Информациона безбедност – компонента националне безбедности

УДК: 355.405.356.255.2 : 316.774 : 623.618

Стеван Синковски

У савременом друштву информациона безбедност је компонента националне безбедности. У склопу објашњења појма безбедности и појма информационе безбедности дате су основне поставке опште науке о безбедности и теорије информационог ратовања. Информациона безбедност се јавља не само као један од облика безбедности, већ и као пресек свих других облика безбедности у којима информационе технологије заузимају важно место. У том контексту приказан је однос информационе, економске и војне безбедности и начин заштите информационе инфраструктуре у САД.

Кључне речи: *безбедност, информациона безбедност, информационо ратовање, информациона супериорност, информационе операције, информационо обезбеђење, модел информационе безбедности, модел информационог обезбеђења, национална безбедност, критична инфраструктура, заштита информационе инфраструктуре.*

Увод

Један од основних мотива делатности човека и друштва посматран кроз историју и, несумњиво, један од глобалних проблема савремене епохе је ***безбедност***. Све донедавно проблем безбедности је подразумевао разматрање, пре свега, војног аспекта. ***Информациона безбедност***, као један од новијих праваца истраживања у сфери безбедности, појавила се као последица настанка и развоја информационог друштва. О значају информационе безбедности говори чињеница да је она једна од основних ***компонената*** у доктринама националне безбедности неких земаља.

Циљ овог рада је да покаже, на примеру САД и Руске федерације, да је информациона безбедност у савременом друштву неодвојиви део проблематике ***националне безбедности*** и да представља једну од њених основних компоненти.

Појам, садржај и суштина безбедности

Општа наука и безбедност

Све време наука је настојала да свет представи као јединствену целину. Међутим, тек крајем XX века сазрели су услови за формира-

ње интегрисаних интердисциплинарних наука које омогућавају развој фундаменталног схватања јединства и интегрисаности светског здања. Поред насталих интердисциплинарних наука (информациологија, ноокосмологија, епиологија, соционика),[1] као очигледна се појавила потреба формирања нове научне дисциплине повезане са човеком, његовом делатношћу и његовим местом у свету – ***наука о безбедности*** човека као индивидуе и његове безбедности у светском окружењу укључујући и безбедност саме средине у којој човек обитава [1].

Развој доктрине безбедности повезан је са решењем низа филозофско-методолошких и теоретских проблема. Један од њих је ***појам безбедности*** као интегративни појам који подразумева све видове безбедности (економску, војну, геополитичку, политичку, информациону, социјалну, демографску, еколошку, генетичку и друге), али који се не своди на њихов прост збир [1].

Општа теорија безбедности је разрада оптималне структуре система безбедности, заснована на циљевима и задацима, месту и улози основних компонената и њихових међусобних утицаја. Уколико је безбедност једна од свеопштих, основних, примарних и водећих потреба и законитости развоја човека и човечанства, неоспорно је да у формирању њене теорије главну улогу треба да има социјална филозофија – наука која се бави најопштијим законитостима развоја човека и друштва водећи рачуна о томе да се човек у њој јавља и као субјекат и као објекат [1].

Неки од аутора, [1], за општу науку о безбедности користе термин секјуритологија.

Предмет испитивања опште науке о безбедности су активности на обезбеђењу свих животних делатности и безбедности природних услова живота у границама ноосфере.[2] Предмет опште науке о безбедности је безбедност човека, друштва, државе, планете, цивилизације у свој различитости претњи – напада, у различитим условима, ситуацијама, у развоју, у простору и времену [1].

Главни ***објекат*** испитивања је човечанство укључујући државе, друштва и појединачна лица.

Главни ***циљ*** опште науке о безбедности је откривање законитости безбедног развоја ноосфере, изучавање, упоређивање, класификација и систематизација сложених догађаја, процеса, појава у области безбедности животних делатности човека, човечанства и израда одговарајућих мера за њихово предупређење, локализацију и отклањање.

---

[1] Информациологија – наука о јединственом информационом пољу Свемира, ноокосмологија – наука о јединствености Свемира, епиологија – наука о енергетско-информационој размени између живе и неживе природе, соционика – наука о јединственом информационо-енергетском организму [1].

[2] Ноосфера је наука о стабилном развоју.

Општа наука о безбедности је наука о законитостима и механизмима обезбеђења безбедности човека, друштва, државе и човечанства од спољашњих и унутрашњих напада [1]).

Појам садржај и суштина безбедности

Кроз историју се види да је потреба за безбедношћу један од основних мотива делатности људи и друштва. Шта је то безбедност? У практичном животу безбедност се манифестује:

– као гарантована (конституционалним, законодавним и практичним мерама) ***заштићеност*** животно важних интереса личности, друштва и државе,

– као наука, искуство и култура,

– као животно важни ***интереси***: економска самосталност, правно и социјално благостање, интегритет и стабилно и ефикасно функционисање, али и

– као свакодневни, тежак, рутински, али крајње важан ***посао***.

Различити су приступи у формулисању појма безбедности. Анализирајући различите приступе, који са различитих позиција откривају природу безбедности, према [1] предложено је издвајање најважнијих, базних елемената појма безбедности:

– велики број аутора под безбедношћу подразумева ***стање*** потенцијалних жртава, објеката напада,[3]

– неки безбедност посматрају као ***способност*** објекта, појаве, процеса да сачува своју суштину и основну карактеристику у условима намерног, деструктивног дејства споља или у самом објекту, појави, процесу,

– по некима је безбедност системска категорија, ***својство система*** изграђено на принципима стабилности, саморегулације, поузданости (безбедност је позвана да заштити свако од тих својстава система),

– неки безбедност разматрају као ***решавајући услов*** (гарант) животних делатности личности, друштва, државе што им омогућава да сачувају и повећају њихове материјалне и духовне вредности,

– за неке је безбедност ***одсуство*** претњи и напада и

– некима је основни елеменат свих појмова ***напад*** као реалан одраз претњи. Напад у том контексту узима својство суштинске карактеристике. Напад и борба са њим је суштина безбедности.

Шта су предмет и суштина појма безбедност? Предмет и суштина појма безбедност су: ***стање заштићености*** личности, друштва, државе, ***стање заштићености*** животних интереса, ***стање заштићености*** националних интереса, ***стабилно стање система*** у односу на непо-

[3] Наведено становиште заступа и Родић Б., Интеракција јавних рачунарских мрежа и рачунарских мрежа специјалних институција (докторска дисертација), Војнотехничка академија, Београд, 2001.

вољна дејства. Важно је уочити да су сви ови парцијални случајеви увек у контексту конкретних друштвених односа. У противном термин заштита је узак. За разматрање појма неопходан је системски прилаз. Он подразумева да су садржај и степен безбедности човека и друштва директно зависни од функционисања свих структура друштва, а, пре свега, економске, политичке, социјалне, правне итд. Као резултат, имамо да систем безбедности има сложену структуру [1].

Појам, садржај и суштина информационе безбедности

Историјски контекст настанка појма информационе безбедности

Примат у теорији и пракси информационе безбедности припада САД. Према речима Даниела Волфа [2],[4] историјски посматрано, прво је третирана (60-их година) комуникациона безбедност (COMSEC – *communication security*). Са појавом компјутера (70-их година) настала је компјутерска безбедност (COMPUSEC – *computer security*). Крајем 80-их година COMSEC и COMPUSEC су интегрисани и појавио се појам ***информациона безбедност*** (INFOSEC – *information security*). Информациона безбедност је интегрисала раније одвојене дисциплине као што су безбедност персонала, компјутерска безбедност, комуникациона безбедност и оперативна безбедност. Већ у том тренутку информациона безбедност је постала један од четири камена темељца националне безбедности САД (дипломатија, економија, војна компонента и информациона компонента).[5] Акценат INFOSEC је стављен на спречавање неауторизованог приступа информационим системима. Разматрана је, пре свега, поверљивост *(confidentiality)* информација. Напредак у компјутерској техници и појава мрежа (LAN и WAN и, пре свега ИНТЕРНЕТ'-а), проширује листу својстава информација, пред које се постављају безбедности захтеви, као што су: расположивост *(availability)*, интегритет *(integrity)*, аутентичност *(authentication)* и непорицљивост *(non-repudiation)*. На основама наведених својстава информација (или безбедносних сервиса информација и информационих система), формулисан је 90-их година појам

[4] Реч је о саслушању Данијела Волфа пред подкомитетом за унутрашњу безбедност сената САД 22 јула 2003. године. Daniel Wolf је директор за информационо обезбеђење *(information assurance)* у америчкој Агенцији за националну безбедност (NSA – *Nacional Security Agency*).

[5] „Препоруке државној дипломатији у вези са циљевима националне безбедности", САД, 1983. Исте године МО САД издало је тзв. „наранџасту књигу" – „Критеријуме процене поузданости компјутерских система" (TCSEC – *Trusted Computer Systems Evaluation Criteria)*, чиме су постављени темељи систематизацији знања о информационој безбедности ван владиних институција.

информационог обезбеђења[6] (IA – *information assurance*). Важно је уочити да разлика није само терминолошке природе, већ да је реч о суштинским променама [2]. Поред наведених безбедносних сервиса, информационо обезбеђење (ИА) има још једну важну карактеристику а то је оперативност у реалности (*operational in nature*) и осетљивост на време (*time-sensitive*). Ову карактеристику изражавају термини детекција (*detection*) и реакција (*reaction*).[7] Реч је о дефанзивним оперативним могућностима које се, заједно са традиционалним IA активностима, од касних 90-их година описују термином одбрамбених информационих операција (DIO – *defensive information operations*).[8] Коначно, тек 2002. године директивом DoDD 8500.1 званично је уведен појам информационо обезбеђење у САД.[9]

Као основно полазиште у дефинисању појмова информационе безбедности, односно информационог обезбеђења у САД послужила је теорија информационог ратовања IW (*information warfare*). Информационо ратовање је прокламовао Пентагон у настојању да пронађе револуционарне промене у војним пословима (RMA – *revolution in military affairs*). Као главни промотер IW, Пентагон је основни покретач напретка у теорији и пракси информационог обезбеђења.[10]

Информационој безбедности (термин који се користи у западним земљама и у Руској федерацији) се придаје посебна пажња на нивоу влада Велике осморице. Председник САД је почетком 2000. год. донео Национални план заштите информационих система у коме је координиран рад на националним програмима информационе безбедности до 2003. год. План обухвата решавање не само војних проблема, већ је усмерен и на консолидацију напора владе, федералних држава и појединачних фирми и у цивилном сектору. У индустријским гранама САД, упоредо са Федерални центром заштите инфраструктуре и Главним федералним центром, предвиђена је организација сопствених компанијских центара анализе токова и заштите информација. На тај начин, у САД, је направљен степенасти систем информационе безбедности. Месец дана после трагичних септембарских збивања 2001. год., председник Буш је донео указ о формирању Управе за унутрашњу безбедност (*Office of Homeland Security*) и Савета за унутрашњу безбедност (*Homeland Securiry Council*). Влада је добила једно

---

[6] У српском језику не постоји адекватан термин. Могућ је превод: информациона гаранција, информационо осигурање или, у нешто слободнијем контексту, информационо обезбеђење. Интересантно је напоменути да руски научници, који се баве друштвеним наукама, иначе користе термин информационо обезбеђење.

[7] Реч је о заштитним могућностима информационих система да детектују напад и да у случају успешног напада обнове основне функције.

[8] За разумевање проблема информационе безбедности у теорији и пракси САД неопходно је познавати теорију информационог ратовања IW (*information warfare*).

[9] Department of Defense Directive number 8500.1 *Information assurance (IA)*, october 24, 2002

[10] Пенагон је, због зависности америчких ОС од информационих технологија, по природи ствари, најзаинтересованији за сферу информационог обезбеђења.

чиновничко место за питања информационе безбедности, а у оквиру обавештајних структура формирана је нова специјална служба са посебним задацима – грађанска одбрана насеља, инфраструктуре и кибер-простора. Уследио је указ посвећен информационој безбедности земље Заштита критичне инфраструктуре у информационом веку (*E. O. 13231 Critical Infrastructure Protection in the Information Age, act 18 2001*) на основу кога је основан Комитет за питања заштите критичне инфраструктуре чија је улога да координира све федералне програме у области информационе безбедности. Европске земље су усвојиле документ под називом Општи критеријуми (преведен у стандард ISO 15408: 1999-1-3) који третира критеријуме безбедности.[11]

Европске земље, у свом схватању појма информационе безбедности, са наглашенијим прагматичним приступом,[12] прате погледе САД.

Разматрање појма информационе безбедности (*информационноя безопасность*) у Руској федерацији је новијег датума.[13] Према неким ауторима [3] бивши СССР је изгубио хладни рат због занемаривања безбедности у информационој сфери друштва. Доктринарни ставови о информационој безбедности дати су у *Федералном закону о информацији, информатизацији и заштити информација* (усвојен 25. јануар 1995.), *Концепцији националне безбедности* (указ председника № 1300 из 1997. и редакција № 24 из 2000. године) и *Доктрини информационе безбедности* (указ председника № Пр-1895 од 9. јануара 2000. године). Информациона безбедност је дефинисана као ***стање заштићености*** *животно важних интереса личности, друштва и државе у информационој сфери од спољашњих и унутрашњих опасности (ризика).* Као полазно становиште при дефинисању појма узета је општа, интердисциплинарна наука о безбедности.

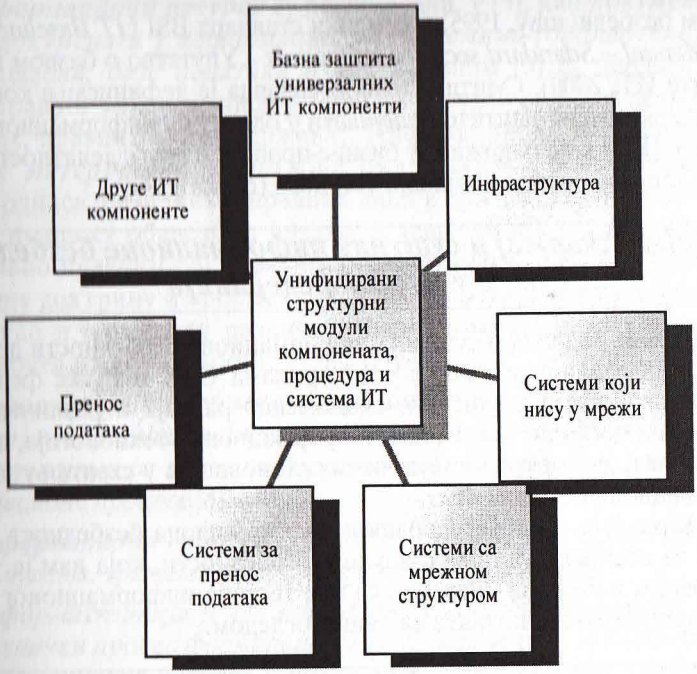
Најзначајнији напредак у области нормативног регулисања информационе безбедности остварен је доношењем међународног стандарда ISO/IEC 15408 (*Information technology – Secutity techniques – Evaluation criteria for IT security* – Општи критеријум оцене безбедности информационих система, 2000). ISO/IEC 15408 представља формални аспект обезбеђења информационе безбедности, тј. дефинише критеријуме које треба да задовољи информациона технологија, даје основу за дефинисање методологије пројектовања и оцене (атестирања) заштићених информационих технологија.

---

[11] "Норме управљања информационом безбедношћу" (*The code of practice for information security menagment*), 1993. и извештај фирме MORI "*Menagment control of information*", 1994. год., донешени у Великој Британији, су претходили "Општим критеријума".

[12] *ISO/IEC 17799 Information security management – Code of Practice Information Security Management, BS 7799 Code of Practice Information Security Management, German Information Security Agency: IT Baseline Protection Manuel – Standard security safeguards, 2000.*

[13] 1992 гоине Гостехкомисија, инсутуција при кабинету председника РФ, издала је серију брошура посвећених проблему заштите од неовлашћеног приступа.



