Примљено: 07. мај 2023.
Прихваћено: 06. јул 2023.

004.056
330.526.33:351.824.1
COBISS.SR-ID 112252681
DOI 10.5937/ssb202301011M

БЕЗБЕДНОСТ ИНФОРМАЦИЈА У ФУНКЦИЈИ УПРАВЉАЊА КОНТИНУИТЕТОМ ПОСЛОВАЊА

Јана Марковић, сарадник у настави*
Универзитет у Београду, Факултет безбедности

* markovicfb22@gmail.com

БЕЗБЕДНОСТ ИНФОРМАЦИЈА У ФУНКЦИЈИ УПРАВЉАЊА КОНТИНУИТЕТОМ ПОСЛОВАЊА*

Сажетак: *Информације као средство схватања света и комуникације добиле су у пословном окружењу улогу корпоративног ресурса који заврeђује бар онолико пажње колико и сваки други ресурс којим било која организација располаже. Када се говори о информацијама као корпоративном ресурсу, неизоставно је бављење проблематиком њихове заштите. Отуда, пажња академске и стручне јавности већ увелико је окупирана питањем безбедности информација, укључујући остваривање безбедности и других информационих ресурса који делују као ослонац и подршка употреби информација. Безбедност информација јесте функција која због свог значаја мора бити континуирана. Са друге стране, пред сваку организацију је постављен задатак обезбеђивања континуитета пословања услед и након поремећаја без обзира на карактер тих поремећаја. У вези са тим, у раду се полази од претпоставке да је један од предуслова континуитета пословања управо (континуитет) безбедности информација. Аутор ће покушати да представи на који начин безбедност информација доприноси управљању континуитетом пословања.*
Кључне речи: *информације, безбедност информација, управљање безбедношћу информација, континуитет безбедности информација, управљање континуитетом пословања*

Увод

У информационом добу и умреженом друштву у којем живимо информације постају све значајнији ресурс, како у приватној сфери живота за обављање свакодневних активности тако и у раду организација у јавном и приватном сектору. Технологија на којој почивају информације постала је толико инкорпорирана у приватној и пословној

* Рад је настао у оквиру пројекта који финансира Фонд за науку Републике Србије у оквиру Програма „ИДЕЈЕ" – Management of New Security Risks – Research and Simulation Development, NEWSIMR&D, #7749151.

сфери живота да је тешко или чак немогуће замислити живот и рад без ње. Сасвим сигурно, данас организације користе информације и савремене (информационо-комуникационе) технологије као обавезни елемент пословања, који се неретко препознаје као крит чна пословна имовина. Услед све веће повезаности комплексних система и мрежа, размене информација и информационих ресурса, као и због широког спектра врло софистицираних претњи, обезбеђивање њихове заштите постаје све амбициознији захтев. Безбедношћу информација треба обезбедити заштиту поверљивости, интегритета и расположивости информација (укључујући ресурсе који наведено обезбеђују и подржавају) од различитих претњи природног, техничко-технолошког и људског фактора. Крајњи циљ је обезбеђивање могућности и услова за континуирано коришћење информација и информационих ресурса. Отуда се може говорити о континуитету безбедности информација, као елементу шире организационе (и менаџмент) функције континуитета пословања. Са друге стране, ефикасан приступ управљања континуитетом пословања препознат је као један од кључних фактора успешне примене система управљања безбедношћу информација (ISO, 2018). С тим у вези, циљ сваке организације би требало да буде имплементација захтева безбедности информација укључујући континуитет безбедности информација у системе управљања континуитетом пословања организације.

Циљ рада је представити на који начин информације и систем њихове заштите доприносе управљању континуитетом пословања организације. Реч је о систему који се успоставља и развија како би се осигурао наставак пословања организације у случају поремећаја, обезбеђујући њено непрекидно функционисање.

Рад је организован тако да се најпре прави осврт на одређење информација и њиховог значаја, како са аспекта њихове употребе у свакодневном животу тако и са аспекта пословања у контексту њихове употребе у организацијама. Даље, у раду се разматрају питања заштите, односно безбедности информација, попут претњи којима информације и информациони ресурси могу бити изложени, система управљања безбедношћу информација, континуитета безбедности информација. Поред захтева за континуитетом безбедности информација, који је представљен као посебан сегмент рада, обрађује се управљање континуитетом пословања, све чешће препознато као посебна функција организације која се ослања на сам менаџмент (управљања) организације.

