DOI: 10.46541/978-86-7233-416-6_46

Рајко Иванишевић
Економски факултет у Суботици,
Универзитет у Новом Саду,
Нови Сад, Република Србија
rajko.ivanisevic@ef.uns.ac.rs

УТИЦАЈ ДИГИТАЛНЕ ТРАНСФОРМАЦИЈЕ НА РИЗИК БЕЗБЕДНОСТИ ИНФОРМАЦИЈА У ИНФОРМАЦИОНИМ СИСТЕМИМА

Апстракт: Информациони системи, у данашње време, доживљавају есконенцијалну експанзију, а један од главних разлога је и дигитална трансформација. Сврха рада била је да се истражи утицај дигиталне трансформације на ризик безбедности информација у информационим системима. Постављена су два истраживачка питања. Прво, који су фактори који највише утичу на ризик безбедности информација и друго, важност фактора са аспекта њиховог посматрања. Метода коришћена за спровођење прегледа литературе базирана је на наративном прегледу и извршена је текстуална наративна анализа. Утврђено је да је главни фактор који утиче на ризик безбедности информацијама, према свим укљученим радовима, човек. Важност фактора са аспекта посматрања је зависила од предмета истраживања укљученог рада, али се провлачи нит тежње ка што већој глобализацији (централизацији података) и стварању „заједничке базе“ на светском нивоу. Ограничавајући фактор представља посматрани период од 2021. до 2023. године. Исти је узет ради актуелности информација, а сходно наглим променама услед криза на светском нивоу, убрзане дигиталне трансформације као последице тога и што присутнијег рада од куће који је у ранијим годинама био минорно заступљен. Будућа истраживања би се могла базирати на корелацији вештачке интелигнеције и ризика безбедности информацијама.

Кључне речи: ризик безбедности информација, информациони ситем, дигитална трансформација

IMPACT OF DIGITAL TRANSFORMATION ON INFORMATION SECURITY RISK IN INFORMATION SYSTEMS

Abstract: Information systems, nowadays, are experiencing exponential expansion, and one of the main reasons is digital transformation. The purpose of the paper was to investigate the impact of digital transformation on the risk of information security in information systems. Two research questions were asked. First, what are the factors that have the greatest influence on the risk of information security and secondly, the importance of factors from the aspect of their observation. The method used to conduct the literature review was based on a narrative review and a textual narrative analysis was performed. It was determined that the main factor influencing the risk of information security, according to all included works, is man. The importance of the factor from the aspect of observation depended on the research subject of the included work, but the thread of striving towards greater globalization (centralization of data) and the creation of a "common base" at the global level runs through. The limiting factor is the observed period from 2021 to 2023. It was taken for the sake of current information, and in accordance with sudden changes due to crises at the global level, accelerated digital transformation as a consequence of that and the ever-present work from home, which in earlier

years was minor. Future research could be based on the correlation of artificial intelligence and information security risks.

Keywords: information security risk, information system, digital transformation

1. УВОД

Дигитална трансформација све више узима маха, а самим тим долази до пораста брзине протока информација, као и количине самих података који постају доступни у системима, а који се до сада нису налазили у електронској форми. Дигитална трансформација, поред свих својих предности, исказује и своју негативну страну, а она је везана за ризик. За ризик који се огледа у неовлашћеном приступу, употреби, ометању, откривању, преправкама или уништавању информација или система, а понекад и информација и система.

Ризик безбедности информација, у савременом пословању, најчешће се огледа кроз сајбер безбедност. Просто је незамисливо да организација користи информациони систем који неће имати додирних тачака са спољним мрежама. Како наводе Hijji и Alam (2022), сајбер безбедност игра суштинску улогу у рачунарству и информационој технологији. Разлог томе проналазе у директном утицају на критична средства и информације организације. Такође, осврћући се на пандемију Ковид-19, говоре и о порасту броја организација које су омогућиле рад од куће и тиме продубиле проблем сајбер безбедности. Предузећа убрзавају дигиталну трансформацију и тиме сајбер безбедност постаје њихова главна брига (Khan и сарадници, 2022).

