УДК: 351.862/.863(497.11)

ИНФОРМАЦИОНА БЕЗБЕДНОСТ: СТАНДАРДИ ИЛИ ПРАВИЛА

Данијела Д. Протић*
Генералштаб Војске Србије,
Управа за телекомуникације и информатику (J-6)

У раду је приказано истраживање о примени стандарда и правила за заштиту информација и информационих система, у складу са ставом Владе Републике Србије о развоју информационог друштва до 2020. године. Посебно су проучавани стандарди из групе ISO/IEC 27k и NIST SP 800. Приказане су активности светских организација ОУН, ЕУ, НАТО и ОЕБС. Презентоване су и активности МО и ВС на пољу реформе система за заштиту информација, које су интегрални део трансформације система одбране, и одговарају захтевима за поштовање Повеље УН, улазак у ЕУ и сарадњу са НАТО и ОЕБС-ом. Дат је посебан осврт на јединице и установе МО и ВС чија је функција заштита информација и информационо-комуникационих система, као и начин за стандардизацију увођења мера заштите у МО и ВС.

Кључне речи: *информациона безбедност, стандардизација, ISO/IEC 27k, NIST SP 800*

Увод

Нагли развој система који су базирани на информационим технологијама утицао је на нов начин размене информација, што је изазвало промену регулативе и омогућило пословање организација различитих интереса, хијерархија и величине. Појава стандарда који регулишу права и обавезе заинтересованих страна довела је до усклађивања неопходних докумената, правила и процедура, што је омогућило транзицију пословања са традиционалног на електронско. Промене су захтевале добро осмишљен информациони систем са едукованим кадром, организованим пословним процесима и савременом технологијом, јер је неопходна брза обрада информација од значаја (финансијски извештаји, персонални подаци, пословне тајне). Свака промена целовитости или садржаја битних информација може да утиче на кредибилитет организације или изазове последице које могу да привремено или трајно зауставе њен рад. Због тога, елиминација или смањење потенцијалног ризика на минимум, и квалитетна организација информационог система, обезбеђују добар основ за борбу против људских и системских грешака или малициозних напада споља. Неопходно је да персонал буде едукован да препозна ситуацију која искаче из свакодневних оквира, да зна како да реагује и коме да се обрати у случа-

* e-mail: adanijela@ptt.rs

ју неочекиваних догађаја. Свака промена у информационим системима захтева добро координирану реакцију, што је посебно важно када су информације поверљиве. Један од начина заштите поверљивости, интегритета и доступности информацијама је стандардизација информационе безбедности. Савремени информациони системи захтевају стандарде који се првенствено односе на генерисање, обраду, пријем и складиштење података, као и на информационо-комуникационе системе. Примери оваквих стандарда ISO[1]/IEC[2] 27k и NIST[3] SP 800 биће приказани у тексту који следи.

Специфичност војних организација је могућност употребе војне силе, односно чињеница да су запослени обучени да користе оружје у мирнодопским условима или у рату, обезбеђујући тако извршење одбрамбене политике. Хијерархија војне организације је стриктна и постоји обавеза поштовања правила субординације. Запослени у оваквом систему у ствари су његови припадници, а правила понашања одређена су правилима службе. Светске цивилно-војне и економско-политичке организације такође имају потребу за заштитом информација или информационих система али, пошто су њихове активности базиране на ратификованим уговорима, не примењују се стандарди за информациону безбедност, већ важе правила која су унапред одређена потписивањем споразума. Оваква правила не важе за војне организације у којима је потреба за брзим дејством (велике силе) условила стриктност.

Влада Републике Србије (у даљем тексту: РС, Србија) смернице развоја информационе безбедности одредила је у оквиру Стратегије развоја информационог друштва до 2020. године (у даљем тексту: Стратегија), што је истовремено утицало на транзиције у оквиру деловања Министарства одбране (МО) и Војске Србије (ВС). Извршена је реформа система одбране у стратешко-доктринарној, правно-нормативној и организационо-функционалној сфери. У складу с реформом система одбране реформисани су постојећи информациони системи, кроз фазе иницијализације, успоставе, контроле, реализације и одржавања система, што се користи и у процесу стандардизације.

Рад је организован на следећи начин: следеће поглавље описује појам информационе безбедности, а затим су приказане карактеристике стандарда. Четврто поглавље описује стандарде за заштиту информација у најпознатијим светским организацијама, а пето у систему одбране РС. Последње поглавље је закључак рада.

Информациона безбедност

Појам *информација* описује инструкцију, знање, упутство или обавештење, у зависности од контекста у којем се користи. Информација указује на смислену поруку која садржи чињенице из којих је могуће извести закључак, а може бити вербална, писана, штампана или дигитално записана. Са становишта савремених информационих технологија, квалитет информационо-комуникационог система одређује на који начин ће подаци бити креирани, обрађивани, складиштени и преношени, али и на који ће начин бити изведена њихова заштита и како ће они бити уништавани.

[1] ISO – International Organization for Standards.

[2] IEC – International Electrotechnical Commission.

[3] NIST – National Institute of Standards and Technology.

Информациона безбедност[4] представља сваку активност која обезбеђује заштиту информација с циљем да буде омогућен континуитет у раду и минимизиран утицај ризика и претњи по информациони систем. Информациона безбедност подразумева заштиту поверљивости, интегритета и доступности података од неауторизованог приступа, промене или уништења, уз примену контролних механизама који треба да буду унапред одређени, уграђени, надгледани, проверавани и побољшавани у реалном времену. Овакав систем по ISO/IEC 27k стандарду познат је као CIA[5] триада, коју карактерише:

– *Поверљивост – осигурати да су информације доступне само ауторизованим особама. У* основи, поверљивост представља етичке принципе дискреције који су познати и општеприсутни у нпр. медицини или праву, али важе и за пословне тајне, персоналне податке и све друге податке који не смеју да постану доступни особама којима нису намењени. Поверљивост пословања данас је базирана на принципима о минимуму информација које је потребно знати, тј. пословне тајне које су доступне запосленима одређене су минимумом знања које им је потребно за обављање конкретног задатка.