О значају информација

Да би се отворила тема рада, скретање пажње на дефинисање информација чини се оправданим. У свакодневном животу информације се могу сматрати садржајем о неком одређеном догађају, збивању, процесу или појму (Мандић и др., 2017: 21), то је „нешто што је речено" (Buckland, 1991: 351) или „чин обликовања ума и чин саопштавања знања" (Capurro & Hjørland, 2003: 351), средство „нашег прилагођавања случајностима спољне околине и нашег настојања да у тој околини делотворно живимо" (Viner, 1964: 32). Нешто слично, али наизглед компликованије одређење, информацију одређује као неку врсту својства или „атрибут примаочевог знања и интерпретације сигнала, а не атрибут пошиљаоца, нити неког свезнајућег посматрача, нити самог сигнала" (Fairthorne, 1954 према Buckland, 1991: 352). Дакле, можемо рећи да информација увек представља знање о неком феномену које има одређено значење. То значење је увек одређено контекстом у који корисник информације исту ставља.

О информацијама се може говорити као о знању, процесу или ствари, а број дефиниција је велики с обзиром на различите научне дисциплине које су се упустиле у проблематику дефинисања овог појма и различите приступе које су при томе користиле (Buckland, 1991; Capurro & Hjørland, 2003; Путник, 2009). Заиста, формулисању једне општеприхваћене дефиниције информација вероватно и не треба тежити с обзиром на то да је немогуће створити такву дефиницију да буде довољно обухватна за све дисциплине у чију појмовну мрежу спада, а опет довољно прецизна да задовољи (тематске) потребе свих тих различитих дисциплина. С обзиром на тему рада, на овом месту биће изнета још и дефиниција информација са аспекта дигиталних технологија. У том контексту, водећа светска организација која припрема и објављује међународне стандарде у области технологије дефинисала је информацију као „знање о објектима, као што су чињенице, догађаји, ствари, процеси или идеје (укључујући концепте) који, у одређеном контексту, имају одређено значење" (IEC, n.d.a). Овај приступ дефинисању је могуће употребити да би се отворило специфичније питање одређења информација у контексту њихове употребе у организацијама или пословној сфери где се о њима може говорити као о корпоративном ресурсу (Мандић и др., 2017: 20). Када говоримо о информацијама као корпоративном ресурсу организације, то би морале бити све информације са којима организација поступа, без

обзира да ли их ствара, користи, преноси, модификује, чува или уништава. Због вредности коју имају, информације су сврстане у исту раван са кадровским и материјалним ресурсима једне организације. Без обзира да ли била у штампаном, дигиталном облику или у виду знања запослених, информација може да се добије или преда, да се купи или прода. Њена вредност, која се може изразити новчано (или материјално), огледа се у значају које информација може имати за организацију која је поседује, односно у губицима које организација може имати уколико остане без ње. Иако је овако објашњена вредност довољна да се испрва иста разуме, у функцији давања озбиљнијег аргумента, могу се навести карактеристике информације, попут њене актуелности, тачности, поузданости, трајности, расположивости и њене могућности да задовољи потребе корисника (Mandić i dr., 2012: 116). Овде, пак, треба упозорити да се наведене карактеристике односе на вредност информације у пословној сфери. У свакодневном животу, вредност се такође може процењивати у односу на наведене критеријуме. Ипак, и ако они (критеријуми) нису задовољени како у свакодневном животу тако и у пословној или било којој другој области живота, то не значи да информација престаје да буде информација, већ само да њена вредност није испуњена. Човек или машина који добију информацију остају „информисани" уз питање да ли је та информисаност потпуна и тачна, и да ли се може искористити у право време и тиме задовољити потребе њеног корисника. У првом случају, информацију употребљава когнитивни систем човека, док у другом случају то чини хардверски систем подржан софтвером, који је програмиран (и често надзиран) од стране самог когнитивног система човека.