Глобализација и интегрисање информационих система на светском нивоу представљају још један фактор који захтева дигиталну трансформацију, откривајући организације, које су до сада биле „испод радара“, за потенцијалне претње у области безбедности информација. Поред организација, на мети се налазе и државе, или више држава које имају заједничке споразуме, те је потребно обратити пажњу и на ризик безбедности информација на националном нивоу и на нивоу међународне сарадње.

Сходно поменутом, формирана су два истраживачка питања. Питање 1: Који су фактори који највише утичу на ризик безбедности информација? Питање 2: Важност фактора са аспекта њиховог посматрања. Одговор на идентификована истраживачка питања и могућност даљег спровођења истраживања представљен је у наредним одељцима рада.

2. ИСТРАЖИВАЧКА МЕТОДОЛОГИЈА И ПРОЦЕС СПРОВОЂЕЊА ИСТРАЖИВАЊА

За спровођење истраживања, идентификацијом два истраживачка питања (фактори који највише утичу на ризик безбедности информација и важност фактора са аспекта њиховог посматрања), коришћена је истраживачка методологија за систематски преглед литературе. Xiao и Watson (2019) предлажу осам корака:

- формулисање истраживачког проблема,
- развој и валидација процеса прегледа,
- тражење литературе,
- преглед за укључивање студије у рад,
- оцењивање квалитета,
- издвајање података,
- анализирање и синтетизовање података,
- извештавање о налазима.

Како је спроведен преглед литературе, одређени делови корака нису примењени попут спровођења истраживања унапред и уназад.