Слика 1: Типични[14] *ИТ системи за које се организују стандарде мере заштите (организационе, кадровске, инфраструктурне и техничке) према немачком стандарду BSI*[15]

Данас су много актуелнији стандарди који више пажње посвећују практичном аспекту информационе безбедности као што су: ISO/IEC 13335 (*Information Technology – Guidelines for menagment of IT Security* – Упутство о управљању информационом безбедношћу, 1999), ISO/IEC 17799 (*Information Security Menagement – Code of ptactice for Information Security Management* – Правила управљања информационом безбедношћу, 2001), британски стандард BS7799 (*Code of Practice for Information Security Menagement* – Практична правила управљања информаци-

[14] Под „типичним" ИТ системима подразумевају се специфичне групе информационих технологија (ИТ) – активи (*assets*) који представљају типична, по распрострањености, решења и имају одлике врсте. „Типични" ИТ системи су вредност са становишта организације и представљају објекат заштите. Они обухватају опрему (физички ресурси), софтверски производ, сервисе и одговарајућу инфраструктуру (организацијску, кадровску, инжењерско-грађевинску, електронапајање и клима уређаје). Према ISO 12207 појам софтверски производ (*softvare product*) подразумева скуп рачунарских програма, процедура и придружене документације и података што одговара руским терминима информациони ресурси и софтвер.

[15] Скрипник, Бондаренко, Горбенко, Ткач, Потий, Методологические аспекты германского стандарта „Руководство по базовому уравню защиты информационных технологий", Харьковский национальный университет радиоэлектроники, УДК 681.3.06.519.248.681

оном безбедношћу, 1995) и немачки стандард BSI (*IT Baseline ProtectionManuel – Sdandard security safeguards* – Упутство о базном нивоу заштите ИТ, 2000). Суштина ових стандарда је дефинисање конкретног комплекса мера заштите (*safeguard*) у односу на информационе технологије (ИТ) које подржавају бизнис-процесе и друге делатности компанија, фирми, организација или установа (слика 1).

Појам, садржај и суштина информационе безбедности у Руској федерацији

Појам, садржај и суштина информационе безбедности дефинисани су на различите начине у доктринама САД и Руске федерације. Различит степен друштвено-економског развоја и различит степен развоја и примене савремених информационих технологија, довео до, на изглед, дијаметрално супротних становишта у схватању појма информационе безбедности.

Како је у Руској федерацији информациона безбедност дефинисана са становишта опште науке о безбедности, која нам је у својим основним начелима ипак ближа" од теорије информационог ратовања, прво ћемо се упознати са овим погледом.

Основни појмови и концептуални модел информационе безбедности

Информација је дефинисана као подаци о лицима, предметима, чињеницама, догађајима, појавама и процесима независно од форме њиховог представљања.[16]

Информације могу бити представљене у различитој форми и на различитим носиоцима (медијумима). Основне форме информација су: документа, акустичке (говорне) информације и телекомуникационе информације. Документа чине слике и алфа-нумерички знаци. Поред документа на папиру разликујемо и електронски документ. Говорне информације су, махом, садржане у акустичким сигналима (од 200...300 Hz до 4...6 KHz).[17] Носилац телекомуникационих информација су електрична струја и електромагнетни (ЕМ) таласи [4]. ***Информативни сигнали*** су, условно речено, електрични сигнали, акустичка, електромагнетна и друга физичка поља у чијим параметрима може бити садржана, преношена, чувана и обрађивана поверљива информација уз помоћ техничких средстава и система. У складу са носиоцем (медијумом), информације се деле на меке (акустичко и ЕМ поље) и тврде информације (папир, магнетни и оптички дискови, полупроводничке меморије).

[16] Федералъный закон об информации, информатизациии и защите информации, Дума, 25. 01. 1995.

[17] Иначе чујни опсег је од 20 Hz до 20 KHz.

Информациони ресурси су дефинисани, у [5], као *документа и масиви докумената у информационим системима (библиотеке, архиве, фондови, базе података и др).* Законом [6] су дефинисане основе правног режима (информациони ресурси су објекти односа физичких, правних лица и држава). Информациони ресурси представљају ***материјално добро*** које има власника и као такви су објекат односа физичких и правних лица и државе. Информациони ресурси подлежу обавезном чувању и заштити што је регулисано нормативно-правним документима. Нормативно-правна документа дефинишу доктрину информационе безбедности и заштите информација као и односе на различитим нивоима друштва у погледу надлежности и одговорности.

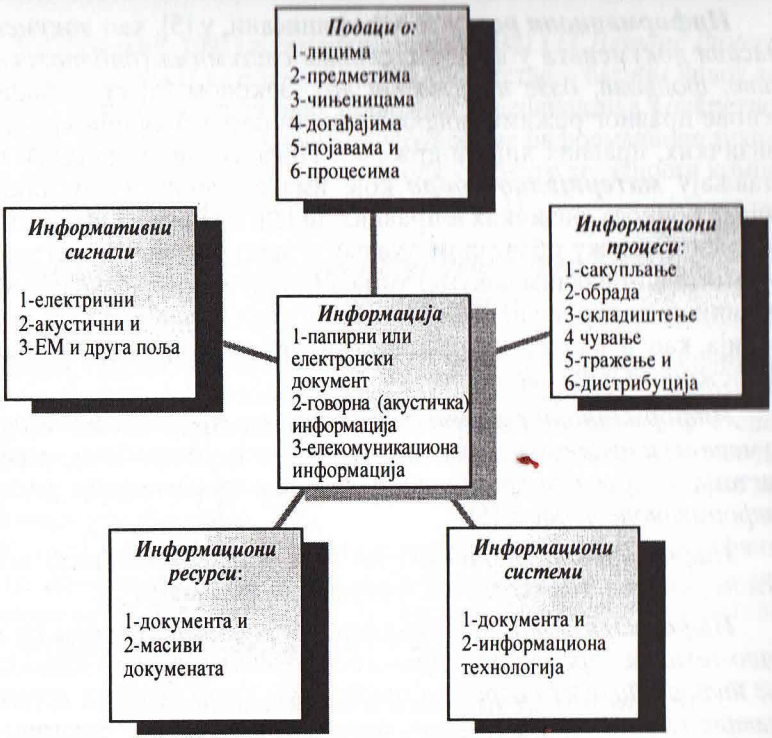
Информациони системи *су свеукупност докумената (масива докумената) и информационих технологија који, употребом средстава и система у којима се врши нека радња са информацијама, реализују информационе процесе* [5].

Информациони процеси *су процеси сакупљања, обраде, складиштење, чувања, тражења и дистрибуције информација* [5].

Информатизација *је организациони социјално-економски и научно-технички процес формирања оптималних услова за задовољавање информационих потреба и реализација права грађана, органа државних власти, органа локалне самоуправе на основу формирање и коришћења информационих ресурса, документирања информација (докумената) – фиксирања на материјалном носиоцу информација са реквизитима који омогућавају њихову идентификацију* [6].

Информациона безбедност је безбедност у информационој сфери – инфосфери. Физички инфосфера се састоји од три елемента: информационе инфраструктуре (уређаји за пренос и обраду информација), информација и њихових токова и персонала који обавља различите делатности. Информациона сфера је настала као последица настанка нове друштвено-економске формације друштва – информационог друштва.

Нова друштвено-економска формација друштва повлачи за собом и нове супротности и нове претње (опасности). Нове претње изискују нове приступе. Концепт „узајамне безбедности“ уступа место концепту „узајамне повезаности“. Поред појма нуклеарни кишобран, актуелан постаје и појам „информациони кишобран“. У домену информационе сфере, с једне стране, потребно је обезбедити друштво информационим ресурсима а, са друге стране, формирати систем заштите информационих потенцијала. Императив информационог друштва је информациона доминација у животно важним областима. ***Основни сукоб информационог друштва је сукоб у могућности приступа информацијама*** [7].



Слика 2: Појмови и њихов смисао У схватањима у Руској федерации-

Ако је безбедност одсуство претњи или могућност поуздане заштите од њих [8], онда је информациона безбедност одсуство информационих претњи, или стање заштићености, и стабилност основних сфера људских делатности у односу на могућа информациона дејства. У том контексту информациона безбедност је својство социјалног система позвана да гарантује такво стање информационих појава које обезбеђују човеку и друштву у целини информационе услове преживљавања и даљег стабилног развоја.[18] Информациона безбедност се распростире на све појаве инфосоциосфере чији елементи, директно или индиректно, раде на оптималној еволуцији друштвеног система обезбеђујући услове за безбедан развој а самим тим и прогрес.

[18] Међународна корпорација података и „Word times" разрадили су ***индекс информационог императива*** који показује способност појединих земаља да примају информације и користе се предностима информационе цивилизације. Земље су подељене у 4 групе: земље вишевековне заосталости које желе информатизацију, али наилазе на отпоре, земље које су кренуле путем прогреса, али се срећу са проблемима, земље у којима се ИТ интегрисала у економске структуре и доприноси укупном развоју и, на крају, земље у којима су ИТ интегрисане у економске и производне сфере и део су свакодневног живота сваког човека делујући као трансфер прогреса и напретка [8].

На тај начин информациона безбедност је **способност** државе, друштва, социјалних група и личности:

1. да **обезбеде** са одређеном вероватноћом довољне и заштићене информационе ресурсе и социјални интелект, оптималну социјалну ентропију и инфосферу за подршку животних делатности и животних способности, стабилног функционисања и развоја социума,

2. да се **супротставе** информационим претњама и нападима, негативним информационим деловањима на индивидуално и друштвено знање и психу људи као и на рачунарске мреже и друге техничке изворе информација,

3. да **формирају** личне и групне навике умећа безбедног понашања,

4. да **подрже** константну расположивост у односу на адекватне мере информационе противодбране,

5. да константно и, по одређеном програму безбедности, **омогуће** итеративно инкорпорирање вештачке интелигенције у социосредину.

У таквој интерпретацији информациона безбедност се јавља не само као један од облика безбедности, већ и **као пресек свих тих облика** у сфери деловања у којима информационе технологије заузимају важно место [8].[19]

Системски прилаз обезбеђења информационе безбедности у инфосфери обухвата три целине:

1. ***хуманитарну*** - повезану са развојем духовне сфере друштва и правима грађана у области информационих делатности (формирање и коришћење информационих ресурса),

2. област ***информатизације*** (формирање и развој јединственог информационог простора региона, земље и светског информационог поља) и

3. област ***подршке безбедности*** функционисања информационе инфраструктуре [8].

Системски прилаз у објашњењу суштине и садржаја појма информационе безбедности представљен је у концептуалном моделу (табела 1).

[19] Аутори рада су А. Д. Урсу (доктор филозофских наука, директор Научно-истраживачког института стабилног развоја и безбедности, председник Међународне академије Ноосфере (стабилног развоја), академик АН Молдавије и РАЕН) и Т.Ф. Цирдја (доктор филозофских наука, академик Међународне академије Ноосфере, академик Међународне академије Информатизације при УН, академик Украјинске академије наука, начелник катедре филозофија и биоетика на ГУМФ им Н. И. Тестимицану).

Табела 1

Концептуални модел информационе безбедности [8]

Информација	
Извори информација	људи, документа, публикације, средства масовних информација, технички носиоци (медијуми), техничка средства, производња, радни материјали
Претње (опасности)	интегритету, поверљивости, потпуности, поузданости приступа
Извори напада	противници, конкуренти, преступници, корупционери, структуре власти
Циљеви	упознавање, модификација, уништавање
Објекти напада	подаци о саставу, стању и делатностима
Начини приступа	на рачун разглашавања, на рачун отицања, на рачун неовлашћеног приступа
Правци заштите	правни, организациони, технички
Средства заштите	физичка, хардверска, софтверска, криптографска
Методе заштите	предупређење, одвраћање, пресецање, противдејства

Концептуалне ***основе*** информационе безбедности су, према мишљењу В. П. Салъникова,[20] садржане у следећим чињеницама: научно-технички прогрес неминовно води ка квалитетно новом ***стању човечанства*** – информационом друштву, последица савремених процеса је формирање ***информационих потреба*** становништва, данас је општеприхваћена теза да је ***информациона безбедност компонента националне безбедности*** чија улога, не само да расте сваког дана, већ избија у први план, ***стратегијски интерес безбедности*** државе и друштва је развој информационе сфере, али и њена заштита јер се кроз информациону сферу реализују претње безбедности у различитим сферама њеног испољавања, информације су данас, без преувеличавања, један од главних ***ресурса развоја*** и, на крају, глобализација процеса информатизације доводи и до ***нежељених социјално-правних последица*** (игнорисање правила размене и употребе информација, информационе пиратерије и информационог паразитизма), ***економских*** (индустријска шпијунажа), политичких и других последица.

Информациона безбедност се може посматрати и у контексту ***концепта узајамне повезаности*** као доминирајућег концепта безбедности информационог друштва [7]. Суштина концепта је прелазак од информационог ратовања ка управљивим сукобима и партнерству (*управляемая конфронтация и сотрудничество*).

Информационо ратовање, као посебан облик информационог супарништва не ограничава се само на дезорганизацију и блокирање механизама управљачких структура. Због природе информационог простора, информациона дејства носе у себи не само логички (подчињавање), већ и социотехнички (управљачки) карактер. Различити од-

[20] В.П.Салъников, доктор правних наука, члан акамемије наука РФ: „Концептуалъные основы обеспечений информационной безопасности российского государства".

носи логичког и социотехничког у информацији, мењају карактер информационе противодбране: од рата (који се води за постизање раније постављених циљева) до информационе игре. Победа у информационој игри је могућност да се дође до одлуке.

Структура информације се представља у виду квазилинеарног модела логичко-семантичких команди које су једнозначно повезане тако да сама информација, у односу на спољашња дејства, поседује познату и стабилну усмереност (значење). У информационој игри, низ комади и везе међу њима у просторно-временском домену су вишезначне и имају стохастички карактер који оставља могућност избора најбољег продужетка, односно доношења одлуке.

За прелазак од информационог ратовања ка управљивом сукобу и партнерству потребно је да ***информације буду свима доступне*** (да буду отворене)[21] јер се на тај начин повећава степен вишезначности и могућност предикције (прогнозе) информација на рачун информационе игре. Парадокс ситуације је чињеница да доступност информација подразумева сагласност и међусобно поверење међу друштвеним и политичким снагама које, без доступности информација, није могуће. Једно од решења је померање тежишта са противодбране на ***прикупљање и аналитичку обраду информација*** као средства предвиђања области системских сукоба. Као решење се јавља и интензивирање информационо-комуникативних дејстава међу субјектима.

На овим основама донесена је доктрина информационе безбедности Руске федерације.

Доктрина информационе безбедности Руске федерације

Под **информационом безбедношћу** Руске федерације подразумева се **стање заштићености** њених националних интереса у информационој сфери, која је дефинисана свеукупношћу избалансираних интереса личности, друштва и државе [9].

Интереси личности у информационој сфери се остварују кроз реализацију конституционих права човека и грађанина на приступ информацијама, коришћење информација у циљу реализације, законом дозвољених, активности, физичког, духовног и интелектуалног развоја, а такође кроз заштиту информација које обезбеђују личну безбедност [9].

[21] Информационо друштво је услов политичког и социјално-економског развоја сваке земље. Њега карактерише информациона отвореност са регулисаним информационим односима на бази информационог права. Ниво филизофске и правне осмишљености информационог друштва је резултат државне информационе политике. Основни циљеви државне информационе полите су информациона безбедност и информациона екологија (М. А. Вус; Ю. М. Нестеров, „Информационное общество. Информационное право. Информационная безопасность").

Интереси друштва у информационој сфери се остварују кроз обезбеђење интереса личности у тој сфери, увођење демократије, конституисање правне социјалне државе, достизање и одржавање опште сагласности у духовној обнови Русије [9].

Интереси државе у информационој сфери се остварују кроз стварање услова за хармоничан развој руске информационе инфраструктуре, кроз реализацију конституционих права и слобода човека и грађанина у области добијања информација и њихове употребе у циљу обезбеђења ненарушеног конституционог устројства, суверенитета и територијалне целовитости Русије, политичкој, економској и социјалној стабилности, у безусловном обезбеђењу законитости и правног поретка, развоја равноправне и узајамно толерантне међународне сарадње [9].

Компоненте националних интереса РФ у информационој сфери су:

– права и слободе грађанина,

– информационо обезбеђење државне политике,

– развој савремених информационих технологија и

– заштита информационих ресурса од неовлашћеног приступа, обезбеђење безбедности информационих и телекомуникационих система [9].

Интегрална безбедности – интегрална заштита информација

Концепција националне безбедности и доктрина информационе безбедности Руске федерације свију практичну реализацију добиле су у концепту интегралне безбедности, односно концепту интегралне заштите информација (*интегрална защита информации*).

