# БЕЗБЕДНОСТ У ЈАВНОЈ УПРАВИ

УДК 35.07:355.02
https://doi.org/10.22182/ajp.1512021.1
Прегледни рад

**Сања Клисарић**

**Сажетак**

Развој јавне управе некопматибилно свом диманичком и интензивном разгранавању не поклања довољно пажње безбедносном аспекту чинећи га неконтинуираним или чак у целости непостојећим елементом који прати развој јавне управе. Овај рад изнеће разлоге за интензивно, систематично и контунуирано имплементирање безбедности у јавну управу, као и разлоге због којих се она занемарује или не остварује.

**Кључне речи:** реформа јавне управе, безбедност, јавна управа, заштита информација, сигурност података, сајбер сигурност.

## УВОД

У анализи на овај начин комплексног садржаја, није лоше осврнути се на чињеницу да је еволуција јавне управе директно повезана и са безбедносним аспектом свог не само развоја, него и постојања. Познато је да је општа динамичност развоја јавне управе последњих деценија унела интензивну непредвидивост администрације која води у својеврсни хаос чија практичност се каткад драматично разликује од периода пре реформи јавне управе (Јовановић 2015, 275-276.) Нарастање ове потребе за регулисањем рада јавне управе у што практичнијем и примењивијем, сврсисходнијем и ескпедитивнијем светлу изискује неопходну безбедност као покриће стабилности јавне управе и њених података. Развојем јавне управе, стављајући фокус на примену садржаја који подразумева еволуција јавне управе стиче се утисак да се запоставља безбедносдни фактор који игра једну од најзначајнијих, ако не и најзначајниху улогу сваког система, па и система јавне управе. О овом раду значајно је сугерисати елементе који доводе до занемаривања безбедности као и неопходност примене безбедносних елемената.

## ЈАВНА УПРАВА КАО ДИНАМИЧАН СИСТЕМ ЧИЈИ ФАКТОРОДРЖИВОСТИ СЕ ОГЛЕДА У БЕЗБЕДНОСНИМ ПИТАЊИМА

Чињеница да је јавна управа заузела велики простор прожимајући све секторе друштва (Јовановић 2011, 396). Уколико се ова фактичка ситуација размотри у аспекту бенефита по функционисање друштва неопходно је унутар система функционисања јавне управе развити својеврсне сигурносне системе. Наведеном у прилог треба додати неопходност имплементације безбедносних садржаја као значајног елемента адекватног, правно легитимног и смисаоног функционисања јавне управе. Па, ипак, на основу реалних околности запажамо да управо сама слојевитост и детерминисаност јавне управе сам концепт излаже безбедносној несигурности. Уколико се осврнемо на основ јавне управе који каже да је смисао рада јавне управе успостављен ради остваривања потпунијег демократског друштва које се јавно може испољити кроз концепте правде, слободе и слојевитије економске прилике за све грађане, те се бави људима, идејама и стварима (Clapp 1948, 169–75), чак и лексички, а нарочито практично се изоставља безбедносни аспект. Занемаривање безбедносног аспекта у раду јавне управе индукује драматично велики простор за манипулације и малверзације. Дос-

тупност незаштићених или недовољно заштићених података којима располаже јавна управа представља само први зид одбране у систему заштите који би јавна управа као поступат превне државе требало да поседује. Индикативно је сугерисати имплементацију безбедносних алата уколико нису импликовани целокупном, систематском, детаљном и свеобухватном безбедносном политиком која би у целости заштитила све садржаје јавне управе.

Један од кључних фактора овог наиме значајног проблема унутар функционисања јавне управе је чињеница да је јавна управа не само крута у свом испољавању већ и ограничена у оквирима који се своде на одговорност упућену на ограничене ресурсе који су директно повезани са процесима рада, стварања и демократских вредности. (Shields 1998, 199). У на овај начин строго и јасно детерминисаном простору нема могућности за маневар безбедносног типа из простог разлога што он и није предвиђен калкулативном рачуницом. Опасност следи из претпоставке као најопснијег оружја за аналитику без покрића, а она гласи да се такви системи неће безбедносно угрозити јер не представљају позиције моћи и интереса који би били атрактивни за заштиту безбедносног типа. У оваквом промишљању лежи основни проблем поузданог и безбедносно неадекватног функционисања јавне управе. Наиме, разматрати јавну управу изван оквира безбедности представља потпуну контрадикторност филозофије формирања једног таквог система.