Често се може чути да живимо у „информационом добу", које је условио развој информационих технологија – технологија које се заснивају на информацијама и које као производ дају нове информације. Иако има аутора који се не слажу са употребом овог појма, јер су информације или „системи комуникације симболима" заправо у основи сваког друштва одувек (Castells, 2000a: 156), данас је употреба овог појма широко заступљена. Критикујући терминологију која се користи, Кастелс (Castells) уводи нови појам – такозвано „умрежено друштво", у чијој основи се налазе информационе мреже које покрећу информационе технологије (2000b: 695). Дакле, са развојем технологија створен је услов за развој мрежа које су заједно омогућиле трансформацију друштва и стварање савременог умреженог

друштва где већу моћ и улогу имају информације и мреже него институције.[1]

Информационе технологије омогућиле су и развој система који се могу посматрати као елемент у основи информационих мрежа. Овакви системи, пак, много чешће кореспондирају у оквиру такозваног „система система" (engl. *System of Systems, SOS*). Реч је о скупу система или системских елемената који су у интеракцији како би обезбедили јединствену способност коју ниједан од конститутивних система не може да оствари сам (ISO, 2019b). У сваком систему система међузависност пропорционално расте са повећањем броја конститутивних система, услед чега рањивост постаје већа. Количина информација која се размењује у таквим системима у комбинацији са рањивошћу намеће потребу за заштитом система и информација све већом.

Безбедност информација

Када је реч о самим претњама које треба узети у обзир када се разматра заштита информација и информационих ресурса, напор (или бар покушај) таксативног навођења свих претњи биће изостављен. У замену за наведено, на овом месту би било оправдано представити претње према три категорије у које се могу разврстати узимајући као критеријум разликовања извора из којег потичу. То би биле претње које имају порекло из природних извора (земљотреси, поплаве), претње које имају карактер техничко-технолошких акцидената (пожари, експлозије) без обзира да ли су проузроковане природним или људским фактором или комбиновано и претње проузроковане људским чињењем или нечињењем. Последња категорија је најризичнија због вероватноће и учесталости претњи које убраја. У њих се убрајају крађа, намерно или ненамерно оштећење или уништење опреме, укључујући и медије за трајно или привремено складиштење од стране инсајдера, аутсајдера или њиховим заједничким деловањем; неовлашћено или незаконито откривање и приступ информацијама, њихово обрађивање, односно неовлашћено читање, умножавање, измена или брисање информација; вршење напада у циљу долажења до жељених информација без обзира да ли се користе малициозни програми,

1 Castells, M. (2004). Informationalism, networks, and the network society: a theoretical blueprint. In *The network society: A cross-cultural perspective* (pp. 3–45). Cheltenham, Northampton: Edward Elgar.

врши опструкција услуга или се користе технике обмањивања корисника; грешке корисника (ненамерна измена или брисање, погрешно усмеравање); технички кварови хардвера, софтверске грешке, сметње у комуникационим мрежама и друге претње попут прекида у снабдевању електричном енергијом, повлачења опреме или дела опреме која се користи у раду. Путник (Putnik, 2012: 40) све претње разврстава у четири категорије: виша сила (пожар, поплава, земљотрес), кварови, људски фактор са атрибутом ненамерности (грешке у пројектовању и коришћењу рачунарских система) и људски фактор са атрибутом намерности (физички, електронски и сајбер напади). Као што је већ наведено, карактеристике ове категорије претњи намећу исту у први ред када се врши пројектовање и имплементација система управљања безбедношћу информација.

У циљу заштите информација од неовлашћеног откривања, преноса, модификације или уништења, било случајно или намерно, без обзира на облик у којем се налазе (IEC, n.d.b), као и без обзира на претње које су идентификоване, успоставља се оно што је познато као безбедност информација или информациона безбедност[2] (engl. *Information security*). Безбедност информација могуће је посматрати као функцију организације која за циљ има заштиту информација, односно заштиту поверљивости, интегритета и расположивости[3] информација као њених основних својстава. Заштиту је потребно обезбедити за све информације са којима организација поступа, без обзира да ли информације припадају самој организацији или некој релевантној трећој страни попут акционара, пословних партнера, добављача, купаца. Такође, заштиту је потребно обезбедити за сваку информацију без обзира на форму у којој се налази, с обзиром на то да могу бити и у штампаном и у електронском облику, или у виду знања запослених. Уз то, информације као корпоративни ресурс, у прва два облика, никада не постоје независно од медија на којима се трајно или привремено складиште, односно како се најчешће може чути, информационо-комуникационих система, које је такође потребно штитити. Реч је о структури повезаних уређаја и средстава (хардвер), подржавајућег софтвера и комуникационе мреже које омогућавају прикупљање,