Основни смисао појма **интегралне безбедности** се састоји у необходности обезбеђења таквог стања услова функционисања **човека, објеката и информација** у ком су они поуздано заштићени од свих реалних видова претњи у току непрекидног производног процеса и свих животних делатности [10]. Наиме, у свакодневном животу људи се сусрећемо са различитим врстама безбедности: од пожара, личној, финансијској, еколошкој итд. Наравно, оваква подела је условна. Ако посматрамо информације, јасно је да је њихова ефикасна заштита могућа само у том случају ако је безбедност, од свих врсти претњи, гарантована не само подацима, већ и уређајима у којима се они обрађују и чувају, као и лицима[22] који раде са тим

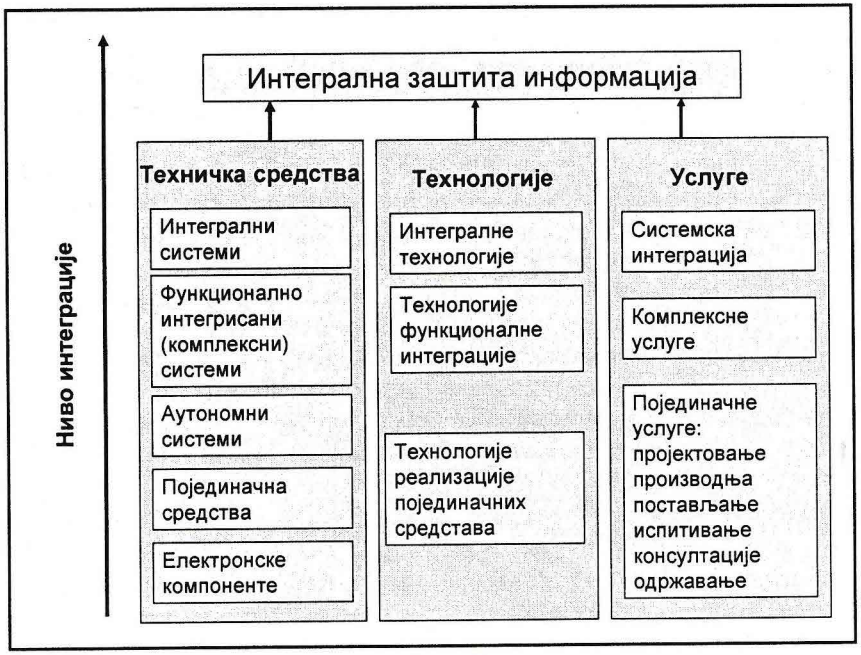
[22] Персонал је подложан различитим врстама информационо-психолошких деловања.

подацима [10]. Због тога се данас све чешће користи појам **интегрална заштита информација**.

Коначан **циљ** интегралне заштите информација је стварање таквих услова при којима је немогуће пресретање, фалсификовање и уништавање информација. Дејство овакве заштите мора бити непрекидно у времену и простору [10].

Један од основних захтева савремене заштите информација је ***системски прилаз***. ***Интегрални прилаз*** информационој безбедности подразумева отклањање свих могућих опасности укључујући и све канале отицања информација (њихово блокирање) користећи се савременим научним достигнућима и интеграционом технологијама (слика 3). Реализација таквог прилаза захтева обједињавање различитих подсистема безбедности у јединствен систем који садржи техничка средства (основна и помоћна), канале за комуникацију, програмску подршку, базе података и обучен персонал.

Предност наведеног концепта је чињеница да поред компјутерске безбедности обухвата и заштиту говорних и видео информација, што је актуелно у контексту индустријске шпијунаже и пословног извиђања. Недостатак је што превише инсистира на техничким аспектима заштите информација не потенцирајући довољно правне, организационе, социолошке и психолошке аспекте.



Слика 3: Интегрална заштита информација [10]

Појам, садржај и суштина информационе безбедности у САД

Појам информационе безбедности у САД, односно информационог обезбеђења изведен је и заснован на теорији информационог ратовања (IW – *information warfare*). Иако имплицитно није наведено, исходиште теорије информационог ратовања је општа наука о безбедности. Она је резултат специфичног угла гледања на проблем безбедности. Наиме, по аналогији са електромагнетним спектром који је домен у коме се одвија електронско ратовање (*electronic warfare*), амерички војни експерти, у настојању да дефинишу револуционарне промене у војним пословима, информациони спектар су назначили као домен у коме се одвија информационо ратовање.

Теорија IW подразумева информациону доминацију (концепт информационе превласти, односно информационе супериорности). Информациона супериорност се реализује кроз обавештајно-осматрачко-извиђачке операције, информациони менаџмент и информационе операције. Елеменат подршке информационих операција је информационо обезбеђење. Упознајмо се са основним појмовима из теорије информационог ратовања.

Природа информација и информационог окружења

Шта се подразумева под појмом „**информација**"? „**Информација**" је податак покупљен из окружења и обрађен у форми која се даље може искористити [12]. „Информација" је и садржај или значење поруке [11].

Суштина појма „информације" произилази из тзв. ***когнитивне хијерархије***. Наиме информација је, у великој мери, сама по себи без значаја. Једино када се подаци обраде, односно уврсте у ситуациони контекст, она добија своје значење и постаје, по дефиницији, информација. На основу информације у процесу сазнања (спознаје) настаје знање. Оно је информација која је испитана и прихваћена као чињеница.[23] Расуђивањем (мишљењем) знање прелази у разумевање (ситуације) чиме су испуњени услови за доношење правилних одлука (команданата, бизнисмена итд.) [12].

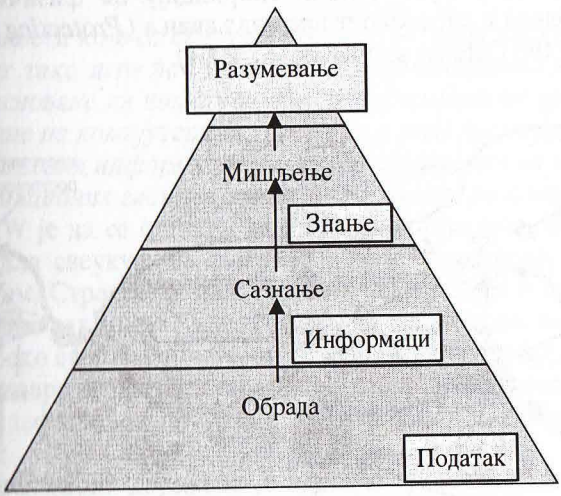
Разликујемо системе знања и системе убеђења (веровања). ***Системи знања*** су они системи који су организовани или вођени да осете или перципирају феноменалне (појавне) индикаторе који се могу верификовати, да преведу те индикаторе у разумљиве реалности које се користе за доношење одлука или директну активност. ***Системи убеђења*** су сви експлицитни и имплицитни емпиријски подаци у облику верификованих опажања и сви други подаци (кошмари, фобије,

[23] Информација постаје знање преко когнитивних активности – менталног процеса који прима и унапређује неверификоване информације – веровања, преко процене или тестирања да би се информација доказала и тако шта се информација прихвата као чињенична.

психозе, неурозе, колективна свест или подсвест итд,) који се не могу или их је тешко верификовати. Системи убеђења су, за разлику од система знања, изразито индивидуализовани и зависе од генетског наслеђа и културних традиција [14].

Релевантне информације су информације које су одабране из велике количине информација а које значајно утичу, доприносе или се односе на извршење дате оперативне мисије [12].

Критеријуми за процену квалитета информација су: *тачност* – информације које верно преносе (представљају) ситуацију, *релевантност* – информације које се односе на дату мисију, задатак или ситуацију, *благовременост* – информације које су на располагању када треба доносити одлуке, *целовитост* – све потребне информације које захтева лице које одлучује и *прецизност* – информације које у себи носе тражени ниво детаљности [12].[24]



Слика 4: Когнитивна хијерархија (ФМ 100–6)

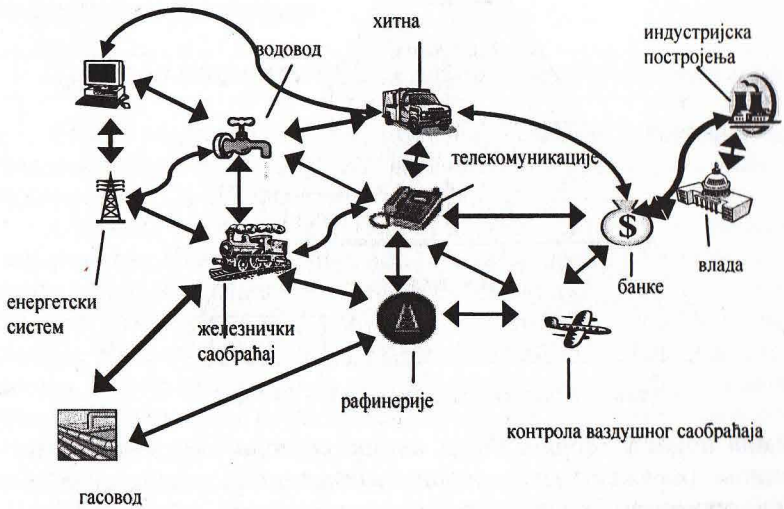
Важан појам у теорији IW је ***информационо окружење***.[25] Информационо окружење *(information environment)* је целина, скуп појединаца, организација или система за прикупљање, обраду или ди-

[24] Први приоритет је да информације морају бити тачне и релевантне. Други приоритет је да морају бити благовремене и у употребљивом облику. И на крају, оне треба да буду целовите и прецизне што је више могуће. У овим односима постоји и једно просто правило које гласи: и некомплетне и непрецизне информације су боље него никакве, неблаговремене и неупотребљиве информације не вреде ништа, а нетачне и нерелевантне информације су горе него никаве.

[25] Неки аутори, по аналогији са електромагнетним спектром, употребљавају термин информациони спектар алудирајући на чињеницу да постоји мноштво различитих и разноврсних информација везаних за дијаметрално супротне области. За разлику од електромагнетног спектра, информациони спектар нема своју физички засновану природу.

стрибуцију информација [12]. Употреба информација експоненцијално расте са развојем друштва. Савремено информационо окружење се манифестује кроз ***информациону инфраструктуру***. Разликујемо глобалну, националну и војну[26] информациону инфраструктуру (GII, NII, DII – *global, national, defense information infrastructure,* JP 3-13, 1998). На слици 5 је приказана NII са својим критичним местима.

МО САД и Одбрамбени научни борд (DSB – *defense science board)* имају визију да, у циљу стварања ефективне безбедоносне архитектуре, изградe ***интегрисану информациону инфраструктуру*** (III – *integrated information infrastructure*). Реч је о глобалној информационој мрежи GIG (*global information grid*) која треба да испуни захтеве информационог обезбеђења (IA): инфраструктура и апликације јавног кључа PKI и PKE, GIG IA тестирање, DID архитектура *(defence-in-depth* – одбрана у дубину), IP sec, IA функције, могућност менаџмента безбедношћу мрежа, линк енкрипцију на физичком нивоу отвореног модела и способност преживљавања (*Protecting the Homeland*, report of the Defense science board, 2001).



Слика 5: Национална информациона инфраструктура

[26] Основне претње информационог окружења су усмерене на један од три објекта: команданта или личност која одлучује, C^2 системе и информационе системе (ИС). Системи командовања и управљања (C^2 системи) су уређена целина персонала, информационог менаџмента, процедура, опреме и средстава (капацитета, постројења, инсталација) који су од пресудног значаја за извршавање операција (ФМ 6-0). Информациони системи су опрема и средстава (капацитета, постројења, инсталација) за прикупљање, обраду, складиштење, приказивање и дистрибуцију информација. Они укључују компјутере (хардвер и софтвер), комуникације али и политику и процедуре за њихову употребу (ФМ 3-0). C^2 системи обухватају информационе системе.

Извори ***претњи*** су: хакери, инсајдери, активисти противдржавних организација, терористи, инострани учесници информационих операција и информационе братоубице (нежељени ефекти на сопствене или пријатељске снаге) [13].

Методе напада су: неауторизовани приступ, злонамерни програми, електромагнетно обмањивање, електронски напад, физичка деструкција и менаџмент перцепцијом [13].

Информационо обезбеђење у концепту информационог ратовања

Начелно, IW је опсег акција које се предузимају са циљем да се оствари информациона супериорност над противником. У том смислу је и војна дефиниција, дата у CJCSI[27] 3210.01 [12], којом се IW дефинише као -

Активности које се предузимају да се оствари информациона супериорност тако што ће се утицати на противникове информације, процесе засноване на информацијама, информационе системе и мреже засноване на компјутерима, док ће се у исто време приступити одбрани сопствених информација, процеса заснованих на информацијама, информационих система и мрежа заснованих на компјутерима.

Циљ IW је да се оствари значајна информациона предност која би омогућила свеукупним снагама да брзо доминирају и управљају противником. Стратешки циљ IW јесте да се добије и одржи одлучујућа предност тако што ће се напасти противникови информациони системи преко експлоатисања, онемогућавања и утицаја, а у исто време ће се остварити заштита савезничких информационих система.

Радна дефиниција IW према Универзитету националне одбране (NDU)[28] је:

Информационо ратовање је приступ оружаном конфликту који се усмерава на менаџмент и користи информације у свим облицима и на свим нивоима да би се остварила одлучујућа војна предност, посебно у интервидовском и комбинованом окружењу. IW је по природи и офанзивно и дефанзивно и креће се од мера којима се противник спречава да експлоатише информације до одговарајућих мера којима се обезбеђује интегритет, расположивост и интероперабилност пријатељских информационих ресурса. IW, мада је у крајњем случају војно по својој природи, води се и у политичкој, економској и друштвеној сфери и применљиво је преко читавог скупа области националне безбедности од мира до рата и од главе до пете.

[27] *Chaiman of the Joint Cheif of Staff* – председавајући здруженог генералштаба

[28] *National Defense University* је највиша војно-политичка школа САД и њени слушаоци су, поред официра и високих службеника администрације САД, и официри других земаља. Слушаоци се примају по позиву, често и по имену.

Информационо ратовање је могуће дефинисати и као облик конфликта[29] којим се директно нападају информациони системи а тиме и системи знања и убеђења противника [14].

Конкретнија и опипљивија је дефиниција IW Мартина Либицког[30] по коме:

1. Информационо ратовање, као посебна техника вођења рата, не постоји. Постоји неколико различитих облика информационог ратовања[31]: **(1) Ратовање у сфери командовања и управљања** C^2W[32] (које је намењено за ударе против „главе и врата" противника); **(2) Обавештајно ратовање** IBW[33] (које је усмерено на директну употребу обавештајне делатности за нишањење на циљеве и процену борбених дејстава, реализацију концепта „стрелац-циљ"); **(3) Електронско ратовање** EW[34] (радио-електронске и криптографске технике); **(4) Психолошко ратовање** PSYW[35] (у коме се информација користи да промени свест човека); **(5) „Хакерско" ратовање** (у коме се нападају рачунарски системи); **(6) Економско-информационо ратовање** EIW[36] (блокирање или усмеравање информација да би се обезбедила економска доминација); **(7) „Кибер" ратовање** (скуп футуристичких сценарија). Сви ови облици су слабо повезани.

3. Информација није, сама по себи, медијум ратовања, сем у ужем смислу речи (нпр. електронско ометање). Информациона надмоћ можда има смисла, али информациона превласт (где једна страна може да задржи другу страну да приступи бојишту) има исто толико смисла као нпр. логистичка превласт [15].

Крајњи циљ информационог ратовања је **информациона супериорност** (IS – information superiority). Информациона супериорност је дефинисана као **оперативна предност** добијена из могућности прикупљања, обраде и дистрибуције непрекидног тока информација при експлоатисању или онемогућавање противника да има те исте могућности (ФМ 3–0).

Информациона супериорност се постиже кроз (слика 6, ФМ 3–0):

1. Информациони менаџмент (IM – *information menagament*)

2. Обавештајну делатност, осматрање и извиђање (ISR – *intelligence, surveillance and reconnaissance*) и

3. Информационе операције (IO – *information operations*)

---

[29] Конфликт, ратовање је скуп свих борбених и неборбених активности које се предузимају да би се потчинила супротстављена воља противника или опонента.

[30] Мартин Либицки је старији сарадник на Институту за националне стратегијске студије (САД) специјалиста за примену информационих технологија за националну безбедност.

[31] Информационо ратовање су конфликти који укључују заштиту, манипулисање и деградацију информација и спречавање приступа информацијама.

[32] C^2W (*comand and control warfare*) – рат против командовања и управљања.

[33] IBW (*intelligence- based warfare*) – обавештајно ратовање.

