и тржишна инспекција. Свега 67 % грађана Србије се слаже да полиција најмање делује као сервис грађана. Грађани процењују да је корупција најприсутнија у саобраћајној полицији, те у делу полиције који се бави сузбијањем привредног криминала и у граничној полицији. Делови полиције који су најчешће у контакту са грађанима су и најлошије оцењени. Ипак, распрострањеност корупције је повећана у односу на пре две године у деловима полиције који се баве борбом против привредног и организованог криминала. Огромна већина грађана сматра да је корупција нешто нормално у нашем друштву, да је има свуда, па и у полицији. То је превасходно став грађана Београда и становника урбаних средина. Мала је могућност да корумпирани полицајци буду ухваћени је такође њихов став. Највише неслагања постоји око тога да ли су мале плате узрок корупције. Половина становништва се слаже са тим, посебно грађани Београда, док друга половина има супротно мишљење.
- Грађани су репресивне мере одредили као главне методе борбе против корупције у полицији. Заступљен је став да је преко потребно строго кажњавати починиоца коруптивне радње (22 %), али и корумпиране руководиоце у полицији (21 %). Ово је у складу са претходним налазом о томе да су високопозиционирани полицајци највише корумпирани. Као и пре две године, присутан је проблем пријављивања случајева корупције у полицији уз обавезу давања личних података грађана.

[58] Регионално истраживање јавног мњења о интегритету полиције, које је осмислила и спровела мрежа Point Plus. Теренски део истраживања обавио је IPSOS STRATEGIC MARKETING на репрезентованом узорку од 1205 пунолетних грађана Србије у јуну 2015. године. (http://www.vreme.co.rs/cms/view.php?id=1314669, 2016, 12.мај)

Главни разлог је страх и лична безбедност. Цивилно друштво би, према мишљењу грађана, највише требало да сарађује са државом у борби против корупције.

Проблем цурења информација је стар колико и сама полиција, а његова учесталост и извесност некажњавања починилаца увећана је у висококорумпираним земљама попут Србије. У извештају организације *Transparency international* за 2014. годину стоји да Србија према индексу перцепције корупције заузима 72. место од 177 земаља. Све земље бивше СФРЈ, изузев Босне и Херцеговине, боље су рангиране. У циљу спречавања „цурења“ информација из полиције, формулисани су различити кодекси и законски чланови, како на нивоу УН, тако и у нашем Закону о полицији. Они налажу да се поверљиве информације морају чувати ради заштите безбедности и слободе лица које је дало обавештење, као и да се подаци о њему могу одати само ако је то у интересу правде или обављања дужности. У МУП-у Србије за ову сврху постоје три одељења: Одељење за заштиту законитости у раду, Сектор унутрашње контроле полиције и Одсек за контролу законитости у Жандармерији. Међутим, насупрот регулативи и прописима, у полицији овај проблем и даље постоји, а истраживањем које је спроведено утврђено је неколико главних разлога због којих долази до „цурења” информација из полиције:

- Ниска примања припадника полиције — продавањем поверљивих информација припадници полиције покушавају да ниска примања надоместе узимањем мита. Иако су у Србији полицајци плаћенији од лекара или, рецимо, од припадника Војске Србије, њихова просечна месечна зарада од око 500 евра далеко заостаје за платама њихових колега у земљама са малим индексом корупције. Ово је означено као проблем и у Стратешко обавештајној процени корупције у полицији, коју је сачинио Сектор унутрашње контроле полиције;
- Поремећен систем вредности у друштву — млади полицајци нису могли остати имуни на опште промене у друштву изазване транзицијом, ратовима и стварањем климе у којој криминалци постају идоли младих;

- Људски ресурси — на негативну селекцију људи који обављају полицијски посао утиче корупција приликом запошљавања припадника полиције. Такође, није довољно уређена обаст којом би се спречио допунски рад полицајаца који може представљати сукоб интереса. На пример, полицајац ради као обезбеђење у локалу неког криминалца, ког би сутра по службеној дужности требало да „обрађују".
- Недовољно развијен систем заштите узбуњивача — овај проблем је у полицији увећан постојањем ћутања о проблему. Према Стратешко обавештајној процени корупције у полицији, коју је сачинио Сектор унутрашње контроле полиције, чак 75 % полицајаца не предузима ништа уколико сазна за неке коруптивне радње својих колега.

„Цурење" информација из полиције оставља тешке последице по рад полиције, међу којима су: рушење дуготрајних истрага, скривање криминалаца од хапшења, угрожавање сигурности заштићених сведока, као и припадника МУП–а, запослених у судству или тужилаштву, обесхрабривање узбуњивача. То коначно води ка губљењу поверења грађана у МУП. Зато је важно под хитно отпочети решавање овог проблема. (Корупција у полицији: случајеви, 2014)

8.3.3. Корупција и компромитација информација у правосуђу

Један од најважнијих задатака држава је организовање правног система који треба да омогући сваком право приступа независним и непристрасним правосудним институцијама организованим на основу закона. „Владавина права и демократија захтева уређење правосудних институција тако да се учини равноправна доступност правде свим грађанима, оснивањем независних и самосталних правосудних институција, које су обезбеђене материјално и са довољним бројем носилаца правосудних функција, способних да у разумном року доносе квалитетне одлуке као основ извршења, односно основ за остваривање појединачних права грађана."

(http://www.antikorupcijasavet.gov.rs/Storage/Global/Documents/izvestaji/Pravosudje%20konacno%20!.pdf, 2016, 10. мај)

Анализа стања корупције у правосуђу је, између осталог, неопходна због прикупљених података који сведоче да је на почетку реформе из 2009. године било укупно 1.318.059 нерешених предмета, на крају 2014. године 2.849.360, а на крају 2015. године 2.837.468. Правосуђе очигледно није учињено ефикаснијим што имплицира да реформа правосуђа није још увек дала очекиване резултате. Иако је основана нова мрежа судова, нису смањени трошкови остваривања правде. Остало је непознато колико је државу коштала реформа мреже правосуђа из 2009. године. О проблемима функционисања судова и тужилаштава говори податак о броју делегираних надлежности[59] који је износио 6.888 за период од 01.01.2014. године до 12.10.2015. године. Број делегираних предмета може да се посматра из угла неравномерне доступности правди, али такође представља индикатор за намештање предмета у циљу спровођења корупције. Савет за борбу против корупције у свом извештају из 2016. године наводи да је имао лоше искуство са делегирањем предмета, нарочито код стечаја, где је било очигледно да се делегирање врши због захтева извршне власти. (http://www.antikorupcijasavet.gov.rs/Storage/Global/Documents/izvestaji/Pravosudje%20konacno%20!.pdf, 2016, 10. мај)

Савет је обрадио у реферату стечаја „Сартида" у току 2002. и 2003. године (један од 24 предмета приватизације) делегацију са Привредног суда у Пожаревцу, који је био један од најажурнијих стечајних судова, на Привредни суд Београд, који је био један од најнеажурнијих судова у стечајним поступцима. Савет је закључио да је Делегација извршена искључиво због тога да би предмет добио судија по жељи извршне власти, јер су министри и други људи из тадашње власти били заинтересовани за циљану продају одређеном купцу без спровођења законског поступка. Савет је поднео иницијативу за покретање кривичног поступка у односу на судију и друге учеснике у овој трансакцији. Овај случај, између осталог, указује на

[59] Преношење овлашћења на други суд да води поступак (lat. forum delegatum)

проблем независности и самосталности правосуђа у Републици Србији. (http://www.b92.net/info/vesti/index.php?yyyy=2013&mm=06&dd=21&nav_category=16&nav_id=725227, 2016, 10. мај)

Једна од препорука којима би се постигли позитивни помаци у оваквој ситуацији јесте доношење групе правосудних закона заснованих на јасним елементима и мерилима поштовања начела „природног судије“. Истраживање Светске банке реализовано 2014. године (http://www.mdtfjss.org.rs/pub/serbia-judical-functional-review/#p=10, 2016, 10. мај) указује на то да правосуђе није независно и да је стање у овој области погоршано у односу на 2009. годину. Наведена институција износи податак да 25 % судија, 33 % тужилаца, и око 60 % адвоката имају утисак да судије и тужиоци нису независни, односно самостални. Дакле, запослени у правосуђу сматрају да у правосуђу није остварен основни стандард и начело да свако има право на правично суђење од стране независног правосуђа.

Перцепција грађана о независности правосуђа према истраживању спроведеном у новембру 2014. године које је обавио „Ипсос” (поглавља 23 и 24) је још више поражавајућа — преко 80 % грађана не верује да је правосуђе у Србији независно од политике и других интересних групација. (http://www.euractiv.rs/pregovori-sa-eu/8212-graani-srbije-ne-veruju-institucijama-, 2016, 10. мај) Проблем представља чињеница да је изузетно мали број поступака у последњих неколико година спроведен од стране надлежних институција против вршилаца правосудних функција. Један од могућих разлога представља непостојање воље за реализацију таквих поступака, а други је садржан у специфичностима и тешкоћама приликом доказивања евентуалних починилаца кривичних дела из ове области.

У Извештају Европске комисије о напретку из 2014. истиче се да је „Србија наставила са спровођењем препорука Групе земаља Савета Европе за борбу против корупције (ГРЕЦО). Имплементација стратегије и акционог плана за период 2013—2018 године тек треба да покаже постојање снажне политичке воље за борбу против корупције, а спровођење неколико предложених мера за смањење корупције је одложено”. (http://www.antikorupcijasavet.gov.rs/Storage/Global/Documents/izvestaji/Prav

osudje%20konacno%20!.pdf, 2016, 10. maj). Извештај такође наглашава да је неопходно да се обезбеди механизам за праћење спровођења стратегије за борбу против корупције и акционог плана, као и да се морају одредити и одговарајући ресурси и људски капацитети за њихово спровођење.

Проблем корупције у судству датира из претходног периода. Ранија истраживања наводе на закључак да је корупција у правосуђу изазивана системским и социјалним узроцима. Системски узроци корупције су резултат недореченост Устава и закона. Судије и председнике судова, деведесетих година прошлог века, бирао је парламент на предлог њеног одбора за послове правосуђа. Министар правде је достављао предлагачу своје мишљење о кандидатима, тако да је извршна власт имала свој утицај на избор судија и на разрешење судија, пошто је и ова иницијатива могла доћи и од ресорног министра и од скупштинског одбора за послове правосуђа. Јавно тужилаштво је било такође декларативно самостални државни орган, на челу са Републичким јавним тужиоцем. Њега је такође бирала Народна скупштина на предлог одбора за послове правосуђа, док је заменике јавних тужилаца бирала Народна скупштина на предлог Републичког јавног тужиоца. Републичког јавног тужиоца разрешавала је Народна скупштина на предлог надлежног скупштинског одбора, док је заменике јавних тужилаца разрешавала Народна скупштина на предлог Републичког јавног тужиоца. Овлашћења политичких власти у поступку избора и разрешења носилаца правосудних функција, као и зависност нижих тужилаца од виших, имали су утицај на вршење судијске, односно јавнотужилачке функције. А они су злоупотребљавани и у коруптивне сврхе. Законом о изменама и допунама Закона о судијама из 2003. године установљено је Веће за питања судске управе које је овлашћено да утврђује предлог за избор и разлоге за разрешење председника судова, што представља још неповољнију околност са аспекта независности правосудних органа. Именовање наведеног већа које чине председник одбора Народне скупштине за послове правосуђа, министар надлежан за послове правосуђа, председник Врховног суда Србије и четири судије које бира Народна скупштина створило је услове за повећање утицаја политичке власти на судове. Један од проблема са којима се данас суочава

судство је смањивање мреже правосудних органа на нижим нивоима што доводи до прекомерне оптерећености и неажурности у вршењу послова. Поједини центри моћи користе затрпаност предметима у раду неких судија, те пребацивањем предмета на рад код других судија, испољавају свој утицај на исход суђења. „Коруптивни насртаји се редовно ослањају на мане у садржини и примени прописа о положају носилаца правосудних функција. А њих је било и превише. Ево неких: Поступак реизбора судија и тужилаца је извршен на нетранспарентан начин. Високи савет судства и Државно веће тужилаца радили су у привременом саставу, кад је реч о члановима из реда судија, односно јавних тужилаца и њихових заменика. Њихов избор извршен је на начин одређен у прелазним одредбама закона о успостављању ових тела, које нису биле предочене Венецијанској комисији. Мандат ових чланова престаје избором сталних чланова из реда судија, односно јавних тужилаца и њихових заменика, али они настављају функцију у непосредно вишем суду, односно непосредно вишем јавном тужилаштву.“ (http://www.nadzor.org.rs/dosije%20korupcija/Zoran%20Ivosevic%20%20Korupcija%20u%20pravosudju%20i%20pravosudni%20sistem.pdf, 2016, 10. мај)

Због уочених недостатака у прописима и недоследној примени, један део судија је поново биран иако нису испуњавали услове за то (судије које су учествовале у изборним крађама (више од 20), за које је Велико персонално веће утврдило да постоје разлози за разрешење (9), које су биле у сукобу интереса, које су доносиле дубиозне одлуке, које су реметиле јавни ред и мир, које су практиковале насиље у породици, које су биле неуспешне и неажурне, које су на разне начине компромитовале судијску функцију. Са друге стране нису реизабране неке судије које су изузетно успешно судиле, биле савесне, посвећене позиву, ефикасне и ажурне. (http://www.nadzor.org.rs/dosije%20korupcija/Zoran%20Ivosevic%20%20Korupcija%20u%20pravosudju%20i%20pravosudni%20sistem.pdf, 2016, 10. мај)

Подиндикатори који указују на проблеме безбедности заједнице и личне безбедности:

- *заступљеност приватних медија у односу на државне* — Однос приватних и државних медија је један од параметара

који указује на степен демократског уређења државе. Заступљеност локалних информативних медија, такође осветљава стање у наведеној области. Злоупотреба медија од стране политичких чинилаца, али и од појединаца, представља један од проблема који директно утиче на политичку безбедност заједнице и националне државе у целини. Злоупотреба медија се може изразити кроз неадекватно коришћење медисјког простора, објављивањем нетачних или полутачних информација, злоупотребом службеног положаја лица на одговорним позицијама, обезбеђивањем неравноправног односа медија у односу на друге медијске субјекте итд.

- *обученост лица која су укључена у борбу против тежих облика корупције и злоупотребе службеног положаја, а пре свега дела која се односе на високо—технолошки криминал* — Квалитет рада истражних органа је у директној вези са њиховом способношћу да препознају актуелне појаве и дела из области криминала који настаје употребом савремених технологија. Едукација запослених у тужилаштву, судству и истражним органима је предуслов успешног супротстављања најсавременијим облицима криминала. Паралелно са развојем ИКТ–а, развијали су се и облици злоупотребе истих од стране лица са лошим намерама, које разним врстама злоупотреба врше криминалне активности усмерене против појединца, али и против државе. С обзиром на међународна обележја кривичних дела из области високотехнолошког криминала, потреба за едукацијом и сарадњом између истражних органа националних држава додатно долази до изражаја.
- *отицање службених података* — Отицање података је један од подиндикатора који указују на могућу корупцију у полицији као и у судским органима. Подаци о лицима која су

> предмет интересовања истражних органа или подаци о прикупљеним доказним материјалима од стране правосудних органа, окривљеним или осумњиченим лицима омогућава избегавање или умањење санкција. На претходно изведене тврдње указује и спорост судства у решавању предмета и мали број осуђених лица у односу на број покренутих тужби и поднетих кривичних пријава, као и намерно склањање и одуговлачење у решавању предмета.[60]

На основу размотрених чињеница може се констатовати да повећано коришћење ИКТ–а доприноси унапређењу политичке безбедности грађана, посебно у делу који се односи на транспарентност рада политичких партија, квалитетнијем информисању грађана о раду власти, као и смањењу корупције јавних и државних органа. Појединачни случајеви неадкеватног коришћења медија у политичке сврхе још увек не угрожавају политичку безбедност грађана Републике Србије у мери која би захтевала хитно реаговање у овој области. Иако политичка безбедност нема битнијег негативног утицаја на стање националне безбедности Републике Србије, повећан степен корупције у виталним државним целинама, као што су судство и полиција, указује на потребу озбиљнијег реаговања надлежних институција, у циљу подизања степена националне безбедности државе.

---

[60] Полицијске операције „Гром 1“ и „Гром 2“ требало је да задају одлучујући ударац нарко–мафији у Србији, играјући пре свега на карту тајности и изненађења. Међутим, након што се слегла медијска прашина, из самог врха власти стигла су упозорења да су поменуте акције дале скромне резултате и да је један од главних разлога за то „цурење” информација из полиције. Пажњу на то скренуо је сам председник Републике Србије, који је навео да те акције нису донеле очекиване резултате јер су шефови нарко–мафије унапред били обавештени о могућим акцијама. Јавност је као и обично уверена да је реч и спрези полиције и криминала, али челници полиције сматрају да је реч о обичној несмотрености полицајаца у свом приватном окружењу и да су на тај начин информације стигле до криминалних кругова. Према мишљењу стручњака из ове области, „цурење” информација из полиције свакако постоји, јер организовани криминал и не би био тако моћан и организован да нема спреге криминалаца и моћи, односно извршне власти. Парламентарна и унутрашња контрола полиције је нешто на чему би требало стално инсистирати. То је процес без краја, на коме се мора радити како би се побољшала ефикасност полиције и смањила корупција у њеним редовима. (http://www.politika.rs/scc/clanak/295374/Sta-je-trulo-u-srpskoj-policiji, 2016, 12. мај)

8.4. ЕКОЛОШКА БЕЗБЕДНОСТ

Управљање животном средином, са аспекта очувања еколошке безбедности као концепта људске безбедности, сложан је процес који захтева одговарајуће алате за поуздану процену ризика и претњи, као и касније доношење квалитетних одлука. Нагли раст светске популације и снажан економски напредак, а са друге стране све већи притисци за побољшање животног окружења и услова за здраву животну средину, представљају сложен и тежак задатак институција које се баве еколошком безбедношћу. Безбедност животне средине представља заштиту животне средине и виталних интереса грађана, друштва и државе од унутрашњих и спољних утицаја, штетних процеса и трендова економског развоја који угрожавају здравље људи и опстанак човечанства, биодиверзитета и одрживост функционисања екосистема. Проблеми, тј. ризици, који се јављају у животној средини одражавају се негативно на здравље људи, а ако узмемо у обзир да је ¼ болести у свету узрокована променама животне средине, схватићемо колико су превентивне мере еколошке безбедности важне за здравље и у крајњем случају, опстанак човечанства (Wenning et al., 2007: 19–36).

