ИНФОРМАЦИОНА БЕЗБЕДНОСТ КАО ЕЛЕМЕНАТ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ

Чедомир Герзић[1],

Резиме: Поред политичке, економске, војне, техничке, технолошке, еколошке и хуманитарне безбедности, информациона безбедност је интегрални део безбедности државе. Информациона безбедност игра кључну улогу у обезбеђивању виталних интереса државе. То је условљено првенствено насушном потребом за стварањем развијеног и заштићеног информационог окружења. Управо кроз информационо окружење остварују се претње националној безбедности у различитим областима деловања државе.

Научни и технички напредак претворио је информације у производ који се може купити, продати и разменити. Често је цена информација вишеструко већа од цене читавог техничког система који чува и обрађује информације. Квалитет комерцијалних информација обезбеђује неопходан економски ефекат за компанију, па је важно заштитити критичне податке од лошег утицаја.

Информационо окружење, као фактор формирања система у свим сферама националне безбедности, активно утиче на стање свих компоненти националне безбедности. Истовремено, оно представља независну сферу националне безбедности у којој је неопходно осигурати заштиту информационих ресурса, системе за њихово формирање, дистрибуцију и коришћење, информациону инфраструктуру, остваривање права на информације државе, правних лица и грађана.

Кључне речи: *држава, информациона безбедност, национална безбедност.*

INFORMATION SECURITY AS AN ELEMENT NATIONAL SECURITY

Cedomir Gerzic[1]

Summary: In addition to political, economic, military, technical, technological, environmental and humanitarian security, information security is an integral part of national security. Information security plays a key role in ensuring the vital interests of the state. This is conditioned primarily by the urgent need to create a developed and protected information environment. It is through the information environment that threats to national security in different areas of the state's activity are realized.

Scientific and technical progress has turned information into a product that can be bought, sold and exchanged. Often the price of information is many times higher than the price of the entire technical system that stores and processes information. The quality of commercial information provides the necessary economic impact for the company, so it is important to protect critical data from bad influence.

The information environment, as a factor of system formation in all spheres of national security, actively influences the state of all components of national security. At the same time, it represents an independent sphere of national security in which it is necessary to ensure the protection of information resources, systems for their formation, distribution and use, information infrastructure, the exercise of the right to information of the state, legal entities and citizens.

Key words: *country, information security, national security.*

[1] Чедомир Гезић, Катедра оперативе, Школа националне одбране, Универзитет одбране, Незнаног јунака 38, Београд, cedomirgerzic@gmail.com

1. УВОД

Појам националне безбедности постао је широко распрострањен последњих неколико деценија. У већини случајева национална безбедност повезана је са активностима посебних служби и углавном се идентификује са одбраном државе. Без обзира што су у савременим схватањима, гаранција безбедности државе њене оружане снаге, велики значај имају економски, политички, морално-етички и други аспекти обезбеђења националне безбедности.

Национална безбедност је стање заштите виталних интереса грађана, друштва и државе од унутрашњих и спољашњих претњи. Витални интереси су права и слободе грађана, који доприносе нормалном функционисању друштва у целини и суверенитету државе. Основни елементи националне безбедности државе су: политичка, економска, војна, техничка, технолошка, еколошка, **информациона** и хуманитарна безбедност.

Основни принципи националне безбедности државе су законитост, поштовање безбедносних интереса грађана и државе, узајамна одговорност за обезбеђење безбедности на међународном плану, веза између националне и међународне безбедности, итд.

Информационе технологије одавно су попримиле глобални карактер и постале саставни део свих сфера активности појединаца, друштва и државе. Њихова ефикасна примена је фактор убрзања економског развоја државе и формирања информационог друштва.

Информациона сфера представља комбинацију информација, информационе инфраструктуре, субјеката који учествују у прикупљању, генерисању, дистрибуцији и употреби информација. Активно утиче на стање политичке, економске, одбрамбене и друге компоненте безбедности државе. Остваривање националних интереса у информационој сфери има за циљ стварање сигурног окружења за кретање поуздане информације и учвршћивање информационе инфраструктуре отпорне на разне врсте утицаја, у циљу обезбеђења уставних права и слобода човека и грађана, стабилног друштвено-економског развоја и националне безбедности. Национална безбедност у великој мери зависи од заштите безбедности информација, а током технолошког напретка та зависност ће се повећавати [1].