Уколико се јавна управа сведе под поље разматрања политичких наука, адекватно је спорити одсуство безбедносног аспекта као неопходног и валидног за адекватно функционисање система. У том случају, имплементација безбедносних наука и процедура унутар јавне управе има логичан и прагматичан ток. Проблем настаје када се у оквиру аналитике јавних управа проблем безбедности таргетира са аспекта административних наука. Процедуре, папирологија и интернет технологије администрације чињеница да нису усаглашене са безбедносним протоколима, напротив. Они управо компликују и отежавају примењивост безбедносних елемената због саме структуре адрминистративних наука. Јер да би се применила безбедносна политика у јавној политици из аспекта административних наука, круцијално је преобликовати саму администрацију, што наизглед делује непримењиво. Са друге стране, уколико размотримо чињеницу да је безбедност основни постулат посматрања било ког државног апарата, оваква недоследност делује директно парадоксално. Управо непримењивост безбедносних стандарда и процедура доводи до дисфункционалости јавне управе. Круцијално у раду јавне управе је направити безбедносну подршку која би имала вишеструке ило-

ге и системима јавне управе. Сводивост безбедности само на оне органе јавне управе који се примарно баве том облашћу је једнако потпуно апсурдно јер управо системи безбедности и постоје како би заштитили све секторе државе и њених садржаја. Јавна управа као веома експониран елемент државе припада сектору државе који неопходно у сваком свом садржају мора да поседује примењиву безбедносну политику. Веома је ризично по безбедност јавне управе манипулативно декларисање реформи јавне управе као позитивних уколико нису и безбедносно заштићене. Овде треба обратити пажњу на контрапродуктивност коју добијамо бенефитима за оне руководиоце који инструисани да глорификују одређене модерне методе унапређења јавне управе управо подржавају политичке идеје, а не и нужну примењивију администрацију (Pollit, Geert 2002, 6). Ова појава није само политички маневар, него је и ризик управо по оне системе који је подржавају. Својом рањивошћу мета је свих оних ентитета који су ангажовани на таргетирању лаких и доступних апарата. А онда када је држава рањива кроз оне пукотине система које су свесно остављене као такве, реализује се простор за све видове опструкција целокупног државног апарата.

Треба истаћи и то да врело често сама структура јавне управе садржи толико много сложених садржаја који сами по себи онемогућавају безбедносну заштиту. Овакви примери немају други начин решавања до тенденцирање ка поједностављењу саме јавне управе. Са друге стране, управо је то процес који је у сталном току и чињеница да се на том питању константно ради и доводи до проблема имплементације безбедносних начела. Тако да схватамо да су околности далеко од математички прецизних и решивих. Управо су јавне реформе довеле до честих проблема, мењаући свој ток у неочекиваном правцу. Јавна управа изложена је динамичним и константим променама како би се формирала стабилна, конзистентна, активна јавна управа усклађена са етичким и политички неутралним принципима. Уколико смо свесни да је њен циљ да пружа адекватне услуге грађанима и влади, безбедност је фактор који би требало да се подразумева. Међутим, чињеница је да је модерна јавна управа фокусирана на пружање услуга, организацију, синхронизацију, менаџмент, али не и на безбедност и контролу.

## ДИГИТАЛИЗАЦИЈА ЈАВНЕ УПРАВЕ И БЕЗБЕДНОСНИ АСПЕКТ

Скоро је сасвим незамисливо да ико сматра да дигитализација и е-управа могу да функционишу без безбедности информационих система. Ово је далеко лакше артикулисати него посвети-

ти се проблему јер технологија иде далеко брже од унапређења и развоја јавне управе која је прихватила нове технологије као алате за рад јер је инерција стварности навела то као једини рационални избор у реформи јавне управе која је континуирана. Поставља се питање има ли држава довољно не само техничких већ и интелектуалних средстава да проблеме безбедности информационих система јавне управе заштити на адекватан начин. Ово изискује далеко већи број запослених у јавној управи у искључиво секторима интернет технологија који би били не само укључени у актуелне проблеме на радном месту, већ и константне технолошке токове у свету који би могли да предупреде заштиту од напада на системе јавне управе. Без овог типа безбедности јавна управа је изложена екстремној рањивости чиме се читав систем доводи у проблем који би скупо коштао и државу и грађане.

