Анђелија ЂУКИЋ, МА[22]
Институт за стратегијска истраживања,
Универзитет одбране у Београду
Др Дејан ВУЛЕТИЋ[23]
Институт за стратегијска истраживања,
Универзитет одбране у Београду

ДОИ: 10.5937/bezbednost2203140D
УДК: 006.065:004.056
Прегледни научни рад
Примљен: 31. 8. 2022. године
Ревизија: 8. 6. 2022. године
Датум прихватања: 12. 12. 2022. године

Основи информационо-безбедносне културе у организацији

Апстракт: *Масовна примена информационо-комуникационих технологија (ИКТ) у организацијама утицала је на повећање њихове рањивости и условила развој функције информационе безбедности. Напади на ИКТ системе све више укључују људе као потенцијалне мете угрожавања, што је створило потребу да се понашању запослених у интеракцијама са елементима ИКТ система и његовим окружењем посвети значајна пажња, и да се изграђује информационо-безбедносна култура (ИБК) као интегративна компонента организационе културе и значајан фактор информационе безбедности. У раду је учињен покушај да се постави свеобухватан концепт ИБК заснован на јединству знања, перцепција, уверења и ставова запослених и њихової усклађеної поступања при примени мера безбедности. Идентификовани су најзначајнији спољни и унутра-*

22 andjelija.djukic@mod.gov.rs. Чланак је резултат рада на научноистраживачком пројекту „Физиономија савремених оружаних сукоба" који се реализује на основу Плана научноистраживачке делатности у МО и ВС.

23 dejan.vuletic@mod.gov.rs. Истраживање спроведено уз подршку Фонда за науку Републике Србије, број пројекта 2803/2021, Management of New Security Risks-Research and Simulation Development – NEWSIMR&D.

шњи фактори утицаја на ИБК, које карактеришe њихова узрочно-последична повезаност, а чији значај и интензитет су променљиви током времена и фаза развоја организације. Међу факторима се по улози и значају издваја менаџмент највишег нивоа због највеће одговорности за информациону безбедност организације, као креатор њене стратегије и политике и носилац политике ангажовања ресурса и осмишљавања и реализације програма за подизање нивоа информационо-безбедносне културе.

Кључне речи: *организациона култура, информациона безбедност, информационо-безбедносна култура, менаџмент, свест о безбедности информација.*

Увод

Развој информационо-комуникационих технологија (ИКТ) донео је многе добробити целокупном човечанству. Увођењем рачунарске технологије и стварањем великих ИКТ система повезаних на интернет, омогућен је приступ огромним количинама и различитим изворима информација, као и успостављање контаката на глобалном нивоу (Вулетић, 2015: 272). Истовремено је повећана њихова рањивост на неовлашћено коришћење, крађу и модификацију података и информација, пословну шпијунажу и деловање високотехнолошког криминала (Đukić, 2018: 128). Нарушавање информационе безбедности организације може да угрози њено функционисање, нанесе финансијске губитке, смањи углед или изазове губитак интелектуалне својине и послова. У доба пандемије ковида 19 и повећања обима „рада од куће", често помоћу личних уређаја без стандардне заштите, повећани су ризици од напада на информационе ресурсе организација, што је повећало захтеве за едукацијом и изградњом свести запослених у организацијама.

Због угрожавања ресурса и интереса организација, информациона безбедност је постала значајна функција која захтева свеобухватност и сталност деловања кроз анализу претњи, дефинисање политике заштите, формализовање и примену протокола, ангажовање финансијских ресурса, примену нових хардверских и софтверских решења и стални процес стицања знања и изградње свести запослених о безбедном понашању. Истраживања показују да су организације и даље недовољно спремне за супротстављање

нарастајућем броју софистицираних претњи у сајбер простору, делимично и због неспособности и необучености запослених, који се све масовније користе за приступ подацима. То је иницирало и повећање броја истраживања информационе безбедности из људске перспективе као критичног ресурса за успех у заштити информационих тековина, где се поред потребних специфичних знања запослених, у фокус истраживања ставља информационо-безбедносна култура (ИБК) (information security culture).