Имајући у виду стални развој информационих технологија, циљ рада је указати на улогу и значај информационе безбедности као елемента националне безбедности, указати на могуће информационе претње, стратешке циљеве и правце обезбеђења информационе безбедности државе уопште.

Рад је обрађен кроз три целине. У првој целини дефинисана је информациона безбедност и објашњена њена улога и значај као компоненете безбедности државе уопште. Друга целина обрађује спољне и унутрашње информационе претње и стање информационе безбедности које се могу појавити у било којој држави. Треће поглавље говори о могућим стратешким циљевима и основним правцима обезбеђења информационе безбедности развијене и економски јаке државе уопште.

2. ПОЈАМ, УЛОГА И ЗНАЧАЈ ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ

Увођење савремених информационих технологија у све области економског и духовног живота доводи до повећања важности заштите националне безбедности у информатичкој сфери.

Информациона безбедност је независна компонента националне безбедности и има директан утицај на заштиту интереса државе у другим сегментима њеног функционисања. Национална безбедност у великој мери зависи од заштите безбедности информација. Даљи технолошки напредак цивилизације довешће до додатног пораста ове зависности. Мишљење, да ће XXI век бити век информационог оружја и "бесконтактних" ратова, постаје све раширенije.

Под информационој безбедности подразумева се стање заштите националних интереса земље (витални интереси појединца, друштва и државе) у информационој сфери од унутрашњих и спољних претњи. Информациона сфера представља комбинацију информационих ресурса и информатичке инфраструктуре објекта заштите. Систем информационе безбедности представља организовани скуп органа, средстава, метода и мера којима се осигурава заштита информација од откривања, цурења и неовлашћеног приступа [2].

Главне компоненте информационе безбедности су заштита података (заштита личних података, државне и службене тајне и других врста информација ограничене дистрибуције), заштита података од случајних или намерних природних или вештачких утицаја, гаранција уставних права и слобода човека и грађанина у погледу активности у информационој сфери и заштита потреба грађана, посебних група и становништва у целини, од негативних (намерних и случајних) информационо-психолошких и информационо-техничких утицаја.

Национални интереси државе у информационој сфери састоје се у поштовању уставних права и слобода грађана у области добијања информација и њиховог коришћења, у развоју савремених телекомуникационих технологија, у заштити државних информационих ресурса од неовлашћеног приступа.

Најважнији услови за заштиту безбедности су законитост, адекватност, одржавање баланса интереса појединца и организације, висока професионалност лица запослених у служби која се бави заштитом информација, обука корисника, поштовање свих утврђених правила чувања поверљивих информација, међусобна одговорност особља и руководства и интеракција са државним установама које спроводе закон. Без ових услова, ниједан систем безбедности информација не може да обезбеди тражени ниво заштите.

3. ОСНОВНЕ ИНФОРМАЦИОНЕ ПРЕТЊЕ И СТАЊЕ ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ

Ширење области примене информационих технологија, је фактор развоја економије и усавршавања функционисања приватних и државних институција, истовремено стварајући нове информационе претње. Могућности размене информација ван граница државе, све чешће се користи за постизање геополитичких, војно-политичких, терористичких, екстремистичких, криминалних и других противзаконитих циљева на штету међународне безбедности и стратегијске стабилности. Пракса увођења

информационих технологија без заштите информационе безбедности суштински повећава вероватноћу појаве информационих претњи.

Један од основних негативних фактора који утичу на стање информационе безбедности, јесте могућност низа развијених земаља да у информационо-техничком смислу утичу на војну информациону структуру. Истовремено се повећава активност организација које врше «праћење рада» државних органа, научних организација и предузећа одбрамбено-индустријског комплекса.

Специјалне службе појединих земаља повећавају размере коришћења средстава информационо-психолошког утицаја, усмерених првенствено на дестабилизацију унутарполитичких и социјалних ситуација у различитим регионима света, што доводи до подривања суверенитета и нарушавања територијалне целовитости других држава. У ту активност увлаче религиозне, етничке и организације за заштиту права, а такође и групе грађана, при чему максимално користе могућности информационих технологија. Повећава се информациони утицај на грађане државе, првенствено на младе, са циљем урушавања традиционалних духовних и моралних вредности државе.