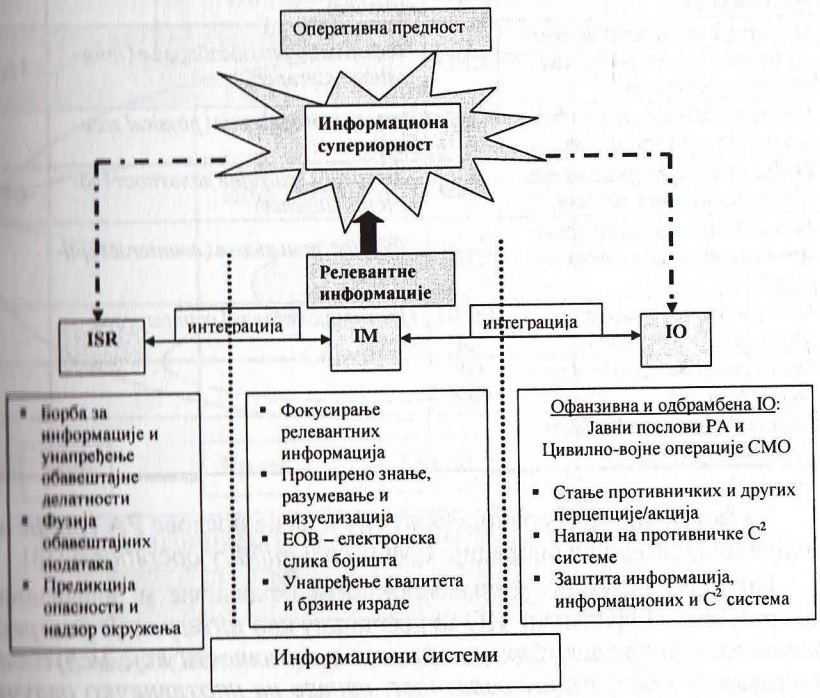
[34] EW (*electronic warfare*) – електронско ратовање.

[35] PSYW (*psychological warfare*) – психолошко ратовање.

[36] EIW (*economic information warfare*) – економско информационо ратовање.

Основа информационе супериорности је обавештајна делатност, осматрање и извиђање (ISR). У складу са тим америчка војна доктрина дефинише и тзв. ISR операције.

Појам ***информационих операција*** (IO – *information operations*) је претрпео знатне промене у периоду од првобитног дефинисања (ФМ 100–5, ФМ 100–6, 1996) до најновијих схватања (ФМ 3–13, 2003). Промену су, пре свега, у садржају, односно компонентама и могућностима које чине IO. Друга суштинска промене је у чињеници да су елементи IO уједно и елементи борбених снага (*combat power*).



Слика 6: Информациона супериорност

Суштина IO је дата у Здруженој доктрини информационих операција (Join Pub 3–13, Joint Doctrine for Information Operations, 1998): информациона операција укључује активности које утичу на противничке информације и информационе системе при чему су једино заштићене сопствене информације и информациони системи.

IO имају једну од најважнијих улога у одбрамбеној доктрини. Тако нпр. Air Force Doctrine Document 2–5 (*Information operations*) каже да је *доминација у информационом спектру* ***данас толико суштински важна****, као превласт у ваздуху и свемиру или заузимање територије у прошлости,* ***да је виђена као неопходна и синергична компонента ваздушно-свемирске моћи*** (AFDD 2–5, 1998:5).

Елементе ІО се чине: језгро (*core*) могућности и могућности које подржавају – епизодне. Преглед елемената ІО дат је у табела 2 (ФМ 3–13, 2003).

Табела 2

Елементи (компоненте) информационих операција

Језгро		*Који подржава*	
Назив	Акроним	Назив	Акроним
Електронско ратовање (electronic warfare)	EW	*Физичко уништавање (physical destruction)*	
Операције засноване на компјутерској мрежи (computer network operations)	CNO	*Информационо обезбеђење (information assurance)*	IA
Напад на компјутерску мрежу (computer network attack)	CNA	*Физичка безбедност (physical security)*	
Одбрана компјутерске мреже (computer network defense)	CND	*Контраобавештајна делатност (counterintelligence)*	CI
Експлоатација компјутерске мреже (computer nerwork exploatation)	CNE	*Противобмањивање (counterdeception)*	
Психолошке операције (psychological operations)	PSYH OP	*Противпропаганда (counterpropaganda)*	
Оперативна безбедност (operations security)	OP-SEC		
Војно обмањивање (military deception)			

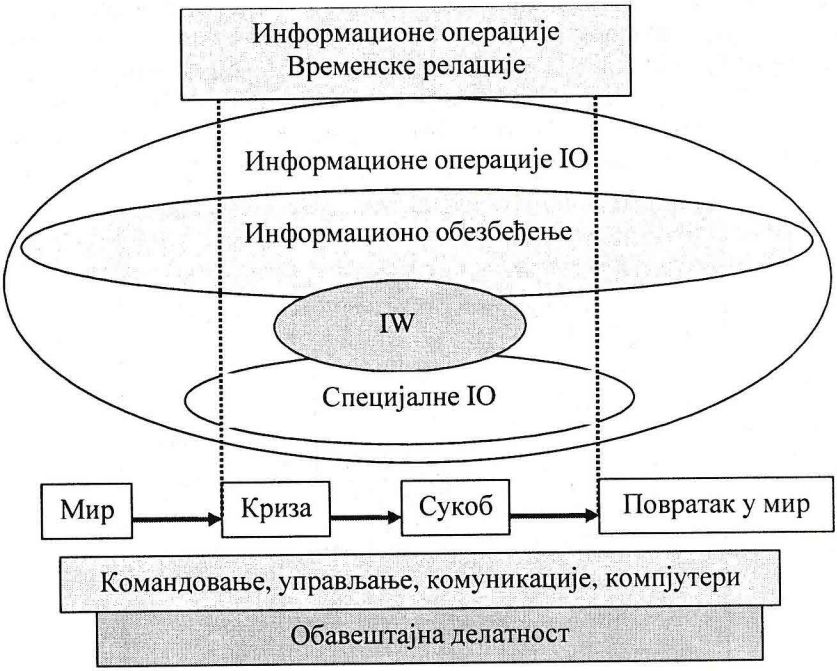
Информационе операције укључују и јавне послове PA (*public affairs*) и цивилно-војне операције CMO (*civil-military operations*) [13].

Информационе операције могу бити офанзивне и дефанзивне (одбрамбене). Офанзивне ИО се дефинишу као *интеграција употребе основних и подржавајућих могућности и активности које међусобно* ***подржавају*** *обавештајну делатност, нападе на противничко одлучивање или утичу и потпомажу друге специфичне циљеве* (ФМ 3–0). Информационе предности офанзивних ІО су: уништавање *(destroy),* прекидање *(disrupt),* деградација *(degrade),* одбијање *(deny),* обмањивање *(deceive),* експлоатисање *(exploit)* и утицање *(influence)* [13].

Одбрамбене ІО (DIO – defence IO) се дефинишу као интеграција и координација политика и процедура, операција, персонала и технологије у **заштити** и **одбрани** пријатељских информација и информационих система. DIO обезбеђују благовременост, тачност и релевантност информација. Одбрамбени елементи DIO су: заштита (protection), детекција (detection), рестаурација (restoration) и реакција (response). Одбрамбене ІО користе техничке и нетехничке активности у циљу ограничавања рањивости пријатељских C^2 система у непријатељским ІО [13].

Заједничка доктрина ІО дефинише информационо обезбеђење (ІА) на следећи начин:

*Информационо обезбеђење је дефинисано као ІО за **заштиту и одбрану** информационих система стварајући услове за њихову расположивост, интегритет, аутентичност, поверљивост и непорицљивост. Ово подразумева рестаурацију информационих система инкорпорираним могућностима заштите, детекције и реакције* (ЈР 3–13, 1998:1–9).



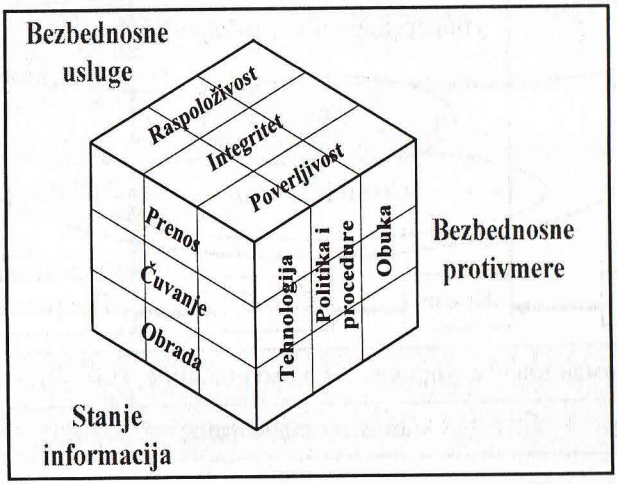
Слика 7: Спектар информационих операција (ЈР 3–13,1998,1–4)

Термини расположивост, интегритет, аутентичност, поверљивост и непорицивост изражавају циљеве ІА и дефинисани су, респективно, као осигуран приступ ауторизованог корисника, заштита од неауторизованих промена, верификација оригиналности, заштита од неауторизованог обелодањивања и неоспоран доказ о учешћу извршеним операцијама (трансакцијама).

Информационо обезбеђење је специфична подкатегорија информационих операција која покрива њену одбрамбену област. На слици 7, преузетој из ЈР 3–13, је илустрована улога ІА у спектру ІО. Слика приказује ІА као континуалан процес који покрива цео опсег ІО од мира, преко главног сукоба до повратка у мирно стање. Истакнут значај информационом обезбеђењу је дат и у Заједничкој визији 2020.

Модели информационог обезбеђења су апроксимативни оквиру који квалитативно и квантитативно, на очигледан начин, представљају проблематику информационе безбедности. За разлику од начелног концептуалног модела информационе безбедности у Руској федерацији, САД су детаљно разрадиле и квалитативне и квантитативне моделе. У тексту који следи упознаћемо се са моделом информационе безбедности (McCumber INFOSEC модел), са квалитативним моделом информационог обезбеђење (модел IA) и са квантитативним моделом информационог обезбеђења (модел Џозефа Богарда).

Модел информационе безбедности (McCumber INFOSEC модел, слика 8) је први пут публикован 1991. године. Реч је о моделу заснованом на интегралном прилазу [11].



Слика 8: Оригинални McCumber модел [11]

Историјски посматрано, информациона безбедност је дефинисана као:[37]

Заштита информационих система против неауторизованог приступа или модификација информација било у складиштењу, обради или преносу и против **лишавања** услуга ауторизованих корисника, укључујући неопходне мере детекције, документовања и отклањања таквих претњи [16].

У складу са наведеном дефиницијом, модел информационе безбедности има три димензије: стања у којима се налазе информације (пренос, чување и обрада), безбедносне услуге (расположивост, интегритет и по-

[37] Реч је о минимуму стандарда и захтева прописаних од стране Комитета за националну безбедност телекомуникацијских и информационих система (NSTISSC).

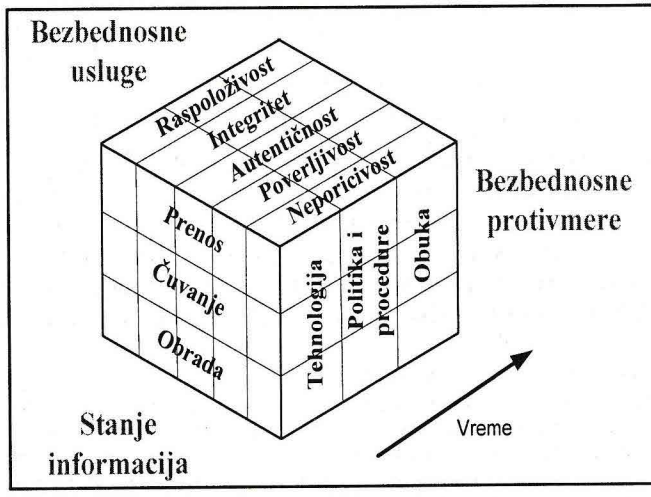
верљивост) и безбедносне противмере (технологија, политика и процедуре и обука) [11]. Модел је тродимензионалан. Дати модел је, у складу са развојем теорије IW и насталим потребама да се обухвате и одбрамбене активности дефинисане дефанзивним информационим операцијама, еволуирао у модел информационог обезбеђења (модел IA).

Информационо обезбеђење IA је, према NSTISSC,[38] дефинисано као:

Информационе операције заштите и одбране информација и информационих система обезбеђујући њихову расположивост, интегритет, аутентичност, поверљивост и непорицљивост. Ово подразумева ***рестаурацију*** информационих система инкорпорираним могућностима заштите, детекције и реакције [11].

Наведена дефиниција је истоветна са дефиницијом датом у Заједничкој доктрини IO (ЈП 3–13, 1998:1–9) и у Правилу КоВ-а ФМ 3–13, 2003. Информационо обезбеђење је дефинисано као информационе операције са скупом свих одбрамбених и проактивних компоненти што њихову разлику чини суштинском, а не само семантичком. Информационо обезбеђење обухвата улогу информационе безбедности [11].

Модел IA представља нови, мултидисциплинарни и мултидимензионални поглед на важне елементе McCumber-ов модела. Формално посматрано, само су безбедносни сервиси проширени са аутентичношћу и непорицивошћу. Међутим, промене су суштинске. Модел је четвородимензионалан и обухвата: стање информација, безбедносне сервисе (услуге), безбедносне противмере и време (слика 9). Помоћу оваквог модела могу су представити сви одбрамбени елементи одбрамбених IO (DIO).

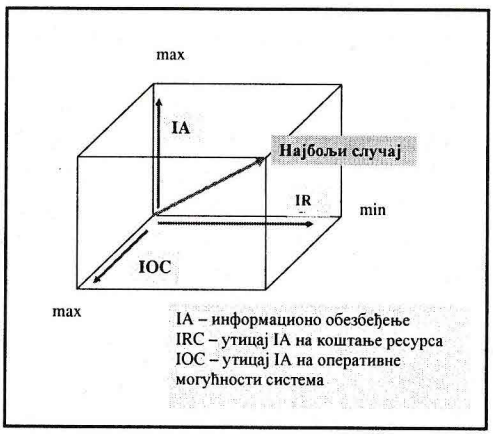


Слика 9: Модел информационог обезбеђења (модел ИА)

[38] NSTISSC – *National Security Telecommunications and Information Systems security Committee.*

За разлику од конвенционалног модела он обухвата и мере заштите система (детекција, реакција) као и резидентне информације у таквом систему (рестаурација). Синоним ових особина информационих система је ***способност преживљавања***. Отпорност на нападе („жилавост") информационих система се у литератури разматрала и раније као способност опстанка, преживљавања (*survivability*). Способност преживљавања је дефинисана као ***способност*** *система да извршава мисије на погодан начин упркос нападима, отказима или непредвиђеним догађајима* [17]. Кључна особина способности преживљавања мрежних система[39] је њихова способност да одрже основне сервисе (одређене нивое интегритета, поверљивости, перформанси и других квалитативних својстава) током напада, пада система или несреће.

Важна димензија овако постављеног модела је време. Поред анализе ризика, временска димензија омогућава и праћење стања модела у времену [11].



Слика 10: Релације између IA, IOC и IRC [18]

Квантитативни модел Џозефа Богарда (Josef Beauregard) заснован је на методологији фокусираног вредоносног мишљења (VFT – *value focused thinking*)[40] и моделу IAAM (*information assurance anylisismodel*)[41]. Модел IAAM омогућава тродимензионално разматрање проблема информационог обезбеђења. Свака од димензија (величина модела IAAM) представљена је вредоносном хијерархијом. Елементи

[39] Мрежни системи су рачунарске мреже. Карактеристика савремених мрежних система је да су организоване као необавезне мреже које повезују различите кориснике. Савремени мрежни системи повећавају ефикасност и ефективност организације применом нових нивоа организације. Такве интеграције су праћене повишеним нивом ризика од упада у систем и компромитовања. Рачунарске мреже су постале критичан елеменат модерног друштва.

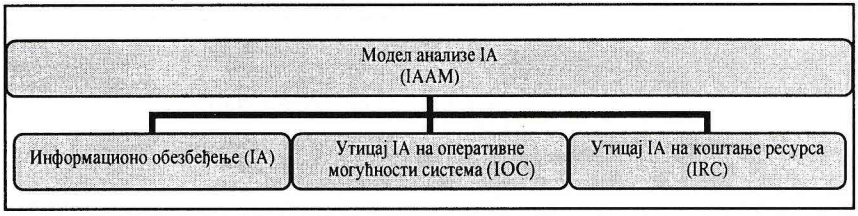
[40] Према речима R. Keeney, пионира VFT, формулисање правих вредности је основа одлучивања.