Циљ овог рада је да се прикажу основе концепта ИБК као значајног интегралног елемента организационе културе неопходног за успешно функционисање информационе безбедности организације. Основни оквир информационе безбедности организације, у који су интегрисани сви битни елементи заштите, чине стратегија и политика, технологија, организованост, људи и окружење, укључујући и сајбер простор. То представља и основни оквир за разумевање и изградњу ИБК. Учињен је покушај да се постави свеобухватни концепт ИБК заснован на јединству знања, перцепција, уверења и ставова запослених и њиховог усклађеног поступања при примени мера безбедности, са израженом улогом менаџмента највишег нивоа, у складу са важећим међународним стандардима у овој области.

Информациона безбедност

Доминантно гледиште на информациону безбедност у литератури садржано је у ЦИА тројству (*CIA triada)*: заштита поверљивости (*confidentiality – C*), интегритета (*integrity – I*) и расположивости (*availability – A*) информација. Поред ЦИА тројства, појединим одређењима се обухватају и други елементи, као што су аутентичност, непорецивост и поузданост података (ISO/IEC, 2018). На тај начин је информациона безбедност дефинисана и у законодавству Републике Србије, по којем „представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица" (Закон о информационој безбедности, 2016: чл. 2 т. 3). У ширем смислу, инфор-

мациона безбедност организације представља укупну безбедности ИКТ система који функционишу у сајбер простору и односи се на безбедносне ризике повезане са употребом ИКТ, укључујући безбедност података, уређаја, информационих система, мрежа, организација и појединаца (Стратегија развоја информационе безбедности, 2017), чиме указује и на релевантне садржаје информационе безбедности којима се обухватају технологија, процеси и људи, односно људска, физичка, техничка и административна компонента организације. Овим одређењима заједничко је ЦИА тројство – кроз очување безбедности информација, хардвера, софтвера и пратећих инсталација, организационих састава и појединаца. На тај начин се сајбер безбедност схвата као процес усмерен на постизање и одржавање заштитних својстава организације у односу на безбедносне ризике у сајбер простору.

Информациона безбедност организације може се значајно унапредити имплементацијом стандарда ИСО 27001 – Систем менаџмента безбедности информација (*Information Security Management System – ISMS*) (ISO/IEC, 2013), као централног стандарда из серије стандарда ИСО 27000 намењених за различита подручја управљања безбедношћу информација. Применом стандарда обезбеђује се модел за успостављање, имплементацију, функционисање, праћење, преиспитивање, одржавање и побољшање система безбедности информација, што представља процесни приступ менаџмента безбедности информација. Стандард укључује процес процене ризика, организациону структуру, класификацију информација, механизме контроле приступа, физичку и техничку заштиту, политику безбедности информација, процедуре и смернице за праћење и извештавање. За изградњу ИБК значајан је и стандард ИСО 27002 као допунски стандард уз ИСО 27001, који је фокусиран на контроле безбедности информација. Стандард ИСО 27002 представља скуп смерница осмишљених да се олакшају увођење стандарда ИСО 27001 и имплементација најбоље праксе на ИСМС (IT Governance, 2021), укључујући избор, примену и управљање контролама према ризицима окружења. После испуњења предвиђених услова и усаглашавања пословања са захтевима стандарда, организације могу добити сертификат о примени стандарда ИСО 27001 као основног стандарда, док се стандард ИСО 27002 не може сертификовати, већ служи као водич за одговоре организације на захтеве усаглашености свог пословног система са стандардом ИСО

27001 (BestPractice.Biz, 2021). Стандард ИСО 27002 даје и додатне смернице за заштиту ИКТ од запослених, постављање и доделу нивоа приступа, успостављање неопходног нивоа свести и едукацију.

Увођење стандарда ИСО 27001[24] и ИСО 27002 у организације нужно доводи до промена и утиче на све аспекте организације, па и на ИБК. Менаџмент организације мора да обезбеди све неопходне ресурсе за имплементацију, функционисање и одржавање ИСМС, а да при томе не утиче на основно пословање. Запослени се најчешће морају додатно обучавати за примену захтева ИСМС, јер се мења и култура рада, што посебно утиче на старије запослене који имају изграђене радне навике. Додатно ангажовање запослених могу изазвати нормативи којима се захтева нова политика заштите и друга процедурална документа. Уопштено, нове технологије (хардвер, процесни и заштитни софтвер) и систем управљања безбедношћу информација, захтевају прилагођавање безбедносне политике и процедура заштите и нова знања корисника, што изазива и трошење различитих ресурса организације.