Еколошка безбедност је термин који се користи за проблеме који повезују стање животне средине са интересима националне безбедности. Деградација животне средине и недостатак ресурса су важни фактори који могу да створе или појачају опасност по националну безбедности и да изазову политичку нестабилност и насилан сукоб. Такође, наведени фактори могу да проузрокују миграције становништва и да појачају већ постојеће тензије на неком простору. Неки од најупечатљивијих узрока деградације животне средине који се могу довести у контекст рада су: неадекватно управљање нуклеарним отпадом, загађење воде, загађење ваздуха, јонизујуће и нејонизујуће зрачење. (Дулић и сар., 2007) У том смислу потребно је одредити индикаторе који утичу на еколошку безбедност, извршити њихово мерење и одредити подиндикаторе којима се превентивно делује на стање еколошке безбедности у Републици Србији. Неки од индикатора који ће бити анализирани у овом поглављу су: емисија NO_2, CO_2 и

SO_2 по глави становника, број дана у години са прекораченом емисијом загађујућих материја, број оболелих од респираторних обољења и број идентификованих загађивача ваздуха.

Квалитет ваздуха је посебно осетљив на следеће, уједно највеће, изворе загађења: термоенергетски објекти (термоелектране, топлане), рафинерије, хемијска индустрија, депоније. Поред тога на квалитет ваздуха снажно утиче и сагоревање моторних горива посебно у случају аутомобила који користе горива са високим процентом сумпора у свом саставу. У циљу праћења степена загађености ваздуха на подручју Републике Србије спроводи се контрола квалитета ваздуха, што подразумева мерење неколико параметара који одређују квалитет: сумпор–диоксид, суспендоване честице (дим, чађ и прашина), азотови оксиди, угљен моноксид и приземни озон. [61]

Загађење ваздуха, контаминација воде, бука и зрачење су најважнији параметри животне средине који утичу на нарушавање здравља људи. Прекомерна изложеност људског организма загађеном ваздуху може да проузрокује директна оштећења респираторног система. Савремен начин живота, савремени животни стилови, свакодневно утичу на промену животне средине. Када говоримо о савременом начину живота, пре свега мислимо на употребу техничких достигнућа којима се човек служи како би себи омогућио комфорнији и лагоднији живот, не водећи при том рачуна како таква средства утичу на животну средину, на здравље човека као појединца и, у крајњем случају, на еколошку безбедност људи. Неумерена употреба аутомобила и пловних објеката са емитовањем издувних гасова у спољну средину, утиче на квалитет ваздуха који удишемо и воде коју конзумирамо, што касније доводи до нарушавања здравља људи. Код људске популације се јављају проблеми на дисајним путевима, затим проблеми са болестима типа дијабетес I и II, неке врсте канцерогених обољења и слично.

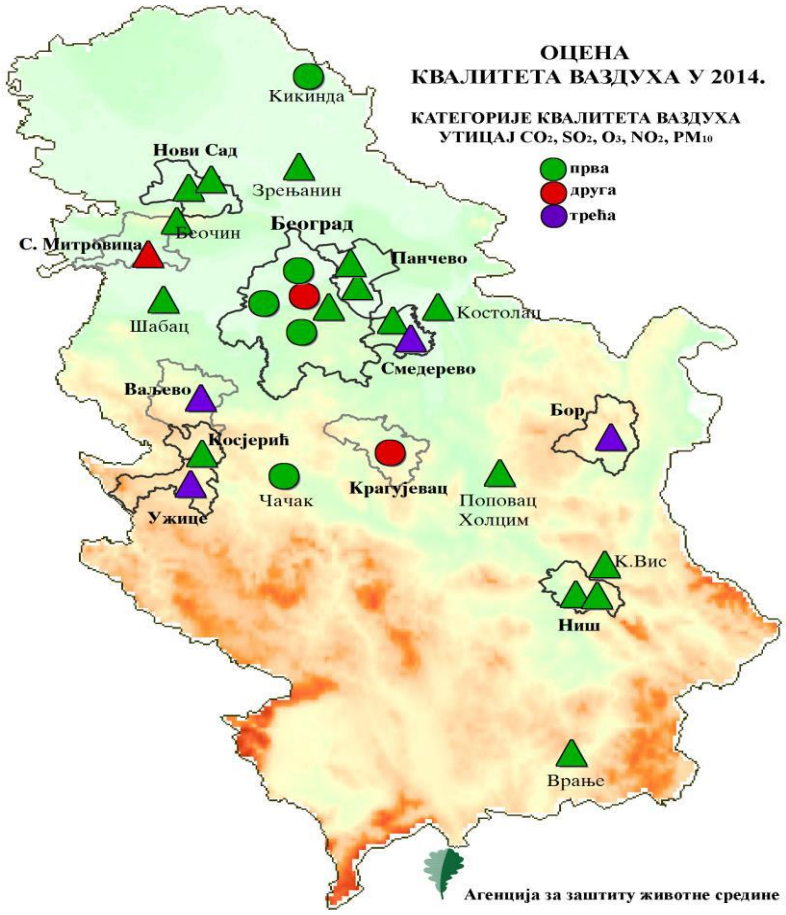
[61] Подаци о квалитету ваздуха дати су на основу систематских аутоматских мерења нивоа загађујућих материја у државној мрежи за праћење квалитета ваздуха на нивоу Републике Србије. Подаци су резултат праћења квалитета ваздуха на основу Уредбе о условима за мониторинг и захтевима квалитета ваздуха (Службени гласник Републике Србије, 11/10 и 75/10), Уредбе о утврђивању програма контроле квалита ваздуха у државној мрежи (Службени гласник Републике Србије, 58/11) и Уредбе о утврђивању зона и агломерација (Службени гласник Републике Србије, 58/11), донетих у складу са Законом о заштити ваздуха (Службени гласник Републике Србије, 36/09).

Без обзира на ком делу земаљске кугле човек живи, он је изложен утицају хемикалија у ваздуху, канцерогеним средствима у храни и другим стварима са којима је у окружењу.

Агенција за заштиту животне средине спроводи континуирано спровођење оперативног мониторинга квалитета ваздуха у државној мрежи за праћење квалитета ваздуха на нивоу Републике Србије. Ова обавеза Агенције је дефинисана у Закону о заштити ваздуха (Службени гласник РС, 36/09, 10/13).

На слици бр. 8 приказана је оцена квалитета ваздуха у Републици Србији за 2014. годину.[62]

[62] Према нивоу загађености, полазећи од прописаних граничних и толерантних вредности, а на основу резултата мерења, утврђују се следеће категорије квалитета ваздуха: прва категорија — чист или незнатно загађен ваздух где нису прекорачене граничне вредности нивоа ни за једну загађујућу материју; друга категорија — умерено загађен ваздух где су прекорачене граничне вредности нивоа за једну или више загађујућих материја, али нису прекорачене толерантне вредности ни једне загађујуће материје; трећа категорија — прекомерно загађен ваздух где су прекорачене толерантне вредности за једну или више загађујућих материја.



Слика бр. 8: Категорије квалитета ваздуха 2014. — оцена у складу са Законом о заштити ваздуха (http://www.sepa.gov.rs/download/VAZDUH2014.pdf, 2016, 9. мај)

Законом о заштити ваздуха уређује се управљање квалитетом ваздуха и одређују мере, начин организовања и контрола спровођења заштите и побољшања квалитета ваздуха као природне вредности од општег интереса која ужива посебну заштиту. Одредбе овог закона не примењују се на загађења проузрокована радиоактивним материјама, индустријским удесима и елементарним непогодама.

Заштита ваздуха остварује се: успостављањем, одржавањем и унапређивањем јединственог система управљања квалитетом ваздуха на територији Републике Србије; очувањем и побољшањем квалитета ваздуха кроз утврђивање и остваривање мера у области заштите како би се спречиле или смањиле штетне последице по здравље људи и/или животну средину; избегавањем, спречавањем и смањењем загађења која утичу на оштећење

озонског омотача и климатске промене; праћењем, прибављањем и процењивањем одговарајућих података о квалитету ваздуха на основу мерења и стандардизованих метода; обезбеђивањем доступности података о квалитету ваздуха; извршавањем обавеза у складу са потврђеним међународним уговорима; међународном сарадњом у области заштите и побољшања квалитета ваздуха и осигурањем доступности тих података јавности.

Оцењивање квалитета ваздуха врши се обавезно у погледу концентрација сумпор диоксида, азот диоксида и оксида азота, суспендованих честица ($ПМ_{10}$, $ПМ_{2.5}$), олова, бензена и угљенмоноксида, приземног озона, арсена, кадмијума, никла и бензо(а)пирена, а понекад и за друге загађујуће материје, које су као такве утврђене релевантним међународним прописима. У табели бр. 7 дате су вредности за неке од наведених елемената загађења.

Табела бр. 7: Емисије загађујућих материја у 2014. години

NO_2	**Gg**	**147,59**	**142,44**	**143,73**	**168,92**	**171,89**	**184,45**	**187,89**	**132,82**
SO2	Gg	489,68	509,85	473,97	436,40	422,23	470,42	433,47	429,45
PM_{10}	Gg	64,92	45,04	47,79	49,08	53,04	51,72	53,20	45,31
Cd	Mg	3,87	2,39	1,93	1,77	1,78	1,89	1,82	1,87
As	Mg	13,12	9,33	7,35	6,38	5,82	6,57	6,10	6,34

(Агенција за заштиту животне средине)[63]

Извори података за извршене прорачуне су: ресорна министарства за поједине области, Републички завод за статистику и пословни субјекти који имају обавезу извештавања Агенцији за заштиту животне средине. (http://webrzs.stat.gov.rs/WebSite/repository/documents/00/01/91/84/11_Zivotna_sredina.pdf, 2016, 10. мај)

Утицај сумпордиоксида на стање квалитета ваздуха је карактеристика агломерације Бор, где условљава прекомерно загађен ваздух, III категорију. Утицај NO2 на стање квалитета ваздуха је најизразитији у агломерацији Београд, где условљава умерено загађен ваздух, II категорија квалитета ваздуха. Прекорачења дневних граничних вредности од 50 $\mu g/m^3$ током 2014. године било је на свим мерним местима: Ваљево 162 дана, Ужице 146 дана,

[63] Вредности емисија добијене су у складу са методологијом EMEP/EEA према UNECE и Конвенцији о прекограничном загађењу ваздуха на великим удаљеностима (CLRTAP).

Смедерево 133 дана итд. Највеће дневне концентрације PM_{10} током 2014. измерене су у Ваљеву 448 μg/m^3 и Ужицу 382 μg/m^3. Услед повећаног присуства PM_{10}, ваздух је био III категорије у Смедереву, Ваљеву и Ужицу. Измерене концентрације угљен моноксида нису ни 2014, у процедури оцењивања квалитета ваздуха, условиле појаву загађеног ваздуха. Током летњег периода концентрације O_3 могу условити епизоде умерено загађеног ваздуха у урбаним подручјима. У 2014. години, у државној мрежи станица за квалитет ваздуха, није прекорачена ниједна гранична ни толерантна вредност за олово нити су биле прекорачене дневне граничне вредности. Средње годишње вредности кадмијума и арсена нису прекорачиле циљне вредности док је средња годишња концентрација никла једино на станици Ужице. (http://www.sepa.gov.rs/download/VAZDUH2014.pdf, 2016, 10. мај)

У циљу ефикасног управљања квалитетом ваздуха успоставља се јединствени функционални систем праћења и контроле степена загађења ваздуха и одржавања базе података о квалитету ваздуха (мониторинг квалитета ваздуха). Кад се прекорачи концентрација о којој се извештава јавност, утврђена актом из члана 18. став 1. Закона о заштити ваздуха, или концентрација поједине загађујуће материје опасне по здравље људи, Министарство, надлежни орган аутономне покрајине и надлежни орган јединице локалне самоуправе, дужан је да обавести јавност путем радија, телевизије, дневних новина, интернета и/или на други погодан начин.

Закон такође прописује да је надлежни орган дужан да обавештава друге органе и организације и јавност путем електронских и штампаних медија најмање у једном локалном листу на сваком од службених језика, као и путем интернета о: квалитету ваздуха; плановима квалитета ваздуха и одлагања на одређено време постизања граничне вредности за азотдиоксид, бензен и суспендоване честице $ПМ_{10}$; плановима за достизање циљних вредности у зонама и агломерацијама у којима је дошло до прекорачења циљних вредности; годишњем извештају о свим загађујућим материјама које су обухваћене овим законом.

Информација о квалитету ваздуха садржи нарочито: ажуриране податке о концентрацијама загађујућих материја у ваздуху које су

обухваћене Законом о заштити ваздуха, а нарочито сумпордиоксид, азотдиоксид, суспендоване честице ($ПМ_{10}$), приземни озон и угљенмоноксид; просечне вредности концентрација у ваздуху у просечном периоду за приземни озон, граничне вредности за заштиту здравља људи, концентрације опасне по здравље људи, критичне нивое за заштиту вегетације, циљну и граничну вредност за $ПМ_{2,5}$.

У случају прекорачења концентрације опасне по здравље људи и концентрације о којој се извештава јавност, надлежни орган има обавезу да обавештава јавност о локацији или подручју прекорачења, врсти концентрације која је прекорачена (концентрација о којој се извештава јавност или која је опасна по здравље људи), времену почетка и трајању прекорачења, највишој једночасовној концентрацији, односно највишој осмочасовној средњој концентрацији у случају приземног озона, географском подручју на коме се очекује прекорачење концентрације о којој се извештава јавност и/или која је опасна по здравље људи, прогнозама за наредни период са очекиваним променама загађења са проценом промене, подацима за посебно осетљиве групе становништва, могућим ефектима по здравље и препорученом понашању (подаци о посебно осетљивим групама, опис могућих симптома, предузимање препоручених мера, нове информације о току догађаја) и подацима о превентивним мерама за смањење загађења. (Службени Гласник Републике Србије, 36/2009, 10/2013)

Подаци о квалитету ваздуха се налазе у информационом систему квалитета ваздуха који води Агенција за заштиту животне средине. Циљеви информационог система су: интегрални приступ подацима о животној средини, централизована база података отвореног типа, аутоматизована размена података и информација у електронској форми, приступ подацима и информацијама коришћењем интернет технологија — свако располаже својим подацима, заштита података од неовлашћеног приступа, основа за анализу стања животне средине, изградња основе система за подршку у одлучивању, размена података са Европском агенцијом за животну средину.

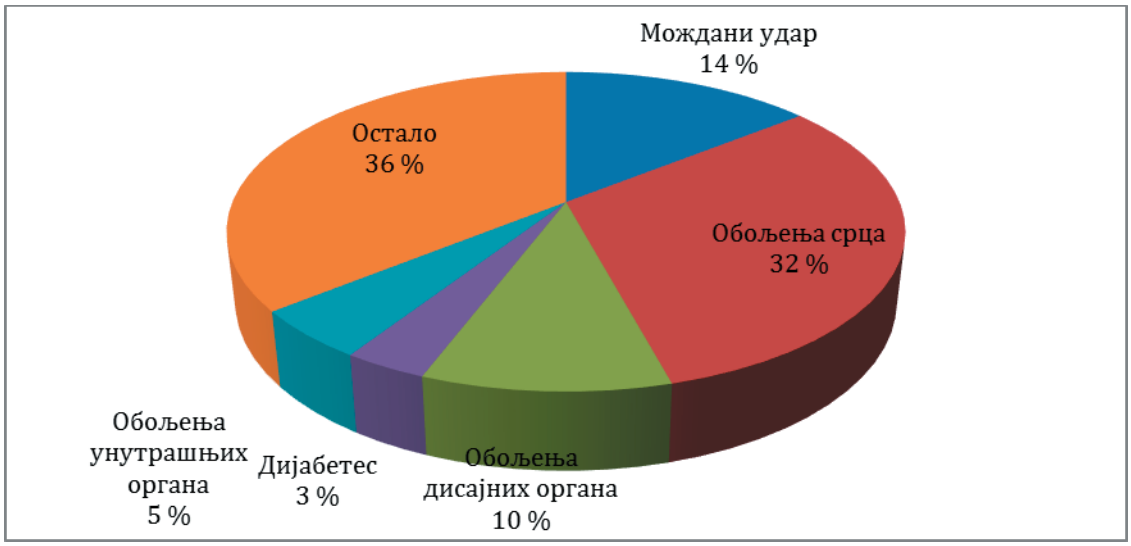
Због проблема загађења ваздуха јављају се разне хроничне болести код становништва. Неке од њих су хроничне незаразне респираторне

болести (ХНРБ), као што су хронична опструктивна болест плућа и астма. Карактеристика ових болести је ограничење протока ваздуха у дисајним путевима. Ово ограничење је обично прогресивно и удружено са поремећеним запаљенским одговором плућа на честице и гасове. Институт за јавно здравље Републике Србије је 2007. године спровео опсежно десетогодишње истраживање које је обухватило и хроничне незаразне респираторне болести којима је изложено становништво Републике Србије. У односу на 1997. годину, стопе морталитета од ХНРБ у свим узрасним групама су у 2007. години биле ниже. Са стандардизованом стопом морталитета од 19,0 на 100.000 становника у 2007. години, Србија се налази у групи земаља Европе са средње високим вредностима стопа умирања од ХНРБ (3). Највеће стопе морталитета од ХНРБ запажене су у Киргистану (99,0/100.000), Казахстану (56,5/100.000) и Молдавији (51,9/100.000), а најниже у Грчкој (0,2/100.000), Бугарској (2,6/100.000) и Француској (8,3/100.000). (http://www.batut.org.rs/download/publikacije/Zdravlje%20stanovnika%201997-2007.pdf, 2016, 9. мај)

Хронична опструктивна болест плућа најчешће се испољава као хронични бронхитис и емфизем плућа. Најважнији фактор ризика за настанак ове болести је активно пушење. Остали фактори ризика укључују генетску предиспозицију, алергију, вирусне и гљивичне инфекције, као и срединске факторе. Астма се дефинише као хронични инфламаторни поремећај дисајних путева, који се испољава понављаним епизодама гушења и „свирања" у грудима, што је последица дифузне, углавном реверзибилне опструкције дисајних путева. Обољење карактеришу егзацербације, које су најчешће провоциране бројним алергенима, иритантима и вирусним инфекцијама.

Према истраживању Светске здравствене организације 2013. године (http://www.who.int/gho/countries/srb.pdf?ua=1, 2016, 7. мај) смртност као последица хроничних плућних болести у Републици Србији је у благом опадању и налази се на осмом месту са процентом од 2.8 % у односу на друге узроке смртности. На десетом месту се налази рак плућа као узрок смртности у проценту од 2.2 % који је такође у врло благом опадању, чак би се могло

рећи да стагнира у односу на посматрани период 2010 — 2012. године (графикон бр. 14).