Различите терористичке и екстремистичке организације широко користе механизме информационог утицаја на лична, групна и друштвена сазнања у циљу стварања међунационалних и социјалних напрезања, распиривања етничке и религиозне мржње и непријатељства, пропаганде екстремистичке идеологије, а такође

Повећавају се размере компјутерског криминала, пре свега у кредитно-финансијској сфери, повећава се број криминалних радњи везаних за уставна права и слободе човека и грађанина, у делу који се тиче живота, личне и породичне тајне, при обради персоналних података коришћењем информационих технологија. Методе, начини и средства криминалних активности постају све софистицираниј[5].

Стање информационе безбедности у области одбране земље карактерише се повећањем размера примене информационих технологија од стране појединих држава и организација, усмерених на подривање суверенитета, политичке и социјалне стабилности и територијалне целовитости државе и њених савезника и представља претњу међународном миру, глобалној и регионалној безбедности.

У области државне безбедности, стање информационе безбедности карактерише се непрекидним повећањем сложености, размере и раста координисаних компјутерских напада на објекте критичне информационе инфраструктуре, повећањем обавештајних активности страних земаља, а такође и повећањем претње примене информационих технологија у циљу наношења штете суверенитету, територијалној целовитости, политичкој и социјалној стабилности државе.

У економској сфери стање информационе безбедности карактерише се недовољним нивоом развоја конкурентних информационих технологија и њихово коришћење за производњу и пружање услуга. Постоји висок ниво зависности домаће индустрије информационих технологија од индустрије информационих технологија других држава, првенствено од електронских компоненти, софтвера, рачунарске технологије и комуникација, што условљава зависност социјално-економског развоја државе од геополитичких интереса других земаља.

Стање информационе безбедности у области науке, технологија и образовања карактерише се недовољном ефективношћу научних истраживања, усмерених на стварање перспективних информационих технологија, ниским нивом увођења домаћих

патената и недостатком кадра у области информационих технологија, а такође ниском свешћу грађана по питањима заштите личне информационе безбедности [3].

Мере заштите безбедности информационе инфраструктуре, укључујући њен интегритет, доступност и стабилно функционисање, коришћењем домаћих информационих технологија, често немају интегрисани оквир.

Стање информационе безбедности у области стратегијске стабилности и равноправног стратегијског партнерства, карактерише се стремљењем појединих држава за коришћењем технолошке предности ради доминирања у информационом пространству.

Одсуство међународних правних норми, које регулишу међудржавне односе у информационом простору, а такође механизме и процедуре њихове примене, уважавајући специфичност информационих технологија, отежава формирање система међународне информационе безбедности, усмерене на достизање стратегијске стабилности и равноправног стратегијског партнерства.

Под претњом безбедности информација подразумева се комбинација услова и фактора који стварају потенцијалну или стварну опасност везану за цурење информација и (или) неовлашћеним и (или) ненамерним утицајима на њих. Претње информационој безбедности државе деле се на спољне и унутрашње.

Спољне претње које представљају највећу опасност за објекте заштите су: све врсте обавештајних активности страних земаља, информативни и технички утицаји (радиоелектронска борба, продирање у рачунарске мреже), саботаже и субверзивне активности специјалних служби страних држава и активности страних политичких, економских и војних структура усмерених против интереса државе у области одбране.

Унутрашње претње представљају посебну опасност у условима погоршања војно-политичке ситуације и укључују: кршење утврђених правила прикупљања, обраде, чувања и преноса информација у државном апарату и предузећима одбрамбене индустрије, намерне грешке као и грешке персонала информационих и телекомуникационих система за посебне намене, непоуздано функционисање информационих и телекомуникационих система за посебне намене, могућа информационо-пропагандна делатност која подрива функционисање безбедносних структура и њихову оперативну способност и нерешена питања заштите интелектуалног власништва предузећа одбрамбене индустрије, што доводи до цурења вредних државних информационих ресурса у иностранству.

Заштита информација треба да буде: централизована, планирана, специфична, фокусирана, активна, поуздана, универзална, нестандардна, отворена и исплатива.

4. СТРАТЕШКИ ЦИЉЕВИ И ОСНОВНИ ПРАВЦИ ОБЕЗБЕЂЕЊА ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ

Стратешки циљ обезбеђења информационе безбедности у области одбране економски и војно јаке земље је заштита виталних интереса појединца, друштва и државе од унутрашњих и спољних претњи повезаних са коришћењем информационих технологија у војне и политичке сврхе, у циљу спречавања непријатељских аката агресије, чији је циљ подривање суверенитета државе, кршење територијалног интегритета држава и угрожавање међународног мира, сигурности и стратешке стабилности.