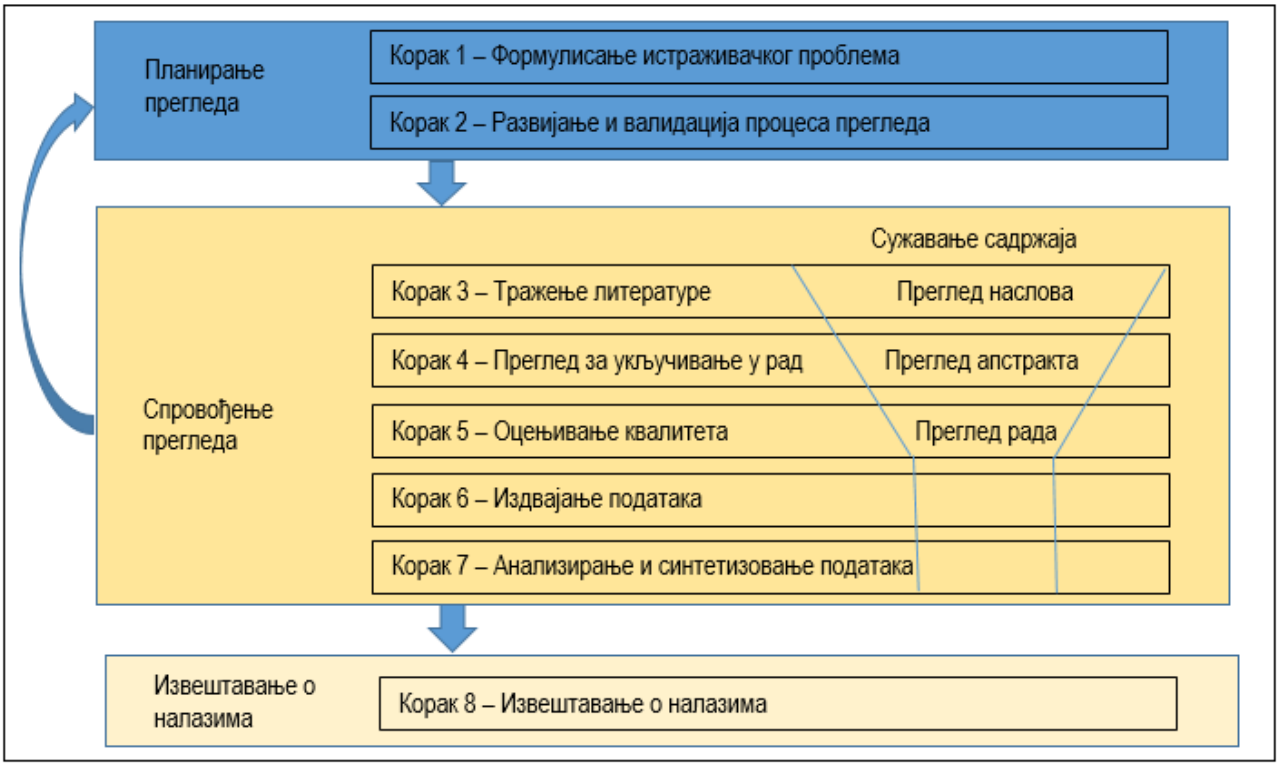

График 1: Процес систематског прегледа литературе
Извор: Креирано на основу Xiao и Watson (Xiao & Watson, 2019)

Приликом формулисања истраживачког питања циљ је био пронаћи актуелну област која је у спрези са дигиталном трансформацијом. Истраживањем дошло се до закључка да је један од главних светских проблема сајбер безбедност, те да глобални напад у тој области може изазвати велике проблеме у другим, зависним областима. Те зависне области су у суштини све области, јер баш убрзањем дигиталне трансформације у претходне три године све организације су убачене у електронски систем, вољно или невољно. Како је сврха постојања организација различита, али област сајбер безбедности фундаментално иста, формулисано је питање фактора који утичу на ризик безбедности информација. Покушано је увидети и спрегу између аспеката посматрања и фактора. Због актуелности теме и релевантности података истраживање је вршено на временском узорку 2021-2023.

У почетку је формулисано питање фактора који утичу на ризик безбедности информација, али то није било засебно довољно (посматрати факторе као издвојену јединку), те смо аспект посматрања увели као додатно питање.

Приликом тражења литературе и прегледа за укључивање у рад коришћен је канал за претраживање литературе – електронска база података *Web Of Science*. Претрага унапред и уназад није спровођена, укључен је само један рад мимо пронађених (претрагом унапред). Период посматрања је ограничен на године 2021, 2022, 2023. За вршење претраге коришћена је фраза *„Information security risk in digital transformation“*. Радови који нису били везани за безбедност нису посматрани. Претрага је вршена 25.1.2023. године и узети су у обзир само објављени радови. Након претраге нису увођена додатна ограничења.

Приликом претраге према унетој фрази на електронској бази података *Web Of Science* дошло се до шездесет и девет (69) радова за период од претходне три године, рачунајући и текућу 2023. Из прегледа су одмах искључени радови који су били у „раном приступу“ (*early access*). Таквих радова је било укупно два (2), те је након тога преостало шездесет и седам (67) радова. Прегледом наслова искључени су радови који, по процени аутора, нису пружали информације значајне за истраживање. Након тога приступило се ишчитавању апстраката преосталих радова. Резултат након овог прегледа јесте једанаест (11) потенцијалних радова који су значајни за преглед литературе. Одређени радови су били већ доступни у електронској бази, до осталих се покушало доћи претрагом по интернету. Након спровођења овог процеса елиминисана су три рада која нису пронађена у пуној форми (целокупан текст). У овом тренутку укупан број одговарајућих радова износио је осам (8).

Читањем радова вршена је оцена квалитета. Рад је требало да пружи информацију значајну за спровођење прегледа литературе, тј. информацију значајну за барем једно од два истраживачка питања. Од осам пронађених радова, који су задовољавали критеријум након читања апстракта да буду укључени у преглед литературе, искључен је један (1) из прегледа јер није пружао информације од значаја за спровођење истраживања и извођење закључака. Од преосталих седам радова дупликата није било и сви су радови били на енглеском језику. Овом броју прикључен је још један рад претрагом унапред, те је укупан број радова осам (8).

Анализирање и синтетизовање података извршено је у седмом кораку, а извештавање о резултатима налази се у наставку рада у посебној тачки.

3. РЕЗУЛТАТИ ПРЕГЛЕДА ЛИТЕРАТУРЕ

Наративни преглед је метода коришћена за издвајање података. Она омогућава блажи критеријум за укључивање рада у преглед литературе. Извршена је и текстуална наративна синтеза, тј. посматрани су фактори и аспекти посматрања заједно, у својој спрези.