Графикон бр.14: Најчешћи узроци смрти у 2012. години
(http://www.who.int/gho/countries/srb.pdf?ua=1, 2016, 9. мај)

Према подацима Агенције за заштиту животне средине, у 2014. години регистрована је највећа концентрација SO_2 је у Београду (Мостар) — 21 микрограма/m^3, затим следе Ваљево — 17 микрограма/m^3, Београд (Врачар) — 16 микрограма/m^3 и Нови Сад (СПЕНС) — 14 микрограма/$м^3$. Могло би се закључити да је у наведеним деловима највећа концентрација узрокована, пре свега, прекомерном употребом аутомобила, који представљају у овом случају највећи извор загађења ваздуха. Ниједан дан није забележена горња гранична вредност концентрације SO_2 која износи 125 микрограма/$м^3$. Анализом присуства NO_2 установљено је да је највећа концентрација натријум диоксида била изражена у Београду (Мостар) — 43 микрограма/$м^3$, затим следи Врање — 33 микрограма/$м^3$, Ужице — 32 микрограма/$м^3$ и Београд (Врачар) — 29 микрограма/$м^3$. Само три дана је забележена повећана концентрација натријум диоксида са вредношћу преко 85 микрограма/$м^3$, која представља горњу граничну вредност за ову супстанцу. На послетку, анализираћемо присуство PM_{10} у појединим регионима у Републици Србији. Највећа концентрација олова је у Крагујевцу и она износи 42 микрограма/$м^3$, следи Панчево (Содара) — 38.1 микрограм/$м^3$, Ниш — 38 микрограма/$м^3$ и Косјерић — 35 микрограма/$м^3$. Крагујевац је у 2014. години 90 дана имао

повећану концентрацију олова која је била већа од горње граничне вредности која износи 50 микрограма/м$^{3.}$ Осамдесет дана прекомерне концентрације олова забележено је у Косјерићу, 79 у Панчеву (Содара), 73 у Нишу и 48 у Београду (Мостар). Велика концентрација олова је последица тешке индустрије, као и издувних гасова моторних возила. (http://www.sepa.gov.rs/download/Izvestaj2014.pdf, 2016, 8. мај)

Проблем складиштења нуклеарног отпада представља такође један од проблема који снажно утичу на стање еколошке безбедности. Од укупног броја извора јонизујућег зрачења који се користе у Републици Србији око 80 % се користи у медицини, 15 % у индустрији и око 5 % отпада на остале делатности. (Дулић и сар., 2007: 115)

Главне врсте јонизујућег зрачења јесу радиоактивна зрачења која настају као резултат спонтаног распада радиоактивних атома. Друга врста је рендгенско или Х–зрачење. Један од највећих проблема са којима се суочава Република Србија када је овај индикатор у питању јесте решавање радиоактивног отпада Института „Винча“, последице НАТО бомбардовања и контаминација делова земљишта осиромашеним уранијумом, што је такође аспект који је потребно узети у обзир приликом анализа јонизујућег зрачења.

Подиндикатори који указују на проблеме у безбедности животне средине и здравља су:

- *пораст броја оболелих од болести респираторних органа у индустријски развијеним регионима*

  Квалитет рада инспекцијских служби у области здравља и исхране грађана може да утиче на пораст броја оболелих на одређеном локалитету. Посебно су неке болести карактерситичне за индустријски развијене регионе у којима се услед производње нарушава квалитет ваздуха, као што је случај са болестима респираторних органа. Иако су захтеви у вези коришћења најсавременијих филтера у производним погонима све већи, поједини производни комплекси се не придржавају прописаних процедура. То чине, пре свега, због обезбеђивања већег профита у односу на конкуренте узимајући у обзир цену

коштања филтера и друге опреме која се користи за прочишћавање ваздуха. Квалитет рада оглашивача који врше мониторинг ваздуха је такође један од параметара који утиче на безбедност здравља грађана. Објављивањем нетачних информација од стране оглашивача о квалитету ваздуха, грађани не предузимају превентивне радње којима би се отклониле или делимично ублажиле штетне последице по њихово здравље.[64]

- *повишен степен радиоактивности и јонизујућег зрачења*

  Повишен степен радиоактивности може да буде узрокован недовољно регулисаном законском регулативом у вези складиштења нуклеарног отпада или складиштења материја које емитују штетно зрачење у околину. Такође, неправилан и површан рад инспекцијцких служби може да узрокује наведени проблем и да здравље грађана доведе у повишен ниво опасности.

[64] У последњих десет година, болести система за дисање су по броју оболелих на првом месту, а по смртности на трећем узимајући у обзир сва заразна обољења у Панчеву и у јужном Банату. Пошто је загађење један од окидача ових болести, оно што је уочено као проблем јесте да, иако се континуирано мери концентрација суспендованих честица, за сада не знамо које загађујуће материје оне носе са собом. Анализа података из здравствених извештаја од 2003. до 2012. године показала је да су респираторне болести најчешће од свих болести на подручју Панчева и јужног Баната. У последњих десет година, болести система за дисање заузимају прво место у оболевању, а треће место у умирању становништва. Најчешће болести од којих становништво умире су упале плућа, опструктивне болести система за дисање и бронхијалне астме, а посебно место заузимају малигне болести респираторног система — карцином плућа и бронхија, а потом и рак ларинкса. Када је реч о факторима ризика за настанак болести дисајних органа, поред генетског наслеђа, као важан фактор издваја се и утицај животне средине. Присуство извесних честица у ваздуху може да представља одређен ризични фактор. Најопасније и најризичније су честице најмањег промера, јер оне најлакше доспевају у дисајни тракт. То су оне које имају одређен хемијски састав, који може да делује неповољно, а честице делују двојако — контактом или хемијским процесима тако што изазивају запаљења. Једино је код чађи познат састав честица, те о његовом хемизму и дејству по здравље може поуздано да се говори. Све друге честице су класификоване по величини. Њихов хемијски састав би морао да буде предмет посебних анализа да би се могло утврдити да ли садрже одређену количину сулфата, нитрата или неких других супстанци. Епидемиолошке студије су показале да пораст честица у ваздуху доводи до пораста умирања и погоршања респираторних болести, као што су астма и хроничне опструктивне болести. (http://rtvpancevo.rs/Vesti/Lokal/od-zaraznih-bolesti-u-pancevu-prva-oboljenja-disajnih-organa.html, 2016, 9. мај)

Заштита ИКС–а у великим постројењима чијим би урушавањем еколошком систему била нанета штета несагледивих размера (хемијска индустрија, термоелектране) је такође важан параметар који посредно утиче на безбедност здравља грађана.

- *повишен степен емитовања штетних гасова у атмосферу*

  У последње време, сведоци смо прекомерне употребе аутомобила и других техничких средстава о којима грађани не поседују тачне информације, у овом случају информације о степену емитовања штетних гасова у атмосферу, а од стране произвођача су окарактерисани као изузетно мали емитери штетних гасова. Злоупотребе произвођача и надлежних контролних органа у вези тачности података о емитерима штетних гасова представљају још један параметар који утиче на безбедност здравља људи. Разлози за прикривање тачних података леже у намери пласирања таквих производа на тржиште у складу са најсложенијим еколошким захтевима, иако ти захтеви од стране произвођача нису испуњени.[65]

На основу размотрених чињеница може се констатовати да повећано коришћење ИКТ–а има изузетан значај за унапређивање еколошке безбедности грађана, посебно у сегменту који се односи на монторинг

[65] Компанија Volkswagen је, од стране Агенције за заштиту животне средине САД, оптужена за скривање података са софтвера у својој популарној дизел линији аутомобила како би заобишла стандарде везане за емисију издувних гасова. Компанија није негирала оптужбе, а продаја поменутих модела је заустављена у САД–у. Volkswagen је у Канади повукао ове моделе са тржишта, док се слична ствар дешавала и у европским земљама. Наиме, софтвер уграђен у аутомобиле је показивао нормалан ниво издувних гасова при тестирањима, док је на путу емисија била далеко изнад законом прописаног нивоа. Акције компаније су пале за 20 %, делом због тога што ЕПА указује да је могућа казна за овакав пропуст чак 18 милијарди УСД, а делом из разлога што је Volkswagen само на тржиште САД–а извезао 482.000 возила. Компанија је имала проблема и када су, 2007. године, донесени нови стандарди о емисји издувних гасова и била присиљена да прекине са продајом својих дизел модела. До преокрета долази 2009. године са такозваним "clean diesel" моделима, који су се сада показали и не толико чистим. Поред штете због високих казни и стајања залиха, најављују се и тужбе. Најнепријатнији део целе приче огледа се у томе што потрошачи сматрају да их је Volkswagen намерно обмануо, да су купили једну ствар, а добили другу. За потрошаче, једноставно, није постојала шанса да не буду обманути јер је превара била сакривена дубоко унутар компјутерских чипова, а аутомобили су, уз то, имали и ЕПА печат са дозволом. (http://lakodokola.com/articles/news/315, 2016, 9. мај)

података о највећим загађивачима који негативно утичу на здравље грађана. С друге стране, евентуална компромитација података о вредностима загађивача утиче на непредузимање превентивних мера на заштити здравља грађана и каснију појаву обољења и здравствених проблема. Важну улогу у спречавању оваквих делатности имају надлежне инспекцијске службе и контролни органи. Узимајући у обзир стратешка државна опредељења о здравственом надзору, контроли ризика и претњи по јавно здравље, могуће је извући закључак да се повећањем степена еколошке безбедности, као концепта људске безбедности, подиже и ниво националне безбедности Републике Србије.

9. ФУНКЦИОНАЛНИ МОДЕЛ ЗАШТИТЕ ПОСЛОВНИХ ИНФОРМАЦИЈА

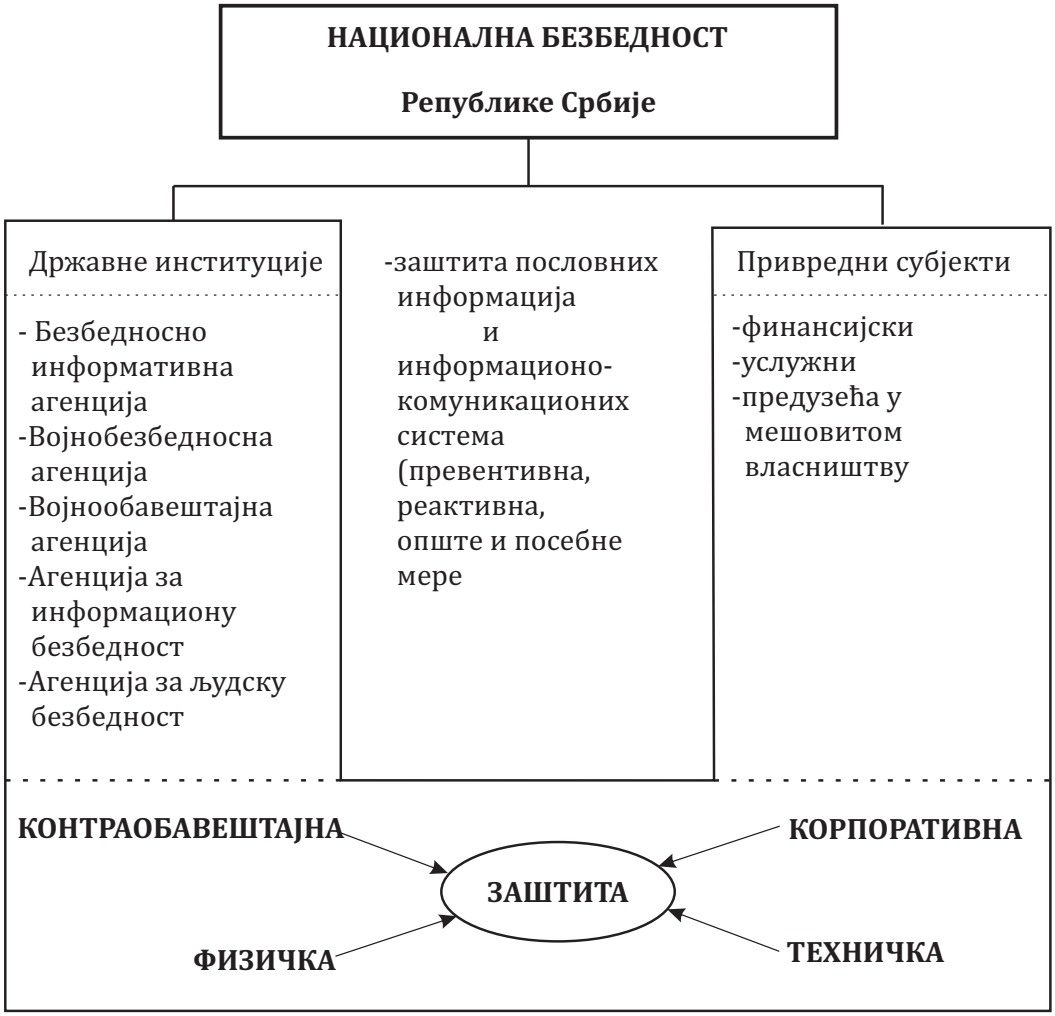
Заштита пословних информација у условима глобализације пословних активности, ограничености суверенитета и свеприсутности информационо–комуникационих мрежа представља велики безбедносни изазов. Угрожавање интегритета пословних система требало би да се посматра слојевито, јер последице могу да се рефлектују на глобалном, националном и нивоу привредних субјеката, односно грађана. Неадекватна заштита критичних информација може да утиче на успешност у пословању, ефикасност рада државне управе и безбедност система на свим нивоима. Имајући у виду потенцијалне последице по безбедност људи неопходно је успостављање система са јасно утврђеним процедурама и поступцима за сваки од могућих сценарија и на свим нивоима у систему.

Националне државе у глобализацијским токовима штите своје интересе усвајањем и имплементацијом законске регулативе у складу са међународним нормама, а које им обезбеђује чланство у међународним организацијама и савезима. Те организације повољно утичу на колективни систем заштите и заштите националних држава, али у исто време отварају питања о могућим негативним контекстима нарушавања државних суверенитета. Међународну сарадњу, у том смислу, спроводе разменом сазнања државних институција и елемената заједничких тела, али и служби безбедносног система, које разменом података и информација безбедност сопствене националне државе подижу на виши ниво. Најзначајнију улогу у спровођењу мера безбедносне и контраобавештајне заштите националних интереса има безбедносно–обавештајни систем националне државе.

Заштитом пословних информација великих компанија, државне обавештајне и контраобавештајне службе, штите и националне интересе, јер је пословање таквих компанија уско повезано са интересима националних држава, посебно у делу који се односи на буџетско финансирање и на повећање стопе запослености. У том смислу, заштита пословних информација се односи на све пословне процесе, без обзира да ли се ради о истраживачким пројектима, производним процесима или кадровским решењима.

Са аспекта заштите пословних информација посебан проблем представљају привредна друштва у мешовитом власништву, нпр. у власништву државе и иностраног партнера. У таквим привредним субјектима тела која се баве корпоративном заштитом налазе се директно под контролом већинског власника, а уколико је то инострана компанија, под контролом те компаније. Под контролом се подразумева да менаџмент компаније, кога поставља већински власник, поставља и разрешава руководство корпоративне заштите. У случајевима када се менаџменту компаније достављају подаци који представљају одређени степен тајности за државу, у смислу заштите критичних инфраструктура или су од значаја за функционисање институција система, онда се с разлогом може поставити питање оправданости такве структуре. Државни интереси би се могли заштитити тако што би се извршила подела надлежности менаџмента који води корпоративну заштиту, на тај начин што би се у оквиру истог поставило стручно лице из државног сектора, које би уједно представљало спону између државе и власника страног капитала. За ефикасно суочавање са оваквом реалношћу, у погледу заштите пословних информација, исправно је овај национални задатак поверити Агенцији за информациону безбедност и Агенцији за људску безбедност[66], дакле државним институцијама које би доприносиле ефикасности националног система безбедности Републике Србије (шема бр. 6).

[66] Агенцију за информациону безбедност и Агенцију за људску безбедност би требало основати по предложеном функционалном моделу заштите пословних информација.



Шема бр.6: Носиоци заштите пословних информација

Формирањем Агенције за информациону безбедност[67], у оквиру надлежног министарства, која би у свом саставу имала стручњаке за безбедност, аналитичаре и друга релевантна лица, а у сарадњи са надлежним државним службама безбедности, могло би да се одговори на захтеве менаџмента таквог привредног субјекта и по потреби врши контрола заштите пословних информација од државног значаја са којима компанија располаже. Такође, Агенција за информациону безбедност би учествовала у вршењу провера и додели безбедносних сертификата корисницима података класификованих као „државна тајна", „строго поверљиво" и „поверљиво", а

[67] Према предложеном функционланом моделу Д.Т.

класификацију пословних тајни би спроводило надлежно тело за корпоративну безбедност. Поред тога, учествовала би на организовању стручних семинара за едукацију запослених на пословима корпоративне заштите.

На шеми број 8 *(Функционални модел заштите пословних информација - прилог бр.1)* приказан је предложени (могући) функционални модел заштите пословних информација у којем су систематизовани паралелни односи, везе и повратне спреге између институција и организација укључених у процес заштите.

У оквиру Агенције за информациону безбедност, у складу са Законом о информационој безбедности[68], дефинисале би се мере заштите од безбедносних ризика у ИКС–у, одговорност правних лица приликом управљања и коришћења ИКС–а и одређивали би се надлежни органи за спровођење мера заштите, координацију између чинилаца заштите и праћење правилне примене прописаних мера заштите. Делови Агенције за информациону безбедност би били: Тело за координацију послова информационе безбедности као координационо тело Владе, у чији састав улазе представници министарстава надлежних за послове информационе безбедности, одбране, унутрашњих послова, спољних послова, правде, представници служби безбедности, Канцеларије Савета за националну безбедност и заштиту тајних података, Генералног секретаријата Владе, Управе за заједничке послове републичких органа и Националног ЦЕРТ–а и Национални центар за превенцију безбедносних ризика у ИКТ системима. Поред привремених чланова, Агенција би требала да има и стално запослене стручњаке чији је задатак да својим радом превентивно делују у циљу спречавања безбедносних ризика у домену информационе безбедности. Привремено учешће представника надлежних министарстава и служби безбедности подразумева да се они састају по потреби, то јест у ситуацијама када се безбедносни инцидент већ догодио. Формирањем Агенције за информациону безбедност, са стално запосленим стручним лицима која се

[68] Усвојен од стране Народне скупштине Репубике Србије јануара 2016. године.