Истина је да реформа јавне управе изискује овакве образовне профиле са акцентуацијом на капацитивне моћи запослених како због динамике посла, тако и због непрекидног учења инвентивних секвенци којима је технологија данас крцата. Јавна управа се суочава са недостатком ресурса да плати интелектуалце који би се бавили овим, свакако приоритетним и најзначајнијим питањем, тако да питање остаје отворено и систем маскира безбедносне позиције оним кадровима који на радна места од најрелевнијег безбедносног значаја долазе попут запошљавања на сва друга радна места где је свако даље учење или имплементација нових знања макар и на дневном нивоу готово незамислива.

У овом случају суочавамо са са кадровским али систематски продуктивним интелектуалним дефицитом за решавање проблема који се гура под тепих. У бити овог проблема стоји још један пређутни проблем, а то је образовање стручњака који се баве модерним технологијама, њиховим праћењем, развојем и имплементацијом. У нашој држави за сада не постоји ни један факултет који пружа директна и конкретна знања за заштиту државне управе од напада. Овакве ствари иако постоје већ сигурно две деценије још увек нису нашле своје едукативно место на нашим факултетима. Стручњаци који изађу са факултета који се баве модерним техологијама упућени су на неке друге ствари и нису у могућности да заштите државу од дигиталних напада. За такву заштиту потребна су дошколовавања која су изван система школства у Србији, а онда у складу са тим иде и логика о цени таквог интелектуалца. Свакако, да када се размотре бенефити и малефици овог проблема, интелектуалац који је способан за заштити јавну управу од дигиталних напада представља запосленог који се по свему котира као веома

значајна карика читавог система, јер уколико похрањени подаци и целокупан рад јавне управе и свих запослених није адекватно безбедносно збринут, он не обавља посао у корист државе и грађана, већ супротно.

Свест о овоме је присутна, и секвенцијално постоје сектори који имају тенденцију да се развију у безбедносна одељења. Али, чињеница је да је ово исувише скромно у односу на оно што стоји као претња.

## ЈАЧАЊЕ ИЛИ ДЕСТАБИЛИЗАЦИЈА ЈАВНЕ УПРАВЕ КРОЗПРОЦЕД ДИГИТАЛИЗАЦИЈЕ - БЕЗБЕДНОСНИ АСПЕКТ

Рањивост система јавне управе је значајан показатељ дестабилизације безбедносног апарата државе. Како би се овај проблем решио, а веома је хитан јер је сама технологија нешто што се сваке секунде развија, мења и застарева је издвајање значајних средстава управо на заштиту која је примарна ставка безбедности владе и грађана. Понекад се чини да за овакво решење има још времена, али околности и чињенице су такве да је сваки тренутак заправо шанса за велику кризу која може да настане дигиталним ратом. Интересантно је нагласити да за дигитални рат није потребно промишљати о неком међудржавном сукобу. Напротив. Држава која нема довољно снажан зид изложена је нападу појединца који може бити солиста те или неке друге државе. Дакле, безбедност у овом смислу није ствар конфликтних политика, нити међудржавних спорова, нити више чак ни тероризма. Сада је јасно да драматичан дигитални напад може да изведе и веома млада особа адекватног знања која неретко може бити и малолетна. Дакле, држава, као и сваки појединац могу бити таргетирани чак и из забаве, ега, самопотврђивања, хира. Овде је већ сасвим јасно колики то може бити проблем. Сматрајући да је појединац најслабија карика, заправо долазимо до тога да је држава управо то.

Чињеница је да је компетентан и адекватан ИТ стручњак веома скупа инвестиција за државу, али је још јасније колико је за владу и грађане скупље да га немају. Јасно је да потреба за развојем дигитализације није хир, већ неопходност, а адекватни и компетентни стручњаци елементарна радна снага сектора безбедности. Ово и није никакава новост ако узмемо за пример државе у Европи, где, рецимо конкретно Немачка већ неколико година спроводи план у ком је зацртан развој јавне управе кроз дигитализтацију, али и развој безбедносних информационих система.