2 У раду ће се користити термин „безбедност информација", а не термин „информациона безбедност".

3 Поверљивост (engl. *confidentiality*) – својство да информације нису доступне или откривене неовлашћеним појединцима, ентитетима или процесима; интегритет (engl. *integrity*) – својство тачности и потпуности и расположивост (engl. *availability*) – својство приступачности и употребе на захтев овлашћеног субјекта.

пренос, складиштење, манипулацију информација, али исто тако и њихову заштиту и уништавање. С обзиром на прогрес у развоју информационе технологије, без икаквих препрека се може говорити и у самој употреби информација од стране исте те информационе технологије. Информационо-комуникациони системи раде подржани од стране људи, који опет поступају (или би требало да поступају) према процедурама рада које су такође у функцији заштите информација. У вези са тим, запослени се могу сматрати информационим ресурсом (ресурсом који омогућава и подржава информације и поступање са њима), а људски фактор се намеће као незаобилазни елемент функционисања ових технологија, али и безбедности информација.

Безбедност информација као крајњи циљ има осигуравање континуитета, и то спречавањем поремећаја и/или минимизирањем и отклањањем последица када до њих дође. Да би то обезбедиле, организације одређују политику, постављају циљеве и пројектују, имплементирају, одржавају и унапређују посебан систем. Тај систем се углавном назива систем управљања безбедношћу информација, који се састоји од политика, процедура, смерница и повезаних ресурса и активности, којима заједнички управља организација, у потрази за заштитом својих информационих средстава (ISO, 2018). За функционисање оваквог система, попут било ког другог система у организацији, неопходна је адекватна организациона структура, хардвер и софтвер за заштиту идентификованих информационих ресурса, и подржавајуће политике, процедуре и њима одређени процеси. Како се може наслутити из назива овог система, да би се управљало безбедношћу информација, неопходно је и управљање ризицима којима су информације и информациони ресурси изложени. Тако, безбедност информација без компромиса обухвата идентификацију, процену, поступање по ризику, праћење и преиспитивање ризика који могу да угрозе информације и системе на којима почивају.

Важно је имати у виду да систем управљања безбедношћу информација под овим називом проистиче из захтева (или препорука) међународног стандарда који су усвојени у области безбедности информација. Међутим, организација може успоставити и систем или функцију, под другачијим називом, која ће имати исти циљ – заштиту информационих ресурса проактивним и реактивним деловањем и обезбеђивање њиховог континуитета. Попут система управљања безбедношћу информација и овај систем или функција мора да буде усклађена са циљевима и потребама организације, величином и структуром организа-

ције, пословним процесима и захтевима за безбедношћу који директно зависе од ризика којима је организација изложена (у овом случају, узимају се у обзир претње по информационе ресурсе).

Континуитет безбедности информација

Да би се све операције које се ослањају на информације и информационе ресурсе могле наставити током поремећаја и опоравка од поремећаја, у оквиру система управљања безбедношћу информација успостављају се одређене контроле, односно мере које обухватају процесе, политике, уређаје, праксе или друге радње које модификују ризик (ISO, 2018). Конкретно, реч је о *аспектима управљања континуитетом пословања безбедности информација*[4] – контролама које захтевају планирање, спровођење, верификацију, преглед и процену континуитета безбедности информација, као и редундантност у смислу доступности уређаја и средстава за обраду информација. Наведено одговара одређењу континуитета безбедности информација као процеса и процедура којима се обезбеђује континуитет операција у оквиру безбедности информација (ISO, 2018).