[41] Овај модел је резултат истраживачког рада на институту технологије РВ САД у Air Force Tecnichal Center (AFTC).

вредоносних хијерархија имају своје квантитативне мере. Прерачунавања, за конкретне стратегије IA, вредоносних хијерархија и њихових квантитативних величина врше се помоћу посебно пројектованог информационог система AMIS (*AFTC Mission information system*) [18].

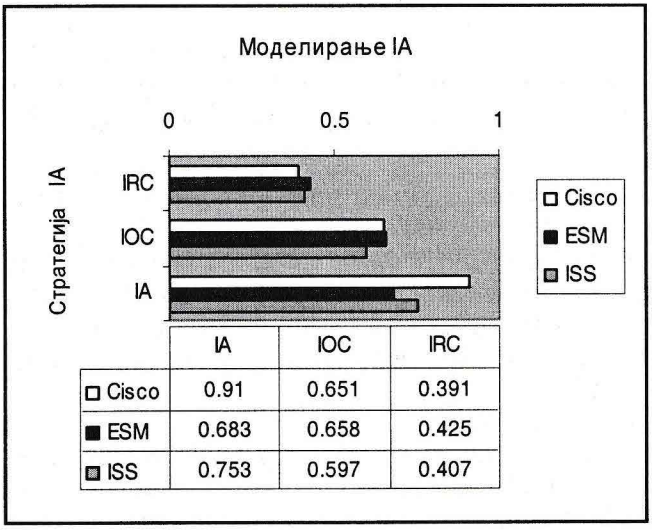
Најбоља стратегија IA настоји да повећа информационо обезбеђење IA и оперативне могућности система IOC (*IA on system operational capability*), а да, при томе, трошкови ресурса IRC (*IA on resource cost*) буду минимални (слика 10).

У модел IAAM (слика 11) је имплементирана стратегија IA јер он обухвата сва три фактора који, сваки за себе, имају своје вредоносне хијерархијске скале.



Слика 11: Модел анализе информационог обезбеђења (IAAM) [18]

При избору стратегије IA врши се прорачун за три случаја: најбољи, вероватни и најгори. Као референтна величина служи основни (базни) систем. Решење квалитета стратегије IA (система) се добија у виду нормираног броја на основу чега се врши класификација. Поред укупног решења, могуће су анализе осетљивости појединих вредоносних категорија.

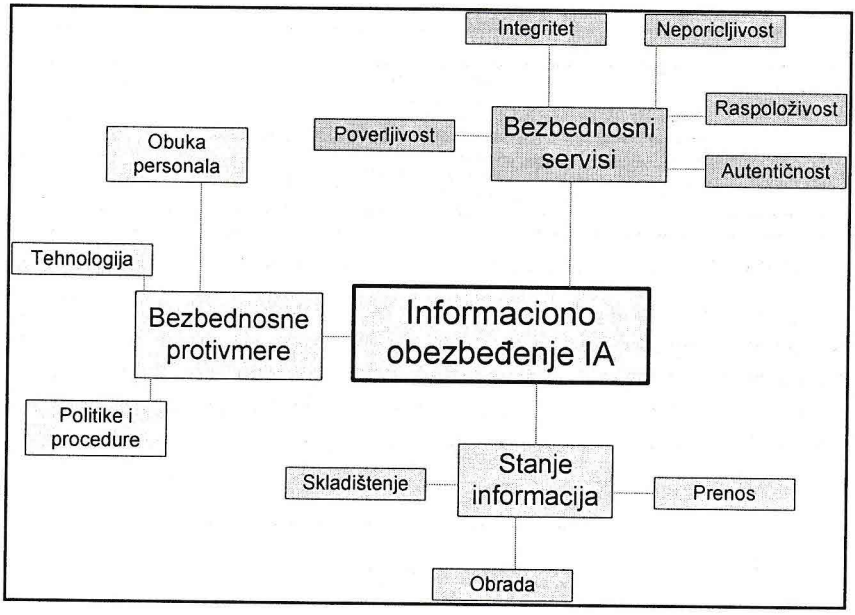


	IA	IOC	IRC
Cisco	0.91	0.651	0.391
ESM	0.683	0.658	0.425
ISS	0.753	0.597	0.407

Слика 12: Резултат моделирања ИА (преузето из [18])

У својству примера и илустрације предложеног метода моделирања ІА, преузет је један од многобројних резултата из [18]. Дијаграм на слици 12 показује квантитативне резултате моделирања на основу којих је могуће извршити избор стратегије ІА.

У складу са моделом информационог обезбеђења. Ејб Ашер (Abe Usher) је предложио класификацију информационог обезбеђења. Као полазна основа су му послужила три аспекта: стање информација, безбедносни сервиси (услуге) и безбедносне противмере (слика 13, [19]). Детаљна разрада поменуте класификације није од суштинског значаја за предмет овог рада те се на њој нећемо задржавати.



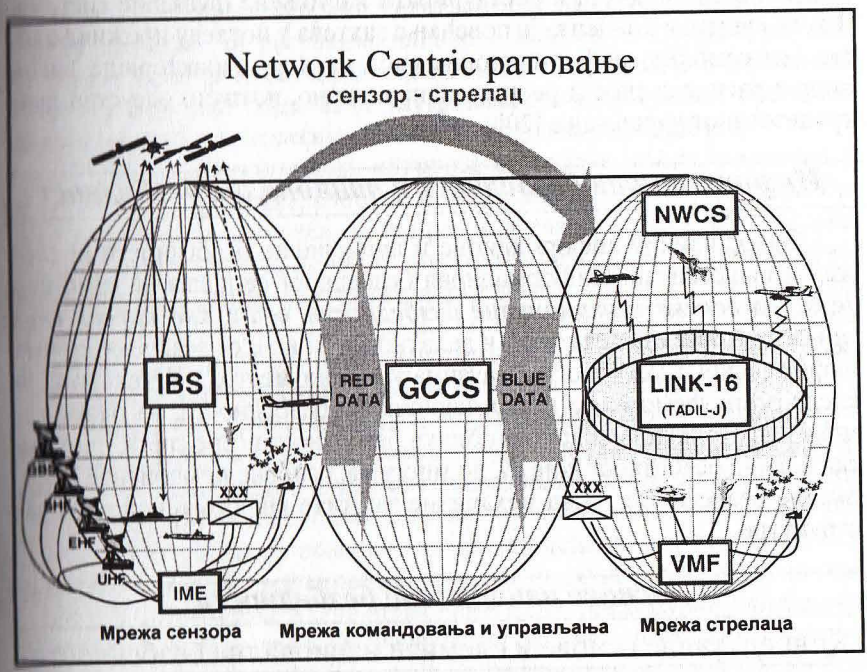
Слика 13: Највиши ниво поделе информационог обезбеђења ІА [19]

Network-centric парадигма информационе безбедности

Са сваким новим достигнућем у области информационих технологија јављају се ***нови аспекти информационе безбедности***. При томе, уз већ постојећа решења, јављају се нове гране које треба посматрати у неком другом контексту и, самим тим, под потпуно новим углом посматрања.

Информациони, телекомуникациони, рачунарски и кадровски ресурси су организовани по принципу информационих матрица које омогућавају флексибилну, безбедну и централизовану расподелу ресурса при формирању тзв. виртуелних организација насталих за решавање проблема у сложеним динамичким околностима.

Један од примера виртуелних организација је ***Глобална информациона мрежа***[42] (GIG – *global information grid*) настала за потребе Пентагона која треба да омогући управљање мобилним и компактним борбеним саставима. Високе маневарске и ватрене могућности борбених састава обједињавају се са ефикасном, флексибилном, безбедном и оперативном расподелом информационих ресурса (слика 14) у реализацији концепта сензор – стрелац [20]. Другим речима, ма која борбена платформа – тенк, авион, сателит или брод – у зависности услова и конкретног задатка у матрици може се појавити и као средство уништавања и као канал везе и као елеменат система планирања и доношења одлуке. Коначан циљ датог пројекта је интегрисање у „матрицу", у својству ватреног, извиђачког, информационог или командног елемента, сваког борбеног система без обзира ком формацијском саставу, роду или виду оружаних снага припада.



Слика 14: Глобална информациона мрежа и network centric ратовање

Као пример виртуелних организација, може послужити и „***виртуелна аналитичка средина***" формирана за потребе обавештајно-извиђачке заједница САД. Помоћу ње се, на основу неструктуираних и нехомогених информација (текст, графика, слике, виде, звук) из различитих извора (агентурних, радиотехничких, оптичких, електронских

[42] Глобална информациона мрежа је планирана концептом развоја ОС САД до 2020. Почетак њеног рада је планиран за 2005. годину.

и др.), формирају нова знања о ситуацији, изводе се упоредне анализе са сличним ситуацијама у прошлости, извлаче се логички закључци, обезбеђује се тимски рад свих заинтересованих институција без обзира на њихову лоцираност [20].

Класичан модел информационе безбедности заснован на аутономности и локалности ресурса информационих система, у оваквим околности, апсолутно не задовољава. Решење је ешелонирани, ***вишеслојни систем информационе безбедности*** настао као резултата напора Пентагона и Агенције за националну безбедност САД а прокламован у стандарду ISO/IEC 15408. Концепт ешелонираног вишеслојног система информационе безбедности обухвата скуп компонената који реализују функције мониторинга, заштите и адаптације информационих ресурса. На овај начин могуће је спречити продор нападача, детектовати напад, локализовати објекат дејства, неутралисати и елиминисати нападача и рестаурирати изгубљене функције система. Значи, суштина концепта је повећање захтева у погледу преживљивости (*survivability*) информационих система које карактерише висок степен расподељености ресурса и, практично, потпуно одсуство централизованог управљања [20].

Информациона безбедност и национална безбедност

Однос између информационе и националне безбедности је сложен и вишезначан. Информациона безбедност се јавља не само као ***један од аспеката националне безбедности***, већ и ***као пресек свих других облика безбедности*** (и делатности за које су везане) у којима информационе технологије заузимају важно место.[43] У тексту који следи осврнућемо се на појам националне безбедности, на однос између информационе и других облика безбедности (пре свега, економске и војне безбедност које су, по многима, основне компоненте националне безбедности) и на механизме заштите информационе инфраструктуре.

Основе националне безбедности

Концептуалне основе и елемнти националне безбедности Руске федерације

Национална безбедност је основа стабилног постојања и прогресивног развоја државе у светској заједници. Она представља стање заштићености животно важних интереса личности, друштва и државе (националних интереса) од спољашњих и унутрашњих претњи [27].

[43] Информационо ратовање, како наводи дефиниција Универзитета националне безбедности САД, *применљиво је преко читавог скупа области националне безбедности од мира до рата и од главе до пете.*

Национална безбедност је оличена у ***систему националне безбедности*** који чине објекти безбедности, субјекти који обезбеђују безбедност и механизам обезбеђења безбедности у складу са којим се реализују практичне акције. Основни ***објекти*** безбедности су: личност – њена права и слободе, друштво – његове материјалне и духовне вредности и држава – њено конституционално уређење, суверенитет и територијална целовитост. ***Субјекти*** обезбеђења безбедности су организације, државни институти, службе и самосталне личности. ***Механизам*** обезбеђења безбедности дефинише динамичку шему обезбеђења националне безбедности кроз скуп мера, акција и поступака [28].

Систем националне безбедности је свеукупност објеката безбедности са избалансираним животно важним интересима, субјеката обезбеђења безбедности са њиховим функцијама, правима, одговорностима, обавезама, облашћу компетентности, средствима обезбеђења безбедности у различитим сферама делатности и односима између њих, у складу са којима се регулише, планира, организује, координира, синхронизује и контролише сврсиходна делатност постизања и одржавања стања безбедности адекватна **унутрашњим** и **спољашњим** претњама животно важним интересима личности, друштва и државе [28].

У основи ***националних интереса*** се налази човек, породица и друштво, њихова права, слободе и гаранција несметаног развоја. Важни национални интереси су: напредак и развој човека, побољшавање квалитета живота, лична и друштвена безбедност, очување суверенитета, територијалног интегритета земље и њеног државног уређења, јединство економског тржишта и економски раст и гарантована државна слобода демократског развоја друштва, очување грађанског мира, друштвеног порекла и националне сагласности [28].

Постизање националне безбедности је повезано са значајним материјалним издацима и у условима ограничених ресурса неопходно је оптимално ***управљање системом националне безбедности.*** Механизми управљања безбедношћу почивају на научно заснованим методама којима се решавају основни задаци: процена постојећег нивоа безбедности (ризика), дефинисање оптималног скупа мера за снижавање ризика и дефинисање плана провођења мера. ***Механизми управљања безбедношћу*** представљају свеукупност законодавних аката, правних норми, мотива и стимуланса, мера и других активности у сфери безбедности који омогућавају ефикасно функционисање и коришћење органа, снага, средстава и метода помоћу којих се реализују практична дејства у постизању циљева безбедности [28].

Системски прилаз решавању проблема националне безбедности подразумева дефинисање концепције, стратегије и политике националне безбедности. ***Концепција националне безбедности*** је систем погледа на реализацију националне безбедности. ***Стратегија националне безбедности*** изражава принципијелне елементе унутрашње, војне и спољне политике интегришући напоре на очувању национал-

них интереса. ***Политика националне безбедности*** има за циљ стварање и подршку политичког, економског, војно-стратегијског и међународног положаја положаја земље који омогућава повољне услове за реализацију националних интереса [28].

Приоритети националне безбедности нису стални и могу да претрпе значајне промене у зависности од конкретне ситуације, карактера и степена угрожености. Компоненте националне безбедности су: економска безбедност, безбедност у политичкој и социјалној сфери, војна безбедност, информациона безбедност, информационо-психолошка безбедност, морално-психолошка безбедност, еколошка безбедност, демографска безбедност и научно-техничка безбедност [28].

Посебну улогу у националној безбедности игра ***економски фактор*** који је не само један од компонената националне безбедности, већ и основа свих других компонената. Економска безбедност је материјална основа националне безбедности. ***Војна безбедност*** је стање заштићености од војних претњи. Предмет њеног интереса је одбрамбени потенцијал друштва и државе. Носилац су оружане снаге (ОС) а механизам њиховог деловања – оружана борба (ОБ). Физиономију ОБ изменила је појава оружја високе прецизности (ОВП) и нове војне концепције - добијања рата без наступања и непосредног додира са противником („бесконтактно ратовање“). Важан садржај савремених ратова је информациона противодбрана (*информационное противоборство*)[44] [28].

Терористички удари 11. септембра 2001. год. по објектима САД поставили су темеље тзв. ***асиметричном ратовању*** које се не води класичним оружаним снагама и оружјем како је то традиционално дефинисано. Асиметрично ратовање створио је савремени међународни тероризам.[45] Један од задатака националне безбедности је заштита државне територије и становништва од невојних форми и метода терористичких дејстава различитих размера – ***борба са тероризмом*** [28].

Информациона безбедност, схваћена у најширем значењу речи[46], не само да добија на значају, већ избија у први план. Као таква

[44] У склопу информационе противодбране у [3] се посебно инсистира на ***информационо-психолошком аспекту*** националне безбедности који треба да обезбеди информационо-психолошку средину, информационе ресурсе (духовне, културне, историјске и националне вредности), систем формирања сазнања (погледа на свет, политичких погледа и духовних вредности), систем јавног мњења, систем доношења политичких одлука и психу и понашање људи.

[45] Карактеристике асиметричног ратовања су: наношење концентрисаних (у времену и по месту) невојних удара са постизањем изненадног, неочекиваног, ошамућујућег ефекта, одсуство класичне линије фронта, скривеност политичких циљева и примена нових неочекиваних средстава и форми насиља [28].

[46] Информациона безбедност је, у претходним главама текста, дефинисана као безбедност информационих система и заштита информација, а не као безбедност иманентна информационом друштву.

она је ***неодвојиви део националне безбедности***. Чак пре, информациона безбедност, у све већој мери, поприма и међународни карактер јер целовитост савременог света, као друштва, заснована је на интензивној размени информација. Елементи информационе безбедности, у контексту националне безбедности, су: информационо право као правна основа информационог друштва, информациони аспект управљања војним снагама и оружјем, информационо ратовање и информациона противодбрана, електронско ратовање као борба за доминацију у електромагнетном спектру, информациона безбедност информационих система и заштита информација, заштита државне тајне, извиђање и служба извиђања, информационо-психолошка противодбрана и психолошко ратовање, информационо-психолошка безбедност и морално-психолошко обезбеђење становништва, ОС и других војних организација [28].