Осми корак обухвата извештавање о налазима прегледа литературе. Сходно истраживачким питањима направљена су два одељка. Раздвојеност у два засебна одељка не треба да рашчлани и отуђи два истраживачка питања. Напротив, потребно их је посматрати у спрези и односу једно према другом. Наведено је урађено због прегледности и систематичности.

3.1. Који су фактори који највише утичу на ризик безбедности информација

На самом почетку треба истаћи да радови укључени у литератури у великој мери сагласни када је реч о главном фактору који има утицај на ризик безбедности информација. Реч је о људском фактору. Остали фактори су били заступљени у зависности од тематике рада.

Astakhova (2021) наводи да без обзира колико се брзо развијају технологије и средства заштите информација, информациони систем постаје рањив ако се његов корисник остави без надзора. У раду се даље наводи да удео интерних цурења информација чини више од половине свих цурења забележених у свету. До тога долази услед грешака или намерних радњи запослених (укључујући и менаџмент) и власнике инфромација.

Како наводе Hijji и Alam (2022), сајбер безбедност игра суштинску улогу у рачунарству и инфромационој технологији због свог директног утицаја на критична средства и информације организација. Они напомињу да је Ковид-19 утицао на пораст броја предузећа која омогућавају рад од куће. Овим чином убрзана је дигитална трансформација, али је и продубљен проблем сајбер безбедности. Према њима сајбер безбедност представља важну улогу у заштити државних података, предузећа, интелектуалне својине и приватне информације од сајбер криминала. Предлаже се пет фаза за спровођење методологије истраживања: преглед литературе и емпиријска истраживања, развијање нивоа и пракси *CAT (Cybersecurity awareness and training)* оквира, развој *CAT* оквира, студије случаја и евалуација повратне информације након студије случаја. Такође, предлажу три критеријума за оцењивање нивоа способности, а то су почетни, који укључује само свест о сајбер безбедности, средњи, који укључује обуку за програм сајбер безбедности и напредни који представља свеобухватне прегледе и практичне и коначне процене свести о сајбер безбедности и праграм обуке. Како је и овде људски фактор доминантан, аутори предлажу укључивање софтверских алата у комбинацији са *AI CAT* оквиром у жељи за импелментацијом мерења свести својих запослених о сајбер безбедности и способности обуке у реалном времену.

У прилог људском фактору као кључном за ризик безбедности информација говоре и наводи Creazza и сарадника (2022), да су људи кључан елемент у побољшању сајбер отпорности у области ланца снабдевања. Рад пружа увид који изазива размишљање о неусклађености између перципиране релевантности људског фактора као извора ризика (висок) и перципиране важности контра мера за ублажавање догађаја ризика који потичу из тог извора (ниско). Ово изазива организације да преиспитају свој приступ ублажавању ризика који долазе од запослених. Наводе да је потребно да организације преиспитају своју перцепцију у вези са појавом догађаја и перципираног нивоа ризика повезаног са тим догађајем.

Yerina и сарадници (2021) разврставају претње на: неовлашћен приступ информационим и телекомуникационим системима и мрежама, циљани сајбер напади на инсфраструктурне објекте који осигуравају живот друштва, нарушавање поверљивости информација које се чувају, преносе и обрађују у информационим и телекомуникационим системима (државне, пословне, банкарске тајне, лични подаци, објекти и интелектуалне својине). Њихова класификација врло је слична као код Hijji и Alam. У класичне сајбер злочине убрајају врсте лажних активности које имају за циљ незаконит приступ поверљивим корисничким информацијама и аутоматизованим базама података – пецање, картирање, хаковање, малвер и пиратерија *(fishing, carding, hacking, malware, piracy)*. Предмет сајбер криминала су лични подаци, банковни рачуни, кориснички подаци, лозинке, други лични подаци и појединаца и предузећа и јавног сектора. Рад обрађује и сајбер шпијунажу, сајбер диверзију и сајбер тероризам.