баве овом проблематиком, квалитет рада на спречавању безбедносних инцидената и решавања захтева мешовитих привредних субјеката, а који се односе на уступање осетљивих информација иностраном партнеру, би се подигао на виши ниво, а решавање таквих захтева добило ефикаснији и ефективнији епилог. Компарацијом анализа безбедносних ризика од стране Тела за координацију послова информационе безбедности и Агенције за људску безбедност, Агенција за информациону безбедност би спроводила додатне активности у циљу заштите и спречавања евентуалне компромитације пословних информација.

Корисници података би, према предложеном моделу, били у обавези да потпишу изјаву којом се обавезују на чување тајних података и по престанку рада у таквим привредним субјектима, те би им се, у том смислу, одредио одговарајући степен одговорности која може да буде кривична, прекршајна, дисциплинска, облигациона или морална. Агенција за корпоративну заштиту, у сарадњи са Агенцијом за информациону безбедност, перманентно би предузимала мере из своје надлежности на заштити података и информација, примењујући притом опште и посебне мере заштите. Опште мере заштите се односе на процену података, физичко–техничку заштиту, избор одговарајуће просторије за рад, избор лица за рад са подацима, забрану уношења и употребе техничких средстава и контролу предузетих мера. Посебне мере заштите би се односиле на дефинисање односа са страним физичким и правним лицима (процена лица, припрема запослених, зоне кретања, забрана непосредног увида), вођење прецизне евиденције о подацима, дефинисање упутстава за рад са подацима, комисијско уништавање радних материјала, дефинисање изјаве о чувању тајности, криптозаштита, примопредаја података и других радних материјала и друге мере. „Сирови“ или необрађени подаци би затим прошли процес класификације, односно одредио би им се одређени степен тајности. Подаци који представљају државну тајну или су такве природе да садрже одговарајући степен поверљивости, достављали би се кориснику у складу са правилом најмањег овлашћења, чиме би се смањила могућност за њихово отицање. Подаци би се перманентно проверавали и вршила би се њихова

анализа од стране стручних тимова запослених у оквиру Агенције за информациону безбедност, а по потреби у сарадњи са Саветом за националну безбедност. Дакле, улога Савета за националну безбедност је да се бави разматрањем основних питања која се односе на заштиту виталних интереса Републике Србије од облика угрожавајућих делатности и да предлаже надлежном министарству (Агенцији за информациону безбедност) мере за унапређење заштите националне безбедности, а све то кроз заштиту пословних информација. Поред тога, Савет се бави питањем сарадње националних безбедносних снага и надлежног министарства, а разматра и сарадњу надлежних државних органа са органима и службама безбедности страних држава и међународних организација[69].

Агенција за информациону безбедност би, према предложеном моделу, поред сарадње у пословима размене података са телом за коорпоративну заштиту предузећа у мешовитом власништву, имала активно учешће у делу који се односи на класификацију података и информација са којима такав пословни субјект располаже, али искључиво у делу који се односи на класификацију пословних информација у складу са Законом о тајности података. Овде се дакле ради о подацима који се односе на националну безбедност Републике Србије, односе Републике Србије са другим државама, организацијама и међународним субјектима, као и пројекте, планове, технолошке, економске и финансијске послове који су од значаја за националну безбедност државе. Поред послова класификације, Агенција би узимала активно учешће на додели безбедносних сертификата

[69] На основу одлуке Владе Републике Србије, улога Савета за националну безбедност је да се стара о националној безбедности тако што: разматра питања из области одбране, унутрашњих послова и рада служби безбедности; разматра међусобну сарадњу органа надлежних за одбрану, органа надлежних за унутрашње послове и служби безбедности и њихову сарадњу с другим надлежним државним органима, као и сарадњу са органима и службама безбедности страних држава и међународних организација; предлаже надлежним државним органима мере за унапређење националне безбедности; разматра предлоге за унапређење националне безбедности које му упућују органи надлежни за одбрану, органи надлежни за унутрашње послове, службе безбедности и други надлежни државни органи; разматра питања из делокруга органа државне управе, аутономних покрајина, општина, градова и града Београда која су значајна за националну безбедност. Савет се такође стара о усаглашеној примени прописа и стандарда за заштиту података о личности, као и других прописа којима се штите људска права која могу да буду угрожена разменом информација или другим оперативним радњама.

корисницима класификованих пословних информација. Доделом безбедносних сертификата уредили би се нивои приступа заштићеним информацијама, утврдило би се тачно која су лица имала права приступа, а применом техничких мера у оквиру самог предузећа, успоставио би се систем надзора. Ово добија на посебној важности у случајевима настанка безбедних догађаја, када је потребно утврдити како је дошло до отицања тајних података и ко су лица која су могући починиоци. Кориснику је потребно унутрашњим актима предузећа одредити дисциплинску и моралну одговорност, док је кривична прекршајна и облигациона одговорност одређена законским решењима Републике Србије.

Надлежне безбедносне службе, према моделу, врше селекцију и анализу података и у складу са Уставом и законима врше контролу рада Агенције за информациону безбедност. Према Закону о основама уређења служби безбедности Републике Србије, службе безбедности Републике Србије су: Безбедносно - информативна агенција (БИА), Војнобезбедносна агенција (ВБА) и Војнообавештајна агенција (ВОА).[70]

Безбедносне службе (БИА, ВБА и ВОА)[71] би, према предложеном моделу, имале улогу оперативног усклађивања који се пре свега односи на селекцију информација које Агенција за информациону безбедност доставља

[70] ВБА и ВОА су органи управе у саставу министарства одбране Републике Србије. ВБА (Војнобезбедносна агенција) је ресорна војна контраобавештајна служба која обавља контраобавештајну заштиту Војске Србије и министарства одбране Републике Србије. Безбедносно информативна агенција (БИА) је централна безбедносна служба Републике Србије која предузимањем обавештајних, контраобавештајних и безбедносних мера штити националну безбедност од носиоца шпијунско–субверзивних делатности. Организациона је целина Владе Републике Србије. Агенција у обављању послова из своје надлежности примењује одговарајуће оперативне методе, мере и радње, као и одговарајућа оперативно–техничка средства којима се обезбеђује прикупљање података и обавештења ради отклањања и спречавања делатности усмерених на подривање или рушење Уставом утврђеног поретка Републике Србије, угрожавање безбедности у земљи и, у вези са тим, предузима друге потребне мере и радње на основу закона и прописа донетих у складу са законом.

[71] У оквиру безбедносне заштите министарства одбране и Војске Србије, послови које ВБА обавља су: безбедносна заштита снага, објеката, средстава и активности; безбедносна заштита тајних података; персонална безбедност (безбедносна провера лица и издавање безбедносних сертификата за лица којима је приступ тајним подацима потребан ради обављања функције или радних дужности у ВБА и ВОА); индустријска безбедност; безбедносна заштита информационо–телекомуникационих система и криптозаштите; безбедносна заштита других субјеката система одбране; остали послови и задаци безбедносне заштите.

кориснику. Разменом информација између безбедносних служби и Агенције за информациону безбедност, избегла би се могућност уступања осетљивих информација и скратиле процедуре у случајевима у којима није до краја јасно поступање. Агенција за информациону безбедност би, у таквим ситуацијама, имала могућност директног обраћања надлежним службама које би у кратком временском року могле да одговоре на захтеве Агенције за информациону безбедност, то јест тела за коорпоративну заштиту предузећа у мешовитом власништву. Представник државе у телу за коорпоративну заштиту би представљао за државу додатну гаранцију да подаци у оквиру предузећа неће бити злоупотребљени нити на било који други начин искоришћени у пословним активностима.

Улога Бироа за координацију служби безбедности је да утврђује задатке који се извршавају оперативним усклађивањем делатности служби безбедности и Агенције за информациону безбедност и да, с тим у вези, координира њихове активности, утврђује начин оперативног усклађивања у појединим случајевима, оснива мешовите радне групе за оперативне задатке који се извршавају оперативним усклађивањем делатности и утврђује њихове задатке, анализира резултате оперативног усклађивања и о томе по потреби извештава Савет за националну безбедност. Биро за координацију у складу са Одлуком Владе Републике Србије: утврђује задатке који се извршавају оперативним усклађивањем делатности служби безбедности и других државних органа и координира њихове активности; утврђује начин оперативног усклађивања у појединим случајевима; оснива мешовите радне групе за оперативне задатке који се извршавају оперативним усклађивањем делатности и утврђује њихове задатке; анализира резултате оперативног усклађивања и о томе по потреби извештава Савет, а најмање једном у шест месеци.

У специфичним ситуацијама, које дакле захтевају оперативно усклађивање делатности служби безбедности и Агенције за информациону безбедност, по потреби се ангажује Биро за координацију служби безбедности. Биро, у складу са потребама и актуелном безбедносном

ситуацијом, оснива мешовите радне групе које се укључују на конкретном решавању безбедносног проблема.

Рад служби безбедности је под надзором Народне скупштине Републике Србије преко Одбора за контролу служби безбедности. Одбор је, између осталог, надлежан да: надзире уставност и законитост рада служби безбедности, надзире поштовање политичке идеолошке и интересне неутралности у раду служби безбедности, надзире законитост примене посебних поступака и мера за тајно прикупљање података, разматра и усваја извештаје. Народна скупштина као законодавни орган, доноси законе из области заштите података. Као највише представничко тело и носилац уставотворне и законодавне власти у Републици Србији, Народна скупштина, између осталог: доноси и мења Устав; потврђује међународне уговоре кад је законом предвиђена обавеза њиховог потврђивања; надзире рад служби безбедности; доноси законе и друге опште акте из надлежности Републике Србије; усваја стратегију одбране; усваја буџет и завршни рачун Републике Србије, на предлог Владе.

Улога Заштитника грађана је да, у складу са Законом о заштитнику грађана[72], као независан државни орган, штити права грађана и контролише рад органа државне управе, органа надлежног за правну заштиту имовинских права и интереса Републике Србије, као и других органа и организација, привредних субјеката и установа којима су поверена јавна овлашћења. Заштитник грађана се стара о заштити и унапређењу људских и мањинских слобода и права. За свој рад одговара Народној скупштини. Улога Заштитника грађана у поступку заштите пословних информација је одређена кроз његово овлашћење да контролише поштовање права грађана, утврђује повреде учињене актима, радњама или нечињењем органа управе, ако се ради о повреди републичких закона, других прописа и општих аката. Заштитник грађана је овлашћен да Влади, односно Скупштини, поднесе иницијативу за измену или допуну закона и других прописа и општих аката, ако сматра да до повреде права грађана долази због недостатака у

[72] Усвојен од стране Народне скупштине Републике Србије септембра 2005. године.

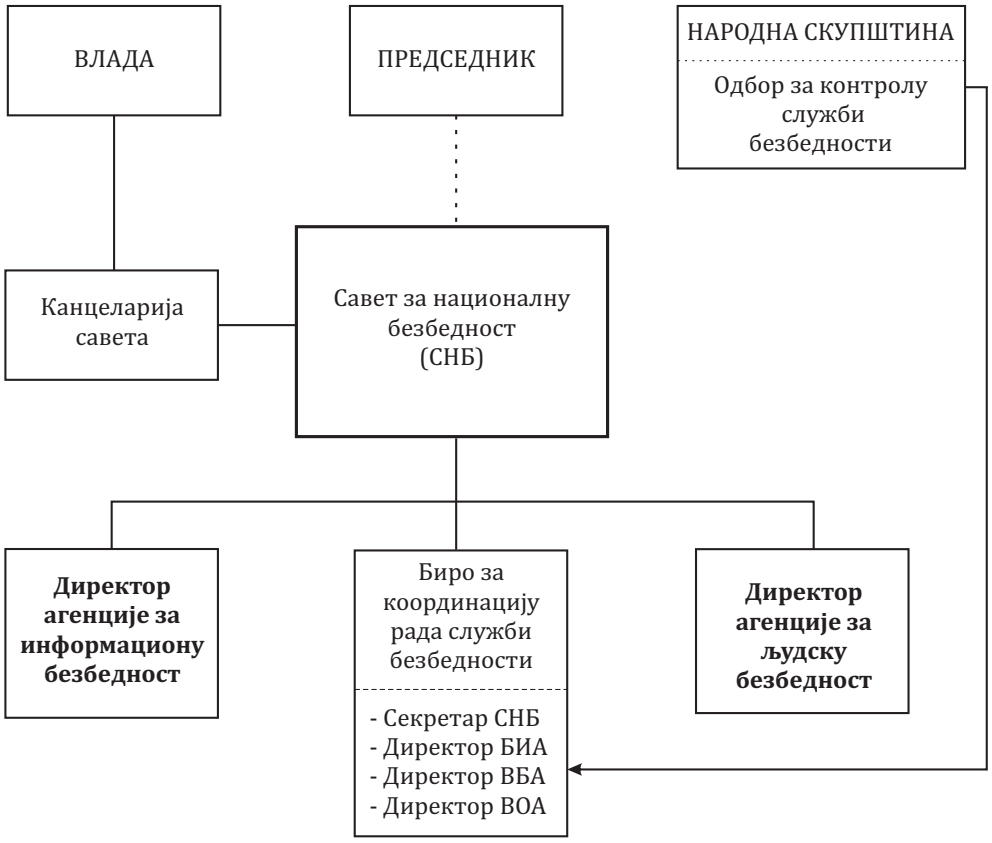
прописима, као и да иницира доношење нових закона, других прописа и општих аката, када сматра да је то од значаја за остваривање и заштиту права грађана.

Улога Повереника за информације од јавног значаја је да, у складу са Законом о слободном приступу информацијама од јавног значаја[73], обезбеди остваривање права на приступ информацијама од јавног значаја којима располажу органи јавне власти. Повереник неће омогућити остваривање права на приступ информацијама од јавног значаја, ако би се тиме, између осталог: озбиљно угрозила одбрана земље, национална или јавна безбедност, или међународни односи; битно умањила способност државе да управља економским процесима у земљи, или битно отежало остварење оправданих економских интереса; учинило доступним информација или докумената за који је прописима или службеним актом заснованим на закону одређено да се чувају као државна, службена, пословна или друга тајна, односно који је доступан само одређеном кругу лица, а због чијег би одавања могле наступити тешке правне или друге последице по интересе заштићене законом који претежу над интересом за приступ информацији.

Ово је посебно важно у условима када Агенција за информациону безбедност врши процену, у сарадњи са надлежним службама и Саветима, да ли одређени податак може да уступи кориснику, то јест да ли исти са аспекта националне безбедности има потребе да се штити и класификује одређеним степеном тајности.

У складу са размотреним чињеницама, модел остваривања националне безбедности Републике Србије који би представљао адекватну заштиту пословних информација, поред садашњих елемената, садржао би још две руководеће функције: директора Агенције за информациону безбедност и директора Агенције за људску безбедност (шема бр. 7).

[73] Усвојен од стране Народне скупштине Републике Србије 2004. године.



Шема бр.7: Остваривање националне безбедности Републике Србије

Председник Републике Србије председава Саветом за националну безбедност и командује Војском Србије, у складу са Уставом и законом. Председник Републике указује на одређена питања и проблеме из домена националне безбедности, покреће њихово решавање и доноси акте из своје надлежности. Влада усмерава и усклађује рад органа државне управе у домену националне безбедности, у складу са Уставом и законом. Влада предлаже и реализује политику националне безбедности, усмерава и усклађује функционисање система националне безбедности, обезбеђује материјална и финансијска средства за потребе система. Савет за националну безбедност је централна владина институција која се бави питањима националне безбедности у домену сарадње служби безбедности Републике Србије и њиховом сарадњом са службама безбедности страних држава. Иако Савет није кровна институција која руководи системом националне безбедности, централна је институција у разматрању питања везаних за

унапређење националне безбедности државе. У том смислу, према предложеном моделу, Савет би се бавио усмерењима Агенције за информациону безбедност и на посредан начин би контролисао њен рад у делу који се односи на старање о усаглашеној примени прописа и стандарда за заштиту података о личности, као и других људских права која могу да буду угрожена разменом информација, у конкретном случају између државних институција (Агнеције за информациону безбедност и Агенције за људску безбедност), предузећа у мешовитом власништву као и других субјеката система одбране.

Улога Одбора за контролу служби безбедности, као дела Народне скупштине Републике Србије, била би истоветна као и до сада, што значи да би њен тежишни задатак и даље представљало надзирање уставности и законитости рада служби безбедности.

У циљу реалнијег и комплекснијег приказа стања безбедности на простору у којем егзистира пословни субјект, потребно је укључити у рад и Агенцију за људску безбедност, која треба да пружи одговор на питања која класичан систем безбедности не уочава. Потреба формирања Агенције за људску безбедност има оправдање у делу који се односи на различит приступ око решавања истог безбедносног проблема. Он би требао само да допуни постојећи концепт и да додатно појасни како евентуално отицање заштићених информација може да утиче на безбедност људи на одређеном простору. Према предложеном моделу, он није критички приказ постојећег инстистуционалног оквира националне безбедности, већ комплементарни приступ који ниво националне безбедности Републике Србије треба да унапреди и додатно систематизује.

У том смислу, подаци се од субјеката система одбране, предузећа у мешовитом власништву и осталих пословних субјеката од значаја за систем националне безбедности, из Агенције за информациону безбедност достављају и Агенцији за људску безбедност. Агенција за људску безбедност као додатни филтер, податке, кроз сет индикатора људске безбедности и предложених подиндикатора, додатно проверава, анализира и систематизује и у складу са добијеним резултатима обавештава надлежна тела о

индикативним променама. Надлежно тело би, према предложеном моделу, била Агенција за информациону безбедност, а по потреби и Савет за националну безбедност, тј. Канцеларија савета као стално тело. С обзиром на могућу колизију са актуелним институционалним оквиром националне безбедности, Агенција за људску безбедност активно сарађује са институцијама Заштитника грађана и Повереника за информације од јавног значаја, као и другим релевантним међународним институцијама које могу да се укључе у решавање проблема. Неопходно је напоменути да се подаци, који би се достављали Агенцији за људску безбедност, не класификују пре достављања, већ да се од стране Агенције за информациону безбедност достављају у изворном облику *(шема бр. 9. - Модел заштите пословних информација са аспекта људске безбедности – прилог бр.2).*

Анализа којом се истражује како компромитација информација утиче на стање националне безбедности, посматрано из угла свих седам димензија људске безбедности, детаљно је разрађена у осмом поглављу ове дисертације. Подаци се, према предложеном моделу, из Агенције за информациону безбедност, паралелно са њиховом анализом, обрадом и класификацијом, достављају на увид Агенцији за људску безбедност, која на основу дефинисаних индикатора врши анализу стања безбедности свих седам димензија. Уколико постављени индикатори укажу на поремећаје и нарушавање једне од димензија људске безбедности, Агенција за људску безбедност обавештава Агенцију за информациону безбедност о промени стања. Такви подаци се поново анализирају у оквиру Агенције за информациону безбедност, пре него што се уступе кориснику. Уколико анализа индикатора не укаже на потенцијалне проблеме, у оквиру Агенције за људску безбедност, врши се анализа подиндикатора. Ако резултати поновљене анализе укажу на промену стања у било којој од димензија људске безбедности, о томе се обавештава Агенција за информациону безбедност, која предузима мере као и у претходном поступку, с тим да је у овом случају вероватноћа да је дошло до компромитације информација много већа у односу на претходну анализу. Уколико анализа подиндикатора не укаже на неку промену стања безбедности, поступак се понавља у оквиру

Агенције за људску безбедност. Овде је потребно издвојити две категорије подиндикатора, једни — који су критични из домена пословних информација и имају утицаја на националну безбедност и други — који имају значај искључиво на стање људске безбедности. У случају компромитације информација први се уступају Агенцији за информациону безбедност на експертску анализу и реаговање, док се други дају на увид Владиним институцијама, Савету за националну безбедност, као и другим релевантним институцијама. Важно је напоменути да Агенција за људску безбедност треба да укључи у свој рад стручњаке разних стручних и научних области и дисциплина као што су: екологија, здравство, исхрана, економија, политикологија, социологија и психологија. Такође, индикатори и подиндикатори, нису константни, тј. потребно их је, у складу са могућностима и друштвеним приликама, перманентно развијати и њихову листу допуњавати. Поред тога, они су и временски променљиви, па је из тог разлога неопходно вршити њихов континуални мониторинг.