У складу са војном политиком економски јаке и развијене државе уопште, главни правци заштите информационе безбедности у области националне одбране могу бити [4]:

- стратешко одвраћање и спречавање војних сукоба који могу настати као резултат употребе информационих технологија,
- усавршавање система обезбеђења информационе безбедности оружаних снага државе и других снага система одбране, укључујући снаге и средства информационог супростављања,
- предвиђање, откривање и процена информационих претњи, укључујући претње оружаним снагама државе у информационој сфери,
- помоћ савезницима у заштити интереса у информационој сфери и
- неутралисање информационо-психолошког утицаја, усмереног на подривање историјских основа и патриотских традиција повезаних са заштитом отаџбине.

Стратешки циљеви обезбеђења информационе безбедности у области државне и јавне безбедности су заштита суверенитета, одржавање политичке и социјалне стабилности, територијални интегритет државе, обезбеђивање основних права и слобода човека и грађана, а такође и заштита критичне информационе инфраструктуре. Основни правци заштите информационе безбедности у области државне и јавне безбедности су [4]:

- сузбијање коришћења информационих технологија за промовисање екстремистичке идеологије, ширење ксенофобије, идеје националног одвајања ради подривања суверенитета, политичке и друштвене стабилности, насилна промена уставног поретка и кршење територијалног интегритета државе,
- сузбијање активности штетних по националну безбедност, које се врше коришћењем техничких средстава и информационих технологија од стране специјалних служби и организација страних држава, као и од стране појединаца,
- повећање заштите критичне информационе инфраструктуре и стабилности њеног функционисања, развијање механизама за откривање и спречавање информационих претњи и отклањање последица њихове примене, повећање заштите грађана и територија од последица ванредних стања изазваних информационо-техничким утицајем на објекте критичне информационе инфраструктуре,
- унапређење безбедности функционисања објеката информационе инфраструктуре, са циљем обезбеђивања одрживе интеракције између државних органа, спречавања стране контроле над радом таквих објеката, обезбеђивање интегритета, стабилности рада и безбедности јединствене телекомуникационе мреже државе, као и обезбеђивање безбедности података који се преносе преко ње и обрађују у информационим системима на територији државе,
- побољшање безбедности функционисања образаца израде оружја, војне и специјалне опреме и аутоматизованих система за контролу,
- повећање ефикасности у спречавању кривичних дела почињених коришћењем информационих технологија и сузбијање таквих кривичних дела,
- обезбеђење заштите информација које представљају државну тајну, других информација ограниченог приступа и дистрибуције, укључујући повећање заштите безбедности одговарајућих информационих технологија,

- усавршавање метода и начина израде и безбедног коришћења производа и пружање услуга путем информационих технологија коришћењем домаћих патената који задовољавају захтеве информационе безбедности,
- побољшање ефикасности информационе подршке у спровођење државне политике и
- неутрализација информационог утицаја усмереног на нарушавање традиционалних духовних и моралних вредности државе.

Стратешки циљеви обезбеђења информационе безбедности државе уопште у економској сфери су свођење утицаја негативних фактора узрокованих недовољним степеном развоја домаће индустрије информационих технологија и електронске индустрије на најмањи могући ниво, развој и производња конкурентских средстава за заштиту информационе безбедности, као и повећање обима и квалитета услуга у области информационе безбедности. Основни правци заштите информационе безбедности у економској сфери могу бити [4]:

- иновативни развој информационе технологије и електронске индустрије, повећање учешћа производа ове индустрије у бруто домаћем производу,
- уклањање зависности домаће индустрије од страних информационих технологија и средстава за заштиту информационе безбедности, стварањем, развојем и широким увођењем домаћих производа, као и производње добара и пружања услуга заснованих на њима
- повећање конкурентности државних компанија које послују у области информационих технологија и електронске индустрије и
- развој, производња и коришћење средстава за информациону безбедност за сопствене потребе и излазак на светско тржиште.