– *Интегритет – заштитити тачност и целовитост информација и процеса.* У најширем смислу интегритет одређују целовитост, временски лимит, тачност и валидност информације, што подразумева да за задате услове информација неће бити измењена у односу на њен изворни облик. Интегритет је нарушен уколико је случајно или намерно дошло до нежељених промена на релевантним подацима или у информационим системима.

– *Доступност – осигурати да ауторизоване особе увек имају приступ информацијама.* Уколико информација није доступна крајњем кориснику постоји вероватноћа да ће доћи до угрожавања задатка за који је она неопходна. ISO/IEC 27k стандард дефинише низак степен угрожености информације уколико она није доступна до 7 дана, средњи ниво од највише 48h, а максимални ниво значи чување информације 24h дневно.

Стратегија Владе Републике Србије о развоју информационог друштва

У складу са постојећим светским, али примарно европским трендовима, на основу члана 45. став. 1, Закона о Влади [1], Влада РС (у даљем тексту: Влада) 8. јула 2010. године донела је Стратегију развоја информационог друштва у Републици Србији до 2020. године [2], која је последица развоја информационо-комуникационих технологија и њиховог утицаја на трансформацију начина интеракције људи, предузећа и јавних институција у РС. Како је дефинисано Стратегијом, информациона безбедност подразумева заштиту система, података и инфра-

[4] Уместо појма информационе безбедности користе се и појмови информациона сигурност, заштита информација и безбедност информација (прим. аут.).

[5] CIA – Confidentiality (поверљивост) Integrity (интегритет) Availability (доступност).

структуре ради очувања поверљивости, интегритета и расположивости информација. Развојем информационе безбедности Влада, поред осталог, жели да постигне поверење у безбедно функционисање информационог система и заштићеност података о личности, ширење свести о неопходности спровођења мера информационе безбедности, заштиту података и информационо-комуникационих система, безбедност електронских трансакција и ефикасне механизме заштите у процесима електронске размене података. Унапређивање правног и институционалног оквира за информациону безбедност Влада је регулисала Законом о тајности података [3], Законом о заштити података о личности [4], Законом о електронском потпису [5], Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала [6], Законом о Војнобезбедносној агенцији и Војнообавештајној агенцији [7] и Кривичним закоником [8]. Наглашено је да је потребно донети прописе из области информационе безбедности којима ће додатно бити уређени стандарди информационе безбедности, као и надлежности и задаци појединих институција у овој области. Такође, потребно је формирати институцију која у области информационе безбедности треба да обавља послове верификације и сертификације метода, софтверских апликација, уређаја и система, као и истраживање и развој. Ова институција треба да надзире и примену стандарда информационе безбедности у државним органима. За подизање нивоа развоја информационе безбедности Влада је одредила још три приоритета: заштиту критичне инфраструктуре, борбу против високотехнолошког криминала и научноистраживачки рад. У вези с наведеним указно је на потребу за утврђивањем критеријума за одређивање критичне инфраструктуре, критеријума за карактеризацију напада применом информационих технологија на такву инфраструктуру и услове заштите у овој области. Такође, предвиђено је формирање посебних државних органа са функцијом борбе против високотехнолошког криминала, а значај научно-истраживачког рада огледа се у праћењу светских достигнућа, што се посебно односи на сигурност криптографских техника.

На основу наведених података из Стратегије, и званично доступних информација, осим указивања на потребу за увођењем информационе безбедности, нема тачних одредница за примарне задатке. Није указано на то шта су тачно критичне инфраструктуре, како их треба пописати, каква треба да буде координација између појединих инфраструктура, под чијом јурисдикцијом, на који начин, ко и колико често ће извештавати о резултатима рада. Такође, не постоји примењени стандард, уговор, или интерни договор за спровођење оваквих активности. Поред тога, није познато у ком временском року треба организовати институцију са задатком развоја информационог друштва до 2020. године, али је наведен низ институција и организација које треба да воде рачуна о усавршавању информационе безбедности у оквиру својих надлежности. Иако научноистраживачки тимови треба да воде рачуна о криптозаштити, указано је само на то да је промена малициозности брза и да је потребно пратити трендове. Није скренута пажња на чињеницу да малициозност прати цео информационо-комуникациони систем, што поред софтвера, хардвера, спојних путева, одговарајуће технологије и технолошких процеса подразумева и људе које учествују у ланцу заштите информација, одн. њихову едукацију и додатно обучавање.

Стандарди у области информационе безбедности

По дефиницији Института за стандардизацију Србије, стандард је „документ, утврђен консензусом и одобрен од признатог тела, којим се утврђују, за општу и вишекратну употребу, правила, смернице или карактеристике за активности или њихове резултате, ради постизања оптималног нивоа уређености у датом контексту". Стандард је, дакле, документ који настаје и развија се као резултат достигнућа у науци и техници, као и на основу искустава, односно најбољих решења из праксе, како би биле повећане ефикасност, ефективност, квалитет производа и услуга с једним циљем – изаћи у сусрет потребама корисника. Систем најбоље праксе[6] подразумева доступност, повезаност са стандардима, едукацију и сертификацију, поновљивост и рентабилност, ефективност, флексибилност, мониторинг, усаглашеност са регулативом и свеобухватност. Стандардизација у области информационе безбедности обезбеђује укључивање у међународно прихваћену праксу, управљање ризицима, смањење последица евентуалних инцидената, борбу против високотехнолошког криминала, континуитет пословања и усаглашеност правних норми. На изради српских стандарда раде стручна тела Института за стандардизацију Србије, комисије за стандарде и стручни савети, чији је основни задатак да припреме и реализују план и програм прописивања стандарда у одређеним областима, прате и учествују у раду одређених техничких радних тела међународних организација за стандардизацију, и обављају активности које су дефинисане Интерним правилима стандардизације. Поступак израде српских стандарда одвија се у фазама: (1) пројекта, (2) предлога, (3) преднацрта, (4) нацрта, (5) јавне расправе, (6) дефинитивног текста нацрта и (7) објављивања. Између бројних српских стандарда који се односе на банкарско и библиотечко пословање, заштиту животне средине, туризам, управљање енергијом, привреду и пољопривреду, рударство и нафтну технологију, металургију, геологију, дрвну индустрију, саобраћај или здравство, постоји шест стандарда који се односе на информације, комуникације или безбедност[7] Пет од тих стандарда односи се на сигурност уређаја, информационо-комуникационе технологије, повезивање и размену података и технике сигурности информационих технологија. Предмет шестог стандарда (II/32) јесте менаџмент, односно управљање подацима, што, истовремено, не подразумева и безбедност информација.