Званични погледи Руске федерације на националну безбедност изложени су у ***Концепцији националне безбедности*** (2000. год.).

Национална безбедност САД

У схватању појма националне безбедности САД полазе од становишта да поред претњи споља (друга или друге државе), постоје и унутрашње претња (тероризам, елементарне непогоде, нарушавање људских права итд.) које су, по много чему, и веће од спољашњих. У складу са тим поред ***Стратегије националне безбедности*** (*National Security Strategy,* 2002) постоји и ***Национална стратегија унутрашње безбедности*** (*National Strategy for Homeland security*, 2002). Чињеница да као основна претња САД фигурише тероризам, не умањује значај суштински нове идеје да унутрашња безбедност има објективно много већи значај и да се ***национална безбедност третира на нови начин***.

За разлику од Руске федерације у којој је заступљен, истина иновиран али ипак, на традиционалан начин изложен проблем националне безбедности, САД (са становишта неоспорног светског лидера који, осим елементарних непогода, има само један реалан проблем – међународни тероризам) проблему националне безбедности приступају из једног другог угла гледања – са становишта заштите своје инфраструктуре.[47]

Још од 90-их година руководећи кругови у САД су показивали забринутост због појаве нових претњи националној безбедности. После Првог заливског рата, због све чешће употребе појмова „информационо ратовање" и „информационо оружје", министарство одбране из-

[47] Председничка комисија о заштити критичне инфраструктуре (*PCCIP - Presidents Commission on Critical Infrastructure Protection, 1997*) је дошла до закључка да је информационо-комуникационо технолошка инфраструктура (ITC – *information and communication technology infrastructure*) основна предност (могућност, актив) друштва коју треба да заштити заједно војна и цивилна одрамбена политика и средства (*E. Luiijf, Information assurance and the information society, 1999*).

дало је директиву TS3600.1 од 21. децембра 1992. године под називом „Информациона противодбрана" у којој је указано на неопходност вођења рачуна о информационим ресурсима при организацији планирања и функционисања система управљања у циљу повећања ефективности дејстава војних снага у условима противдејстава противника. Од тог време интензивно се ради на задацима истраживања и развоја „борбе са системима управљања" са основни циљем – остваривањем информационе супериорности. Већ 1993. год. Комитет здруженог генералштаба доноси меморандум МОР-30 са детаљним концептом борбе са системима управљања. 1994. год. следе публикације Комитета за науку МО САД о специјалним организационо-техничким мерама заштите информационе инфраструктуре. У фебруару 1996. год. КоВ САД издаје FM-106 „***Информациона операција***" (*Information operations, 1996*). 1998. год. уследила је директива PDD-63 (*Critical Infrastructure Protection*) да би, као коначан след збивања, уследио почетком 2000. године „***Национални план заштите информационе инфраструктуре***" (*National critical infrastructure plan, 2000*). Практично са овим Планом почиње ***нова иницијатива*** администрације САД у области националне безбедности. План представља свеобухватно гледање на проблеме заштите кључних сектора националне економије, националну безбедност, општу здравствену заштиту и личну безбедност грађана.

План садржи 10 независних програма обједињених општим циљем. Важна тезе Плана је ***консолидација*** напора владе, федералних министарстава и приватног сектора у ***заштити информационе инфраструктуре*** као најважнијег националног ресурса. Програми Плана су:

1. ***Дефинисање критично важних ресурса инфраструктуре***, њихових узајамних веза и претњи које стоје пред њима,
2. ***Детекција напада*** и неовлашћених упада у компјутерске системе,
3. Разрада ***деловања обавештајне заједнице и правних аката***,
4. Благовремена ***размена*** информација о нападима,
5. Дизајнирање ***средстава*** реаговања, реконфигурације и реконструкције,
6. Активирање ***научно-истраживачких задатака*** на подршци програма 1 до 5,
7. Припрема и расподела неопходног броја ***специјалиста*** у области информационе безбедности,
8. ***Информисање*** америчког друштва о неопходности прогреса на плану информационе безбедности,
9. Доношење допуна и измена у ***законодавство*** у интересу програма 1 до 8 и
10. Обезбеђење заштите ***грађанских слобода*** свих американаца [29, 30].

Преглед програма „Националног плана заштите информационих система" показује озбиљне намере САД да проблем информационе безбедности, а самим тим и националне безбедности, решава на нови начин. У ***центар разматрања поставља критичну инфраструктуру***, а она је, по природи информационог друштва, информациона структура. С друге стране, ***проблем информационе безбедности је подигнут на општенационални ниво*** при чему је сваки грађанин не само корисник који брине о личној безбедности, већ и о безбедности друштва у целини.

Појам **критична инфраструктура** је дефинисан у закону „О патриотизму" (USA Patriot Act of 2001, October 2001) као свеукупност физичких или виртуелних система и средстава важних за САД у тој мери тако да њихово избацивање из строја или уништавање може довести до фаталних последица у области одбране, економије, очувања здравља и безбедности нације. Критичну инфраструктурну чине јавне и приватне институције у секторима пољопривреде, прехране, воде, здравства, хитних служби, владе, одбране, информација и телекомуникација, енергетике, саобраћаја, банкарства и финансија, хемијских и опасних материјала, поште и шпедиције.

Унутрашња безбедност, као део националне безбедности САД, регулисана је законом ***„О унутрашњој безбедности"*** (*Home Security Act, H. R, 5005,* 25. 11. 2002). За праћење његовог спровођења надлежан је Комитет за унутрашњу безбедност (*House Homeland Security Committee*). У оквиру њега, за питања ***„Кибер безбедности, науке, истраживања и развоја"*** (*House Homeland Security subcommittee on Cybersecurity, Science and Research and development),* формиран је подкомитет који се бави *безбедношћу компјутерских и комуникационих мрежа, информационих технологија, система управљања производњом, системом електроснабдевања и база података, како владиних тако и приватних, од унутрашњих и спољашњих напада предупређујући губитке становништва и инфраструктуре.*[48] Како је киберпростор[49] ***нервни систем*** – управљачки систем САД од кога зависи економија и национална безбедност земље, то је 2003. год. донешена ***Национална стратегија безбедности кибер простора*** (*The Nacional Stategy to secure Cyberspace, feb 2003*).

Међутим, основни носилац посла у области унутрашње безбедности је новоформирано министарство – ***Министарство унутрашње безбедности*** (*Depertment of Homeland Security*). При формирању министарства пошло се од схватања да је безбедност државе неодвојива од безбедности грађана. У том смислу су његове основне функције: спре-

[48] *Leadership selected for new cybersecurity panel GCN*, By William Jackson, 03/21/03

[49] ***Киберпростор*** *се састоји од стотина хиљада међусобно повезаних компјутера, сервера, рутера, свичева и фибер оптичких каблова који омогућавају нашим инфраструктурама да функционишу* [26].

чавање терористичких напада, смањење рањивости САД на терористичке акције, смањење последица тероризма, елиминисање последица техногених, антропогених и природних катастрофа, сагледавање економских интереса САД у склопу мера унутрашње безбедности, борба против наркомафије и њених веза са тероризмом и, коначно, и друге функције које нису директно везане за унутрашњу безбедност [24].

Министарство чине 4 директората:

– **анализа информација и заштита инфраструктуре** (Information Analisys and Infrastructure Protection),

– безбедност граница и транспорта (*Border and Transportation Security*),

– приправност за ванредно стање и реаговање (*Emergency Preparednes and response*) и

– наука и технологија (*Science and Technology*).

Унутар Министарства, посебно место припада првом директорату који обједињава анализу обавештајно-извиђачких информација о терористичким претњама (што је повукло за собом реорганизацију обавештајно-извиђачке заједнице САД) и заштиту критичне инфраструктуре. Интересантно је напоменути да су све функције унутрашње безбедности покривене нормативним документима. Тако је већ 2003. год. донешено неколико стратегија: ***Национална стратегија борбе са тероризмом*** (*The Nacional Stategy for Combating Terrorism*), ***Национална стратегија безбедности кибер простора*** (*The Nacional Stategy to secure Cyberspace*) и ***Национална стратегија физичке заштите критичне инфраструктуре*** (*The Nacional Stategy for the Physical Protection of Critical Infrastructures and Key Assets*).

Нове стратегије, по први пут официјално, признају потпуну зависност инфраструктуре САД од информационих система и мрежа и захтевају од свих друштвених чинилаца (јавног и приватног сектора) формирање ***Јединственог националног система реаговања на кибер нападе*** (*National Cyberspace Security response System).* Национални програм сарадње у области информационе безбедности (*The National Information Assurance Partnetship* – NIAP) присутан је још од 1997. год. Неактивност локалних органа, али и сама природа проблема је довела до тога да влада САД преузме све прегогативе у овој области. И наравно донешени су одговарајући закони: ***закон о повећању кибер безбедности*** (*Cyber Security Enhancment Act of 2002*, H. R.3482), ***закон о финансирању обавештајне делатности у 2003*** (*Intelligence Authorization Act For Fiscal Year 2003*) и ***закон о размени информација у интересу унутрашње безбедности*** (*Homeland Security Information Sharing Act*, 2003).

Последица нових схватања оличених у стратегијама, директивама и законима су: рад на развоју националног система веза[50] (*National*

[50] Врућа линија (*Emergency response Link* – ERLink), перспективна интелигентна мрежа (*Advanced Intelligent Network* – AIN), мрежа упозорења и координације

Communications System – NCS), реорганизација обавештајно-извиђачке заједнице (*intelligence community*), физичка заштита важнијих објеката критичне инфраструктуре, инсистирање на кључној улози информационих технологија у повећање унутрашњу безбедности[51], подршка технолошкој надмоћи САД, истраживање у области заштите информационе инфраструктуре[52] и обука грађана у стицању навика преживљавања у условима техногених и природних катастрофа и терористичких напада.

Нови приступ решавању питања унутрашње безбедности, у условима глобализације, не делује само на америчко друштво, већ одражава и на остала друштва.[53] Network-centric парадигма, заснована и још увек присутна само у САД, прелиће се и на остале земље света, а она подразумева висок степен зависности безбедности националне информационе инфраструктуре од информационе безбедности свих њених елемената, како државног тако и приватног сектора. На тај начин, информациона безбедност било које компаније постаје фактор националне и унутрашње безбедности државе у целини. ***Изградња ефективне безбедносне инфраструктуре***, тзв. интегрисане информационе инфраструктуре (III – *integrated information infrastructure*), ***није питање добре воље, већ ствар националне безбедности земље***.

Однос информационе и других одлика безбедности

Као што смо већ рекли, информациона безбедност се јавља не само као ***једна од компонената националне безбедности***, већ и ***као***

(*Alerting and Coordination Network* – ACN), владин телекомуникациони сервис у ванредним приликама (*Government Emergency Telecomminications Service* – GETS), национални координациони центар (*National Coordinating Center* – NCC), размена информација о ресурсима везе (*Communications Resource Information Sharing* – CRIS), дистрибуирани ресурси (*Shares Resources* – SHARES), приоритетни телекомуникациони сервис (*Telecommunications Service Priority* – TSP), бежични приоритетни сервис (*Wireless Priority Service* – WPS) и обука, планирање и техничка подршка (*Training, Planing and Operational Support* – TPOS).

[51] Информационе технологије ће играти кључну улогу у повећању унутрашње безбедности нације пред будућим потенцијалним опасностима. У суштини, информационе технологије ће помоћи нацији да одреди потенцијалне претње, да оперативније дистрибуира информације, да обезбеди механизме заштите земље и разради одговарајуће противмере (*Homeland Security – Information Technology Funding and Associated Management Issues*, GOA-03-250, decembar 2002.).

[52] Перспективне области истраживања и развоја: управљање безбедношћу компанија, безбедност дистрибуираних аутономних група, истраживање безбедности и анализа „рањивих" места, реконструкција безбедности система и мрежа, безбедност бежичних система, показатељи и модели и питања законодавства, политике и економије (*Cyber security research and development agenda*, Institut for information infrastructure protection, January 2003).

[53] Тако нпр. већ 11.03.2003.год. извршена је реорганизација руских специјалних служби [24].

пресек свих других облика безбедности у којима информационе технологије заузимају важно место. Најочигледнији пример тога су војна и економска безбедност

Однос војне и информационе безбедности већ је изложен (за САД у тачки 3.3 и за Руску федерацију у тачки 4.1.1) па се на њему нећемо задржавати. Однос информационе и економске безбедности није до сада третиран. Због значаја економског фактора за националну безбедност и савремених тенденција у националним економијама и светској економији која настаје на крилима глобализације, потребно је рећи нешто о областима пресликавања информационе безбедности и пословања (бизниса) као главног садржаја економске безбедности.

Однос информационе и економске безбедности

У тесној вези са пословањем, поред ***економске безбедности***, је и информациона безбедност. Економска безбедност има за циљ стабилно привређивање и стабилно одвијање бизнис-процеса. Информациона безбедност се протеже и на економику у смислу информација и информационих система који су, реално, део те области друштвених делатности. Према схватањима на Универзитету националне одбране САД, информационо ратовање, *„мада ... у крајњем случају војно по својој природи, води се и у политичкој, **економској** и друштвеној сфери"* – И у дефиницији М. Либицког инсистира се на односу економике и информационе безбедности. Чак пре, он, као један од облика информационог ратовања, наводи економско-информационо ратовање EIW (*economic information warfare*) које се своди на блокирање (***информациона блокада***) или усмеравање информација да би се обезбедила економска доминација (***информациони империјализам***).

Заштита информација је предмет интересовања државних и војних структура од настанка државе. Међутим, данас, и све велике компаније сматрају да је информациона безбедност један од најважнијих приоритета у вођењу бизниса. У складу са тим евидентне су радикалне промене у организацији службе информационе безбедности у фирмама. Питања информационе безбедности и проблем заштите информација су са, све донедавно, крајњих маргина доспели у ситуацију да буду делокруг рада самог топ-менаџмента компанија.

Зашто је потребно штитити пословне информације? Различите организације из различитих разлога треба да штите информације. За банке је од пресудног значаја ***интегритет*** информација (неизменљивост новчаних трансакција) због финансијског пословања. За провајдере Интернет-услуга најважније су ***расположивост и поузданост*** (доступност и поуздан рад кључних елемената система) због континуитета пружања услуга. За државне организације и установе од пресудног значаја је ***поверљивост*** (приступ информацијама имају само овлашћена лица).

Пословне информације могу отицати путем техничких канала отицања (у литератури је најзаступљеније разматрање компјутерског канала)[54] или путем тзв. унутрашњих канала (сарадници са својим мотивима и радним навикама). Последице неадекватне заштите информација се огледају као финансијски губици, губитак угледа или тржишних позиција и могу имати катастрофалне последице. Очигледност потребе заштите информација је посебно изражена у различитим облицима електронског пословања (*e-business*).

Ако пођемо од чињенице да су информације и информациони ресурси материјална добра, очигледно је да је информациона безбедност неодвојиви део пословања.

Када говоримо о пословању и информационој безбедности, предмет разматрања су информациони системи и информације које спадају у пословне и банкарске тајне. ***Пословне тајне*** подразумевају информације пословног карактера и персоналне податке особља коме су доступне пословне информације. ***Пословне информације*** су основна документа фирме, финансијски обрачуни, кредитни аранжмани, подаци о перспективним робама, тржиштима, изворима средстава или сировина, подаци о конкурентима, подаци о технолошким поступцима, подаци о потенцијалним партнерима, подаци о месту чувања, времену и маршрутама превожење товара, подаци о лицима која треба врбовати и поткупити, подаци о везама и могућностима менаџера и подаци о сталним купцима (потрошачима). ***Персонални подаци*** су подаци личног карактера сарадника фирме: извори прихода, однос према актуелним друштвено-економским питањима, лични живот топ-менаџмента и чланова њихових породица, подаци о пороцима, штетним навикама, сексуалној оријентацији, подаци о дружењима и начину организације личног и породичног живота, подаци о месту чувања драгоцености, брачној верности и проблемима између родитеља и деце.