Активности невладиног сектора и усклађивање законских решења са захтевима међународних институција су један од предуслова којима се ова област регулише, а степен људске безбедности подиже на виши ниво.

10. ЗАКЉУЧАК

Појава великог броја информација у свим подручјима људског деловања довела је до развоја информатичких наука. Посебно место и улогу у свету информација заузимају пословне информације, јер обезбеђују квалитетну пословну праксу у свим сферама пословања, од производње, продаје, маркетинга до услуга. Пословне информације изузетну важност имају и у функционисању државног система. Правовремене и проверене пословне информације обезбеђују квалитетан рад државних органа и државног руководства. У пословном свету је све заступљеније мишљење да су пословне информације највреднији пословни ресурс, јер их је могуће више пута употребљавати. Самим тим, у зависности од намене и тренутка употребе, могу бити предмет сукобљавања конкурентских привредних субјеката или сукобљених држава. Прикупљање квалитетних информација представља тежак задатак посебних целина пословних субјеката које се баве пословном обавештајном делатношћу. Дакле, пословна обавештајна делатност би требало да одговори на сва она питања која се тичу пословног субјекта, а односе се на пословно окружење, процену кретања пословних дешавања у будућности, и оно што је потребно учинити у циљу постизања максималног пословног успеха. Организациона целина која се бави пословном обавештајном делатношћу таква сазнања доставља менаџменту пословног субјекта који на основу својих процена доноси пословне одлуке. Дакле, пословна обавештајна и контраобавештајна делатност саставни су део политике пословног субјекта усмереног на остварење основног циља

пословања и постизања пословног успеха, тј. део су његових укупних пословних активности.

Нагли развој ИКТ–а довео је до нових видова комуникације и размене података који се суштински разликују у односу на до тада разрађен традиционални систем. У циљу регулисања међусобних права и обавеза дошло је до усклађивања докумената, процедура, правила између учесника комуникационог процеса, што је захтевало професионалан кадар, квалитетну организацију пословних процеса и примену савремених технологија. ИКТ–е у савременом свету врло брзо постају незаобилазна компонента у савременим друштвеним токовима у готово свим областима људског живота. Паралелно са развојем ИКТ–а развијају се и злонамерне активности лица и организација које настоје да их угрозе. У циљу супротстављања таквим намерама, пословни субјекти примењују све расположиве мере заштите информација које се спроводе у циљу превентивног деловања и спречавања случајног или намерног негативног утицаја на рад ИКС–а и злоупотребе информација. Дефинисањем облика угрожавања пословних информација које се налазе у оквиру ИКС–а и формулисањем конкретних мера које ће се предузимати у циљу спречавања неовлашћених лица да дођу до заштићених информација, наведена активност се конкретизује и унапређује. Проблем посебно долази до изражаја у случају нарушавања ИКС–а значајних за свеопште функционисање друштва, које може да доведе до катастрофалних последица по целу друштвену заједницу, а у неким случајевима и по међународно окружење. У циљу безбедносне заштите ИКС–а, потребно је константно деловати у правцу супротстављања свим облицима угрожавања, чиме се заштита ИКС–а доводи на прихватљив ниво. Неопходно је истаћи да се заштита задржава на прихватљивом нивоу, а не апсолутном, пошто апсолутна заштита, узимајући у обзир претходна искуства о облицима угрожавања ИКС–а, не постоји. У екстремним случајевима ИКС може бити

угрожен од стране елементарних непогода на које човек не може да утиче, а потенцијално проузрокована штета може бити немерљива. Последице угрожавања ИКС−а узроковане природним непогодама и стихијама тешко је предвидети, а самим тим супротстављање овом облику угрожавања је ослоњено искључиво на предузимање превентивних мера које обухватају квалитетну процену ризика у зависности од подручја на којем ИКС егзистира.

Заштита пословних информација у области привредног пословања је актуелан задатак државних институција и посебних организационих целина привредних субјеката. Државне службе, обавештајне и контраобавештајне, на тај начин, штите и националне интересе јер је пословање великих националних компанија уско повезано и са интересима националних држава, посебно у делу који се односи на буџетско финансирање и на повећање стопе запослености. Заштита пословних информација се, у том смислу, односи на све пословне процесе, без обзира да ли се ради о истраживачким пројектима, производним процесима или кадровским решењима. Носиоци пословних информација су лица запослена у пословном субјекту и информације похрањене на техничким медијима. У складу са тим, организациона целина задужена за безбедносну заштиту предузима мере којима спречава отицање тајних информација и других информација које су од значаја за пословање пословног субјекта. Конкуренти доласком до таквих информација стичу предност у пословним активностима и обезбеђују сопственом пословном субјекту пословни успех. Једна од мера заштите пословних информација јесте подизање безбедносне културе и односа према информацијама, што је неопходно уградити кроз одговарајуће садржаје у образовни систем, као и путем стручног усавршавања запослених како би развили свест о значају информација које су им доступне у радном процесу. Наиме, постоји лажни осећај сигурности да затворени информациони системи нису угрожени. Неопходно је упознати све запослене, који су задужени за заштиту критичних информација, да су и појединачни рачунари, који нису ни на који начин повезани са осталим деловима информационих система, могуће мете.

Представљеним резултатима истраживања потврђена је хипотеза

и доказано да обим информатизације пословних активности захтева сразмерно ангажовање на контраобавештајној заштити пословања јер позитивни ефекти увођења информационо – комуникационих технологија у пословне системе зависе од њихове адекватне заштите.

У циљу постизања максималног безбедносног ефекта потребно је квалитетно одредити безбедносну процену, која представља основ за планирање и предузимање мера против разних врста угрожавања пословног субјекта или државе. Циљ израде квалитетне безбедносне процене је да се неизвесност пословних активности сведе на минимум, како би пословне одлуке биле ваљаније и исправније. То подразумева у неким ситуацијама толерантност, а у неким искључивост у фази предвиђања, као и разраду више варијанти могућег угрожавања пословног субјекта. О квалитету безбедносне процене у потпуности може да се говори тек након сагледавања проблема са временске дистанце. Проценом се обухватају сви познати фактори који утичу и могу да утичу на безбедност пословног субјекта. На основу постојећег стања и прикупљених сазнања о објекту и његовом окружењу, прогнозирају се будући токови кретања догађаја који могу да утичу на његову безбедност, безбедност информација које се у њему чувају као и на безбедност запослених лица. У изради безбедносне процене битно је придржавати се основних принципа објективности, прецизности и проверљивости, како би се стекла реална слика о достигнутом степену безбедности пословног субјекта.

Индикатори за процену стања безбедности пословног субјекта представљају средство за евалуацију и могу да укажу на слабе тачке у систему. Они руководству безбедносног менаџмента олакшавају постављање безбедносних циљева на заштити пословног субјекта. Правилним и уколико је то могуће, прецизним дефинисањем индикатора и подиндикатора нарушавања безбедности система, постиже се виши ниво заштите пословних информација.

У складу са размотреним и анализираним чињеницама могуће је закључити да је потврђена и хипотеза како квалификована безбедносна процена са јасно дефинисаним елементима и индикаторима угрожавања подиже ниво безбедности система.

Савременим пословним организацијама потребан је поуздан нормативно–оперативни систем заштите који гарантује адекватан ниво безбедности лица, имовине и пословања. То важи за све субјекте у привредној и ванпривредној области пословања, а посебно за колективе који обухватају готово све сегменте рада, велике техничко–технолошке системе и јавна предузећа од виталног значаја за функционисање државе и друштва у целини. Такође, потребно је законску регулативу стално унапређивати како би њена примена имала потпуну имплементацију у пракси, посебно у делу високотехнолошког криминала. С обзиром да је Република Србија на путу ка чланству у Европској унији, која велику пажњу посвећује безбедности информација, један од захтева је да се ускладе и прилагоде приступи ове области са њеним стандардима. Једно од основних полазишта Европске уније је да је безбедност информација предуслов развоја информационог друштва, па се, самим тим, посебна важност придаје нормативном уређењу и успостави система информационе безбедности на територији свих држава, чланица уније. Институције Европске уније посебну пажњу поклањају мрежној и информационој безбедности, увођењу ISO стандарда, примени дигиталних потписа и аутентификације у јавним услугама, размени података уз примену норми мрежне и информационе безбедности. Свака од држава која приступа Европској унији, према безбедносној политици организације, потребно је да поседује тело за акредитовање ИКС–а, тело за безбедност комуникација, стручни тим за безбедносне инциденте на интернету и другим мрежама и координаторе информационе безбедности.

Дакле, заштита ИКС–а у смислу потпуне заштите информација, података и њихових корисника је врло сложен задатак који подразумева и укључивање фактора међународне заједнице. Потребно је усвојити минималан консензус о основним правилима и нормама понашања у информационо–комуникационом свету, посебно интернету, те о примени постојећих норми односа и понашања. Пословни субјекти сами морају

озбиљно да се позабаве овим питањем, не чекајући да се глобални систем безбедности побрине за њихово безбедно пословање. У складу са тим, пословни субјекти би требало да (уважавајући међународне норме и стандарде): установе политику и план провођења информационо–комуникационе безбедности; анализирају постојеће стање безбедности; реализују процене угрожености и могућих ризика; ураде план заштите као основ за поступање и деловање свих запослених, развијају руковођење пословним субјектима у свим сегментима; дограђују ИКС у складу са уоченим недостацима и развојем ИКТ–а.

Потребно је да нормативно правне мере заштите пословног субјекта буду утемељене на међународним и националним прописима, нормама, стандардима и специфичностима сваке организације. Пословни субјекти израђују документа као што су правилници, упутства и статути у којима дефинишу мере заштите информационе безбедности. Неки од докумената које би сваки пословни субјект требало да разради су правилници о: заштитним мерама на прикупљању, обради, складиштењу и употреби података и информација; пословно–обавештајној делатности; коришћењу електронске поште; антивирусној заштити; заштити од шпијунских програма; заштити од спама (spam); чувању копија података (beckap); руковању поверљивим подацима; заштити личних података и коришћењу информационих система од стране спољних корисника. Посебан проблем имају пословни субјекти којима ИС представља основ успешног пословања пружањем он-лајн (on line) услуга, као што су банке, осигуравајућа друштва, јавне службе, који захтевају предузимање свих мера заштите како би постигли одређени пословни успех.

Могло би се закључити да је усклађивање правних прописа Републике Србије са прописима Европске уније изузетно важан, сложен и дуготрајан процес са аспекта заштите информација, који не подразумева само усвајање нових закона, већ и њихову доследну примену. Таква активност подразумева модернизацију правосудног система, информисање пословних субјеката,

државне управе и других институција државног система. Примена усвојених и усаглашених закона и других прописа се спроводи од стране институција држава чланица, које су у обавези да право Европске уније спроводе у складу са потписаним споразумима. Ово је изузетно важно с обзиром да Европска унија нема могућност принуде на поштовање права. У случају постојања сукоба између домаћег права и права ЕУ, предност у том случају има право ЕУ („надређеност права“).
(www.Euinfo.rs/files/Publikacije-srp/35_koraka_za_web.pdf, 2016, 10. мај)

Будућа истраживања у овој области би се могла односити на истраживање утицаја имплементације усвојених поглавља на заштиту пословних информација субјеката пословања.

Претходно установљене чињенице потврђују постављену хипотезу да се усвајањем и применом адекватне законске регулативе од стране надлежних државних институција, постиже виши степен заштите пословних информација.

Тежиште дисертације било је на истраживању анализе утицаја компромитације информација на стање националне безбедности у свих седам димензија људске безбедности. Циљ овог истраживања је био систематизовање савремених сазнања о заштити пословних информација у условима масовне информатизације људских активности. Потребно је било доказати везу између степена заштићености пословних информација унутар система и нивоа безбедности његових елемената. Анализом су обухваћени најбитнији аспекти заштите информација, односно обавештајна делатност, са једне стране, и контраобавештајне мере, с друге стране. Циљ је био да се путем прецизног дефинисања сета индикатора и подиндикатора у склопу концепта људске безбедности омогући квантификовање стања безбедности. Могућност мерења битних параметара омогућава креирање адекватног модела, захваљујући коме је могуће обезбедити виши ниво заштите пословних информација, а уједно подићи и степен националне безбедности.

Метода анализе садржаја је омогућила да се на систематичан и објективан начин дође до постојећих сазнања, резултата и анализа о предмету истраживања. Анализа садржаја коришћена је приликом изучавања

релевантних законских и нормативних решења, као и код изучавања резултата истраживања који се односе на анализу постављених индикатора и подиндикатора и њиховог утицаја на стање људске безбедности у оквиру сваке од димензија појединачно. Анализа утицаја људске безбедности на стање националне безбедности у области заштите пословних информација изучавана је такође применом наведене методе.

У циљу квалитетнијег супростављања уоченим претњама усмерених ка заштићеним информацијама, у дисертацији се предлаже формирање Агенције за информациону безбедност и Агенције за људску безбедност. Агенција за информациону безбедност би, према предложеном моделу, била стално тело које би у складу са надлежностима имало могућност бржег реаговања на безбедносне инциденте, ризике и претње. Превентивним деловањем Агенције за информациону безбедност, у највећем броју случајева, безбедносни ризици и претње би се свели на минимум. Ово је карактеристично за државне институције, пословне субјекте који представљају део критичне инфраструктуре Републике Србије, као и за привредне субјекте од значаја за државни систем, без обзира на њихову власничку структуру. Формирањем Агенције за људску безбедност унапредио би се још један систем анализе заштићености и могуће компромитације пословних информација, кроз призму свих седам димензија људске безбедности. Управо су резултати истраживања показали да се анализом постојећег сета индикатора и правилним дефинисањем подиндикатора, у свакој од седам димензија људске безбедности, област заштите пословних информација подиже на виши ниво. Уступањем правовремених информација о промени стања, надлежни органи и државне институције се иницирају да предузму превентивне мере којима се безбедносне претње умањују до прихватљивог нивоа или се врши њихово потпуно отклањање, чиме се ниво националне безбедности подиже на захтеван ниво. Компаративном методом је на систематски начин извршена упоредна анализа стања безбедности у различитим временским периодима изучавања проблема. Наведена метода је показала да је применом и спровођењем адекватних законских и других решења од стране надлежних

државних институција, као што су полиција и правосуђе, стање националне безбедности у области криминала у опадању, у односу на претходни период, што имплицира на закључак да је корупција у тим институцијама смањена, а безбедност грађана подигнута на виши ниво. У области еколошке безбедности компромитација информација се спроводи у највећем броју случајева у спрези са органима локалне власти, тако што се грађанима презентују нетачни подаци о загађивачима и квалитету основних елемената од важности за квалитет живота, као што су ваздух и вода. Тиме се доводи у питање безбедност здравља грађана, који услед незнања, не предузимају превентивне мере на сопственој заштити. Наведени проблем посебно долази до изражаја приликом анализе безбедности исхране грађана, када необјављивањем тачних информација о исправности артикала исхране и последицама њихове конзумације, долази до нарушавања здравља становништва. Корист од тога имају само произвођачи или увозници хране сумњивог порекла и корумпирани државни службеници задужени за инспекцијски надзор. Улога надлежних државних институција би била да, на основу правовремених информација о повећаном броју случајева тровања храном сумњивог порекла, утврди како је наведена храна дошла до крајњег потрошача и спречи масовно угрожавање здравља грађана. Ово је посебно важно код случајева конзумације неисправне хране која изазива ефекте видљиве по здравље тек после дужег временског периода. Такође, применом ове методе, вршена је анализа промене стања пре и после измене улазних варијабли у склопу функционалног модела заштите пословних информација.

Иако је законска регулатива у области заштите пословних информација у највећем броју случајева усклађена са регулативом развијених земаља, и даље остаје проблем њене доследне примене и контроле најодговорнијих органа, који услед разних чиниоца, а између осталог и корупције, толеришу грађанима непридржавање обавезујућих норми. Тиме се наноси озбиљна штета држави и већини грађана који поштују законске одредбе. Корупција, као најизраженији феномен у овој области, се најчешће спроводи компромитацијом и „отицањем“ пословних информација, што оставља негативне последице по систем националне безбедности Републике

Србије. Представљене чињенице кроз резултате истраживања доказују постојање корелације између ефикасности заштите пословних информација и стања безбедности државе.

11. ЛИТЕРАТУРА

Монографије

1. Аврамов, С. (1998). *Трилатерална комисија, светска влада или светска тиранија*. Ветерник: Идиј.
2. Adams, J. (1995). *New Spies: Exploring the Frontiers of Espiionage*. London: Pimlico.
3. Albanese, J. S. (2010). *Organized crime in our times.* New York: Routledge.
4. Ацин, Ђ. (1995). *Међународни економски односи*. Нови Сад: Пигмалион.
5. Бајагић, М. (2012). *Међународна безбедност*. Београд: Службени гласник.
6. Bernhardt, D. (2003). *Competitive Intelligence: How to acquire and use corporate intelligence and counter /* intelligence. London: Prentice Hall Financial Times.
7. Бжежински, З. (1994). *Изван контроле — глобална превирања уочи 21. стољећа*. Загреб: Отворено свеучилиште.
8. Бжежински, З. (1999). *Велика шаховска табла*. Подгорица: ЦИД.
9. Бжежински, З. (2013). *Америка — Кина и судбина света*. Београд: Албатрос Плус.
10. Boni, W. C. & Kovacich, G. L. (2000). *Netspionage: The global threat to information.* Boston: Butterworth–Heinemann.
11. Бошковић, М. (2002). *Социјална патологија*. Нови Сад: Правни факултет.
12. Buckland, S. B., Schreier, F., i Winkler, H. T. (2010) *Demokratsko upravljanje izazovi sajber bezbednosti*. Beograd: FBD, Forum za bezbednost i demokratiju.
13. Buzan, B., Wæver, O., & Wilde, de J. (1998). *Security: A New Framework of Analysis*. London: LynneRienner.