У светским размерама примат у области стандардизације имају Сједињене Америчке Државе (САД), али се стандарди примењују и у државама чланицама Европске уније (ЕУ), али и у свету.

Потребно је нагласити да је примена стандарда добровољна, а не обавезујућа, али указује другима да онај ко има лиценцу неког стандарда задовољава

[6] Best practice (енгл.)

[7] N108 – Безбедност електронских уређаја у области аудио, видео, информационе и комуникационе технологије, II/06 – Телекомуникације и размена информација међу системима, II/25 – Међусобно повезивање уређаја информационе технологије, II/27 – примена техника сигурности у информационој технологији, , II/32 – Информационе технологије – сервиси за менаџмент подацима.

критеријуме који су тачно дефинисани и познати јавности. Примена стандарда који се односе на информациону безбедност може обезбедити сигурност корисника у процес аутентификације (уколико је тестирана и доказана безбедност генерисаних кључева или криптографског алгоритма), интероперабилност, праву меру извршавања потребних операција како би информације остале заштићене, њихову доступност на захтев, проверу идентитета ауторизованих особа, ограничен приступ информацијама, и друго. За сваку од функција користе се различите технике од широко примењених криптографских метода до биометрије. Треба имати у виду да један стандард за информациону безбедност не покрива све области у којима је потребна заштита података, тако да постоји низ стандарда за функционално специфичне информационе системе, као што су нпр. ISO/IEC 15408 за интеграцију захтева за безбедност у софтверске процесе, спецификацију карактеристика производа и проверу испуњености захтева за информациону безбедност, ISO/IEC 113335 за управљање безбедношћу информационих технологија, ISO/IEC 17799 стандард за информациону безбедност који је еволуирао у стандарде ISO/IEC 27k и стандарди NIST SP 800 [9], који су описани у тексту који следи.

СтандардиISO/IEC 27k

С обзиром на то да је сваки стандард резултат отворене комуникације различитих релевантних страна, које системом глобалног приступа проблему размењују позитивна и негативна искуства из праксе, исто важи и за стандарде из групе ISO/IEC 27k [10], [11], за управљање системом заштите информација – ISMS.[8] Три стандарда ISO/IEC 27000,[9] ISO/IEC 27001[10] и ISO/IEC 27002[11] описују терминологију, начин увођења система за заштиту информација и сам систем заштите, респективно. Међутим, серија ISO/IEC 27k покрива широк спектар тема, не само приватност, поверљивост и доступност информацијама или техничка питања безбедности. Стандард је конципиран тако да свака организација, без обзира на величину и делатност, може да процени безбедносне ризике и спроведе адекватне мере у складу са својим потребама, користећи унапред задате смернице и препоруке. Концепт управљања безбедношћу информација обухвата правила која се односе на информациону безбедност, управљање ризицима, размену повратних информација о систему и унапређење активности менаџмента за реакцију на нежељене догађаје. Активности за увођење система за управљање безбедношћу информација изводе се у PDCA[12] циклусу, у фазама (1) планирај, (2) уради, (3) провери, (4) делуј, што је приказано на слици 1.

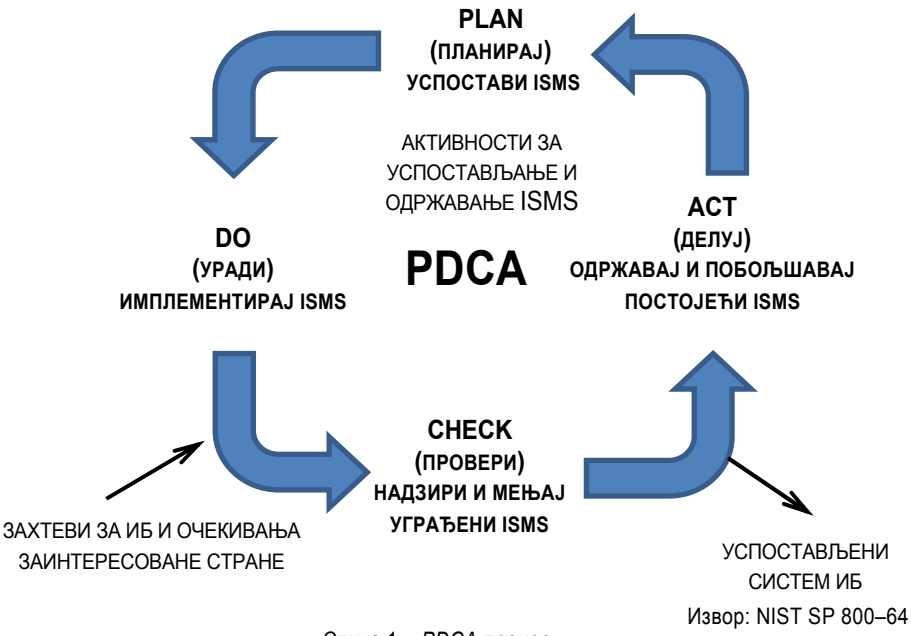
[8] ISMS - Information Security Management Systems (енгл.).

[9] ISO/IEC 27000 - ISMS – Преглед и речник.

[10] ISO/IEC 27001 - ISMS – Захтеви за систем управљања безбедношћу информација.

[11] ISO/IEC 27002 - ISMS – Начин примене.

[12] PDCA – Планирај–уради–провери–делуј.



Извор: NIST SP 800–64

Слика 1 – *PDCA процес*

Стандарди ISO/IEC 27k за управљање безбедношћу информација припадају једној од следећих група:

(1) *ISO/IEC 27000 – ISMS – Overview and vocabulary* – обезбеђује преглед и увид у фамилију ISO/IEC 27k стандарда. У овом стандарду прецизно је дефинисано шта који термин значи, које су скраћенице и шта терминолошки није дозвољено.