У овој агенди коју је Немачка прописала јасно је стављено до знања да је дигитализација неопходна и да је рад на њеној имплементацији приоритетна ствар јавне управе. Али, овде се поред тога истиче бескомромисно улагање у ИТ сектор, тачније безбедносну политику информационих система истичући непредвидивост напада рањивих система чије би последице биле прескупе како за владе, тако и за грађане. Стога се истиче импозантан значај едукованих стручњака који би се бавили заштитом од сајбер напада.

Неко ће на ово рећи да Немачка има далеко веће ресурсе за тај подухват од наше државе, али ствар није фокусирана на ресурсе колико на неопходност стручњака у сектору безбедности нових технологија и дигитализације јер се сам проблем безбедности намеће дигиталним развојем јавне управе. Сама дигитализација аутоматски изискује интелектуалце који ће се бавити безбедносним питањима у интнернет технологијама кроз видове заштите државе, владе, грађана кроз развој јавне управе. У новембру 2017.године на дискусији од сајбер безбедности и приватности, др Ханс–Георг Масен, председавајући Немачке федералне канцеларије за безбедност закључио је чињеницу да што је интензивнија комуникација са спољним светом, то је не само већа шанса за остваривање пословних шанси, прилика и могућности, већ се увећавају ризик и опасност по безбедност система (https://www.verfassungsschutz.de/de/aktuelles/zur-sache/zs-2017-004-gastbeitrag-handelsblatt-20171127). Овакве и сличне констатације опомињу да времена у сајбер безбедности заштиту нема. Ту је евдентно да чим је систем једном експониран, он уколико нема адекватну заштиту неминовно треба рачунати може да буде компромитиван и нападнут. Консеквенце напада на необезбеђен систем су несагледиве. Јер чињеница је да развојем јавне управе кроз дигиталитацију треба истовремено решавати питања сајбер безбедности. Управо тај детаљ узрокује нове изазове са којима се суочавају државе у реформи јавне управе[1].

## ЉУДСКИ ФАКТОР И ТЕХНОЛОГИЈА КАО БЕЗБЕДНОСНИ ПРЕДУСЛОВ

Један од релевантнх стандарда за Менаџмент система информационе безбедности (ISMS) ИСМС је Међународна организација за стандардизацију (ISO) ИСО и Међународна Електортех-

1 Federal Office for Information Security. 14. Deutscher IT Sicherheitskongress. Knowing risks, accepting challenges, designing solutions. In: Conference Proceedings for the 14th German IT Security Conference, Preface. Bonn, Bad Godesberg; 2015.

ничка комисија (IEC) ИЕЦ.[2] ИСМС (ISMS) се састоји од четири компоненте: менаџмента, средстава, процеса спровођења сајбер безбедности и особља. Процес спровођења сајбер безбедности укључује полису сајбер безбедности у којој је сајбер безбедност спецификована, детерминисана и стратешки деларисана у складу са адекватном имплементацијом која се документује, затим је истакнут сам концепт сајбер безбедности и развој сајбер безбедности институција. Једном када се ИСМС имплементира, од круцијалног је значаја да информације и подаци буду адекватно похрањени и да запослени имају потпуну свест о последицама неадекватног коришћења осетљивих података[3].

На овај начин се оставља довољно простора професионалцима који се баве заштитом сајбер система да раде свој посао, јер онда када запослени на осталим радним местима воде рачуна о безбедносним процедурама простор за малверзације се смањује. Одговорна јавна администрација обликује информациону безбедност у виду превенције, откривања проблема, реакције владе, пословних токова и друштва[4].

Јасно је да је иако у веома сложеном, великом и разгранатом систему улога појединца има значајно место. Увиђа се да је адекватна едукација заштите информација и примена безбедносне политике повезана не само са системом као таквим већ и са појединцем као основном безбедносном јединицом система. Сада је већ видљиво колико је велика улога запослених у превенцији безбедносних напада и малверзација. Због тога је неопходно да сви запослени буду едуковани не само о својој улози у безбедносном смислу већ и о свим елементима који су посредно неопходни да буду примењивани као и јасно детерминисани у функцији безбедногпословног окружења и профеионалних активности у сајбер окружењу. Суштински је обучити запослене не само да буду свесни онога што представља безбедносну опасност, као и како да се поступају у складу са сајбер безбеднсосно исправним корацима, него и да уколико се затекну у зони сајбер напада, знају како да поступају[5].