Концепт информационо-безбедносне културе

Општа сазнања из истраживања организационе културе као свеобухватног контекста рада у организацији и информационе безбедности као процеса постизања и одржавања њених заштитних својстава у односу на безбедносне ризике у сајбер окружењу, условила су њихово повезивање и постављање у основ истраживања ИБК као квалитативно новог концепта културе. Организациона култура је култура једног организационог система и представља збир традиција, вредности, политика, уверења и ставова, који чине свеобухватан контекст за све што се ради у организацији. (Deal, Kennedy, 1983; Mullins, 2005). Суштину организационе културе представљају њен садржај и манифестације, при чему се садржај, код већине истраживача, представља према структури на три нивоа коју је поставио Едгар Шејн (*Edgar Schein*): основне претпо-

24 Истраживања (ISO, 2021) показују да је у Србији у 2020. године издат 351 сертификат ИСО 27001, што представља повећање у односу на 2019. годину, када је издато 258 сертификата (ISO, 2020). Највише сертификата 2020. године издато је у секторима информационих технологија (127), грађевинарства (77) и инжењеринга (35).

ставке и веровања, вредности и предмети (Schein, 2009: 21-27). Она се често примењује и при одређењу ИБК.

Због значаја ИБК, истраживања у овој области су интензивирана последњих година, али и даље не постоји општеприхваћена дефиниција ИБК, посебно због различитих приступа у њеном изучавању. Ако се ИБК сматра интегралним делом организационе културе (или поткултуром), уз уважавање специфичности везаних за употребу ИКТ система и њихову безбедност, може се представити као скуп друштвено-културолошких мера које подржавају техничке активности заштите, а које су производ понашања запослених у вези са информационом безбедношћу и природан су аспект дневних активности запослених (Martins, Eloff, 2002; Schlienger, Teufel, 2003a). У складу са Шејновим трослојним моделом организационе културе, ИБК представља скуп ставова, претпоставки, уверења, вредности и знања које чланови организације и друге заинтересоване стране изван организације у сваком тренутку користе у интеракцијама са ИКТ системом и уз поштовање процедура организације, а резултати интеракција су видљива (прихватљива или неприхватљива) понашања запослених (Da Veiga, Eloff, 2010; AlHogail, Mirza, 2014). На тај начин се ИБК одређује ослањањем на три главна нивоа: 1) основне претпоставке 2) видљиве предмете и творевине; и 3) колективне вредности, норме и знање (Schlienger, Teufel, 2003b: 405-406), што су преовладавајући ставови и у академским радовима (Da Veiga et al., 2020; Nasir et al., 2019). Претпоставке (навике, перцепције и очекивања) јесу суштина ИБК и на њима се изграђују друге видљиве компоненте (политика, процедуре, норме, знање) и остварују колективне вредности садржане у одразу ИБК кроз понашање запослених у заштити ИКТ система. Резултати спровођења политике видљиви су у предметима и творевинама организације и понашању запослених, чиме се ствара окружење поверења и успоставља интегритет организације (Da Veiga et al., 2020: 36). Знање представља значајан фактор у сваком од постојећих нивоа, али се може издвојити и као посебан, четврти ниво (Van Niekerk, Von Solms, 2010: 479). Тиме се истиче значај специфичних знања запослених о информационој безбедности, која се не смеју претпоставити, већ је потребно да се периодично процењују и по потреби надограђују. Према представљеним нивоима, као и при класификацији садржаја организационе културе (Janićijević,

2011: 72), садржаји ИБК се могу сврстати у две групе елемената: 1) когнитивни (претпоставке, вредности и ставови), који се не могу опажати, креирају заједничко мишљење и понашање и тешко се мењају; 2) симболички (материјални и семантички елементи и симболи понашања), који испољавају когнитивне елементе кроз понашање запослених и видљиви су део организације.