(2) *ISO/IEC 27001 – ISMS – Requirements* – даје формалну спецификацију система управљања, односно захтеве за добијање лиценце за ISO/IEC 27k стандард. За испуњене захтеве подразумевано је да организација може бити проверавана, у складу са стандардом који обезбеђује модел за успостављање, имплементацију, руковање, надзор, ревизију, одржавање и побољшање система за управљање информацијама. Дизајн и имплементацију система за сваку организацију одређују њени захтеви за безбедности, као и пословни процеси, величина и структура. Стандард дефинише примену процесних система унутар организације, укључујући и идентификацију и интеракцију ових процеса и управљање. Иако организације углавном имају контролу безбедности информација, без имплементираног система за управљање безбедношћу, контрола је често интерно успостављен систем или примена договорених конвенција, што указује на чињеницу да су аспекти информационе безбедности само делимично покривени, што не важи за стандарде. При увођењу стандарда ISO/IEC 27001 менаџмент треба:

1. да систематски процењује ризике по информациону безбедност,
2. осмисли свеобухватан пакет контрола информационе безбедности и
3. усвоји свеобухватан поступак управљања, како би осигурали континуитет у примени мера информационе безбедности.

(3) *ISO/IEC 27002 – Code of practice for ISMS* – стандард одређује опште принципе за планирање, имплементацију и побољшање система за управљање информацијама. Контроле наведене у стандарду намењене су за проверу специфичних захтева за информациону безбедност, што је одређено на основу процене ризика. Стандард, такође, обезбеђује упутства за ефективно управљање безбедношћу информација у пракси, као и помоћ менаџерима при успостављању односа поверења између организација. ISO/IEC 27002 се дели на 12 области:

1. процена ризика,
2. политика безбедности,
3. организовање система управљања безбедношћу информација,
4. управљање имовином – инвентар и класификација средстава везаних за информације,
5. људски ресурси (аспекти информационе безбедности који су одређени запошљавањем кадра, променом радног места или напуштања организације),
6. физичко обезбеђење објеката у којима се налази ИТ-базирана технологија,
7. комуникације и оперативни менаџмент, тј. управљање контролама техничке безбедности рачунарских система и мрежа,
8. контрола и ограничење права приступа рачунарским мрежама, системима, апликацијама, функцијама и подацима,
9. обнављање, развој и одржавање информационих система уграђивањем безбедоносних елемената и апликација,
10. управљање инцидентима везаним за информациону безбедност (предвиђање и адекватне реакције на нарушавање система информационе безбедности),
11. управљање пословним континуитетом и
12. усаглашеност политике информационе безбедности са стандардима и законима.

(4) *ISO/IEC 27004/5/6/7* – ова четири стандарда изведена су из претходна три, а значајни су због могућности примењене у реализацији захтева за информациону безбедност из Стратегије; обезбеђују метричке методе, тј. процену ефикасности имплементираног система за управљање информацијама (ISO/IEC 27004[13]), процену ризика (ISO/IEC 27005[14]), акредитацију организација које ће издавати лиценце (ISO/IEC 27006[15]) и ревизију система (ISO/IEC 27007[16]).

NIST SP 800

NIST[17] је национална институција САД, чија је основна функција да прописује стандарде и врши њихову ревизију. Циљ NIST-а је увођење стандарда за продуктивно коришћење информационих технологија, што укључује развој техничких, физичких, административних и управљачких стандарда, и смернице за безбедност

[13] ISO/IEC 27004 – Управљање информационом безбедношћу – мерења.

[14] ISO/IEC 27005 – Управљање ризицима по информациону безбедност.

[15] ISO/IEC 27006 – Захтеви за ревизорска и сертификациона тела.

[16] ISO/IEC 27007 – Упутство за ревизију система управљања безбедношћу информација.

[17] National Institute of Standards and Technology (енгл.) – Национални институт за стандарде и технологију.

осетљивих информација, примарно у државним информационим системима, али и у индустрији, владиним институцијама и академским организацијама. Серија NIST SP 800 је резултат истраживања који су резултирали упутствима за примену постојећих и развој нових мера безбедности информационих система у пракси [12]. Интеграција, која је позната као SDLC (System Development Life Cycle[18]), изводи се кроз фазе: (1) иницијације, (2) развоја/успоставе система, (3) имплементације/провере, (4) одржавања и (5) завршних активности (пуштање новог информационог система у рад). Специјална издања NIST-а која се директно односе на информациону безбедност су: NIST SP 800–30, NIST SP 800–53 и NIST SP 800–64.

(1) *NIST SP 800–30 – Computer Security – Risk Management Guide for Information Technology Systems*[19]

Управљање ризиком омогућује организацији да постигне задате циљеве на следећи начин: (1) квалитетним обезбеђењем система који су базирани на информационим технологијама у којима се складиште, обрађују или преносе информације везане за организацију, (2) потребно је омогућити менаџменту да доноси одлуке које су резултат добро процењених ризика (у складу са буџетом), и (3) треба да постоји подршка менаџменту при акредитацији система и ауторизацији, што подразумева и одговарајућу документацију. Стандард је намењен ауторитетима који доносе одлуке, програмерима, особама које су задужене за безбедност информација, консултантима и ревизорима, и особљу техничке подршке. Процена ризика базирана је на идентификацији претњи и рањивости одређеног система, контроли и анализи ризика, одређивању вероватноће да неочекивани или нежељени догађај наруши информациону безбедност, анализи могућег утицаја таквог догађаја на информациони систем, опису препорука за смањење ризика и резултирајућој документацији. Поред тога, стандардом се одређују мере и стратегије за смањење ризика и избегавање потенцијалних криза које могу нарушити информациону безбедност.

(2) *NIST SP 800–53 – Information Security - Recommended Security Controls for Federal Information Systems and Organizations*[20]

Стандард даје препоруке за контролу безбедности у државним информационим системима и организацијама. Контрола информационог система је неопходна, јер је конзистентност основа функционисања организације. У овом случају постоји неколико питања везаних за контролу на која менаџмент треба да одговори када успоставља заштиту информационих система: (1) Шта је потребно за адекватну процену ризика, који су везани за информације или информационе системе, а који би могли да наруше пословање или функције организације? (2) Да ли је уведена контрола безбедности и постоји ли реалан план за њено увођење? (3) Колики ниво безбедности (најнижи степен поверљивости) може бити постигнут, уколико се примењују изабрани контролни механизми? Додатно, одговоре на ова питања не треба посматрати изоловано, већ у контексту примене ефикасног система заштите ин-

[18] Животни циклус развоја система.