Шта се постиже наведеним контролама? *Планирање континуитета безбедности информација* односи се на одређивање захтева за безбедност информација и континуитет безбедности информација у неповољним ситуацијама попут криза или катастрофа (ISO, 2013). Да би се адекватно реаговало у случају напада неким малициозним софтвером или сајбер напада, у случају намерно изазваног пожара, прекида напајања електричном енергијом или плављења хардверских компонената информационог система неопходно је планирати деловање према идентификованим претњама. У оквиру ове контроле, адекватно је имати план са свим детаљима о идентификованој претњи и корацима које је неопходно предузети у вези са њом.

Спровођење континуитета безбедности информација као наредна контрола треба да обухвати успостављање, документовање, имплементирање и одржавање процеса, процедура и мера како би осигурала потребан ниво континуитета током неповољне ситуације (ISO, 2013). То би значило да је потребно дефинисати политике и процедуре, одредити физичке и техничке мере, односно обезбедити све услове

4 Како је 2022. године усвојен нови стандард у области информационе технологије, наведене контроле су замењене новом – *безбедност информација током прекида* (контрола 5.29), о чему ће касније бити нешто речи.

неопходне за примену ове контроле. Пример је одређивање одговорности, активности и временских оквира за спровођење ових активности, као и конкретних мера које би обезбедиле континуитет у остваривању безбедности информација.

Све мере које су успостављене и примењене у циљу континуитета безбедности информација морају бити под сталном *верификацијом, прегледом и проценом*, а у циљу утврђивања да су валидне и ефикасне током неповољних ситуација због којих се планирају и спроводе (ISO, 2013). Оваква контрола треба бити редовна и периодична, све мере морају бити тестиране, процењене и оцењене, и редовно модификоване у односу на интерно и екстерно окружење, а посебно у односу на промене у технологијама, пословању и идентификованим претњама.

На крају, нопходно је разматрати обезбеђивање *редундантности* у погледу обезбеђивања довољног броја и квалитета уређаја и средстава за обраду информација који могу да испуне захтеве доступности. Редундантност треба да обезбеди континуирану услугу тако што спречава да било какав поремећај угрози доступност информација.

Препознавање ових аспеката управљања континуитетом пословања безбедности информација учињено је како би се подвукао значај и осигурало да безбедност информација настави да функционише и након поремећаја. Међутим, сама безбедност информација нема нарочито значајну улогу када су нарушени други аспекти пословања организације, па се намеће да је континуитет безбедности информација само део целокупног континуитета пословања организације. Оно што је заједничко за оба процеса јесте то што су усмерена на обезбеђивање (заштиту) доступности информација.

Безбедност информација и управљање континуитетом пословања

Континуитет пословања препознат је као „способност организације да настави испоруку производа и услуга на прихватљивом, претходно дефинисаном нивоу, током поремећаја" (ISO, 2019). Односно, управљање континуитетом пословања представља процес идентификације претњи којима је организација изложена[5], одређивања

5 У основи планирања и управљања континуитетом пословања јесте претпоставка да, иако свака претња која изазива поремећај може показати неке јединствене карактеристике, оне такође деле неке заједничке обрасце који омогућавају организацијама да се припреме за њих.

критичних ресурса који су неопходни организацији за функционисање и процену могућих последица тих претњи по критичне ресурсе, као и одређивање ресурса (стратегија, капацитета, мера и временских оквира) неопходних за превазилажење последица поремећаја. На овај начин ствара се основа за изградњу отпорности организације која јој омогућава да ефикасно штити интересе њених кључних заинтересованих страна, вредности и активности које су кључне за њен опстанак и функционисање. Крајњи циљ јесте обезбеђивање непрекидног функционисања организације током и након поремећаја. Ради испуњења овог општег циља, систем управљања континуитетом пословања усмерава своје деловање према реализацији специфичнијих циљева. Управо на основу одређених циљева континуитета пословања уз захтеве за континуитетом ИКТ планира се, имплементира, одржава и тестира се спремност ИКТ (ISO, 2022a), која се може дефинисати као „способност организације да подржи своје пословне операције спречавањем, откривањем и одговором на прекид и опоравак ИКТ услуга" (ISO, 2011). Из наведеног се уочава директна зависност, са једне стране, безбедности информација у чијој основи су, поред информација, и информационо-комуникационе технологије и, са друге, стране континуитета пословања.