2 International Organization for Standardization (ISO) Survey, The ISO Survey of Management System Standard Certifications (2006-2015): ISO/IEC 27001—Information Technology—Information Security Management Systems—Requirements, ISO/IEC 27001: 2013/Cor 2:2015. 2015.

3 PCI Security Standards Council. Security Awareness Program. Special Interest Group, PCI Data Security Standard (PCI DSS), Version 1.0; 2014.

4 https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html;jsessionid=70E868EBB5E530CDA1AF059A22A5D485.1_cid341

5 www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_3_Sensibilisierung_und_Schulung.html

Једном када се развије систем непрекидне имплементације стечених знања из оквира безбедности информационих технологија, лако је редефинисати их, пратити, унапређивати јер је онда када је свест запослених на довољном нивоу да се може посматрати и тумачити у оквиру свакодневних радних процеса као саставни, а не екслузивни део система и радних обавеза. У околностима где се безбедносна политика инкапсулира у секторе који су надлежни за тај проблем, а сви остали запослени искључе из примарног фокуса на безбедносни аспект, логично је очекивати веће проблеме које изазива разгранавање јавне управе дигитализацијом. Јасно се намеће закључак да сваки запослени у јавној управи не само да треба да буде свестан опасности коју дигитализација и имплементација информационих технологија може да донесе систему, влади и грађанима, већ и да буде активна карика у борби против сајбер напада ма које врсте, а у домену своје надлежности, знања и могућности.

Овде треба разматрати и чињеницу да се овде небезбедност проматра кроз и као опасност од саме примене информационих технологија и алатки за рад јавне управе, стога је степен заштите на позицијама запослених крајње лимитиран и неретко најрањиви, а стога и најатрактивнији за контунуирано унапређивање. [6] Јасно је да техничка решења сама по себи показују одређене мањкавости усредсређене на периодичне и очекиване слабости попут вируса, одбране система од напада и сличног. Сасвим је јасно да се безбедност овде највише своди на саму технологију, али је човек круцијали фактор у разумевању развоја и могућности, као и употребе те технологије у циљу заштите система. Овде је најмање реч о појединцу као окидачу за реакцију, а највише реч о самој технологији као таквој. [7] Јер информациони системи сами по себи индикују инволвираност људског фактора у процес рада и неретко је случај да се корисници не опходе у складу са очекиваним и прихватљивим понашањем. Због овога се имплицира да је човек неретко „слаба карика“ система укључујући извештаје и садржаје из области информационе безбедности у процресу рада.

У сваком случају, значајно је нагалсити да се данас сусрећемо са ревалоризацијом и рекаракретизацијом људи, зато што су уочени фундаментални стратешки дефицити у самим институцијама, а као директна последица људског фактора. (Kruger, Steyn 2018, 2235-2244)

6 Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern (BAköV)/ Federal Academy of Public Administration in the Federal Ministry of Interior. Manual of IT Security Officer in the Public Administration, version 3.0. Brühl; 2009.

7 Security Education. IFIP – International Federation for Information Processing. Vol. 237. Boston, MA: Springer; 2007, 33-40.

На тему човека као елемента безбедности у процесу дигитализације и развоја јавне управе широм света било је више студија које су валоризовале вредности појединаца који су били безбедносно едуковани у контексту сајбер опасности од напада или малфункција. И испоставило се, потпуно шокантно да највећи број менаџера јавне управе радије прихвата да плати шестоцифрену новчану суму уцењивачу, него да имплеменира нов дигитални безбедносни систем. [8]

Ако један оволико значајан елемент узмемо у разматрање, поставља се пуно питања о суштинској улози менаџмента и проблема који оваква решења праве јавној управи. Није случајност да се окави догађају одвијају, али је недопустив исход који заправо охрабрује сајбер нападе. Менаџери би требало да сто постотно учествују у циљевима јавне управе и дословно никад не омогуће реализацију уцена. Уколико се правовремено обезбеде заштитни системи и кадар који ће се уско и искључиво бавити тим питањима, а остали запослени пролазити адекватне обуке, менаџмент не би смео да има ову врсту проблема на који је пристанак на уцену је неприхватљив. Па, ипак, када се у обзир узме расположивост информација захваћених пленом сајбер уцењивача, поставља се јасна импликација да је менаџменту било јефтиније да прихвати уцену него у кратком року покуша да реши проблем, ризикујући да нашкоди систему.