[19] *З*аштита рачунара – Водич за управљање ризицима за системе за заштиту информација.

[20] Безбедност информација – Препоруке за контролу безбедности за федералне информационе системе и организације.

формација који, поред замисли и договора на нивоу одговорних особа, треба да прати и документација. Стандард SP 800–53 даје смернице које помажу менаџменту да из понуђених механизама изабере онај начин контроле информационог система који одговара партикуларној организацији.

Контрола је организована у 17 фамилија, које описују функционалност система. Контроле се сврставају у четири групе: (1) управљање ризицима, (2) категоризација информационе безбедности у зависности од поверљивости, интегритета и доступности информацијама, (3) спецификација конкретних контролних механизама и (4) надзор. Поред наведеног, постоје и три класе контроле: (1) управљање (контрола приступа и ауторизације, планирање, процена ризика, надзор система, програм менаџмент), (2) операционална употреба (едукација и тренинг, управљање конфигурацијом, планирање реакције и одговор на инциденте, одржавање, физичка заштита, безбедност персонала, интегритет информација и система) и (3) технике (приступа, надзора, идентификације, аутентификације, заштита система и комуникација) [13].

(3) *NIST SP 800–64 – Information Security – Security Considerations in the System Development Life Cycle*[21]

Специјално издање NIST SP 800–64 служи федералним агенцијама да интегришу основне безбедносне активности у своје информационе системе. Ово издање служи као водич за имплементацију информационе безбедности: (1) лицима задуженим за управљање информационим системом, (2) званичницима организације, (3) лицима задуженим за развој информационог система и (4) лицима задуженим за имплементацију информационе безбедности [14]. SP 800–64 базиран је на управљању ризицима, што подразумева процену најосетљивијих/најслабијих тачака у систему, идентификацију критичних процеса или операција и процену рањивости ради смањења или избегавања утицаја малициозности, кварова и случајних или намерних грешака персонала. SDLC обезбеђује и да свака фаза у имплементацији мера заштите буде документована, што убрзава евентуалне промене у успостављеном систему. Свака фаза у стандарду описана је прецизно како би била обезбеђена разумљивост читаоцу. Наведене су њене почетне и крајње тачке, а описано је на који начин је дозвољен прелаз из једне фазе у другу и шта могу бити узроци евентуалног прекида SDLC-а. Свака од фаза треба да буде део флексибилног система који важи за одређену организацију. Прилагодљивост организацији омогућава постојање интерних правила заштите информационих система. Безбедност је примарна, па мора да постоји начин континуалне провере квалитета информационог система, а једном идентификовани ризици треба да буду потпуно познати свима. У иницијалној фази потребно је да постоји опис основних активности сваке од следећих фаза, с посебним осврtом на оно што је неопходно да се реализују постављени задаци. Потребно је поставити (очекиване) циљеве са сугестијама о томе како их реализовати или, уколико је неопходно, како променити правац деловања. У свакој фази мора да постоји повратна спрега у систему извештавања. Резултат активности мора бити познат менаџменту који имплементира мере безбедности, што повлачи информисаност и добру комуникацију између сарадника, тј. обезбеђује синхронизацију. На крају, неопходно је да нема колизије у реализацији задатака.

[21] Безбедност информација – Животни циклус развоја система са становишта безбедности.

Информациона безбедност као стандард светских унија

И поред стандарда који се примењују уколико је потребно заштитити информације или информационе системе, постоји низ организација и институција у свету које су, често и пре настанка ових стандарда, усвајале заједничка правила о информационој безбедности. Ове организације базиране су на кооперацији више заинтересованих страна, а основа њиховог постојања је споразум који важи за све. Често се у њиховим именима могу срести називи као што је унија, заједница, савез или друштво, нарочито код организација које делују на глобалном нивоу. Најпознатији примери оваквих савеза су Организација уједињених нација (ОУН), ЕУ, НАТО[22] и Организација за европску безбедност и сарадњу (ОЕБС). Занимљиво је, међутим, да велики број организација које делују на основу принципа потписивања заједничких споразума не прецизира начин на који ће штитити информације. Код војних организација, као што је НАТО, прецизирани су сви стандарди и правила деловања за заштиту информација или информационих система, без обзира на то да ли се ради о процесуирању података, процесима за одржавање система, степену тајности података или физичкој заштити. Код економско-политичких савеза, чак и кад они имају могућност војне интервенције, као што је нпр. ОУН, ови подаци изостају; споразуми указују на добровољност и поштовање принципа, али не и на обавезу заштите информација и информационих система. Безбедност се подразумева, па је, у општем случају, сваку информацију могуће учинити доступном појединцу или јавности. Из тог разлога свака држава-чланица организације треба тачно да одреди које информације могу, а које никако не смеју да постану широко доступне. Наиме, иако је приступ организацији добровољан, уговор о поштовању правила је обавезујући. И поред наведеног, свака добровољност ипак не подразумева и неаутономност државе чланице, већ напротив. Заједнички интереси су важни, али аутономност држава чланица, у ствари, потиче варијабилност, а самим тим и квалитет донетих одлука. У тексту који следи приказане су карактеристике четири најпознатије светске организације, које функционишу на овај начин.

Организација уједињених нација

Принципи савремене ОУН датирају још од 1942. године, а Повеља УН ратификована је у Сан Франциску 26. јуна 1945. године. Иако настала још у периоду Другог светског рата збуњује чињеница колико је ОУН модерна и призната данас, што је евидентно са становишта њене распрострањености и утицаја у свету. Главни органи ОУН су Генерална скупштина, Савет безбедности (у даљем тексту: Савет), Економски и социјални савет, Старатељски савет, Међународни суд и Секретаријат. Генерална скупштина разматра начела опште сарадње у очувању мира и безбедности и може, у погледу тих начела, да даје препоруке члановима ОУН или Савету. Савет је орган УН за брзе и ефикасне акције при одржавању међународног мира и безбедности. С обзиром на чињеницу да Савет ради уз помоћ Комитета војног штаба, за сваку

[22] НАТО – North Atlantic Treaty Organization.