Како су новоусвојеним стандардом у области безбедности информација направљене извесне измене, укључујући и оне које се односе на контроле које се успостављају у организацији, на овом месту, пажњу завређују контрола 5.29 и контрола 5.30. Прва контрола се назива још и *безбедност информација током прекида* и представља контролу превентивног и корективног карактера која треба да осигура поверљивост, интегритет и доступност информација и обезбеди оперативна прилагођавања које организација треба да усвоји када дође до поремећаја. Као што је већ истакнуто, ова контрола је заменила контролу која се односи на аспекте управљања континуитетом пословања безбедности информација, предвиђене претходним стандардом. Друга контрола или *спремност ИКТ за континуитет пословања*[6] представља корективну контролу која треба да осигура доступност информација након поремећаја, указујући на улогу коју технологије имају у обезбеђивању континуитета пословања (ISO, 2022b).

6 Постоји посебан стандард који се бави проблематиком спремности информационо-комуникационе технологије за континуитет пословања – International Organization for Standardization [ISO] (2011). *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity* (ISO Standard No. ISO/IEE 27031: 2011). Тренутно је у фази развоја друга едиција овог стандарда (стање из априла 2023).

Управљање континуитетом пословања захтева документовање информација, које се огледа у изради докумената попут стратегија, планова и процедура континуитета пословања. Сваки документ, без обзира да ли је у штампаној или електронској форми, представља место чувања информација. Уз то, сваки документ који се изради у функцији остваривања континуитета пословања за организацију садржи информације које се намећу као круцијалне за превазилажење поремећаја и зато представља документ који је потребно третирати као тајни и у зависности од националне легислативе поступати са њим на тачно прописан начин. Дакле, према сваком документу који се изради кроз овај процес управљања потребно је примењивати опште принципе и елементе безбедности информација и оне специфичне које су прописане од стране националних и наднационалних[7] институција. Стратегија континуитета пословања основа је за целокупан систем управљања континуитетом пословања, док су планови вероватно најкритичнији документ за наставак активности организације и опоравак од последица поремећаја, с обзиром на то да садрже информације о улогама и одговорностима, мерама, временским оквирима, потребним ресурсима, захтевима за комуникацију и извештавање и другим информацијама неопходним за обезбеђивање функционисања и пословања организације без прекида услед поремећаја. У оквиру планова континуитета ИКТ-а, контрола 5.30 истиче као три главне смернице: 1) ИКТ инциденти често захтевају доношење брзих одлука у вези са безбедношћу информација од стране искуснијих запослених, како би се убрзао опоравак; 2) Плановима континуитета ИКТ треба посветити велику пажњу, укључујући редовна тестирања и евалуације, и одобрење од стране вишег руководства и 3) Планови континуитета ИКТ-а треба да садрже захтеве за перформансама и капацитетима било ког система или процеса који се користе за постизање опоравка; јасан циљ времена опоравка (РТО) за сваку ИКТ услугу и начин на који организација намерава да их обнови; циљ тачке опоравка (РПО) који је одређен за сваки ИКТ ресурс и процедуре које обезбеђују могућност враћања информација[8] (ISO, 2022b).

7 На пример, Европска унија.

8 РТО подразумева „временски период у којем се минимални нивои услуга и/или производа и пратећи системи, апликације или функције морају опоравити након што је дошло до поремећаја", док је ПРО „тренутак у којем се подаци морају опоравити након што је дошло до прекида" (ISO, 2011).