14. Вељић, З. (2004). *Дипломатски протокол*. Београд: Дипломатска академија МСП СЦГ – Службени лист СЦГ.
15. Вељковић, В. и Јовановић, М. (2011). *Етичко–морални основи безбедности*. Београд: М-copy studio.
16. Вујовић, М., Михаиловић, М., Петовар, К. и Михаиловић, С. (2013). *Корупција против достојанственог рада*. Београд: Графолик.
17. Вукадиновић, Р. (1994). *Политика и дипломација*. Загреб: Отворено свеучилиште.
18. Вукадиновић, Р. (2006). *Међународни политички односи*. Загреб: Политичка култура.
19. Вукчевић, Д. (2013). *Европска унија као стратешки актер: теорија и пракса безбедносне и одбрамбене политике*. Београд: Еселоге.
20. Галтунг, Ј. (2009). *Мирним средствима до мира: Мир, сукоб, развој и цивлизација*. Београд: Службени гласник, Југоиток XXI.
21. Гаћиновић, Р. (2010). *Тероризам у политичкој и правној теорији*. Београд: Evro–Giunti.
22. Гиденс, Е. (1997). *Социологија.* Београд: ЦИД.
23. Глигорић, Т., Филиповић, М. и Кукић, С. (2007). *Особине народа: од значаја за пословне менаџмент* активност. Бања Лука: Бина.
24. Глишић, М. (2011). *Заједница безбедности у региону Организације за европску безбедност и сарадњу*. Београд: Медиа центар „Одбрана".
25. Грубор, Г. и Милосављевић, М. (2010). *Основе заштите информација, методолошко–технолошке основе*. Београд: Универзитет Сингидунум.
26. Даничић М. и Стајић Љ. (2008). *Приватна безбједност*. Бања Лука: Висока школа унутрашњих послова.
27. Dearth, H. D. & Goodden, R. T. (1989). *Strategic Intelligence*: *Theory and Application*. Washington, DC: JMITC.
28. Dedijer, S. & Jéquier, N. (1987). *Intelligence for economic development: an inquiry into the role of the knowledge industry*. Oxford: Berg Publishers.
29. Diamond, J. (2005). *Collapse: How societies choose to fail or succeed*, London: Penguin Books Ltd.
30. Димитријевић, В. (1982). *Тероризам*. Београд: Радничка штампа.

31. Димитријевић, В. и Рачић, О. (1988). *Међународне организације*. Београд: Рад.
32. Димитријевић, В. и Стојановић, Р. (1996). *Међународни односи*. Београд: Радничка штампа.
33. Драгишић, З. (2007). *Безбедносни менаџмент*. Београд: Службени гласник РС, Факултет безбедности.
34. Драгишић, З. (2011). *Систем националне безбедности Републике Србије*. Београд: Чигоја штампа.
35. Дракулић, М. (1996). *Основи компјутерског права*. Београд: Допис.
36. Дулић, Д., Цветковић, В., Ђурић, С. и др. (2005). *Индикатори људске безбедности у Србији — извештај за 2004. Годину*. Београд: Факултет цивилне одбране.
37. Дулић, Д., Цветковић, В., Ђурић, С. и др. (2007). *Стање људске безбедности у Србији — Извештај за 2005—2006. Годину*. Београд: Фонд за отворено друштво.
38. Дулић, Д. (2009). *Људска безбедност I* (Зборник текстова I). Београд: Фонд за отворено друштво.
39. Dunkley, G. (2004). *Free Trade: Myths, Realities and Alternatives*. London: Zed Books.
40. Дурманов Н. Д. (1942). *Гасударственнаја и веденнаја тајна*. Москва.
41. Ђорђевић, И. (2007). *Безбедносна архитектура у условима* глобализације. Београд: Службени гласник РС, Факултет безбедности.
42. Ђорђевић, И. и Мијалковски, М. (2010). *Неухватљивост националне моћи,* Београд: Службени гласник РС, Факултет безбедности.
43. Ђорђевић, И. (2013). *Људска безбедност*. Београд: Досије студио.
44. Ђорђевић, М. (2008). *Анализа макроекономских показатеља у земљама Западног Балкана*. Нови Сад: Школа бизниса.
45. Ђорђевић, О. (1978). *Шта је шпијунажа*. Београд: Политика.
46. Ђукић, С. (2009). *Време енергије — више од дипломатије*. Београд: Службени гласник РС.
47. Ејдус, Ф. (2012). *Међународна безбедност: теорије, сектори и нивои*. Београд: Службени гласник РС.

48. Eliot, M. A. (1962). *Криминал у модерном друштву*. Сарајево: Свјетлост.
49. Збигњев, Б. (2013). *Америка — Кина и судбина света*, Београд: Албатрос плус.
50. Zbigniew, B. & Brent, S. (2008). *Conversation on the future of American foreign policy*. New York: Basic books.
51. Зиндовић, И. (2008). *Мултинационалне компаније и економска шпијунажа*. Краљево: Alisa Press.
52. Иваниш, Ж., Младеновић, М. и Драгишић, З. (2006). *Политички систем*. Београд: ФЦО.
53. Игњатовић, Ђ. (1988). *Организовани криминалитет — други део*. Београд: Полицијска академија.
54. Inmon, W. H. (2005). *Building the data warehouse*. New Jersey: John Wiley & Sons.
55. Јаворовић, Б., Биланџић, М. (2007). *Полсовне информације и business intelligence*. Загреб: Голден маркетинг.
56. Jenkins, B. M. (1985). *International terrorism*. Santa Monica: The Rand Corporation.
57. Јовић, Р. и Савић, А. (2004). *Биотероризам, биолошки рат и биолошко* оружје. Београд: Институт за политичке студије — Центар за истраживање безбедности и тероризма.
58. Johnson, Loch K. (2007). *Handbook of intelligence studies*. New York: Routledge.
59. Кант, И. (1995). *Вечни мир — филозофски нацрт*. Београд: Гутенбергова галаксија.
60. Kahaner, L. (1996). *Competetive Intelligence: How to Gather, Analyze and Use Information to Move Zour Busines to the Top*. New York: Touchtone.
61. Кековић, З. (2011). *Системи безбедности*. Београд: Чигоја штампа.
62. Kenneth, J, Г. (2007). *Dobro društvo: humani plan*. Beograd: Algoritam.
63. Kimball, R. & Ross, M. (2011). *The data warehouse toolkit: the complete guide to dimensional modeling*. New Jersey: John Wiley & Sons.
64. Кисинџер, Х. (1999). *Дипломатија I*. Београд: Верзал прес.
65. Ковач, М. (2003). *Стратегијска и доктринарна документа националне безбедности — теоријске основе*. Београд: Свет књиге.

66. Kovacich, G. L. (2003). *The Information Systems Security Officer's Guide: Establishing and managing an information protection* program. Oxford: Butterworth–Heinemann.
67. Ковачевић М. (1986). *Тајна народне одбране и њена заштита у СФРЈ*. Београд: Пословна политика.
68. Комазец, С. (1990). *Савремене економске теорије*. Сплит: Економски факултет свеучилишта у Сплиту.
69. Комазец, С. (2004). *Неолиберализам, приватизација и финансијски капитал*. Београд: Јантар.
70. Комазец, С., Ковач, Ј. и Ристић, Ж. (1993) Лавиринти дужничке екомоније. *АБЦ* ГЛАС.
71. Kosuma, S. & Thompson, S, W. (2005). *Ethnic conflicts in southeast Asia*. Singapore: ISEAS Publication.
72. Кукрика, М. (2002). *Мала енциклопедија квалитета — Управљање сигурношћу информација*. Београд: Текон системи.
73. Lainteigne, M. (2009). *Chinese foreign policy*. London: Routeledge.
74. Матијашевић, Д. (2013). *Безбедност југоисточне Европе — константа стратешких концепата НАТО–а*. Докторска дисертација. Београд: Факултет безбедности.
75. Матић, Г. (2013). *Практични аспекти примене закона о тајности података из 2009. године*. ОЕБС.
76. Мијалковић, С. (2005). *Трговина људима.* Београд: БеоСинг.
77. Мијалковић, С. (2011). *Обавештајно–безбедносне службе и национална* безбедност. Београд: Безбедност.
78. Мијалковић, С. (2011). *Национална безбедност*. Београд: Scanner studio.
79. Мијалковић, С. и Милошевић, М. (2013). *Савремене обавјештајне службе — организација и методика обавјештајног, безбједносног и субверзивног дјеловања*. Бања Лука: Висока школа унутрашњих послова.
80. Мијалковски, М. (2005). *Одговор тероризму*. Београд: ФЦО.
81. Мијалковски, М. (2009). *Обавештајне и безбедносне службе*. Београд: Факултет безбедности, Службени гласник РС.

82. Мијалковски, М. (2010). *Тероризам и организовани криминал*. Београд: Факултет безбедности.
83. Мијалковски, М., Марић, П., Томић, Д. и Шаљић, Е. (2012). *Тероризам и организовани криминал*. Пирот: Pi–press.
84. Мијалковски, М. и Томић, Д. (2013). *Обавештајни* системи. Пирот: Pi–press.
85. Millard, M. (2004). *Jihad in paradise.* New York: M. E. Sharpe.
86. Милосављевић, М. и Адемовић, С. (2013). *Основи теорије информација и кодовања*. Београд: Сингидунум.
87. Милошевић, М., (2005). *Одбрана од тероризма*. Београд: Свет књиге.
88. Милошевић, М. (2011). *(Контра)шпијунажа: настанак и развој у Србији и свету.* Београд: Медиа центар „Одбрана".
89. Миљуш, М. (2010). *Заштита класификованих података у великим техничко–технолошким системима*. Магистарски рад. Београд: Факултет безбедности.
90. Haj, Ц. (2004). *Парадокс америчке моћи*. Београд: БГМ.
91. Нешковић, С. (2011). *Међународна економска шпијунажа*. Нови Сад: Фимек.
92. Никач, Ж. и Павловић, Г. (2012). *Право приватне* безбедности. Београд: Scanner studio.
93. *Our Common Future: World Commission on Environment and Development*. (1987). Oxford: Oxford University Press.
94. Perkins, J. (2006). *Confessions of an economic hit man*. USA: A plume book.
95. Петковић, Т. (2009). *Пословна шпијунажа и економско ратовање*. Нови Сад: Protexi Group System.
96. Петровић, П. (1998). *Карактеристике савременог тржишта*. Београд: Пословни круг.
97. Петровић, П. (2004). *Улога и значај државе у привредном животу у условима глобализације*. Београд: Институт за међународну политику и привреду.
98. Петровић, П. (2011). *Приватизација безбедности у слабим државама: случај Србија*. Београд: Чигоја штампа.
99. Печуљић, М. (2003). *Глобализација: два лика света*. Београд: Гутенбергова галаксија.

100.Покрајац, С. (2002). *Технологија, транзиција и глобализација*. Београд: Војна штампарија.

101.Првуловић, В. (2005). *Компаративни политички системи*. Београд: Мегатренд.

102. Првуловић, В. (2008). *Савремени међународни односи.* Београд: Мегатренд.

103. Првуловић, В. (2010). *Економска дипломатија*. Београд: Мегатренд.

104. Путник, Н. (2009). *Сајбер простор и безбедносни изазови.* Београд: Факултет безбедности.

105. Радичевић, П. (1995). *Минералне сировине у рату и миру*. Београд: „Војска".

106. Радовић, В. (2013). *Безбедност животне средине, еволуција и савремени приступи*, Нови Сад: EDUCONS.

107. Радун В. (2008). *Конкуренција на нишану*, Београд: Hesperiaedu.

108. Раичевић, М. (2003). *Интернационална економија — са основама економске дипломатије*. Београд: ФИМ.

109. Родић С. (1965). *Појам, карактер и улога тајне у друштвеном животу*. Београд: „13. мај".

110. Роквић, В. (2012). *Парламентарна контрола сектора безбедности у Републици Србији*. Докторска дисертација. Београд: Факултет Безбедности.

111. Ruth, A. & Hudson, К. (2004). *Сертификат Security+, Microsoft* Corporation. Чачак: Светлост.

112. Samuelson, P. & Nordhaus, W. D. (2010). *Economics 19e.* New York: McGraw–Hill/Irwin.

113. Sapsford, R. & Jupp V. (2006). *Data collection and analysis*. Thousand Oaks: Sage.

114. Сејџмен, М. (2006). *Терористичке мреже*. Београд: Алтера.

115. Симеуновић, Д. (2000). *Тероризам.* Београд: Правни факултет.

116. Симић, Д. (2002). *Наука о безбедности: савремени приступ безбедности*. Београд: Службени лист СРЈ и ФПН.

117. Симић, Д. (2007). *Савремене теорије безбедности*. Београд: ISAC Fond.

118. Стајић, Љ. и Лукић, Т. (2011). *Право приватне безбедности*. Нови Сад: Футура.
119. Станаревић, С. и Николић, В. (2010). *Стање људске безбедности у Србији — ка индексу људске безбедности*. Београд: Фонд за отворено друштво.
120. Стевановић, О. (2012). *Безбедносни менаџмент*. Београд: Scanner studio.
121. Стиглиц, Џ. (2004). *Противречности глобализације*. Београд: SBM-x.
122. Sun,T. (2007). *Umijeće ratovanja*. Zagreb: Mladost.
123. Shireen, T,H. (2010). *Iran's foreign policy in the post soviet era*. Santa Barbara: Praeger.
124. Shmalleger, F. (1996). *Criminology today*. London: Englewood cliffs.
125. Талијан, М. и Талијан, М. (2011). *Општи и безбедносни менаџмент*. Бања Лука: Висока школа унутрашњих послова.
126. Тасић В. и Бауер, И. (2004). *Речник компјутерских термина*. Београд: Микро књига
127. Триван, Д. (2012). *Корпоративна безбедност.* Београд: Досије студио.
128. Tucker, B. N. (2005). *Dangerous strait*. New York: Columbia university press.
129. Унковић, М. (2007). *Међународна економија*. Београд: Универзитет Сингидунум.
130. Урошевић, В. (2014). *Везе cyber криминала са иррегуларном миграцијом и трговином људима*. Београд: МУП Републике Србије.
131. Фримерман, А. (2000). *Пословно право.* Београд.
132. Фукујама, Ф. (2007). *Грађење државе — управљање и светски поредак у двадесетпрвом веку*. Београд: Филип Вишњић.
133. Heijden van der, K. (1997). *Scenarios: The art of Strategic Conversation*. New Jersey: John Wiley & Sons.
134.Хелд, Д. (1997). *Демократија и глобални поредак*. Београд: Филип Вишњић
135. Homer–Dixon, T. F. (2010). *Environment, scarcity, and violence*. New Jersey: Princeton University Press.
136. Horowitz, S., Heo, U. & Tan, C. A. (2007). *Identity and change in east Asian conflicts*. New York: Palgrave Macmillan.

137. Carpenter, G. T. (2005). *America` s coming war with China*. New York: Palgrave Macmillan.
138. Cialdini, R. B. (2009). *Influence: Science and practice (Vol. 4)*. Boston: Pearson Education.
139. Combs, E. R. & Moorhead, D. J. (1993). *Competitive Intelligence Handbook*. Lanham: Rowman and Littllefield.
140. Cooper, H. A. (1976). *The terrorist and the victim*. Victimology.
141. Corson–Finnerty, A. D. (1982). *World citizen: action for global justice*. Ossining New York: Orbis Books.
142. Чомски, Н. (1994). *Шта то (устварі) хоће Америка?*. Београд: Институт за политичке студије.
143. Чомски, Н. (1998). *Светски поредак — стари и нови*. Београд: СКЦ.
144. Чомски, Н., Попович, М. и Секулић. В. (1999). *Контролисана демократија*. Београд: ЦИД.
145. Чомски, Н. (2000). *Модел само за богате*. Београд: Економски сигнали.
146. Џенкинс, Р. (2001). *Етницитет у новом кључу*. Београд: XX век.
147. Џигурски, О. (2002). Информатика. Београд: Факултет цивилне одбране.
148. Џозеф, Н. (2006). *Како разумевати међународне сукобе*. Београд: Стубови културе.
149. Waltz, K. N. (2010). *Theory of international politics*. Long Grove, Illinois: Waveland Press.
150. Watson, A. (1982). *Diplomacy: the dialogue between states*. Psychology Press.

Законска и нормативно–правна регулатива

1. Устав Републике Србије, Службени гласник Републике Србије, 98/06.
2. Кривични закон Републике Србије, Службени гласник Републике Србије, 85/05, 88/05, испр. 72/09, 111/09, 121/12, 104/13.
3. Закон о организацији и надлежности државних органа у сузбијању организованог криминала, корупције и других посебно тешких кривичних дела, Службени гласник Републике Србије, 42/2002, 27/2003, 39/2003,

67/2003, 29/2004, 58/2004 - др. закон, 45/2005, 61/2005, 72/2009, 72/2011 - др. закон, 101/2011 - др. закон, 32/2013.

4. Закон о одбрани, Службени гласник Републике Србије, 116/07, 88/09, 104/09.

5. Закон о ВБА и ВОА, Службени гласник Републике Србије, 88/09, 17/13.

6. Закон о БИА, Службени гласник Републике Србије, 42/02, 111/09.

7. Закон о основама уређења служби безбедности, Службени гласник Републике Србије, 116/07, 72/12.

8. Закон о заштити пословне тајне, Службени гласник Републике Србије, 72/11.

9. Закон о тајности података, Службени гласник Републике Србије, 104/09.

10. Закон о слободном приступу информацијама од јавног значаја, Службени гласник Републике Србије, 120/04, 54/07, 104/09, 36/10.

11. Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине, Службени гласник Републике Србије, 46/06, 104/09.

12. Закон о ауторским и сродним правима, Службени гласник Републике Србије, 104/209, 99/2011, 119/2012.

13. Закон о патентима, Службени гласник Републике Србије, 99/2011.

14. Закон о заштити података о личности, Службени гласник Републике Србије, 97/08, 104/09.

15. Закон о информационој безбедности, Службени гласник Републике Србије, 6/16.

16. Закон о основама уређења служби безбедности, Службени Гласник Републике Србије, 116/2007, 72/2012.