Овакве чињенице сасвим јасно показују рањивост система и изложеност сајбер криминалу чије спречавање обавезује динамичну службу безбедности инкорпорирану у дигитализацију јавне управе, али и едуковање запослених о чему је било речи.

Технологија сама по себи не може да буде довољно решење у заштити јавне управе. Технологија је још увек у сврси сервиса људском фактору и за сада још увек већина јавне управе ради у кохерентном радном окружењу где је човек кључна карика на коју се технологија надовезује али је човек и даље тај који се пита за њену контролу, експолатацију или дисфункционалност. С тим у вези велики значај је став који заузима менаџмент, али и понашањае свих запослених (Singh, Picot, Kranz, Cupta, Ojha 2013, 225-239). Руководиоци сектора јавне управе у највећем броју случаја имају свест о опасностима сајбер напада али је на њима да користе све алате како би избегли исходе које нико не жели. Проблем увек настаје у организацији едукације и имплементације решења што је још један чвор у низу чворова комплексног функционисања јавне управе. Делује као да менаџерима који воде секторе јавне управе

8 https://www.intechopen.com/books/public-management-and-administration/information-security-awareness-in-public-administrations#B19.

само фали још комплкесан безбедносни пакет који треба имплементирати и за који треба обучити људе како би се још више хаоса унело у њихово радно окружење. Али је факат да је овај вид безбедности неизбежан.

Када се посматра безбедност у смислу технолога наизглед делује да је човек сувишан фактор. У циљу заштите информација и рада система јавне управе неопходно је укључити и људски фактор и то у смислу едукације о социјалном инжењерингу као виду напада којим могу бити изложени и са којим би могли бити суочени. Људски фактор данас има значајну улогу у организацији информационих безбедносних система и понашање усклађено са безбедносно исправним поступањем указује на свест запослених о личној потенцијалној изложености ризику. Свакако да је простора за унапређење и пораст свести од опасности сајбер напада увек довољно у оквиру развоја јавне управе и да ће га протоком времена логично бити све више. Због тога се са сигурношћу може рећи да руководиоци институција јавне управе имају значајну улогу у питањима безбедности јавне управе. Између осталог треба нагласити да су управо руководиоци ти који имају највишу могућу одговорност и слободу у хијерархији да коригују проблеме унутар институција. Стављање проблема под тепих и ишчекивање да се реше сами од себе не само да неће допринети решењу проблема, него ће отворити још несагледиво више простора за малверзације, а несносни трошкови не превенирања сајбер безбедносних напада ослабиће буџет уливајући новац управо тамо где не би требало- у руке сајбер мафије.

## ЗАКЉУЧАК

Сватајући неопходност и брзину дигитализације у развоју јавне управе, закључује се да је безбедносни фактор од круцијалног значаја за адекватно, сигурно и правилно функционисање свих сектора јавне управе. Заштита владе и грађана државе кроз институције јавне упрве уобличена је кроз технологије, али свакако и неизоставан људски фактор који за циљ има превенцију, препознавање и сузбијање сајбер напада у циљу безбедносне заштите. Јавна управа у смислу безбедности може да се посматра само кроз призму интеракције технологије и људског факотра са сталним надоградњама и имплементацијом нових знања из области технологије у циљу заштите система јавне управе. Када се размотри читава ситуација јавна управа има значајну потребу за системима безбедности од људског факора до интерферентног односа човека и технологије, до технологије које морају бити инвентивне и усклађе-

не са актуелним технолошким токовима у свету у сектору сајбер безбедности. Јавна управа пред собом још веома дуго неће имати простора да ствар препусти само техологији и како околности показују унутар овог система који је још увек у свом развоју постоји веома много простора за имплементацију безбедносних система и едукацију запослених али и највишег менаџмента управе.