Интегрисањем наведених дефиниција и описа ИБК, за ниво непосредних корисника ИКТ и уз претпоставку да постоји потребно знање и рационално ангажовање менаџмента највишег нивоа и стручних тимова на заштити информационе имовине, предлаже се концепт према коме: *ИБК представља јединство знања, перцепција, уверења и ставова запослених о информационој безбедности организације и потреби примене мера и поступака (дефинисаних политиком информационе безбедности и формализованих процедурама) и њиховој усклађеној поступања у свакодневној примени тих мера, као и способност препознавања претњи, минимизирања ризика и доношења одлука из домена сопствене одговорности у вези са безбедношћу ИКТ система.*

Концепт интегрише претпоставке, предмете, норме и знања у понашање запослених, а уједно даје значај активностима менаџмента у дефинисању и спровођењу политике и процедура у интеракцијама запослених са окружењем и унутар организације. Датим концептом се политика информационе безбедности поставља као темељни програмски документ за заштиту информационе имовине организације, а тиме и за изградњу ИБК запослених. Политика треба да представља сублимацију знања, закључака из анализе спољних и унутрашњих утицајних фактора и визију менаџмента о изградњи ефективног система заштите у оквиру расположивих технолошких, материјалних, финансијских и кадровских ресурса. У садржајном смислу, рационална политика информационе безбедности је скуп одлука, смерница, принципа и препорука, специфичних и/или стандардних, којих треба да се придржавају сви запослени, како би се обезбедило њихово хомогено поступање и усклађено деловање у контексту информационе безбедности, чиме се поставља и оквир за изградњу ИБК. Предложеном одређењем ИБК су, поред примене формализованих мера и поступака, обухваћена и понашања запослених у ситуацијама које нису предвиђене, или их није било могуће превидети, и када се очекује да корисници

препознају претње и могуће ризике од угрожавања ИКТ система и самостално доносе одлуке у делокругу свог рада и одговорности, што представља и нови квалитет у развоју ИБК.

Због когнитивних карактеристика запослених, деловања неформалних група и специфичности организационих подсистема, у организацији се не може очекивати јединствена или униформна информационо-безбедносна култура. Најчешће се могу идентификовати једна доминантна ИБК и више поткултура. *Доминантна ИБК* карактерише целокупну организацију и изражава опште вредности свих чланова организације у којој информационо-безбедносне вредности, перцепције и принципе политике дели већина чланова организације. *Поткултуре ИБК* могу настати због различитости организацијских подсистема, њихових садржаја или функција, локација, националних култура и других фактора, а препознатљиве су по томе да вредности, перцепције и принципи политике информационе безбедности код неких група запослених одступају од оних које има већина чланова организације (Da Veiga, Martins, 2017: 78). Поткултуре ИБК својим деловањем могу јачати ИБК (развој иновативних идеја), или је слабити (угрожавање безбедности и сметње ефикасном и ефективном раду), што захтева њихово лоцирање, анализу утицаја, и, зависно од карактера утицаја, промене или надградњу у складу са актуелном безбедносном политиком организације.

Фактори утицаја на информационо-безбедносну културу

Информационо-безбедносна култура се изграђује под утицајем мноштва фактора који се могу класификовати према различитим критеријумима: нивои утицаја (микро и макро утицаји), средине из којих потичу (спољни и унутрашњи), објекти на које утичу (заштита информација или корисника ИКТ), важност (важни и мање важни); степен дистрибуције (фактори општег и локалног деловања) и други критеријуми (Da Veiga et al., 2020: 12). Са становишта системског приступа организацији, фактори који утичу на организацију, па тако и на ИБК, могу потицати из окружења као претежно објективни фактори или из унутрашње структуре и процеса у организацији као претежно субјективни фактори.

Спољни фактори утицаја на ИКБ углавном су опредељени стањем у држави у којој функционише организација, а садржани су у елементима опште друштвене (националне) културе и економском и технолошком степену развоја државе. Степен дигитализације у држави, који се одражава кроз њен иновативни развој, и деловање владе државе на спровођењу политике безбедности информација (закони, безбедносне мере, заштита елемената инфраструктуре, организациони системи за превентивно деловање), имају знатан утицај на ИБК организације. Ти фактори се „преливају" и манифестују у организацијама стварајући повољан (или неповољан) амбијент за развој ИБК. Специфичан спољни утицајни фактор испољава се кроз злонамерно деловање појединаца и удружења (група), криминалних и других организација (и појединих држава) и инсајдера према информационој имовини организације.