акцију ОУН потребно је да гласа девет од 15 његових сталних чланица. Повеља ОУН обавезује сваку од држава чланица да стави на располагање Савету своје оружане снаге, одобре право проласка јединицама, пруже помоћ и дају олакшице.[23]

У складу са Повељом ОУН, термин *информациона безбедност* не налази се ни у једном члану оригиналне повеље, док се термин *безбедност* среће искључиво у оквиру оних чланова који се односе на очување међународног мира и безбедности.

Европска унија

Европска унија је економски и политички савез 27 држава чланица, које су потписнице Лисабонског споразума из 2009. године. Први споразум на којем је заснована данашња ЕУ потписан је педесетих година прошлог века и њиме је одређен основни принцип функционисања који важи и данас – саодлучивање. Оно подразумева постојање Европског парламента (у даљем текст: Парламент), поред којег делују још три институције и тела ЕУ: Европски савет, Европска комисија и Суд правде. Иако у основи монетарна унија, циљ ЕУ је остваривање владавине права и демократије, усвајање закона и контрола генералне економске политике држава чланица, предлагање и обезбеђивање примене нове политике и решавање спорова. Политика ЕУ утиче на бројне области живота, као што су спољна трговина и унутрашње тржиште, конкуренција, фондови, правосуђе, спољна политика, здравство, итд. Поред саодлучивања, ЕУ се такође придржава принципа субсидијарности, односно не меша се у области локалне политике, осим ако су мере ЕУ делотворније од мера на националном, регионалном или локалном нивоу. Због тога информациона безбедност није примарна у ЕУ, него је остављена државама чланицама.

НАТО

За велики систем, као што је НАТО, могло би се очекивати да информациону безбедност третира кроз оквир савремених технологија, што је у принципу тачно. Међутим, основе заштите информација и информационих система НАТО-а настале су првим потписивањем уговора између будућих чланица, у априлу 1949. године. У декларацији, поред осталог, пише да се потписнице уговора обавезују на: „међусобну заштиту поверљивих информација које морају бити размењиване између влада држава-чланица, а оквир деловања утврђен је кроз увођење стандарда за заштиту и, уколико је захтевано, одређених процедура“ [15]. По амандманима из 2002. године НАТО дели приоритете заштите на седам области: уговори о безбедности, основни принципи безбедности, заштита персонала, физичка заштита, информациона безбедност, INFOSEC и индустријска безбедност. Информација је дефинисана као: „свако знање којим се може комуницирати у било ком облику“, поверљива информација је: „информација или материјал за које је потребна заштита од неауторизоване промене, при чему реч ’материјал’ укључује документе, маши-

[23] Текст је преузет из Повеље Уједињених нација (прим. аут.).

не, пратећу опрему или оружје који су финални производ или се налазе у процесу производње, а реч 'документ' подразумева записану информацију без обзира на њену физичку форму или карактеристике што укључује писани или штампани материјал, податке који се налазе на картицама, тракама, мапама, графиконима, фотографијама, сликама, радним белешкама, као и звук, глас, магнетни, електронски, оптички или видео запис у било којој форми, преносива опрема и рачунари, итд.".

Основни принципи стандарда информационе безбедност за НАТО чланице односе се на цивилна и војна тела, а стандарди се користе за заштиту поверљивости, интегритета и доступности информацијама од значаја. Принципи се примењују на поверљиве податке који важе за НАТО, информације које НАТО прима од других извора и информације о НАТО-у до којих могу доћи особе од поверења (консултанти, сарадници из индустрије или са универзитета). Информациона безбедност подразумева примену општих мера и процедура безбедности ради превенције, детекције или реконструкције информација након њиховог губитка или компромитације, уколико се то десило у периоду када је информација била поверљива. Степен мера заштите зависи од важности информација, које су класификоване на: Cosmic – строго поверљиво, НАТО тајна, НАТО поверљиво, НАТО са ограниченим приступом и НАТО доступно без ограничења[24]. INFOSEC је примена мера информационе безбедности како би се заштитиле поверљиве информације у току обраде, преноса или складиштења да се спречи губитак поверљивости, интегритета и доступности, без обзира на то да ли се ради о малициозној намери или случајности.

У фебруару 2005. године НАТО је донео Директиву о безбедности информација, са допунама претходних директива о безбедности информација и информационих система, у којој су додати нови елементи информационе безбедности, у складу са променама на глобалном нивоу. Директивом се описују: класификација и означавање информација, контрола и рад са информацијама, репродуковање, пренос и екстраховање информација, ширење и пренос информација физичким путем, пријем и запис информација, њихово излагање и уништавање, кршење правила, закона, споразума и договора, и начин на који ће поверљиве информације постати доступне интернационалним организацијама или државама које нису чланице НАТО-а [16]. Поред тога, допуна је изведена и на пољу INFOSEC-а, у девет категорија: улога и одговорност INFOSEC-а, дозволе или акредитације за безбедност, управљање ризицима, документација везана за све аспекте безбедности, верификација имплементације свих захтеваних параметара пре издавања дозволе или акредитације, провера после добијања дозвола или акредитација, процена рањивости, дозволе или акредитације за интерконекције и генерални аспекти INFOSEC-а [17].

Партнерство за мир[25] је политичко-војни програм НАТО-а за билатералну сарадњу НАТО-а са евроатлантским државама. Програм омогућује да свака од држава, у складу са својим приоритетима, оствари сарадњу са НАТО-ом. Сврха овог програма је да се повећа стабилност, смање претње миру и ојачају безбедносне везе између партнерских земаља и НАТО-а. Сарадња се, поред осталог, усредсређује на комуникације и информационе системе, управљање кризама и планирање у случају ванредних ситуација. Србија је програму Партнерство за мир приступила у децембру 2006. године.

[24] Cosmic (Top Secret), НАТО Secret, НАТО Classified, НАТО Restricted, НАТО Unclassified, респективно.
[25] Partnership for Peace (PfP), (енгл.).