Значајан елемент управљања континуитетом пословања јесте *анализа утицаја на пословање* дефинисана као процес анализирања утицаја на организацију током времена поремећаја чији исход су изјава и образложења захтева континуитета пословања (ISO, 2019a). Да би организација одабрала адекватне стратегије, као и да би успоставила адекватне планове и процедуре, неопходно је да изврши ову анализу. Сама анализа никада није једна, већ се спроводи онолико анализа колико је потребно (на пример, у односу на претње по организацију или организационе целине или пословне процесе). Уз то, сама анализа незамислива је без информација (података), попут оних који се односе на ресурсе, системе и операције организације, а који се прикупљају, сређују и обрађују. Основни елемент ове анализе и јесу информације, како оне које се користе као инпути тако и оне који се производе као аутпути. Све што је потребно за израду ових анализа, укључујући спровођење радионица, попуњавање упитника и интервјуа садржи информације које је потребно континуирано штитити, јер би у супротном оне изгубиле своју вредност, а квалитет анализе утицаја на пословање довели под знак питања. Контрола 5.30 указује да организације у оквиру ове анализе треба да буду у могућности да прецизно одреде које ИКТ услуге и функције су потребне за постизање опоравка (ISO, 2022b).

Најновији стандарди који су коришћени у овом раду, а који се односе на системе менаџмента безбедношћу информација, усвојени су и у Републици Србији под називом *Безбедност информација, сајбер безбедност и заштита приватности – Системи менаџмента безбедношћу информација – Захтеви* (SRPS ISO/IEC 27001:2022) и *Безбедност информација, сајбер безбедност и заштита приватности – Контроле безбедности информација* (SRPS ISO/IEC 27002:2022).

Уместо закључка

Суштина и основна намена континуитета пословања као система управљања у било којој организацији јесте обезбеђивање наставка рада током и након поремећаја функционисања, односно испољавања претње било каквог карактера. У вези са тим, континуитет пословања незамислив је без (података и) информација које су кључне за обезбеђивање непрекидности у раду. Самим тим, безбедност информација се намеће такође као кључна за сваки сегмент

система управљања континуитетом пословања или сваки корак који се реализује са циљем континуираног функционисања и пословања било које организације, невезано за њену делатност, величину или структуру.

Врло значајан корак у заштити информација, обезбеђивању континуитета те заштите, као и обезбеђивању континуитета пословања организације јесте постојање свести и спремности за предузимање потребних активности. Дакле, није довољно имати развијене системе, софистицирану технологију (хардвер), најновији софтвер, беспрекорне мреже, до детаља развијене политике, стратегије, планове и процедуре, већ је потребно имати, уз све наведено, и људе који су обучени да користе ресурсе на располагању и предузимају прописане мере у функцији заштите информација и управљања континуитетом пословања. С обзиром на тему рада, то би најпре значило да организација има руководство (менаџмент) који схвата значај који информације и информациони ресурси имају за управљање континуитетом пословања. Запослени би морали бити обучени да одговорно користе расположиве ресурсе, односно да ефикасно користе ИКТ и сву другу опрему и средства којима се обезбеђује заштита информација и информационих ресурса, да поступају по усвојеним документима, да примењују мере којима се обезбеђује заштита информација и информационих ресурса и све то како у условима нормалног рада тако и у условима поремећаја и опоравка од истих, а у циљу континуираног обављања пословних процеса.

На крају, у Републици Србији, у најновијој стратегији усвојеној у области информационе безбедности, препозната је опасност од прекида континуитета вршења послова или пружања услуга ИКТ система тако што је одређено да су оператори ИКТ система од посебног значаја дужни да пријаве инциденте у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности (Стратегија развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године, 2021). Ова стратегија је, за разлику од своје претходнице, препознала значај непрекидности рада ИКТ система и наведеном одредбом потврдила обавезе оператора предвиђене чланом 11а Закона о информационој безбедности[9] (у даљем тексту: Закон). Оператор је тај који је, између осталог, одговоран за предузимање мера које обезбеђују континуитет обављања посла у ванредним околностима (члан 7 Закона). Поред

9 *Закон о информационој безбедности* (2016). „Сл. гласник РС", бр. 6/2016, 94/2017 и 77/2019.

оператора ИКТ система од посебног значаја, улогу у обезбеђивању континуитета услуга у области информационе безбедности има и Национални ЦЕРТ (Национални центар за превенцију безбедносних ризика у ИКТ системима). У циљу обезбеђивања континуитета рада, Национални ЦЕРТ, између осталог, треба да обезбеди инфраструктуру чији је континуитет осигуран, односно да обезбеди редундантне системе и резервни радни простор (члан 15 Закона).