Информациона безбедност пословања (бизниса) подразумева заштиту од организованих преступа, заштиту од нарушавања закона и заштиту од несавесне конкуренције.[55] Интересантно је, да је у пракси, најзаступљенија потреба за заштитом од несавесне конкуренције и њене најгрубље форме – ***индустријске шпијунаже.***[56]

---

[54] Појавом Интернета омогућено је формирање погодне глобалне комуникационе инфраструктуре која пружа могућност приступа, у светским размерама, фирмама, купцима, произвођачима опреме и кључним партнерима. Реч је о несумњиво проширеним могућностима међусобне размене информација и ефикаснијег пословања, али и о повећању ризика и опасности када је у питању рачунарска мрежа компаније.

[55] Према резултатима анкетирања проведених у РФ о формама и методама прибављања пословних тајни конкурентских фирми на корупцију (мито) и уцену отпада 42%, на добијање информација помоћу компјутера и друге технике отпада 35%, на копирање или крађу докумената, цртежа и експерименталних или пробних примерака отпада 13%, на прислушкивање – 5% и на остале методе 5%.

[56] Индустријска шпијунажа је везана за најсавременије технологије, производњу роба широке потрошње и фирме које се баве снабдевањем становништва. Предмет индустријске шпи-

Однос између пословања и информационе безбедности, посматран у контексту класичног (традиционалног) и електронског пословања, има четири различита аспекта (слика 15).

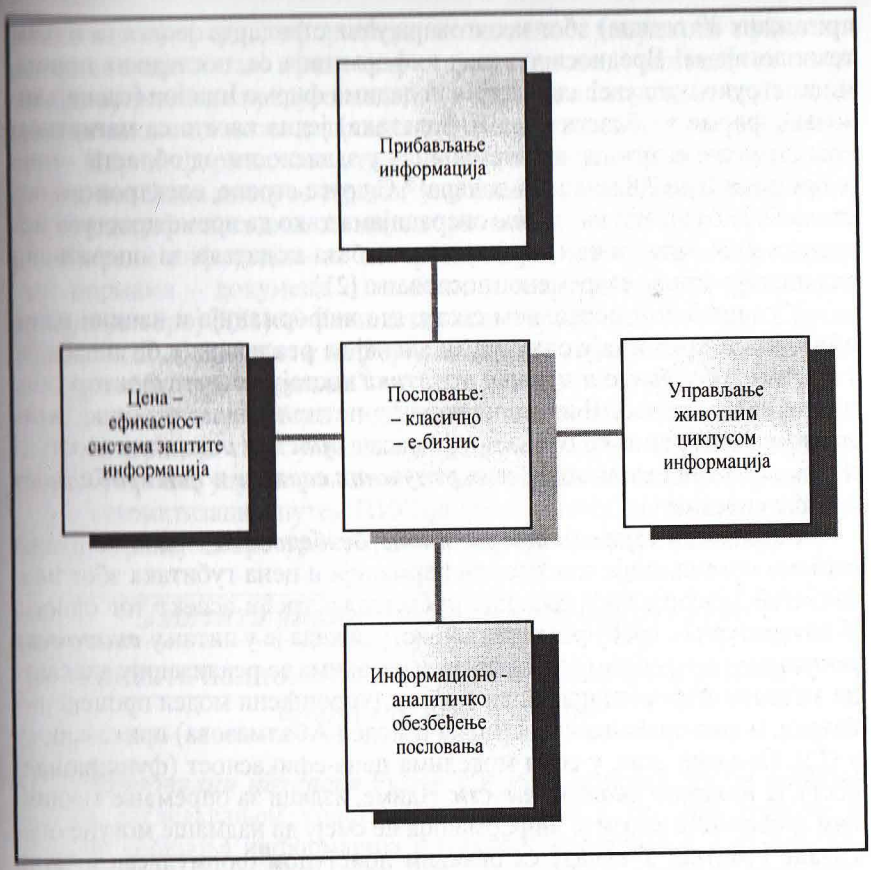
Први се односи на процес ***прибављања*** пословних информација о конкурентима и њиховим пословним плановима. Када је реч о ***прибављању економских информација***, срећу се различити термини: ***конкурентско извиђање*** (*competitive intelligence*), бизнис извиђање, комерцијално извиђање, пословно извиђање и индустријска шпијунажа. Основна разлика међу њима је да ли се користе законским (конкурентско извиђање) или незаконским (индустријска шпијунажа) средствима. Све врсте извиђања основно упориште имају у легитимности (етичности), односно прибављању информација само законским и етичким методама (проспекти, објављени извештаји, радови из стручне литературе, предавања, организоване посете, размена литературе, различити облици пословне сарадње итд.). За разлику од конкурентског извиђања, индустријска шпијунажа је добијање информација или података (било законитим или незаконитим путем) о конкуренту из области научног истраживања, производње са најновијим технологијама као и персоналних података руководећих људи (са циљем њихове злоупотребе).

Индуструјска шпијунажа се организује на државном нивоу. Као једна од најугроженијих земаља, када је реч о индустријској шпијунажи, САД су 1996. год. донеле закон о индустријској шпијунажи. Непосредан повод је био извештај начелника федералног истражног бироа (FBI), по коме је у 1995. год. подигнуто 700 оптужница за индустријску шпијунажу Индустријска шпијунажа је проглашена за једну од претњи (ризика) за америчку економију. Према извештају Едвина Фридмана (објављеном у *Public Administration Reiview*, 1995. год.), агената ФБИ и асистента на факултету криминалног права при министарству за друштвено управљање (Њујорк), индустријска шпијунажа је нанела штету америчкој економији од 25 до 100 милијарди USD.[57]

Други аспект је проблем ***чувања*** пословних информација у базама података. Вођење пословања претрпело је корените промене последњих година. Његова стабилност и динамичност у многоме зависи од техничке опремљености. Посебно место у оквиру тзв. техничке опремљености припада инфраструктури чувања података. Наиме, раст бизнис-трансакција довео је до енормног пораста обима података који се чувају на различитим медијумима. У складу са тим настао је ***проблем чувања података*** (у базама података) јер губитак опреме не мора да значи губитак бизниса, али губитак података – обично то јесте (нпр. банкарски подаци о извршеним трансакцијама, подаци о испорученим робама у компанијама итд.).

јунаже, пред високих технологија, су и стартегијски маркетинг планови и спискови клијената! Индустријска шпијунажа је најзаступљенија у најразвијенијим земљама, при чему свака има свој модел деловања (САД, Феанцуска, Јапан, Немачка, РФ, Јужна Кореја итд.).

[57] М. Расчётов, Идеология и методология промышленого шпиюнажа, Лан, № 3, 2002.



Слика 15: Области пресликавања односа информационе безбедности и пословања

Термин чување података, са својом терминолошком назнаком некакве статичности, постао је преузак за *on-line* бизнис-процесе и прерастао је у нови – управљање информацијама, односно управљање животним циклусом информација (ILM – *Information Lifecycle Management*). Иначе, пословни информациони системи (ПИС) и управљање информацијама представљају окосницу будућих трендова развоја. У складу са тим, значај и улога управљања информацијама (чување података), добија на значају и у инфраструктури информационих технологија. Зашто? Системи обраде података мењају се сваких 5 година, са променом технологије, а системи чувања података треба да обезбеде компатибилност и функционисање од 25 до 250 година![58] Познат је „ефекат НАСА" када је америчка космичка агенција изгубила 1,2 милиона магнетних трака са информацијама о космичким летовима (у

[58] Чиняков Р., Сети хранения в ретроспективе и перспективе, Журнал „LAN" №7 2004., Издательство „Открытые системы".

протеклих 30 година) због неодговарајућих стандарда записа са новим технологијама! Вредност чуваних информација се, последњих година, многоструко пута увећала. Према подацима фирме Imation (специјализоване фирме у области чувања података) једна касета са магнетном траком може садржати информације – у зависности од области – чија је вредност и до 2,8 милиона долара![59] С друге стране, електронско пословање је базирано на *on-line* операцијама тако да време приступа подацима и 24-четворочасовна спремност база података за оперативни рад постају основа савременог пословања [21].

У савременом пословном свету, где информација и начини њене обраде и чувања имају одлучујући значај за реализацију бизнис-задатака, ***центри обраде и чувања података*** постају кључни фактор свих пословних збивања. Њих карактеришу четири важне особине: ***поузданост*** (отпорност на отказе), ефикасан ***приступ подацима*** (доступност), успешна реализација свих ***услужних сервисе*** и ***флексибилност*** конфигурисање.

Економска страна информационе безбедности – цена коштања система организације заштите информација и цена губитака због неадекватне заштите информација, представља трећи аспект тог односа. У литератури се срећу различити приступи када је у питању ***економска рачуница*** о потребним финансијским издацима за реализацију адекватне заштите информација. Неки модели (упрошћени модел процене губитака, модел враћања инвестиција и модел Абалмазова) приказани су у [22]. Полазни став, у свим моделима цена-ефикасност (функционалност), је ***принцип економичности***. Наиме, издаци за опремање техничким средствима заштите информација не смеју да надмаше могуће очекиване губитке. У складу са оваквим приступом формулисан је ***концепт управљања ризицима*** као доминирајући у свим стандардима о информационој безбедности. Најпознатији софтверски пакети који реализују концепт управљања ризицима су: CRAMM (енглеска компанија *Insight Consulting*), RiskWatch (америчка компанија *RiskWatch*) и ГРИФ (руска компанија *Digital security*) [23].

Као четврти аспект, имамо тзв. ***информационо-аналитичко обезбеђење пословања***. Проблематика информационог-аналитичког обезбеђења проистиче из схватања да је ***доступност*** (*открытость* – отвореност) ***информација*** саставни део појма информационе безбедности,[60] односно сигурности друштва и појединаца да ниуком погледу нису ускраћен за информације које им припадају.[61] Посматрано

[59] Keller M., Правильное обращение (превод на руски), Журнал ЛАН №7 2004., Издательство Открытые системы".

[60] Минаев Ю., Информационная открытость – составная часть национальних интересов Рассии в информационной сфере, Међународни форум Технологије безбедности, Москва 2002. год.

[61] У уводном делу је напоменуто да је појам информационе безбедности свеобухватан и да прожима све сфере људског битисања. Филозофски, социјални и психолошки

у економској сфери, информациона отвореност доприноси ефикасности економије на тај начин што информационо – аналитичка подршка доприноси да предузетништво располаже са адекватним проценама ризика и да може доносити правилне одлуке о пословним потезима. Нпр. информациона отвореност у области инвестиционих пројеката, повећава интерес страног улагања на рачун смањених системских и специфичних инвестиционих ризика.

Питање информационе отворености је регулисано и међународним нормама – документ о глобалном информационом друштву и Препорука број Р(81) 19 Комитета министара држава чланица Савета Европе – ***О доступности информација које се налазе на располагању у државним установама.***[62]

Друга страна проблема информационог-аналитичког обезбеђења је инкорпорација свеобухватних ***пословних информационих система*** (ПИС) у процес управљања пословањем. Проблематика информатизације и аутоматизације путем ПИС оличена је у тзв. системима планирања корпорацијских ресурса (ERP – *Enterprise Resource Planning*).

Заштита информационе инфраструктуре

Заштита националних интереса Руске федерације у информационој сфери

„***Национални интереси*** Русије у информационој сфери завршавају се сагледавањем конституционих права и слобода грађана у области добијања информација и њиховог коришћења, у развоју савремених телекомуникационих технологија и у заштити државних информационих ресурса од неовлашћеног приступа[63]. Као и **Концепција националне безбедности**, тако и **Доктрина информационе безбедности**, у делу о компонентама националних интереса у информационој сфери[64], о заштити информационе инфраструктуре говори на општем нивоу. У оба документа наводе се само државни органи и институције задужене за реализацију датих интереса без детаљније разраде њихових међусобних односа и задужења. Имајући на уму чињеницу да до 1992. год. у Руској федерација информациона безбедност

аспекти информационе безбедности су предмет разматрања не само само руских, већ и западних истраживача.

[62] Проблематика информационе отворености се у Руској федерација озбиљно третира од 1991. год. о чему сведоче међународни форуми и округли столови.

[63] *Концепцији националне безбедности* (указ председника № 1300 из 1997. и редакција № 24 из 2000.године)

[64] Права и слободе *грађанина*, информационо обезбеђење *државне политике*, развој савремених *информационих технологија*, заштита *информационих ресурса* од неовлашћеног приступа и обезбеђење безбедности *информационих и телекомуникационих система*

није уопште разматрана и да информациона инфраструктура није ни приближно развијена као у САД, правна регулатива и значај који се придаје информационој безбедности представљају велики напредак.

За разлику од Руске федерације, САД (као земља са најразвијенијом и најрањивијом инфраструктуром у свету и као земља којој се догодио 11. септембар), имају разрађен концепт заштите информационе инфраструктуре до најситнијих детаља. Са наведеним концептом ћемо се упознати у основним цртама колико је потребно да илуструјемо чињеницу да је информациона безбедност једна од компонената националне безбедности.

Изградња ефективне безбедносне инфраструктуре

МО САД и Одбрамбени научни борд (DSB – *defense science board*) су идејни творци ефективне безбедносне архитектура - ***интегрисане информационе инфраструктуре*** (III – *integrated information infrastructure*). Интегрисана информациона инфраструктура представља глобалну информациону мрежу GIG (*global information grid*) која испуњава све захтеве појма информационо обезбеђење (IA). Њу карактерише: инфраструктура и апликације јавног кључа PKI и PKE, GIG IA тестирање, DID архитектура (*defence-in-depth* – одбрана у дубину), IP sec, функције информационог обезбеђења, могућност менаџмента безбедношћу мрежа, линк енкрипција на физичком нивоу отвореног модела OSI и способност преживљавања [25].

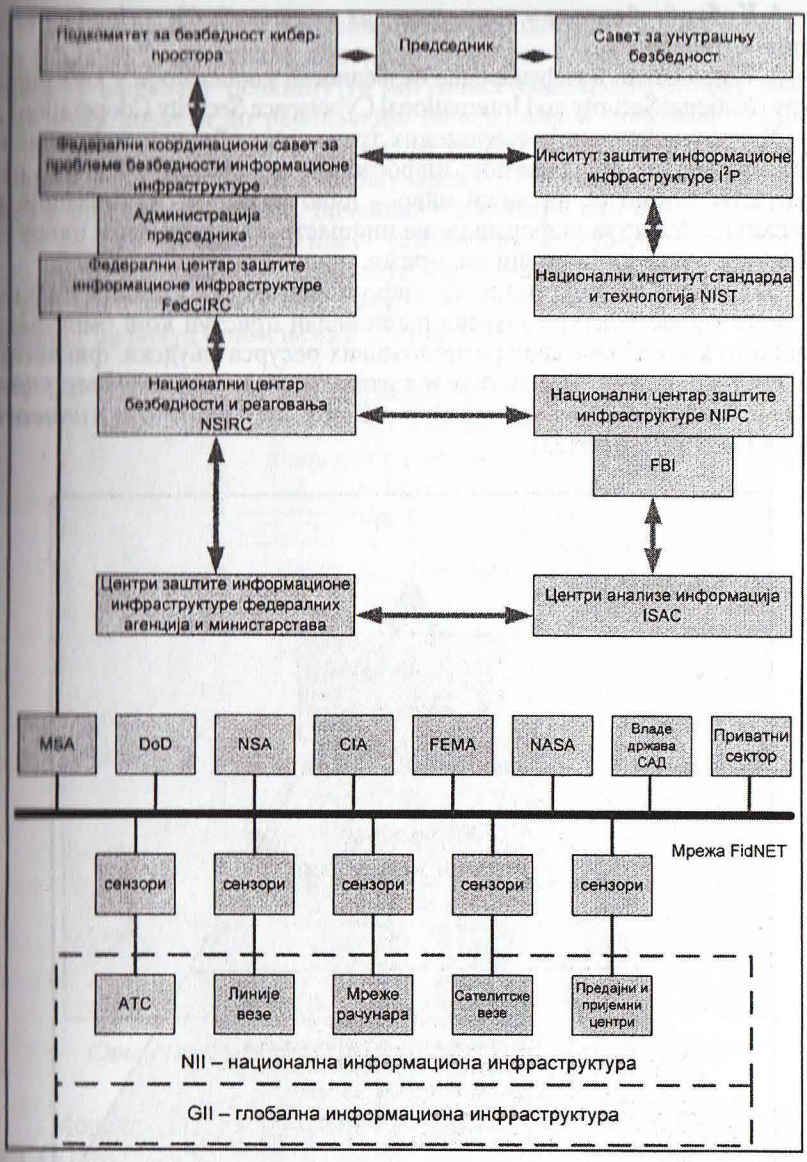
Елементи правног и организационог карактера заштите информационе инфраструктуре изложени су у тачки 4.1.2. Са председничком директивом ПДД-63 (PDD/NSC-63, *Americas Critical Infrastructures, may 22, 1998*) и „Националним планом заштите информационих система" (8. април 2000. год.) започет је процес изградње ефективне безбедносне инфраструктуре. То су први документи у којима су директно повезане информациона безбедност и безбедност инфраструктуре као оличења националне безбедности.