Људски фактор треба посматрати и са становишта свести. Syuntyurenko (2022) тврди да ескалација глобализације доводи до промена у развоју човечанства, тј. преоријентације технолошког напретка са стварања нових производних технологија на стварање технологија за циљано формирање свести за настанак нових људских потреба. Даље се образлаже да ови процеси манипулисања људском свешћу (свешћу заједница, друштвених група) потенцијално садрже континуитет друштвених ризика у будућем развоју човечанства. Људи су створили свет који је превише сложен за њихов сопствени интелект као појединца. Наводи да компликујући свет, информационе технологије смањују његову препознатљивост индивидуалном свешћу. Човек перципира информациони свет док живи у физичком, стога све више реагује не на стварни свет, већ на виртуелни, губећи критеријум истине. Такође, наводи да осим дигиталног јаза расту и ризици повезани са дигиталном зависношћу.

Остали фактори везани су за факторе начина заштите мрежа, коришћене технологије како у области хардвера, тако и у области софтвера, итд. Нису појединачно истражени из разлога што су пронађени радови били изузетно усредсређени на корисника (човека) као најзначајнију карику код безбедности информација.

3.2. Важност фактора са аспекта њиховог посматрања

Аспект посматрања, тј. област у којој се идентификује ризик безбедности информација, показао се као значајан. Са становишта рада мреже Di и сарадници (2022) наводе предности генетског алгоритма. Наиме, рад говори о ефикаснијем раду мрежне организационе структуре засноване на генетском алгоритму од традиционалне мрежне организационе структуре. Структура организације мреже заснована на генетском алгоритму може не само да унапреди ефикасност рада предузећа, већ и да унапреди безбедност информација. Они предлажу побољшани генетски алгоритам који отклања недостатке традиционалног генетског алгоритма. Побољшани генетски алгоритам има јачу способност претраживања и већу брзину конвергенције.

Један од значајних аспеката јесте и правни аспект. Yerina и сарадници (2021) и Koltays и сарадници (2021) наводе значај уговорних страна. Koltays и сарадници (2021) посматрају безбедност у дигиталној трансформацији са аспекта поверења уговорних страна. Премињују математичке моделе за процену веродостојности супротне стране. Слично томе Yerina и сарадници (2021) наводе изазове и претње у области сајбер безбедности са аспекта међународне сарадње и националне безбедности. Укључују у свој оквир посматрања и светски ниво, наводећи да је сајбер безбедност предмет разматрања Генералне скупштине УН, али и низа међународних организација попут Г7, ЕУ, НАТО, ОЕЦД, АПЕС, Светски економски форум, итд. Наводе да они раде заједно на областима стварања јединствене базе података о сајбер претњама и система за сталну размену информација, унапређења техничких стандарда и правила, итд. Наводи се и основ за међународну сарадњу и координацију земаља – *GCA (The Global Cybersecurity Agenda)*. Свака земља мора имати тим који је заслужан за брзо реаговање у случају напада – *CERT (Computer Emergency Response Team)*. Koltays и сарадници (2021) предлажу три групе приликом приступања проблему идентификацији вероватних прекршилаца и креирања модела прекршиоца: избегавање ризика, пренос ризика друге уговорне стране на друга предузећа, ублажавање ризика и прихватање ризика. Наводе да избегавање ризика обухвата *ISO 27001* који се фокусира на обезбеђивање да кршење безбедности информација не доведе до значајне финансијске штете за организацију и/или до значајних потешкоћа у њеним активностима. Такође, да има довољно добро обучених запослених који могу да спроведу процедуру за минимизирање могућих штетних последица у случају озбиљнијег инцидента *(ISO 2005)*. Пренос ризика друге уговорне стране образлажу да друга предузећа се баве усвајањем, утврђивањем и преносом процене ризика од поверења на друга предузећа. Све ово не смањује ризик од кривичних дела и злочина који представљају претњу безбедности и за појединачне организације и за целу државу. Аутори предлажу и модел који са разумном тачношћу даје процену ризика на основу улазних података. Начин на који се на светском нивоу анализира безбедност, а који помињу Yerina и сарадници (2021), јесте *GCI (Global Cybersecurity Index)* који служи за праћење статуса глобалног мрежног простора земаља чланица УН. Ово врши УН, а тело задужено за мерење/израчунавање индекса је *ITU (International Telecommunication Union)*. Индекс се утврђује годишње због процене укључености земаља у сајбер безбедност. Наводи се да се ослањају на законске, техничке, менаџерске институције, њихове образовне и истраживачке способности, доступност механизама сарадње и система за размену информација у мрежама. Сврха *GCI* је да омогући државама чланицама УН да идентификују потенцијалне начине за јачање заштите глобалног мрежног простора од сајбер претњи. Рад представља још један индекс, *NCSI (National Cyber Security Index)*. Он представља спремност земаља да спрече реализацију фундаменталних сајбер претњи, управљају сајбер инцидентима и сајбер кризама великих размера.