ЛИТЕРАТУРА

Buckland, M. K. (1991). Information as thing. *Journal of the American Society for information science, 42*(5), 351–360.

Capurro, R., & Hjørland, B. (2003). The concept of information. *Annual Review of Information Science and Technology, 37*, 343–411.

Castells, M. (2000a). The contours of the network society. *Foresight, 2*(2), 151–157.

Castells, M. (2000b). Toward a sociology of the network society. *Contemporary sociology, 29*(5), 693–699.

Castells, M. (2004). Informationalism, networks, and the network society: a theoretical blueprint. In *The network society: A cross-cultural perspective* (pp. 3–45). Cheltenham, Northampton: Edward Elgar.

Mandić, J. G., Jeftić, Z., & Mladenović, M. (2012). Corporate resources threatened by social engineering. In D. Čaleta (Ed.), *Corporate security in dynamic global environment – challenges and risks* (pp. 115–128). Ljubljana: Institute for Corporative Security Studies.

Мандић, Г., Путник, Н. и Милошевић, М. (2017). *Заштита података и социјални инжењеринг – правни, организациони и безбедносни аспекти*. Београд: Факултет безбедности.

Путник, Н. (2009). *Сајбер простор и безбедносни изазови*. Београд: Факултет безбедности.

Putnik, N. (2012). Krizni menadžment u funkciji zaštite informaciono-komunikacionih sistema obrazovno-vaspitnih ustanova – Identifikacija pretnji i formulisanje plana za krizne situacije. U: B. Kordić, A. Kovačević i B. Banović (Ur.), *Reagovanje na bezbednosne rizike u obrazovno-vaspitnim ustanovama* (37–53). Beograd: Fakultet bezbednosti.

Стандарди

International Electrotechnical Commission [IEC]. (n.d.a). *Electropedia*. https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=171-01-01.

International Electrotechnical Commission [IEC]. (n.d.b). *Electropedia*. https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=871-04-16.

International Organization for Standardization [ISO]. (2011). *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity* (ISO Standard No. ISO/IEE 27031:2011).

International Organization for Standardization [ISO]. (2013). *Information technology — Security techniques — Code of practice for information security controls* (ISO Standard No. ISO/IEE 27002:2013).

International Organization for Standardization [ISO]. (2018). *Information technology — Security techniques — Information security management systems — Overview and vocabulary* (ISO Standard No. ISO/IEC 27000:2018).

International Organization for Standardization [ISO]. (2019a). *Security and resilience — Business continuity management systems — Requirements* (ISO Standard No. 22301:2019).

International Organization for Standardization [ISO]. (2019b). *Systems and software engineering — System of systems (SoS) considerations in life cycle stages of a system* (ISO Standard No. ISO/IEC/IEEE 21839:2019).

International Organization for Standardization [ISO]. (2022a). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO Standard No. ISO/IEE 27001:2022).

International Organization for Standardization [ISO]. (2022b). *Information security, cybersecurity and privacy protection — Information security controls* (ISO Standard No. ISO/IEE 27002:2022).

Правни извори

Стратегија развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године. (2021). „Сл. гласник РС", бр. 86/2021-5.

Закон о информационој безбедности. (2016). „Сл. гласник РС", бр. 6/2016, 94/2017 и 77/2019.

INFORMATION SECURITY IN THE FUNCTION OF BUSINESS CONTINUITY MANAGEMENT

Jana Marković, Teaching Associate
University of Belgrade, Faculty of Security Studies

Summary

In the business environment, information as a means of understanding the world and communication, has taken on the role of a corporate resource that deserves at least as much attention as any other resource that any organization has. When talking about information as a corporate resource, it is indispensable to deal with the issue of its protection. Therefore, the attention of the academic and professional public is already largely occupied by the issue of information security, including the implementation of security and other information resources that act as support for the use of information. Information security is a function that must be continuous due to its importance. On the other hand, every organization is faced with the task of ensuring business continuity due to and after disruptions, regardless of the nature of those disruptions. In this regard, the paper starts from the assumption that one of the prerequisites for the business continuity is the (continuity) of information security. The author will try to present how information security contributes to business continuity management.

Keywords: *information, information security, information security management, information security continuity, business continuity management.*