17. Уредба о посебним мерама надзора над поступањем са тајним подацима, Службени гласник Републике Србије, 90/2011.

18. Уредба о посебним мерама физичко–техничке заштите тајних података, Службени гласник Републике Србије, 97/2011.

19. Уредба о посебним мерама заштите тајних података у информационо–телекомуникационим системима, Службени гласник Републике Србије, 53/2011.

20. Уредба о обрасцима безбедносних упитника, Службени гласник Републике Србије, 30/10.
21. Уредба о садржини, облику и начину достављања сертификата за приступ тајним подацима, Службени гласник Републике Србије, 54/10.
22. Уредба о одређивању послова безбедносне заштите одређених лица и објеката, Службени гласник Републике Србије, 72/10.
23. Уредба о увећању плате државних службеника и намештеника који обављају послове у вези са заштитом тајних података у Канцеларији Савета за националну безбедност и заштиту тајних података и Министарству правде, Службени гласник Републике Србије, 79/10.
24. Уредба о садржини, облику и начину вођења евиденција за приступ тајним подацима, Службени гласник Републике Србије, 89/10.
25. Уредба о начину и поступку означавања тајности података, односно докумената, Службени гласник Републике Србије, 8/11.
26. Уредба о ближим критеријумима за одређивање степена тајности „Државна тајна" и „Строго поверљиво", Службени гласник, 46/13.
27. Уредба о ближим критеријумима за одређивање степена тајности „Поверљиво" и „Интерно" у Безбедносно–информативној агенцији, Службени гласник Републике Србије, 70/13, Канцеларији Савета за националну безбедност и заштиту тајних података, Службени гласник Републике Србије 86/13 и Министарству унутрашњих послова, Службени гласник Републике Србије 105/13.
28. Уредба о посебним мерама заштите тајних података које се односе на утврђивање испуњености организационих и техничких услова по основу уговорног односа, Службени гласник Републике Србије, 63/13.
29. Правилник о службеној легитимацији и начину рада лица овлашћених за вршење надзора над спровођењем закона, Службени гласник Републике Србије, 85/13.
30. Стратегија развоја информационог друштва у Републици Србији, Службени гласник Републике Србије, 51/2010.
31. Стратегија безбедности Републике Србије, Министарство одбране, Београд.

32. Стратегија националне безбедности Републике Србије, Службени гласник Републике Србије, 28/09.
33. Стратегија одбране Републике Србије, Службени гласник Републике Србије, 28/09.
34. Стандарди из области безбедности и заштите информација (информациона безбедност): ИСО 27001, ИСО 17024, ИСО 17025.
35. Конвенција о заштити људских права и основних слобода (енгл. *Convention of protection of human rights and fundamental freedoms*).
36. Универзална декларација о људским правима.
37. УН Резолуција 54/164 – људска права и тероризам, усвојена на Генералној скупштини 17.12.1999; Савет Европе, Смернице о људским правима и борби против тероризма.
38. Défense et Sécurité nationale Le Livre Blanc, Odile Jacob/La documentation français, Paris, juin 2008, p. 133.
39. Бечка конвенција о конзуларним односима.
40. Бечка конвенција о дипломатским односима.
41. Хашки правилник из 1907. године.
42. Женевска конвенција о заштити грађанских лица за време рата из 1949. године.

Интернет извори

1. https://www.coe.int/t/dghl/monitoring/trafficking/Source/PDF_Conv_197_Trafficking_Serbian.pdf
2. http://pt.uninp.edu.rs/wp-content/uploads/2014/01/INFORMACIONE-TEHNOLOGIJE-I-SAVREMENI-TRENDOVI-POSLOVANJA-U-SRBIJI.pdf
3. http://www.blic.rs/Vesti/Svet/520728/AFERA-PROFUMO-Ona-je-akterka-najveceg-seks-skandala-20-veka
4. https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf
5. http://eur-lex.europa.eu/legalcontent/HR/TXT/?uri=CELEX%3A32013D0768

6. http://www.dw.com/sr/uspon-i-pad-dominika-stros-kana/a-18229848
7. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33168
8. https://www.nafta-sec-alena.org/Home/About-the-NAFTA-Secretariat
9. http://www.cefta.int/
10. http://www.efta.int/about-efta/history
11. http://www.oecd.org/general/organisationforeuropeaneconomicco-operation.htm
12. http://www.iss.rs/la/button_4.html
13. http://www.vreme.co.rs/cms/view.php?id=640079
14. https://www.un.org/disarmament/about/
15. https://www.epo.org/index.html
16. http://www.newsweek.rs/foto/54057-u-hirosimi-obelezen-dan-secanja-na-zrtve-atomskih-bombi-foto-video.html
17. http://ruskarec.ru/articles/2012/10/26/rusija_se_seca_zrtava_nord-osta_17681.html
18. https://www.zeitenschrift.com/artikel/haarp-das-wetter-als-waffe-wahn-oder-wirklichkeit
19. http://www.pks.rs/PoslovnoOkruzenje.aspx?id=794&p=1
20. http://www.novosti.rs/vesti/naslovna/reportaze/aktuelno.293.html:456820-Sredinom-veka-u-svetu-97-milijardi-ljudi
21. http://www.mod.gov.rs/cir/dokumenta/strategije/strategije.php
22. http://www.euractiv.rs/odrzivi-razvoj/3578-zabranjeni-azbest-i-dalje-opasnost
23. https://sustainabledevelopment.un.org/content/documents/Agenda21.pdf
24. http://www.scribd.com/doc/222308340/Izvestaj-Rimskog-Kluba-1974-Granice-Rasta-i-Definicija-Kapitalizma-Vernera-Zombarta-Kao-Proizvodnog-Sistema#scribd
25. http://hdr.undp.org/en/content/human-development-report-1994
26. http://www.novosti.rs/vesti/planeta.299.html:474249-Osamdesetpet-najbogatijih-ima-para-kao-i-35-milijardi-najsiromasnijih
27. http://www.gs.gov.rs/lat/strategije-vs.html

28. http://www.vesti-online.com/Vesti/Svet/122853/Japan-Zemljotres-podigao-cunami-html
29. http://asean.org/
30. http://www.politika.rs/vesti/najnovije-vesti/Bomba-u-Oslu-napravljena-od-vestackog-djubriva-i-dizela.lt.html
31. http://www.paragraf.rs/propisi/zakon_o_autorskom_i_srodnim_pravima.html,
32. http://www.paragraf.rs/propisi/zakon_o_patentima.html
33. www.pcchip.hr/?cmd?=21&arh=1&solo_id=7470
34. http://www.iso.org/iso/home.html,
35. http://www.zakon.hr/z/98/Kazneni-zakon
36. www.thearling.com/text/hr.com/dw.htm
37. http://www.mfa.gov.rs/sr/images/stories/komisija/MKCK%20-%20Izvori%20MHP.pdf
38. http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm
39. http://social-engineer.org/wiki/archives/PenetrationTesters/Pentest-Winkler.html
40. http://www.vs.rs/content/attachments/CMO/Radni_materijal_za_pripremu-MHP_zbirka_2013_Srb_Eng.pdf
41. http://www.ius.bg.ac.rs/prof/Materijali/milboj/Konvencija%20o%20diplomatskim%20odnosima.pdf
42. http://demo.paragraf.rs/combined/Old/t/t2003_08/t08_0075.htm
43. www.security-and-peace.de/archiv/PDF/2005-1/SuF_01_2005_5.pdf
44. http://www.srbijadanas.com/clanak/ziteh-14-do-2020-cyber-kriminal-ce-nadmastiti-klasican-13-06-2014
45. http://mtt.gov.rs/download/potrosacka-korpa/KUPOVNA%20MOC%20-%20JANUAR%202015.pdf
46. https://www.unodc.org/documents/dataandanalysis/statistics/corruption/Korupcija_u_Srbiji_-_Iskustva_gradjana_withcover.pdf
47. http://www.novosti.rs/395.html:167431-Mito-kao-u-svetu
48. http://www.kpa.edu.rs/cms/data/akademija/nbp/NBP_2010_2.pdf
49. http://www.mup.gov.rs/cms_lat/sadrzaj.nsf/informator.html

50. http://www.batut.org.rs/download/izvestaji/higijena/Zdravstvena%20ispravnost%20predmeta%20opste%20upotrebe%202012.pdf
51. http://www.fda.gov/downloads/Food/GuidanceRegulation/HACCP/UCM077957.pdf
52. http://www.batut.org.rs/download/publikacije/IstrazivanjeZdravljaStanovnistvaRS2013.pdf
53. http://www.paragraf.rs/propisi/strategija_razvoja_sistema_javnog_informisanja_u_republici_srbiji_do_2016
54. http://www.antikorupcijasavet.gov.rs/Storage/Global/Documents/izvestaji/izvestaj%20mediji%2026%2002.pdf
55. http://nuns.rs/reforma-javnog-informisanja/21561/prikrivena-kontrola--ugrozavanje-medija-u-srbiji.html
56. http://www.transparentnost.org.rs/index.php?option=com_content&view=category&id=39&Itemid=51&lang=sr
57. http://www.kombeg.org.rs/Komora/udruzenja/UdruzenjeTrgovine.aspx?veza=3539
58. http://www.mup.gov.rs/cms_lat/sadrzaj.nsf/informator.html
59. http://www.b92.net/info/vesti/index.php?yyyy=2013&mm=06&dd=21&nav_category=16&nav_id=725227
60. http://www.mdtfjss.org.rs/pub/serbia-judical-functional-review/#p=10
61. http://www.euractiv.rs/pregovori-sa-eu/8212-graani-srbije-ne-veruju-institucijama-
62. :http://www.nadzor.org.rs/dosije%20korupcija/Zoran%20Ivosevic%20%20Korupcija%20u%20pravosudju%20i%20pravosudni%20sistem.pdf
63. http://webrzs.stat.gov.rs/WebSite/repository/documents/00/01/91/84/11_Zivotna_sredina.pdf
64. http://www.sepa.gov.rs/download/VAZDUH2014.pdf.
65. http://www.batut.org.rs/download/publikacije/Zdravlje%20stanovnika%201997-2007.pdf
66. http://www.who.int/gho/countries/srb.pdf?ua=1
67. http://www.sepa.gov.rs/download/Izvestaj2014.pdf

68. http://www.psmsc.com/Downloads/TechnologyPapers/SecurityWhitePaper_v3.0.pdf
69. www.scribd.com/embeds/249691006/content?start_page=1&view_mode=scroll&show_recommendations=true
70. www.Euinfo.rs/files/Publikacije-srp/35_koraka_za_web.pdf,
71. http://www.novosti.rs/vesti/naslovna/aktuelno.69.html:334644-Otrov-okovao-Srbiju
72. https://mattmarenic.wordpress.com/2014/12/15/20141215nike-tui-svoje-dizajnere/,
73. http://www.personalmag.rs/it/uhapseni-organizatori-i-clanovi-kriminalne-grupe-zbog-falsifikovanja-i-zloupotrebe-platnih-kartica/,
74. http://www.blic.rs/vesti/drustvo/agencija-za-privatizaciju-neovlasceno-objavila-podatke-pet-miliona-gradana-srbije/7g8tytc
75. http://www.rts.rs/page/stories/sr/story/10/Svet/915474/Rusija+zabranila+uvoz+mleka+i+mesa.html
76. http://www.vesti-online.com/Vesti/Tema-dana/503434/Koliko-je-hrana-zatrovana-pesticidima-1-Veseli-trovaci-na-srpskim-njivama,
77. http://www.nature.com/news/china-sacks-officials-over-golden-rice-controversy-1.11998,
78. http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf
79. http://www.globalstudies.gu.se/digitalAssets/1274/1274383_abrahamsson_kina.pdf)
80. http://www.prviprvinaskali.com/clanci/svet/nova-studija-ukazuje-na-vezu-izmedju-herbicida-glifosata-i-raka.html,
81. http://www.politika.rs/scc/clanak/295374/Sta-je-trulo-u-srpskoj-policiji
82. http://www.srbijadanas.net/skandal-u-cacku-nestalo-27-predmeta-iz-prekrsajnog-suda/
83. http://rtvpancevo.rs/Vesti/Lokal/od-zaraznih-bolesti-u-pancevu-prva-oboljenja-disajnih-organa.html,
84. http://www.novosti.rs/vesti/naslovna/aktuelno.69.html:334644-Otrov-okovao-Srbiju

85. http://www.kurir.rs/petrohemija-zagadila-hlorom-vazduh-u-pancevu-clanak-1002227
86. http://lakodokola.com/articles/news/315
87. http://www.zmne.hu/aarms/docs/Volume2/Issue1/pdf/02NOWA.pdf
88. http://worrydream.com/refs/Shannon%20-%20A%20Mathematical%20Theory%20of%20Communication.pdf
89. http://www.sveiby.com/articles/Information.html
90. https://www.britannica.com/

Енциклопедије, речници

1. *Војна енциклопедија*. (1974). Београд: Редакција војне енциклопедије, ВИЗ.
2. *Војни лексикон (друго издање)*. (1981). Београд: ВИЗ.
3. Војно дело.(2002—2016). Београд: Медиа центар „Одбрана“
4. *Мала енциклопедија (прво издање)*. (1959). Београд: Просвета.
5. *Економски речник*. (2001). Београд: Економски факултет.
6. *Enciklopedia of modern Asia*. (2002). Detroit: Gale group.
7. *Политичка енциклопедија*. (1975). Београд: Савремена администрација.
8. *Правна енциклопедија*. (1979). Београд: Савремена администрација.
9. *Worldmark Encyclopedia of national* economies (Volume I–V). (2002). Detroit: Gale group.

Чланци из књига, збирки, часописа и зборника

1. Albanese, J. S. (2007). The causes of organized crime. *Journal of contemporarz criminal justice, Thousand oaks, No 1/2000*, 409–423.
2. Anderson, C.J. & Pontusson, J. (2007). Workers, worries and welfare states: Social protection and job insecurity in 15 OECD countries. *European Journal of Political Research*, *46*(2), 211–235.
3. Andrew, M. (2002). Civil war: Academic Research and the policy community. *Journal of peace resaerch*, *vo. 39, No 5*, 515–525.

4. Ahmad, A., Bosua, R. & Scheepers, R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective, *Computers and Security, 42*, 27–39.
5. Бјелић, П. (2000). Међузависност спољне политике и међународне трговине. *Међународни проблеми,* 1–2.
6. Bora, A. A. (2013). The private use of the social networks by the civil servants — A possible "achilles' heel" of personal data protection in public order and security institutions?. *Masaryk University Journal of Law and Technology*, *7*(2), 347–360.
7. Bosold, D. & Werthes, D. (2005). Human Security in Practice: Canadian and Japanese Experiences. *Internationale Politik und Gesellschaft /International Politics and Society, 1*, 84–101.
8. Влаховић, Б., Томић, Д. и Пушкарић, А. (2010). Паритети цена одабраних инпута и основних ратарских производа у Србији. *Field & Vegetable Crops Research*/Ратарство и повртарство, *47*(1), 57–66.
9. Von Solms, R. & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102.
10. Гонан Божац, М. (2008) SWOT анализа и TOWS матрица — сличности и разлике. *Економска истраживања*, *21*(1), 19–34.
11. Gonçalves, M.E. & Jesus, I. A. (2003). Security policies and the weakening of personal data protection in the European Union. *Computer Law and Security Review, 29*(3), 255–263.
12. Грубач, М. (2009). Организовани криминал у Србији. *Зборник радова правног факултета у Сплиту*, *4*, 701–709.
13. Gurkaynak, G., Yilmaz, I. & Taskiran, N.P. (2013). Protecting the communication: Data protection and security measures under telecommunications regulations in digital age. *Computer Law and Security Review*, *30*(2), 179–189.
14. Dallinger, U. (2014). Globalisierung und die Nachfrage nach sozialer Sicherheit. Eine kritische Analyse des "domestic demand"–Ansatzes, *Berliner Journal fur Soziologie*, *24*(1), 59–88.
15. Dedijer, S. (1996). Development and Management by Intelligence: Japan. *Information, Development and Social Intelligence*, 302-323.

16. den Dekker, G. & Coppen, T. (2012). Termination and Suspension of, and Withdrawal from, WMD Arms Control Agreements in Light of the General Law of Treaties, *Journal of Conflict and Security Law*, *17*(1), 25–47.

17. Дракулић, М. и Дракулић, Р. (2014). Cyber криминал. *Везе Cyber криминала са ирегуларном миграцијом и трговином људима*, *XII*, 365–386.

18. Дракулић, М. и Дракулић, Р. (2010). Европска перспектива регулисања интернет услуга: изазов традиционалном европском праву. *Телекомуникације*, *6*, 49–63.

19. Драшковић, В. (2007). Манифестације економске глобализације. *Економија, 14*, 257–274.

20. Drury, A. C. & Olson, R. S. (1998). Disasters and political unrest: An empirical investigation. *Journal of Contingencies and Crisis Management,* 6(3), 153–161.

21. Дураковић, А. (2007). Разлика између пословног информационог система и индустријске шпијунаже. *Транзиција – Међународни научни – стручни часопис за економију и политику*, *19–20*.

22. Ђокић, З. и Живановић С. (2008). Безбедност пословања, појам, законодавство и карактеристике, ЦД са предавањима, Ечка

23. Ђорђевић, И. (2008). Економске основе безбедности. *Годишњак Факултета безбедности*, 193–208.

24. Ђорђевић, М. (2008). Анализа макроекономских показатеља у земљама Западног Балкана. *Школа бизниса*, 3–10.

25. Ђорђевић, И. и Мијалковски, М. (2011). Национална моћ у условима глобализације. *Национални интерес, 1*, 338–339.

26. Ђорђевић, Н. (1986). Обавештајне службе и кривично дело шпијунаже. *Правни живот*, *10*, 977.

27. Erasmus, J. (1952). Der geheime Nachrichtendienst (Vol. 6). *Musterschmidt Wissenschaftlicher Verlag*.

28. Живков, Д. (2008). *Глобализација и проблеми* екологије. Школа бизниса: научно–стручни часопис, 113–121.

29. Zimmerman, P.R. (2014). The deterrence of crime through private security efforts: Theory and evidence. *International Review of Law and Economics*, *37*, 66–75.