ОЕБС

Организација за европску безбедност и сарадњу[26] је унија 56 земаља Европе, Северне Америке и Азије, и представља највећу организацију за регионалну безбедност. Она нуди могућност за мирно решавање криза (рана упозорења, превенција конфликата, кризни менаџмент и помоћ након конфликата), обухватајући политичко-војне и економске циљеве, као и деловање са аспеката људских права. Поред осталог, ОЕБС покрива области као што су: контрола наоружања, контрола границе, борба против тероризма, економске активности, избори, родна равноправност, заштита мањина, људска права, слобода медија, толеранција и едукација, државне реформе и реформе полиције. Међутим, није описан начин на који се изводи заштита информација, иако ове реформе подразумевају нпр. заштиту података о личности, заштиту поверљивих информација, степеновање докумената по тајности, итд. Због тога, у оним областима које подразумевају војне и државне тајне или персоналне податке, ОЕБС треба да буде посматран као саветодавна организација.

Мисија ОЕБС-а у Србији промовише демократске стандарде и принципе једнакости, а један од кључних приоритета је подршка развоју професионалних медија који грађанима, на објективан и тачан начин, треба да пруже информације од јавног значаја. Формирана је канцеларија Повереника за информације од јавног значаја која сарађује са мрежом невладиних организација како би била обезбеђена примена Закона о слободном приступу информацијама од јавног значаја. Са становишта информационе безбедности, циљ ове канцеларије је инсистирање на усвајању закона о заштити личних података и о класификованим информацијама.

Информациона безбедност и реформа система одбране

Визија система одбране заснива се на визији савремене и модерне Србије, чланице ЕУ, интегрисане у колективне системе безбедности, са војском која својом снагом може да гарантује мир и стабилност у региону и учествује са својим капацитетима у очувању регионалног и глобалног мира. Државе југоисточне Европе, следећи свој приоритетни заједнички интерес да испуне потребне услове за прикључење ЕУ, улажу узајамно поверење и преузимају свој део одговорности за безбедност заједничког простора и доприносе његовом укупном развоју. Регионална безбедност се у све већој мери заснива на заједничким и усаглашеним активностима у области безбедности, политике и економије, и у другим областима усмереним на очување стабилности и предупређивање криза у региону. У том смислу, циљеви политике одбране Србије су стварање ефикасног система одбране, мир и повољно безбедносно окружење, као и интеграција у европске и друге међународне безбедносне структуре. У остваривању тих циљева МО спроводи реформу ради изградње ефикасног система одбране, његовог стабилног функционисања и стварања усло-

[26] OSCE – Organization for Security and Co-operation in Europe (енгл.).

ва за интероперабилност са системима одбране држава укључених у европске безбедносне структуре и НАТО програм Партнерство за мир [18].

Реформа система одбране одвија се у три компатибилне сфере: стратешко-доктринарној, правно-нормативној и организационо-функционалној [19]. Стратешко-доктринарни основ чине Стратегија националне безбедности Републике Србије и Стратегија одбране Републике Србије из 2009. године. Стратегија националне безбедности Републике Србије одређује њена опредељења за поштовање Повеље УН, јачање улоге ОУН, ОЕБС-а и ЕУ, евроатлантске интеграције и учешће у НАТО програму Партнерство за мир [20]. Стратегија одбране Републике Србије представља основу за уређење система одбране и функције одбране државе. Основна начела функционисања система одбране су јединство, непрекидност, ефективност, поузданост, ефикасност, професионалност, прилагодљивост, свеобухватност, кооперативност, транспарентност и интероперабилност. Начела функционисања система одбране заснована су на основним уставним и законским одредбама, међународном праву, као и другим подзаконским актима [21]. Поред тога, Законом о тајности података уређен је јединствен систем заштите тајности података који су од интереса за националну и јавну безбедност, одбрану, унутрашње и спољне послове РС, заштите страних тајних података, приступ тајним подацима и престанак њихове тајности, надлежности органа и надзор над спровођењем овог закона, као и одговорност за неизвршавање обавеза из овог закона, и друга питања од значаја за заштиту тајности података. У уређивању система одбране, са становишта заштите информација, учествују како органи МО, тако и јединице ВС.

У оквиру МО ове задатке обављају Војнобезбедносна агенција (ВБА) и Војнообавештајна агенција (ВОА), чији је рад дефинисан Законом о Војнобезбедносној агенцији и Војнообавештајној агенцији и подзаконским актима за његово спровођење. ВБА обавља послове који се, поред осталог, односе и на заштиту тајности података, безбедност информационих система и рачунарских мрежа, телекомуникација и криптозаштите. Такође, ВОА је надлежна за обављање обавештајних послова од значаја за одбрану који се односе на прикупљање, анализу, процену, заштиту и достављање података и информација о потенцијалним и реалним опасностима, активностима, плановима или намерама страних држава и њихових оружаних снага, међународних организација, група и појединаца.

У оквиру ВС делују Бригада везе (у даљем тексту: Бригада) и 210. батаљон везе. Специфичност Бригаде огледа се у томе да свој најважнији задатак – обезбеђење и размену информација у МО и ВС, извршава на исти начин непрекидно и у рату и у миру. Своје задатке Бригада реализује на целој територији РС, извршава велики број комплексних задатака из области телекомуникационог и информационог обезбеђења, и заштите говорних и писаних информација за потребе МО и ВС. Најважнији задаци Бригаде су остваривање јединствене команде и непрекидности веза, заштита свих информација и интеграција система веза са другим телекомуникационим системима у земљи. Двесто десети батаљон везе намењен је да опслужује елементе стационарног центра везе Команде Ваздухопловства и противваздухопловне одбране (В и ПВО), поставља покретни центар везе и реализује телекомуникационо и информационо обезбеђење за потребе В и ПВО у миру, ванредним условима и рату, обезбеђујући непрекидност система и заштиту информација.

Велику улогу у развоју информационих система уопште, и система за заштиту података у ужем смислу, има и научноистраживачки рад. Због тога је МО извршило реформе и у организационо-функционалној структури нових научноистраживачких институција, што је приказано на слици 2.