Спектар унутрашњих фактора утицаја на ИБК је разнолик и обухвата четири скупа фактора (Da Veiga et al., 2020; Nel, Drevin, 2019) селектованих према заједничким носиоцима активности на развоју ИБК (организација, менаџмент, запослени) или према њиховим односима (поверење и усклађивање понашања):

а) *организациони фактори* се односе на унутрашње стање организације, ниво опште организационе културе, расположиве ресурсе као битан фактора физичке, хардверске и софтверске заштите, организацију обуке и образовања кадра и сл.;

б) *фактори менаџмента* се испољавају кроз методе и праксу управљања, одговорности, постигнуте ефекте, стварање повољних услова у функцији безбедности информација (стручност особља, ефикасност процедура, безбедносне методе и сл.), организовање и спровођење образовања, обуке и програма за изградњу свести, мониторинг и контролу понашања запослених и друге облике деловања;

в) *фактори повезани са запосленима* се односе на индивидуалне карактеристике људи и њихове вредности (одговорност, интегритет, поверење, етичност, мотивација, лични развој), потребе, задовољство и емоционално стање (радно време, друштвена атмосфера, ниво зарада, и сл.), ниво знања о информационој безбедности, разумевање информација о безбедносној политици и др.;

г) *фактори међусобног поверења* обухватају односе запослених (међусобно поверење и усклађивање знања, вредности, потреба

и понашања) и поверење клијената у погледу очувања приватних података и других безбедносних гаранција.

Значај и интензитет деловања наведених фактора разликују се у различитим организацијама и фазама њиховог развоја, али су међузависност фактора и њихова узрочно-последична веза увек присутне. Истичу се улога и значај менаџмента највишег нивоа кроз дефинисање стратегије и политике безбедности, ангажовање ресурса, формирање стручних безбедносних тимова, одлучивање о опремању хардверском и софтверском заштитом, као и кроз подршку, осмишљавање и реализацију програма за подизање нивоа ИБК. Процес изградње (доградње) ИБК, сагласно са елементима системске анализе, има неколико етапа, почевши од евалуације и процене постојећег стања (нивоа ИКБ), разматрања алтернатива и избора најприхватљивијег решења, до спровођења програма доградње ИБК и поновне евалуације ради установљавања новог стања. Образовање, обука и изградња свести о безбедности неке су од најефикаснијих и најзначајнијих мера којима се организација може супротставити угрожавању информационе безбедности (Parsons et al., 2010; Peltier, 2005), почевши од једноставних водича, па све до добро развијених образовних програма. Образовање се односи на школовање стручног кадра кроз оспособљавање и интегрисање различитих знања и вештина ради супротстављања безбедносним претњама, док се обуком изграђују знања, трајне вештине и способности осталих запослених потребне да се, употребом одговарајућег софтверског алата или начином комуникације и понашања, супротставе претњама. Сврха изградње свести јесте усмеравање пажње на безбедност, тако да се напори на изградњи свести фокусирају на промену понашања и примену добре безбедносне праксе.

Закључак

Правилна политика информационе безбедности, добра хардверска и софтверска заштита ИКТ система и обученост кадра у чијој је надлежности информациона безбедност организације, представљају добар предуслов, али не и гаранцију високог нивоа заштите информација. Повећање броја и све већа софистицираност претњи у доба масовне употребе интернета, поред техничких и организационих претпоставки добре информационе безбедно-

сти, утицали су да се пажња све више усмерава на непосредне кориснике ИКТ и мере и поступке које они морају да предузимају у области безбедности информација. Пандемија ковида 19, повећан обим рада од куће и коришћење личних уређаја за приступ информацијама организације, често без стандардне безбедносне заштите, створили су нове изазове организацијама у очувању информационе безбедности. То је довело до повећаног броја софистицираних сајбер напада и потребе да се анализира понашање корисника у новонасталим околностима и појачају активности на подизању њихове свести. Показатељи ефеката успешних напада на ИКТ системе организација требало би да буду добро упозорење менаџменту организације на могуће претње и последице напада на ИКТ системе. Усвајањем и имплементацијом стандарда ИСО/ИЕЦ 27001 организацијама пружају се могућности за унапређење процеса управљања безбедношћу информација и смањење ризика од претњи и напада на ИКТ систем.