Стратегија развоја глобалне информационе мреже, препоруке, архитектура ефективног информационог обезбеђења (*information assurance*) и предности које она са собом доноси детаљно су изложени у [25]. На овом месту ћемо рећи још само пар чињеница – да је глобална информациона мрежа предмет Визије 2020 и да њен настанак почиње са 2005. годином.

Организациона структура управљања безбедношћу националне информационе ифраструктуре САД приказана је на слици 16.

Национална стратегија безбедности кибер простора дефинисала је пет националних ***приоритета*** у области заштите информационе инфраструктуре, и то:

1. Национални **систем за безбедносни одговор** у киберпростору (A National Cyberspace Security Response System)



Слика 16: Структура управљања безбедношћу националне информационе инфраструктуре САД (преузето из [20])

2. Национални **програм за смањење безбедносних претњи и рањивости** у киберпростору (A National Cyberspace Security Threat and Vulnerability Reduction Program)

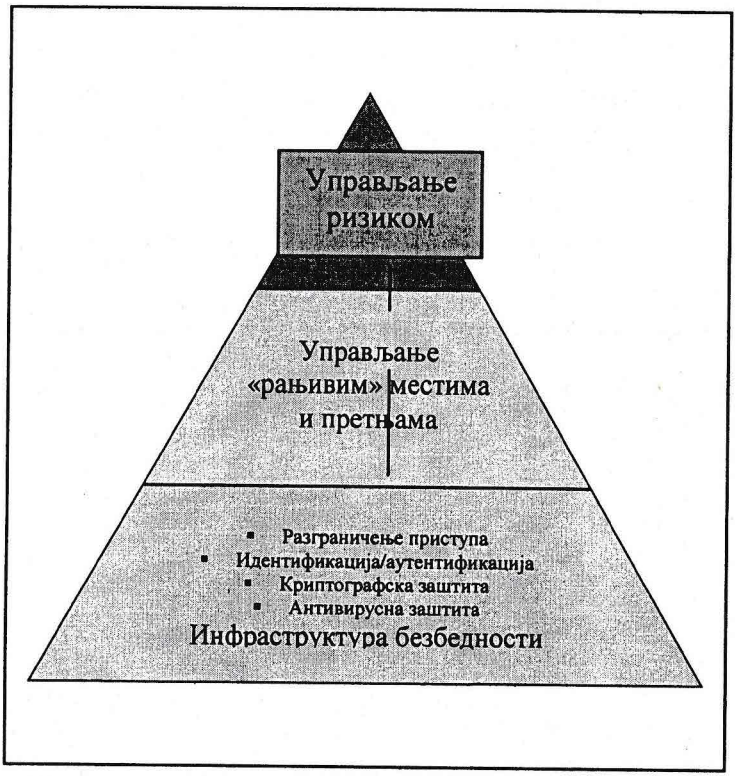
3. Национални **програм безбедносног упозорења у киберпростору и програм обуке** (A National Cyberspace Security Awareness and Training Program)

4. **Кибербезбедност** у раду владиних инситуција (Securing Governments' Cyberspace)

5. Национална и међународна **безбедносна кооперација** у киберпростору (National Security and International Cyberspace Security Cooperation)

У циљу илустрације савремених трендова у области информационе безбедности појединачних информационих система, условно речено, спустићемо се на нижи ниво – ниво државне организације и компаније. Заштита информационе инфраструктуре на овом нивоу је темељ глобалне информационе мреже.

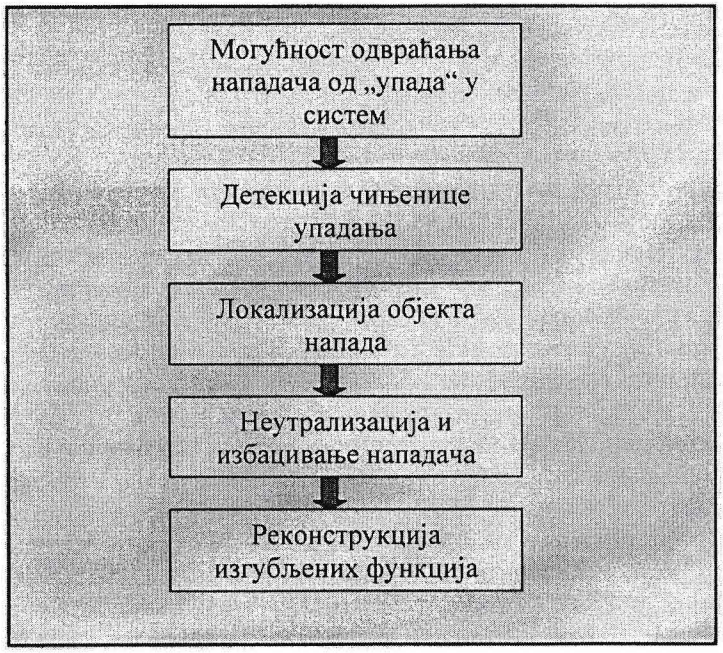
Савремена теорија и пракса информационе безбедности информационе ифраструктуре захтева рационалан приступ који омогућава ефикасно коришћење свих расположивих ресурса (људски, финансијски и материјални). Овај услов задовољава ***модел адаптивног управљања безбедношћу*** (*adaptive network security*)[65] на основу ***концепта управљања ризиком*** [22].



Слика 17: Модел адаптивног управљања безбедношћу компјутерских мрежа

[65] Један од метода модела адаптивног управљања безбедношћу је ADDME метод назван по првим словима његових етапа – оцена (*asses*), пројектовање (*design*), постављање (*deploy*), експлоатација (*manage and support*) и обука (*education*).

Модел адаптивног управљања безбедношћу компјутерских мрежа (слика 17) омогућава контролу практично свих претњи и благовремену ефикасну реакцију уз могућност отклањања слабих места, која могу довести до реализације напада, али и могућност анализе услова под којима долази до појаве таквих места у систему. Модел смањује могућност злоупотреба у мрежи (70% напада долази из мреже) и спречава скривање чињеница о нападима или покушајима који су се десили. Модел адаптивног управљања безбедношћу не одбацује већ постојеће механизме заштите информација (разграничење приступа, идентификацију итд.), већ само проширује њихову функционалност на рачун примењених технологија.



Слика 18: Концепција ешелонираног система информационе безбедности [20]

Модел адаптивног управљања безбедношћу уграђен је у стандард ИСО/ИЕЦ 15408. Према њему за заштиту информационе инфраструктуре у САД примењује се ***модел ешелониране вишеслојне информационе безбедности*** (слика 18)[66] који реализује функције мониторинга, заштите и адаптације информационих ресурса. На тај начин могуће је спречавање продора, детекција нарушавања безбедности, локализација нападнутог објекта, неутрализација, елиминисање напа-

[66] Пре избора хардверско-софтверских система заштите неопходно је разрадити политику безбедности, узимајући у обзир све специфичности технологије обраде информација у датој организацији.

дача и реконструкција изгубљених функција система. У основи датог модела лежи примена пасивних (филтера, међумрежних екрана – *firewal*) и активних (сензора детекције напада, распознавања аномалија, адаптивних алгоритама реконструкције) техничких средстава заштите. Најпознатија од савремених технологија ове намене је технологији IDS (*Intrusion detection Systems – detekcija napada na sistem*).

Модел ешелониране вишеслојне информационе безбедности своју детаљну, прегледну и лако схватљиву разраду, на нивоу појединачног информационог система,[67] добио је у ***моделу заштитних прстенова*** [31] који, информациону безбедност информационих система, разматра са више аспеката: правне норме, организационе мере, мере непосредне заштите, заштита опреме, заштита програмске подршке и заштита база података. Заштитни прстенови су:

– хумани прстен (персонал који ради са својим мотивима, спремношћу и могућношћу деловања),

– нормативни прстен (обавезује и прописује извршење и начин извршења неке радње, дефинисан матрицом овлашћења),

– организациони прстен (мере и активности, надлежности и обавезе корисника и извршилаца),

– прстен физичке заштите (онемогућава физички приступ нападача),

– заштита софтвера (контролисано чување и копирање оперативног система и апликативних програма),

– заштита (резидентних) података (обухвата ограничење приступа подацима, евидентирање приступа подацима и спречава неовлашћени приступ подацима),

– заштита инфраструктуре (обезбеђује оптималне услове за функционисање свих компоненти ИС),

– противпожарна заштита (грађевинске мере, примена одговарајућих средстава за гашење и обуку особља),

– заштита ИС у раду у мрежном окружењу (контрола приступа мрежи и криптозаштита порука које се преносе у дифузној рачунарској мрежи) и

– криптозаштитни безбедносни прстен (криптозаштита података транзицијом или супституцијом).

У моделу заштитних прстенова уочавамо, на нивоу појединачног информационог система, ешелонирану по дубини заштиту информација. Модел покрива широку лепезу могућих напада што је карактеристично за услове савременог живљења. У њему се виде елементи интегрисаних система.[68]

---

[67] Из организационе структуре управљања заштитом информационе инфраструктуре, евидентно је да модел ешелониране вишеслојне заштите подразумева, на нивоу националне информационе инграструктуре, просторну и кибер-просторну дубину.

[68] На вишем нивоу уопштавања заштитне прстенове можемо дефинисати као: легалну и друштвену контролу (правни оквир), административну контролу (организационе мере), физичку заштиту и контролне процедуре у систему.

Заштита информационе инфраструктуре је предмет живог интересовања у САД. Тако нпр. Институт за заштиту информационе инфраструктуре[69] (чине га 23 државне организације), на основу опсежних испитивања, издао је листу приоритетних истраживања у овој области: управљање безбедношћу компанија, безбедност дистрибуираних аутономних група, испитивање безбедности и анализа рањивости, регенерација система и мрежа, идентификација, безбедност бежичних система, критеријуми и модели (заснованост инвестиција и дозвољени ниво ризика) и питања законодавних, политичких и економских аспеката информационе безбедности [24].

Закључак

Промени погледа на свет, насталој на граници трећег миленијума, претходила је технолошка револуција у области информационих и комуникационих система. Масовна компјутеризација и примена и развој нових информационих технологија довели су до неслућеног напретка у сфери масовних медија, бизниса, индустријске производње, ратовања, научних истраживања и образовања.

Глобалне социјалне промене, настале као последица ових промена, захтевају објективну анализу формиране информационе средине светске заједнице. Проблем информационе безбедности, у досадашњој историји, разматран само у контексту заштите информација и то, пре свега, путем тоталне физичке заштићености и различитих ограничења, тешко да може задовољити савремене потребе. ***Информационо друштво***, које доноси са собом трећи миленијум, ***носи са собом нове претње али и нове начине за њихово решавање***.

Савремена геополитичка ситуација и еволуције целог спектра геополитичких фактора међу којима је један од најважнијих – информациони, ***захтева принципијелно другачији прилаз проблему националне безбедности***. Данас је свима јесно да је, уз исте остале услове, стратегијска предност државе у њеним могућностима у информационој сфери.

До недавно се сматрало, у теорији и пракси националне безбедности, да је најважнија војна компонента. Данас су очигледни недостаци оваквог прилаза (вероватно најбољи пример је војно и политичко руководство бившег СССР) јер је научно-техничка револуција довела до формирања информационог друштва у коме је ***информација главни фактор управљања светом и основни инструмент власти***.

Полазећи од искустава из сукоба последње деценије и одређења информационог ратовања, као ***деловања на систем знања и уверења некооперативних опонената***, јасно је да проблем националне безбедности захтева и решење проблема информационо-психолошких дej-

[69] И^{3}П – *инситут инфраструктуре протецтион*

става на психу човека као појединца. Информационо ратовање, мада је у крајњем случају војно по својој природи, води се и у ***политичкој, економској и друштвеној сфери и примењиво је преко читавог скупа области националне безбедности од мира до рата и од главе до пете.***

Чињеница да времена која долазе информациону безбедност стављају у први план, само наговештавају њен даљи развој и у теоријском и у практичном смислу.

Литература

1. Ярочкин В., И, ***Секьюритология – наука о безопасности жизнедеятельности***, http://kiev-security.org.ua.
2. Daniel G. Wolf, ***Statement before the House Select Committee on Homeland Security Subcommittee on Cybersecurity, Science and Research & Development***, Nacional Security Agency US, Juli 22, 2003.
3. Панарин И., Н., ***Проблемы обеспечения информационной безопасности в савременных условиях***, http//kiev-security.org.ua, 1997.
4. Хорев А. А., ***Способы и средства защиты информации***, МО РФ, Москва, 1998 г.
5. Решение Коллегии Гостехкомиссии России № 7.2/02.03.01 г., ***Специальные требования и рекомендации по технической защите конфиденциалъной информации***, Москва, 2001.
6. ***Федералъный закон об информации, информатизациии и защите информации***, Дума, 25.01.1995.
7. П. В. Константинович, ***От информационных войн к управляемой конфронтации и сотрудничеству***, журнал Факт № 9, 2001.
8. А. Д. Урсул, Т. Н. Цырдя, ***Информационная безопасностъ, сущностъ, содержание и принципы ее обеспечения***, журнал Факт № 2, 2000.
9. ***Доктрина информационной безопасности Российсой Федерации***, Президент, 09. 09. 2000.
10. Барсуков Д., ***Интегралъная защита информации***, „Электроника. Наука, технология, бизнес“ № 3–4,1998 г.
11. Maconachy V., Schou C., Ragsdale D., Welch D., ***A model for Information assurance: an integrated approach***, Proceedings of the 2001 IEEE, Workshop on Information Assurance and Security, United States Military Academy, West Point, 2001.
12. Field manuel No. 100–6, ***FM 100–6 Information operations***, Department of the Army, Washington, DC, 1996.
13. Field manuel No. 3–13, ***FM 3–13 (FM 100–6) Information operations: Doctrine, Tactics, Technigues, and Procedures***, Department of the Army, Washington, DC, nov 2003.
14. Szafranski R., ***A theory of information warfare: preparing 2020***, Airpower Journal, Spring, 1995 .
15. Libicki M., ***What is information warfare?*** Strategic Forum, No. 28, http://www.ndu.edu/inss/ actpubs/act003/actppub. htm.
16. Nacional Security Agency, ***Nacional Information Systems secutity Glossary***, NSTISSI No 4009, Fort Meade, MD spt 2000.

17. **Survivability** – ***A New Technical and Business Perspective on Security***, Proceedings of the 1999 New Security Paradigms Workshop. Caledion Hill, ON, sep 21–24, 1999, Nwe Jork, NY: Association for Computer Machinery, 2000.
18. Beauregard J., **Modeling information assurance**, Air Force Institute of tehnology, 2001.
19. A., Usher: ***Towards a Tahonomy of information assurance***.
20. Леваков А., ***Анатомия информационной безопасности США***, Jet info online № 6 (109), 2002.
21. Жилкина Н., ***Данны в порядке?***, Журнал „LAN", № 4/2004., издательство Открытие системы (http://www.osp. ru).
22. Синковски С., ***Неки аспекти и проблеми заштите информација***, „Безбедност", 04/2004, стр. 586–602.
23. Медведовский И., ***Современные методы и средства анализа и контроля риском информационных систем компаний***, Учёбный центр Информзащита, 12.01. 2004.
24. Леваков А., ***В интересах внутренней безопасности США***, http:// Jet info online.
25. ***Protecting the Homeland***, report of the Defense science board, 2001.
26. ***The national strategy to secure cyberspace***, The White house, ashington, - february 2003.
27. ***Концепция националъне безопасности,*** указ председника № 1300 из 1997 и редакција № 24 из 2000).
28. ***Основы националъной безопасности,*** приказ књиге Б. А. Демидова „Концептуалъные основы и елементы националъной безопасности", http://domarev. ru.
29. Леваков А., ***В США принят план защиты информационных систем***, Jet Info № 8/2000.
30. J. Miteff, ***Critical infrastructure: background, policy, and iplementacion***, CRS report for Congres, 4. feb 2002 .
31. Родић Б., ***Интеракција јавних рачунарских мрежа и рачунарских мрежа специјалних институција*** *(докторска дисертација)*, Војнотехничка академија, Београд, 2001.