Слично изнад поменутом, Creazza и сарадници (2022) посматрају сајбер безбедност са аспекта ланца снабдевања (сличност се огледа у постојању више пружалаца услуга, уговорних страна). Издвајају значај пружаоца логистичких услуга као „оркестратора“ *CSCRM (Cyber Supply Chain Risk Management)* процеса. Сматрају да би организације требало да излазе из својих оквира, прелазећи своје границе, и тако створе заједничко знање о ризицима које би им помогло да ближе процене ниво ризика у својим ланцима снабдевања.

Даље, један од аспеката уско везаних за најзначајнији фактор (људски) јесте *ISC (Information Security Culture)*, тј. култура информационе безбедности. Astakhova (2021) тврди да свака организација има карактеристике унутрашњег и екстерног окружења, те да сходно томе проблеми самосталног избора на основу одређене стратегије развоја културе информационе безбедности су веома актуелни. Међутим, у теорији информационе безбедности овај проблем није проучаван и још није постао предмет посебних студија. Рад наводи да се организације налазе у окружењу које се константно мења, те да је потребно базирати се на ситуационом приступу ради адаптирања стратегије. Предлаже се дефанзивна стратегија и офанзивна (развојна) стратегија информационо-безбедносне културе. Одбрамбена стратегија је усмерена на минимизирање претњи по безбедност информација, циљна група су запослени као потенцијални прекршиоци, а спроводи се првенствено путем принудних мера. С друге стране, стратегија развоја има за циљ стварање система за смањење претњи потенцијалне позиције жртве (запосленог као жртве), повећано учешће у производним и управљачким процесима, као и кроз развој психолошког својства запослених. Предлаже се допуна *ISO/IEC 27000* стандарда о управљању безбедности информација и њихове одељке о безбедности информације који се односе на особље применом нацрта стандарда Култура инфомрационе безбедности. Овај нацрт стандарда, у раду, се састоји од седам делова у којима су формулисане дефиниције појмова људског фактора, људских ризика, културе, развојних

стратегија; фактора утицаја на културу информационе безбедности на индивидуалном и организационом нивоу; циљева, праваца, средстава и метода његовог формирања и развоја; организациони принципи и организационо-методолошки захтеви (захтеви за организацију и методологија за њено планирање, процену, контролу и унапређење); и захтеви за документовање ових процеса (за политику развоја културе информационе безбедности и друга локална документа за организовање ове теме) као дело имплементације како заштитних тако и развојних стратегија културе информационе безбедности.

На послетку Syuntyurenko (2022) посматра безбедност информација кроз холистички приступ, приступ човеку као бићу у читавој информатичкој збрци. Наводи да прекршиоци који почине дело кршења безбедности не само да су у могућности да копирају информације до којих су допрели, већ могу да ускладиште вирусе који уништавају апликативне програме који почињу да раден након одређеног времена, што отежава њихово откривање. То доводи до функционалног поремећаја информационих система, система заштите критичне инфраструктуре, контролних објеката, појаве друштвених тензија, итд. Наводи да се осим дигиталног јаза, појављује и пораст ризика повезаних са зависношћу. Савремене технологије стављају корисника у позицију дилера или корсиника лиценце, а као доказ томе наводи трансформацију интелектуалне својине у оруђе за злоупотребу монополског положаја власника технологије, пре свега информационих технологија.