Слика 2 – *Организациона структура војних научних институција у МО*
(Извор: Бела књига одбране Републике Србије)

У области истраживања и развоја система информационе безбедности делује Центар за примењену математику и електронику (ЦПМЕ), који је јединствена, специјализована истраживачко-развојна установа у области криптозаштите. ЦПМЕ је организационо и функционално везана за Управу за телекомуникације и информатику (УТИ) (J-6) Генералштаба ВС. ЦПМЕ се, за потребе МО, ВС и других функционалних система криптозаштите у Републици Србији, бави: (1) истраживањем, развојем и верификацијом криптолошких алгоритама, (2) развојем и имплементацијом криптолошких алгоритама у телекомуникационим и информационим системима домаће и стране производње, (3) истраживањем и развојем нових, одржавањем и модернизацијом постојећих хардверских и софтверских криптолошких решења, (4) пројектовањем решења и дефинисањем критеријума за заштиту од компромитујућег електромагнетног зрачења на уређајима и системима криптозаштите, (5) генерисањем, израдом и дистрибуцијом криптопараметара и специјалних докумената криптозаштите и (6) издавањем електронских сертификата и персонализацијом електронских идентификационих докумената.

Правила се, на пољу информационе безбедности, мењају у складу са променом правила и увођењем стандарда у светске војне организације, што је примењено и на реформу система одбране. Постојеће доктрине, и правна акта која их прате, део су иницијалне фазе – фазе планирања, док је реформа организационе структуре почетак фазе реализације. У наредном периоду, са становишта информационе безбедности, биће реализована и проверавана заштита информационо-комуникационих система, и одржаван у раду постављени систем. На овај начин и активности МО и ВС одговарају процесима стандардизације, што је, финално, у складу са Стратегијом Владе и задовољава циљеве за сарадњу са ОУН, ЕУ, НАТО и ОЕБС.

Закључак

Број стандарда који служе као смернице за постизање оптималног нивоа функционалности одређеног система расте из дана у дан. Овај раст условљен је активностима које су резултат развоја савремене технологије и технолошких процеса, као и глобализације у општем смислу. Основу стандарда чине добровољност, искуства из праксе, поштовање задатих услова и редовна ревизија, а постојање лиценце указује на чињеницу да организација задовољава критеријуме на које се стандард односи. На исти начин примењују се стандарди за информациону безбедност, као што су ISO/IEC 27k и NIST SP 800. Заштита информација у оквиру ових стандарда подразумева поверљивост, интегритет и доступност, а, осим на информације, стандарди се примењују и на информационо-комуникационе системе. Међутим, примена стандарда није увек добар основ за постизање захтева одређене организације, па је чест случај да се примењују интерна правила или, у случају сарадње више организација, правила која настају као резултат договора између заинтересованих страна. Велики број организација у свету настао је потписивањем конвенција о заједничкој сарадњи, у којима су прецизно дефинисана права и обавезе сваке чланице. У организацијама које у својој основи немају могућност примене силе, информациона безбедност није примарна и често је остављена локалним властима. Код организација које имају могућност примене војне силе стандарди и поштовање правила су обавезни.

Србија сарађује са ОУН, ЕУ, НАТО-ом и ОЕБС-ом, који имају своје стандарде и правила везана за информациону безбедност, па је, у складу са својим циљевима, донела стратегије развоја у различитим областима друштвеног живота. Поред осталих, промене су неопходне у институцијама и организацијама државе, цивилног и приватног сектора. На основу директива Владе, МО изводи реформу система одбране у стратешко-доктринарној, правно-нормативној и организационо-функционалној сфери, што је поткрепљено Стратегијом националне безбедности Републике Србије и Стратегијом одбране Републике Србије. Стратегијама су одређена опредељења Србије за поштовање Повеље УН, јачање улоге ОУН, ОЕБС-а и ЕУ, евроатлантске интеграције и учешће у програму Партнерство за мир.

Литература

[1] Закон о Влади, *Службени гласник Републике Србије* бр. 55/05, 71/05-исправка, 101/07, 65/8, 2008.

[2] Стратегија развоја информационог друштва у Републици Србији до 2020. године, *Службени гласник Републике Србије* бр. 5/2010, 2010.

[3] Закон о тајности података – Указ о проглашењу, *Службени гласник Републике Србије*, бр. 104/2009, 2009.

[4] Закон о заштити података о личности, *Службени гласник Републике Србије*, бр. 97/08, 2008.

[5] Закон о електронском потпису, *Службени гласник Републике Србије*, бр. 51/2009, 2009.

[6] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, *Службени гласник Републике Србије*, бр. 61/2005, 104/2009, 2009.

[7] Закон о Војнобезбедносној агенцији и Војнообавештајној агенцији, *Службени гласник Републике Србије*, бр. 88/2009, 2009.

[8] Кривични законик, *Службени гласник Републике Србије*, бр. 85/2005, 88/2005 – испр., 105/2005 – испр. 72/2009 и 11/2009, 2009.

[9] Mellado D., E. Fernandez-Medina, M. Patini: A common criteria based security requirements engineering process for the development of secure information systems. *Computer Standards & Interfaces* 29 (2007) pp 244–253, 2007. Доступно на web сајту: www.sciencedirect. com

[10] ISO/IEC 27001:2005. Information technology – Security techniques – Information security management systems, 2005.

[11] ISO/IEC 27002:2005. Information technology – Security techniques – Code of practice for information security management, 2007.

[12] Stonenburner G., A. Goguen, and A. Feringa: Risk Management Guide for Information Technology Systems. Recommendation of the National Institute of Standards and Technolgy. *NIST Special Publication 800–30*, 2002.

[13] Information Security, Recommended Security Controls for Federal Information Systems and Organizations. *NIST Special Publication 800–53*. Revision 3, 2009.

[14] Information Security. Security Considerations in the System Development Life Cycle. *NIST Special Publication 800–64*. Revision 2, 2008.

[15] Security within the North Atlantic Treaty Organization (HATO). North Atlantic Council. HATO Unclassified Document C-M(2002)49, 2002.

[16] Directive on the Security of Information, AC/35-D/2002-REV2, HATO SECURITY COMMITTEE, 2005.

[17] INFOSEC Management Directive for CIS, AC/35-D/2005-REV1, 2006.

[18] Бела књига одбране Републике Србије. Медија центар „Одбрана“, 2010.

[19] Форца, Б.: Стратешки менаџмент у систему одбране, *Војно дело*, стр. 196–220. Министарство одбране Републике Србије. Медија центар „Одбрана“, зима/2011, година LXIII, 2011.

[20] Стратегија националне безбедности Републике Србије, 2009.

[21] Стратегија одбране Републике Србије, 2009.