Схватањем значаја људске компоненте, активности организације се, поред стварања технолошких предуслова заштите, усмеравају и на анализу и изградњу ИБК као континуираног процеса. ИБК је сложена појава која се заснива на усклађеном деловању њених, такође сложених, елемената. Зато су за разумевање садржаја и изградњу ИБК потребна мултидисциплинарна знања из области управљања, информатике и заштите, социјалне психологије, андрагогије, као и друга менаџерска и стручна знања. Као јединство когнитивних и симболичких садржаја, ИБК се обликује под утицајем циљева, структуре, политике, процеса и руководства организације. Стратешки циљ изградње ИБК јесте остваривање адекватног нивоа информационе безбедности организације, при чему он мора бити усклађен са организационом структуром и безбедносним ризицима.

Већина познатих концепата ИБК базирана је на ставовима, претпоставкама, знању, нормама и вредностима запослених у односу на безбедност информација, опредмећених у њиховом прихватљивом понашању у раду са ИКТ системима. Концепт ИБК који је представљен у овом раду заснован је на стратегији и политици информационе безбедности, примени технологија, организацији, деловању људи и утицајима фактора окружења. У том контексту, ИБК представља јединство знања, перцепција, уверења и ставова запослених и њиховог усклађеног понашања, чиме се тежиште кон-

цепта поставља на разумевање и примену мера политике информационе безбедности. Концепт интегрише когнитивне и симболичке елементе културе и поставља у његов фокус менаџмент највишег нивоа и политику информационе безбедности као тежишног документа изградње и одржавања захтеваног нивоа ИБК.

У складу са датим концептом, адекватна ИБК постоји када је постигнута усклађеност проактивног приступа организације информационој безбедности са организационим компонентама културе (политика, процеси, менаџмент, друштвене норме) и појединачним обележјима запослених (ставови, знање, претпоставке и др.), која се одражава у безбедном понашању запослених у раду са ИКТ системом. Развијена ИБК ствара повољан и безбедан радни амбијент и обезбеђује да организација ради уз мање напора, усмеравајући се на основну делатност. Таква ИБК повољно утиче и на задовољство запослених, на раст организације услед дигиталног поверења сарадника и повећања репутације у окружењу.

Литература

1. AlHogail, A., Mirza, A. (2014). *Information security culture: a definition and a literature review*, In: 2014 World Congress on Computer Applications and Information Systems (WCCAIS), IEEE, pp. 1-7. DOI: 10.1109/WCCAIS.2014.6916579.
2. BestPractice.Biz. (2021). What Is the Difference Between ISO 27001 and 27002, https://bestpractice.biz/what-is-the-difference-between-iso-27001-and-27002/, доступан 6. 6.2022.
3. Da Veiga, A., Eloff, J. H. (2010). A framework and assessment instrument for information security culture. Computers & Security, 29 (2): 196-207. DOI: 10.1016/j.cose. 2009.09.002.
4. Da Veiga, A., Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, 70: 72-94. DOI: 10.1016/j.cose.2017.05.002.
5. Da Veiga, A., Astakhova, L. V., Botha, A., Herselman, M. (2020). Defining organisational information security culture — Perspectives from academia and industry. *Computers & Security*, 92: 1-52. DOI: 10.1016/j.cose.2020.101713.
6. Deal, T. E., Kennedy, A. A. (1983). Culture: A new look through old lenses. *The journal of applied behavioral science*, 19(4): 498-505.

7. Đukić, A. (2018). Organizovani visokotehnološki kriminal - pojam, razvoj i osnovne karakteristike. *Vojno delo*, *70*(3), 128-156. DOI: 10.5937/vojdelo1803128D.
8. International Organization for Standardization / International Electrotechnical Commission (ISO/IEC). (2018). *ISO/IEC 27000 - Information technology - Security techniques, Information Security Management System - Overview and vocabulary*, https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en, доступан 25.1.2022.
9. International Organization for Standardization / International Electrotechnical Commission (ISO/IEC). (2022). *ISO/IEC 27002* - Information security, cybersecurity and privacy protection — Information security controls, https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:en, доступан 25.1.2022.
10. International Organization for Standardization (ISO). (2020). ISO Survey 2019, https://isotc.iso.org/livelink/livelink?func=ll&objId=21897526&objAction=browse&viewType=1, доступан 07.06.2022.
11. International Organization for Standardization (ISO). (2021). ISO Survey 2020, https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1, доступан 7.6.2022.
12. IT Governance. (2021). ISO 27001 vs. ISO 27002: What's the difference?. https://www.itgovernance.co.uk/blog/understanding-the-differences-between-iso-27001-and-iso-27002, доступан 7.6.2022.
13. Janićijević, N. (2011). Methodological approaches in the research of organizational culture. *Economic Annals*, 56 (189): 69-99. DOI: 10.2298/EKA1189069J.
14. Martins, A., Eloff, J. (2002). *Assessing Information Security Culture*. In: Proceedings of the ISSA 2002, *Johannesburg:* Information for Security for South-Africa 2nd Annual Conference, pp. 1–14.
15. Mullins, L. J. (2005). *Management and organisational behavior*. Pearson Education Limited, Edinburgh Gate, United Kingdom.
16. Nel, F., Drevin, L. (2019). Key elements of an information security culture in organisations. *Information & Computer Security,* 27(2): 146-164. DOI: 10.1108/ICS-12-2016-0095.
17. Parsons, K., McCormac, A., Butavicius, M., Ferguson, L. (2010). *Human factors and information security: individual, culture and security environment*. Command, Control, Communications