4. ДИСКУСИЈА И ИЗВОЂЕЊЕ ЗАКЉУЧАКА

Прегледом литературе на тему утицаја дигиталне трансформације на ризик безбедности информација у информационом систему дошло се до следећих закључака. Како је прво истраживачко питање било из области фактора који утичу на ризик безбедности информација, може се рећи да је једногласно људски фактор најзначајнији и да представља највећи ризик. Поред људског фактора идентификовани су и фактори попут хардвера, софтвера, мреже, уговорних страна, итд. Ови фактори су зависили од аспекта посматрања, тј. области из које су радови написани. Аспекти посматрања су предочили да област ризика безбедности информација у дигиталној трансформацији има импликације како на микро нивоу, почевши чак од појединаца (индивидуални ниво), преко предузећа, па све до макро нивоа, држава, и на послетку до међународног, па чак и светског (глобалног) нивоа.

Утисак аутора овог рада на основу спроведеног прегледа литературе јесте да ризик безбедности није довољно разрађен, тј. да није успео да испрати дигиталну трансформацију. Тиме се створио јаз између области функционисања појединца, привреде и њихове заштите и сигурности на мрежама, али и у локалним окружењима. Подизањем свега дигиталног на интернет практично долази до могућности глобалног приступа подацима чак и онима са микро и индивидуалног нивоа. Ово даје простора за могућност насумичних али и координисаних сајбер напада који би могли да паралишу и појединца и организацију, али и државу и међународну заједницу. Светски догађаји говоре у прилог датој тврдњи, тако да треба бити обазрив у периоду који се налази пред нама.

Још једна чињеница у прилог кашњења области ризика безбедност информација за дигиталном трансформацијом јесте незавидан број радова у претходне три године који се баве овом тематиком. Сматрам да је несумњиво људски фактор најизраженији, а као потајни најзначајнији аспект назире се правни аспект јер све има правне и економске импликације. Рад има простора за даље истраживање и за примену конкретних емпиријских анализа у наредном периоду, а претходно написано може служити као темељна теоријска основа за даље истраживање.

РЕФЕРЕНЦЕ

Astakhova, L. V. (2021). Transformation of Strategic Models for Managing Human Risks of Information Security of an Enterprise as an Imperative of the Digital Industry. *Scientific and Technical Information Processing*, *48*(2), 71–77. https://doi.org/10.3103/S0147688221020027

Creazza, A., Colicchia, C., Spiezia, S., & Dallari, F. (2022). Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. *Supply Chain Management: An International Journal*, *27*(1), 30–53. https://doi.org/10.1108/SCM-02-2020-0073

Di, Z., Liu, Y., & Li, S. (2022). Networked Organizational Structure of Enterprise Information Security Management Based on Digital Transformation and Genetic Algorithm. *Frontiers in Public Health*, *10*. https://doi.org/10.3389/fpubh.2022.921632

Hijji, M., & Alam, G. (2022). Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. *Sensors*, *22*(22), 8663. https://doi.org/10.3390/s22228663

Khan, F., Zahid, M., Gürüler, H., Tarimer, I., & Whangbo, T. (2022). An Efficient and Reliable Multicasting for Smart Cities. *Computers, Materials & Continua*, *72*(1), 663–678. https://doi.org/10.32604/cmc.2022.022934

Koltays, A., Konev, A., & Shelupanov, A. (2021). Mathematical Model for Choosing Counterparty When Assessing Information Security Risks. *Risks*, *9*(7), 133. https://doi.org/10.3390/risks9070133

Syuntyurenko, O. V. (2022). Predicting Potential Threats and Megarisks in Information Technology Development. *Scientific and Technical Information Processing*, *49*(1), 48–59. https://doi.org/10.3103/S0147688222010130

Xiao, Y., & Watson, M. (2019). Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research*, *39*(1), 93–112. https://doi.org/10.1177/0739456X17723971

Yerina, A., Honchar, I., & Zaiets, S. (2021). Statistical Indicators of Cybersecurity Development in the Context of Digital Transformation of Economy and Society. *Science and Innovation*, *17*(3), 3–13. https://doi.org/10.15407/scine17.03.003