Стратешки циљ заштите информационе безбедности у области науке, технологије и образовања је подршка иновативном и убрзаном развоју система заштите информационе безбедности, индустрије информационих технологија и електронске индустрије. Главни правци заштите информационе безбедности у области науке, технологије и образовања најчешће су [4]:

- постизање конкурентности државних информационих технологија и развој научног и техничког потенцијала у области заштите информационе безбедности,
- стварање и примена информационих технологија отпорних на разне врсте утицаја,
- реализација научних истраживања и експеримената у циљу стварања напредних информационих технологија и средстава за заштиту информационе безбедности,
- развој људских ресурса у области заштите информационе безбедности и примене информационих технологија и
- обезбеђивање заштите грађана од информационих претњи, укључујући формирање културе личне информационе безбедности.

Стратешки циљ заштите информационе безбедности у области стратешке стабилности и равноправног стратешког партнерства међу најразвијенијим земљама света су формирање стабилног система неконфликтних међудржавних односа у информационом простору. Главни правци заштите информационе безбедности у области стратешке стабилности и равноправног стратешког партнерства могу бити [4]:

- заштита суверенитета државе у информационом простору путем спровођења самосталне и независне политике усмерене на остваривање националних интереса у информационој сфери,
- учествовање у формирању међународног система безбедности информација који пружа ефикасно супростављање коришћењу информационих технологија у војне и политичке сврхе,
- стварање међународних правних механизама који узимају у обзир специфичности информационих технологија, у циљу спречавања и решавања међудржавних сукоба у информационом простору и
- промоција положаја државе у оквиру активности међународних организација, које разматрају равноправну и обострано корисну сарадњу свих заинтересованих страна у информационој сфери.

5. ЗАКЉУЧАК

Национална безбедност државе је део глобалне међународне безбедности и представља инструмент за заштиту интереса грађана, друштва и државе у целини од спољних и унутрашњих претњи. Објекти националне безбедности су уставом загарантована права и слободе грађана, вредности цивилног друштва, суверенитет државе. Законодавни и извршни органи државе формирају и спроводе стратегију националне безбедности, преносећи своја овлашћења на безбедносне и небезбедносне снаге.

У савременим условима политичког и друштвено-економског развоја, контрадикције између потребе за проширењем слободне размене информација и потребе за одржавањем одређених ограничења у њеном ширењу, погоршавају се.

Тенденција повећања отворености друштва, повећања интензитета размене информација, широка употреба напредних технологија за прикупљање и обраду информација, ствара претпоставке за могуће незаконите радње у вези с информацијама и њеним корисницима. Уз транспарентност информација, треба обезбедити и остваривање уставних права личности, друштва и државе на заштиту информација са ограниченим приступом.

Повећање степена отворености државе према друштву диктира потребу за максималним могућим смањењем броја информација које су класификоване као државне тајне, отвореношћу опште листе категорија информација које се на њих односе и механизама њихове класификације.

Информациона безбедност развија се и расте последњих година. У оквиру ње, појавило се много специјалистичких области, као нпр. безбедност мрежа и одговарајуће инфраструктуре, заштита софтвера и база података, ревизија информационог система, планирање континуитета пословања, детекција електронских записа и рачунарска форензика. Стручњаци за информациону безбедност имају веома стабилно запослење и тражени су на тржишту рада.

Обезбеђење информационе заштите државе један је од кључних задатака формирања информационог друштва. Његово решење укључује обезбеђење информационе безбедности грађана и саму информациону инфраструктуру, у условима информационог деловања.

Истраживање је актуелно и оригинално, засновано на коришћењу дела литературе која се користи у изучавању садржаја дисциплине Национална безбедност на

Генералштабној академији Оружаних снага Руске Федерације у Москви и анализи неколико чланака који се баве овом проблематиком, а из новијег су периода. С обзиром да се у Републици Србији о информационој безбедности мало пише, овај рад може представљатиј скроман допринос теоријском изучавању наведене проблематике.

6. ЛИТЕРАТУРА

[1] Баранова, Е.К. *Информационная безопасность и защита информации*: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018.

[2] Доктрина информационной безопасности Российской Федерации*, Указ Президента Российской Федерации от 05.12.2016, № 646*.

[3] Гришина, Н.В. *Информационная безопасность предприятия*: Учебное пособие / Н.В. Гришина. - М.: Форум, 2018.

[4] Партыка, Т.Л. *Информационная безопасность*: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2018.

[5] Шаньгин, В.Ф. *Информационная безопасность компьютерных систем и сетей*: Учебное пособие / В.Ф. Шаньгин. - М.: Форум, 2018.