30. Ишљамовић, С., Јеремић, В. и Петровић, Н. (2009). Еколошка свест студената Универзитета у Београду, VII Скуп привредника и научника — СПИН 09, Операциони менаџмент и глобална криза, *Зборник радова,* 429–435.
31. Jenkins, B. M. (1975). International Terrorism a New Mode of Conflict; International Terrorism and World Security. *International Terrorism and World Security*, 13–49.
32. Јовић, Р. и Савић, А. (2012). Биотероризам, биолошки рат и биолошко оружје. *Центар за истраживање безбедности и тероризма*, 62.
33. Јурчић, Љ. (2013). Индустријска политика у глобалним процесима/Industrial policy in global processes. *Acta Economica*, *11*(18), 117–128.
34. Капаравловић, Н. (2011). Утицај креативног рачуноводства на квалитет финансијског извештавања. Економски хоризонти, 13(1), 155-168.
35. Карић, Д, Зечевић, Р и Карић, Д. (2012). Економске интеграције — последица процеса глобализације и економског развоја. *Социоекономика, 1*, 246–254.
36. Kim, Y. U. & Ozdemir, S. Z. (2014). Structuring corporate boards for wealth protection and/or wealth creation: The effects of national institutional characteristics, *Corporate: An International Review, 22*(3), 266–289.
37. Колев, Д. (2011). Геополитичка димензија енергетске безбедности. *EMC Review — Часопис за економију — APEIRON*.
38. Кукић, С. (2012). Глобализација — пројекат наде или пријетња будућности?. *Социолошки дискурс*, *3*, 5–17.
39. Лакић, Н. (2011). Да ли је глобализација изазов или претња националним државама као доминантном облику политичке организације?. *Безбедност западног Балкана, 21*, 6–17.
40. Li, Q. (2013). Study of information system security of government data center based on the classified Protection, *Proceedings of the 8th International Conference on Computer Science and Education, ICCSE 2013*, art. no. 6554125, 1315–1319.
41. Марковић, Д. Ж. (2007). Научно–технички прогрес, информатизација друштва и виртуализација друштвеног живота, *Зборник радова Технолошког факултета у Лесковцу,* 14–24.

42. Martin, A. (2005). Environmental conflict between refugee and host communities. *Journal of Peace Research, 42*(3), 329–346.
43. Милић, Д. (2010). Биотероризам и употреба биолошког оружја. *Ревија за безбедност*, 103–116.
44. Murray, A. T., & Grubesic, T. H. (2012). Critical infrastructure protection: The vulnerability conundrum. *Telematics and Informatics*, *29*(1), 56–65.
45. Нешковић С. (2013). Економска шпијунажа и нове технологије у глобализованој међународној заједници. *Општевојни научно–теоријски часопис ВОЈНО ДЕЛО*, 57–76.
46. Niggli, M.A. & Maeder, S. (2014). Punishment and Security. *Asian Journal of Criminology,* 1–15.
47. Nichols, E. A. & Sudbury, A. (2006). Implementing Security Metrics Initiatives. *Information Systems Security,* 30–38.
48. Новичић, Ж. (2005). Нуклеарно оружје у међународној политици. *Међународни проблеми*, *LVII*, *4*, 505–528.
49. O'Connor, T., Kinsella, S. & O'Sullivan, V. (2014). Legal protection of investors, corporate governance, and investable premia in emerging markets. *International Review of Economics and Finance*, *29*, 426–439.
50. Park, J. S., Kwiat, K. A., Kamhoua, C. A., White, J. & Kim, S. (2014). Trusted Online Social Network (OSN) services with optimal data management, *Computers and Security, 42*, 116–136.
51. Петровић, Д. Л. (2007). Информациона сигурност у савременом свету. *Инфо М 6.24,* 10–17.
52. Петровић, П. (2010). Резервисани домени као препреке нормативног уређења приватног сектора безбедности у Србији. *Ревија за безбедност, 3*, 257–273.
53. Pickton, D. W. & Wright, S. (1998). What's swot in strategic analysis?. *Strategic change*, *(7),* 101–109.
54. Protic, D. (2013). Information security: Standards or rules. *Vojno delo*, *65.1*, 133–150.
55. Quirk, P. (1996). Macroeconomic Implications of monez laudering. *IMF Working paper, 96/66*.

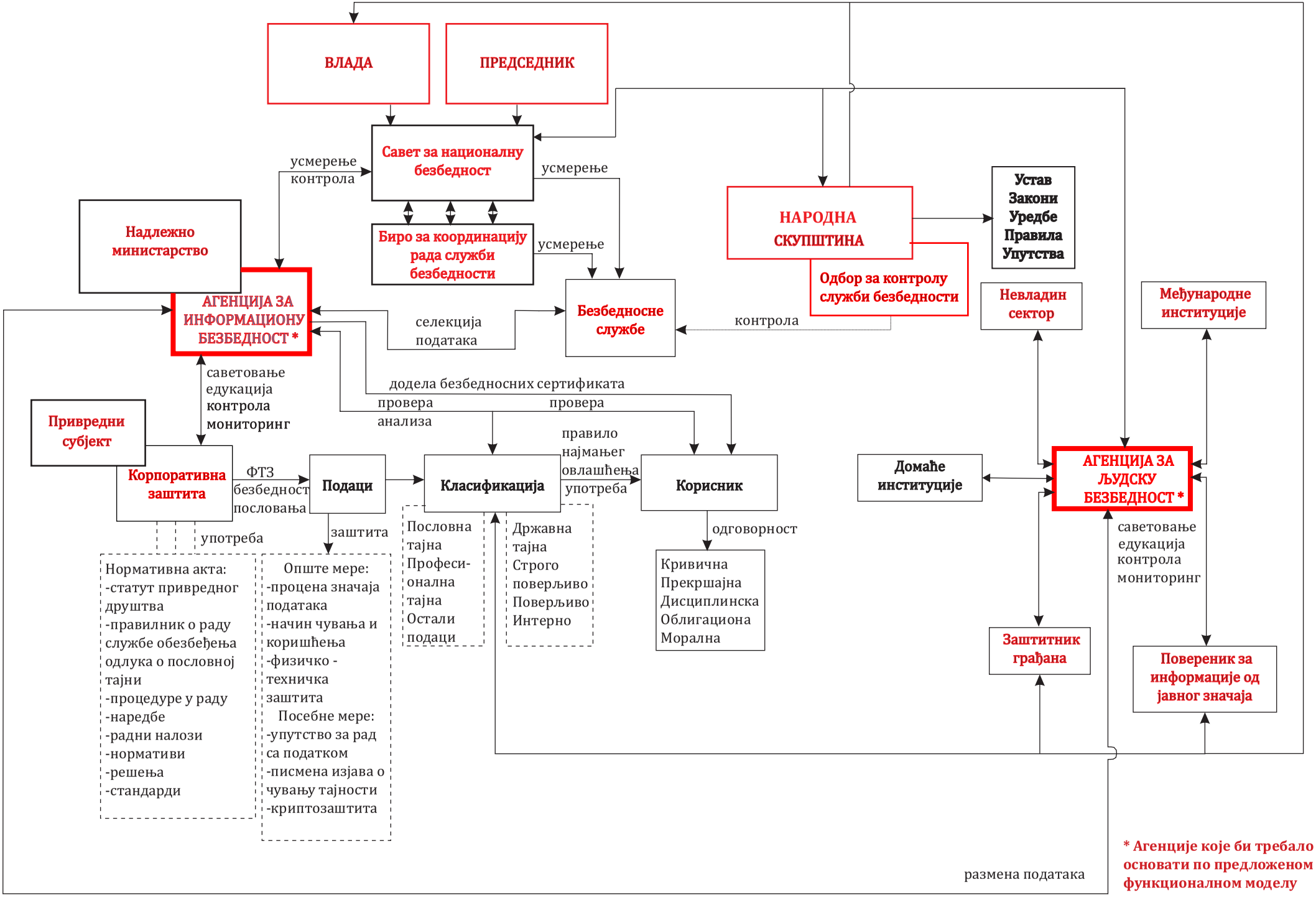
56. Радовић, В. (2008). Економска шпијунажа: мотиви и методе. *Економика*, 3–4, 142–152.
57. Sagan, S. D. (1994). The perils of proliferation: Organization theory, deterrence theory, and the spread of nuclear weapons. *International Security*, 66–107.
58. Slocum, N. & Langenhove, L. V. (2004). The meaning of regional integration: introducing positioning theory in regional integration studies. *Journal of European Integration*, *26*(3), 227–252.
59. Спасовски, М. (2001). Популациона експанзија и демографска подељеност света у 20. веку. *Демографски процеси у СР Југославији, IX Еколошка истина.*
60. Стошић, И., Брњас, З., & Дедеић, П. (2010). Утицај приватизације на пословање привредних субјеката и економски раст Србије.
61. Suda, Y. (2013). Transatlantic Politics of Data Transfer: Extraterritoriality, Counter-Extraterritoriality and Counter-Terrorism. *Journal of Common Market Studies*, *51*(4), 772–788.
62. Таталовић, С. (1998). Етнички аспекти сигурности југоистока Европе. *Политичка Мисао,* (*02*), 65–78.
63. Telser, Л. Г. (1981). Why there are organized futures markets. *Journal of Law and Economics*, 24.
64. Тепавац, Д. (2016). Кретања становништва као последица нарушавања еколошке безбедности и безбедноснти животне средине. *Војно Дело*, (6/2016), 83-99.
65. Ћатовић А., Црнишанин, А. и Мушовић, М. (2013). Глобализација привреде и трнснационални. *Socioeconomica — The Scientific Journal for Theory and Practice of Socio–economic Development*, (*3*), 139–150.
66. Ђурић, Б. и Јегеш, М. (2011). Србија у маказама енергетске безбедности. *CIVITAS, 2*, 80–89.
67. Findeiß, A. (2002). Kein staat - Keine sicherheit? Die verunsicherung der soziologie angesichts neuer und alter phänomene. *Soziale Welt*, *53*(4), 481–486.
68. Friedewald, M., Vildjiounaite, E., Punie, Y. & Wright, D. (2007). Privacy, identity and security in ambient intelligence: A scenario analysis, *Telematics and Informatics*, *24*(1), 15–29.
69. Fuchs, B. (2013). Forschen für die Innere Sicherheit. *Kriminalistik*, *67*(12), 730.

70. Harmon, E. G., Machlup, F. & Mansfield, U. (1987). The interdisciplinary study of information: A review essay. *The Journal of Library History, 22*(2), 206–227.
71. Chen, M. (2008). Informality and social protection: Theories and realities. *IDS Bulletin, 39*(2), 18–27.
72. Cooper, H. H. A. (1978). Terrorism: The problem of the problem definition, *Chitty law journal*, (*26*), 105–108.
73. Council Directive 2008/114/EC of 8 Decembar 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. *Official Journal of the European Union* L, 345–375.
74. Шкарић, Ј. К., (2009.) Форензичко рачуноводство - инструмент заштите интереса рачуноводствене јавности, Зборник радова са 13. Конгреса СРР Републике Српске: Рачуноводство, ревизија и финансије у условима глобалне кризе, Бања Врућица.
75. Warner, M. (2002). Wanted: A Definition of „Intelligence" — Understanding Our Craft. *Studies of Intelligence, vol 46*, *No 3*, 21.
76. Watson, D. (2007). Honeynets: a tool for counterintelligence in online security. *Network Security,* 4–8.
77. Wæver, Ole (2003). Securitization: Taking Stock of a Research Programme in Security Studies. (unpublished manuscript).
78. Wenning, R. J., Apitz, S. E., Belluck, D. A., Chiesa, S., Figueira, J., Filip, Z., ... & Xenidis, Y. (2007). Environmental Security. *Environmental Security in Harbors and Coastal Areas,* 19–36.
79. Winkler, I. S. (1996). Case study of industrial espionage through social engineering. *Proceedings of 19th national information systems security conference.*
80. Yergin, D. (2006). Ensuring energy security. *Foreign Affairs*, *85*(2), 69–82.

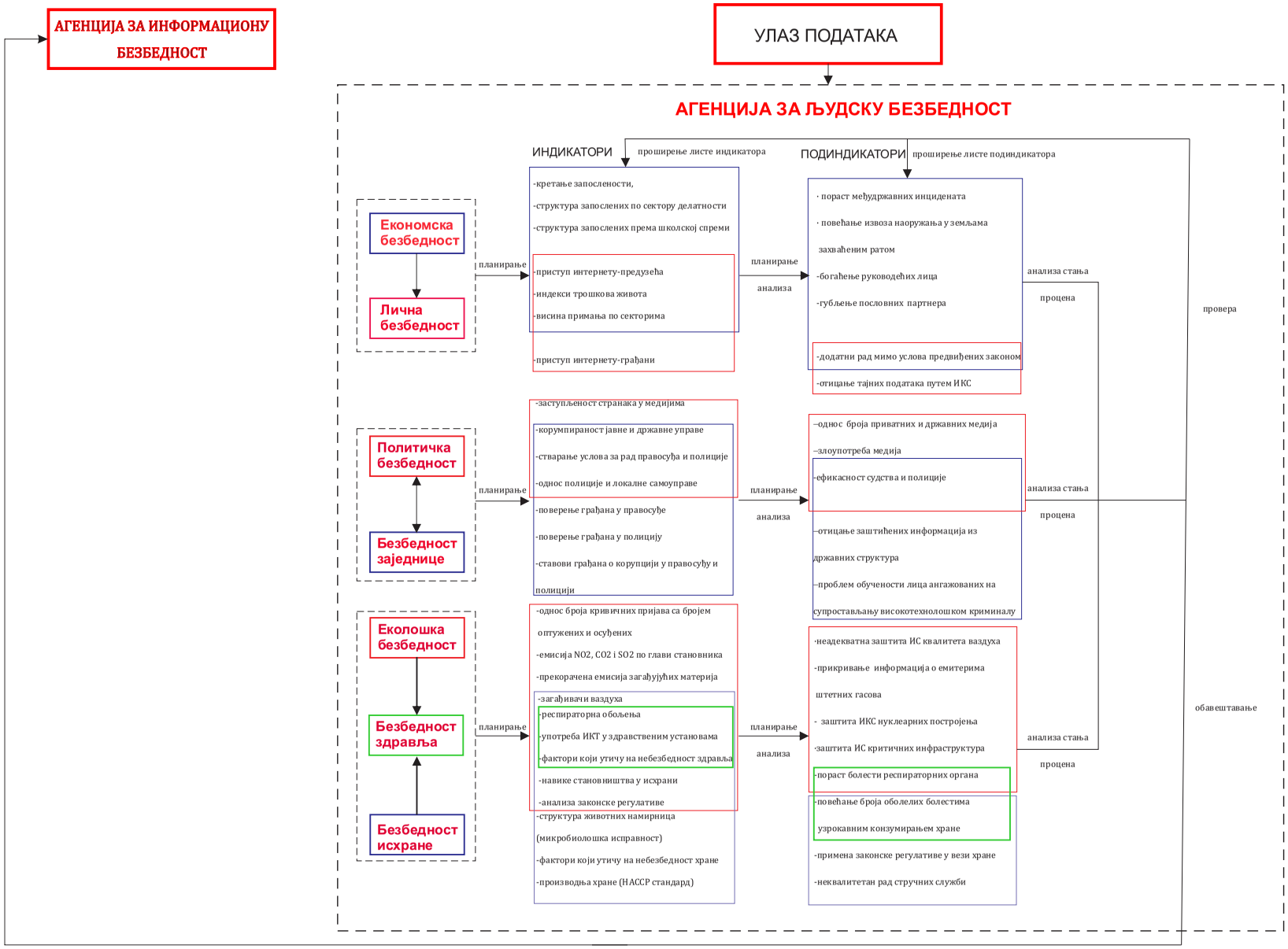
Табеле, графикони, слике и шеме

12. ПРИЛОЗИ

1. Прилог бр. 1 Функционални модел заштите пословних информација
2. Прилог бр. 2 Модел заштите пословних информација са аспекта људске безбедности



Шема бр.8: Функционални модел заштите пословних информација



Шема бр.9: Модел заштите пословних информација са аспекта људске безбедности

13. БИОГРАФИЈА

Дејан Тепавац је рођен 15.05.1976. године у Карловцу, Република Хрватска. Основну и средњу школу, Гимназију општег смера, завршио је у Кореници. На Војној Академији у Београду дипломирао је 1998. године, а магистрирао 2006. године на Пољопривредном факултету у Новом Саду из научне области Маркетинг у агроекономији. Учествовао је, као коаутор, у изради неколико радова у којима је разматран економски потенцијал Републике Србије на међународном тржишту агроиндустријских производа. Завршио је више различитих, специјалистичких, с аспекта безбедности, курсева и семинара у организацији Војнобезбедносне агенције, Министарства одбране Републике Србије.

Учесник је, такође, више пројеката и активности из области одбране. Од 2004. године запослен је у Министарству одбране Републике Србије, у Војнобезбедносној агенцији. Говори немачки, енглески и руски језик.

Дејан Тепавац живи у Новом Саду, ожењен је и отац је двоје деце.

Прилог 1.

Изјава о ауторству

Потписани-а Дејан Н. Тепавац

број уписа _____

Изјављујем

да је докторска дисертација под насловом

„Заштита пословних информација у функцији националне безбедности“

- резултат сопственог истраживачког рада,
- да предложена дисертација у целини ни у деловима није била предложена за добијање било које дипломе према студијским програмима других високошколских установа,
- да су резултати коректно наведени и
- да нисам кршио/ла ауторска права и користио интелектуалну својину других лица.

Потпис докторанда

У Београду, _____

_____

Прилог 2.

Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора Дејан Тепавац

Број уписа _____

Студијски програм Наука безбедности

Наслов рада "Заштита пословних информација у функцији националне безбедности"

Ментор проф. др Ивица Ђорђевић

Потписани Дејан Н. Тепавац

изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла за објављивање на порталу **Дигиталног репозиторијума Универзитета у Београду.**

Дозвољавам да се објаве моји лични подаци везани за добијање академског звања доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис докторанда

У Београду, _____

_____

Прилог 3.

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

“Заштита пословних информација у функцији националне безбедности“

која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигитални репозиторијум Универзитета у Београду могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. Ауторство

2. Ауторство - некомерцијално

3. Ауторство – некомерцијално – без прераде

4. Ауторство – некомерцијално – делити под истим условима

5. Ауторство – без прераде

6. Ауторство – делити под истим условима

(Молимо да заокружите само једну од шест понуђених лиценци, кратак опис лиценци дат је на полеђини листа).

Потпис докторанда

У Београду, _____

_____

1. Ауторство - Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце, чак и у комерцијалне сврхе. Ово је најслободнија од свих лиценци.

2. Ауторство – некомерцијално. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела.

3. Ауторство - некомерцијално – без прераде. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела. У односу на све остале лиценце, овом лиценцом се ограничава највећи обим права коришћења дела.

4. Ауторство - некомерцијално – делити под истим условима. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца не дозвољава комерцијалну употребу дела и прерада.

5. Ауторство – без прераде. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца дозвољава комерцијалну употребу дела.

6. Ауторство - делити под истим условима. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца дозвољава комерцијалну употребу дела и прерада. Слична је софтверским лиценцама, односно лиценцама отвореног кода.