## РЕФЕРЕНЦЕ


Јовановић Зоран, „Утицај омбудсмана (заштитника грађана) на делатност јавних служби“, у зборнику: XXI век - век услуга и услужног права (приредио: Миодраг Мићовић), књ. 2, Правни факултет Универзитета у Крагујевцу, Институт за правне и друштвене науке, Крагујевац, 2011, стр. 396.

Јовановић Зоран, „Изазови и трендови у управљању људским ресурсима у јавној управи“, у зборнику: XXI век - век услуга и услужног права (приредио Миодраг Мићовић), књ. 6, Правни факултет Универзитета у Крагујевцу, Институт за правне и друштвене науке, Крагујевац, 2015, стр. 275-276.

Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern (BAköV)/Federal Academy of Public Administration in the Federal Ministry of Interior. Manual of IT Security Officer in the Public Administration, version 3.0. Brühl; 2009.

Clapp, Gordon. 1948. „Public Administration in an Advancing South“, Public Administration Review Vol. 8. no. 2 pp. 169–75.

Federal Office for Information Security. 14. Deutscher IT Sicherheitskongress. Knowing risks, accepting challenges, designing solutions. In: Conference Proceedings for the 14th German IT Security Conference, Preface. Bonn, Bad Godesberg; 2015.

International Organization for Standardization (ISO) Survey, The ISO Survey of Management System Standard Certifications (2006-2015): ISO/IEC 27001—Information Technology—Information Security Management Systems—Requirements, ISO/IEC 27001: 2013/Cor 2:2015. 2015.

Kruger H, Drevin L, Steyn T. Email security awareness: A practical assessment of employee behaviour. In: Futcher L, Dodge R, editors. Fifth World Conference on Information Scholl M, Fuhrmann F, Scholl LR. Scientific Knowledge of the Human Side of Information Security as a Basis for Sustainable Trainings in Organizational Practices. In: Proceedings of the 51th Hawaii International Conference on System Sciences (HICSS), Big Island, Hawaii; 2018. pp. 2235-2244. Available from: http://hdl.handle.net/10125/50168.

Pollit Christopher, Geert Bouckaert, Public Management Reform, A

Comparative Analysis, Oxford University press, 2002, стр. 6.

PCI Security Standards Council. Security Awareness Program. Special Interest Group, PCI Data Security Standard (PCI DSS), Version 1.0; 2014.

Security Education. IFIP – International Federation for Information Processing. Vol. 237. Boston, MA: Springer; 2007:33-40.

Shields, Patricia. 1998. „Pragmatism as a Philosophy of Science: A Tool for Public Administration“, Research in Public Administration Vol. 4. p. 199.

Singh AN, Picot A, Kranz J, Cupta MP, Ojha A. Information security management (ism) practices: Lessons from select cases from India and Germany. Global Journal of Flexible Systems Management. 2013;14:225-239.

Workman M. Gaining access with social engineering: An empirical study of the threat. Information Systems Security. 2007;16:315-331.

https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html;jsessionid=70E868EBB5E530CDA1AF059A22A5D485.1_cid341

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_3_Sensibilisierung_und_Schulung.html

https://www.verfassungsschutz.de/de/aktuelles/zur-sache/zs-2017-004-gastbeitrag-handelsblatt-20171127

https://www.intechopen.com/books/public-management-and-administration/information-security-awareness-in-public-administrations#B19

http://www.bmwi.de/Redaktion/EN/Dossier/digitisation.html

**Sanja Klisaric**

## SECURITY IN PUBLIC ADMINISTRATION

### Resume

As we are facing the growing need for the development of public administration, there is a certain importance of the adequate security systems implementation. This paper refers that all data could be used for the right or malicious purpose. Because security is much more than must, it is important to implement all possible ways to protect important data and secure real life and people behind that. It is common to think that public administration has to many tasks, but

all will fell down if security problems are not on the level that could be controlled as any threat even unseen must be exterminated. This paper signifies how strong is bond between state and security systems, and how vulnerable is public administration. The importance of cyber security is a crucial segment of developing and functioning of every part of the public administration. This paper suggest that security as an endless field always confronts with new challenges as the main reason of its own existence protecting the citizens as well as state.

**Keywords:** public administration reform, security, public administration, information protection, data security, cyber security.

* Овај рад је примљен 22. јануара 2021. године, а прихваћен на састанку Редакције 21. јуна 2021. године.