and Intelligence Division, DSTO Defence Science and Technology Organisation, Edinburgh.
18. Peltier, T. R. (2005). Implementing an Information Security Awareness Program. *Information Systems Security*, 14 (2): 37-49.
19. Schein, E. H. (2009). *The corporate culture survival guide*. John Wiley & Sons, San Francisco, USA.
20. Schlienger, T., Teufel, S. (2003a). *Information Security Culture - From Analysis to Change*. In: Information Security South Africa - Proceedings of ISSA 2003, 3rd Annual Information Security South Africa Conference, ISSA, Sandton Convention Center, Johannesburg, South Africa, pp.183-195.
21. Schlienger, T., Teufel, S. (2003b). *Analyzing information security culture: increased trust by an appropriate information security culture*, In: 14th International Workshop on Database and Expert Systems Applications, 2003 (DEXA 2003), IEEE, Computer Society, Prague, Czech Republic, pp. 405-409.
22. *Стратегија развоја информационе безбедности*, Службени гласник Републике Србије, бр. 53/2017.
23. Van Niekerk, J. F., Von Solms, R. (2010). Information security culture: A management perspective. *Computers & security*, 29 (4): 476-486. DOI: 10.1016/j.cose.2009.10.005.
24. Вулетић, Д. (2015). *Сајбер тероризам*, У Зборник радова "Савремени тероризам", ЈП Службени гласник и Институт за међународну политику и привреду, Београд, стр. 265-330.
25. *Закон о информационој безбедности*, Службени гласник Републике Србије, бр. 6/2016, 94/2017 и 77/2019.

Basics of Information Security Culture in the Organization

Abstract: *The mass application of information and communication technologies (ICT) has facilitated the functioning of organizations, but has also increased their vulnerability and conditioned the development of the information security function. Attacks on ICT systems involve people as potential targets of vulnerability, highlighting the importance of paying close attention to an employee's behavior in interactions with elements of the ICT system and its environment, as well as developing an information security culture (ISC) as an integrative component of organizational culture and an important factor in the organization's information security. The paper attempts to set a comprehensive concept of ISC based on the unity of knowledge, perceptions, beliefs and attitudes of employees and their coordinated actions in the application of security measures, which emphasize the role of the organization and its management in creating, building and maintaining ISC. The focus of determining ISC is on understanding and applying information security policy measures, but it also includes the behavior of employees in situations that are not or could not be predicted, when employees are expected to protect the information assets of the organization. The paper identifies the most important external factors that are mostly objective, determined by the situation in the country in which the organization operates and contained in the elements of general social (national) culture and country's economic and technological development. As a specific impact on ISC, the activities of malicious individuals, groups and organizations in cyberspace – stand out, manifested through threats and endangerment to the integrity of the ICT system. Internal factors are mostly subjective and dependent on general organization; the knowledge, vision and actions of management in the field of information security; individual characteristics of people, their values, needs, knowledge, understanding and application of information security policy measures. Among the factors, the highest level of management stands out for its role and importance due to the greatest responsibility for organization`s information security, but also as the creator of its strategy and policy, the holder of resource engagement policy, shaper of professional security teams, decisionmaker on hardware and software protection, and supporter, creator and implementer of programs for ISC level raising.*

Keywords: *organizational culture, information security, information security culture, management, information security awareness.*