Оригиналан научни рад

351.74:008]:004
doi:10.5937/zrpfns57-48426

Љубомир С. Стајић
Универзитет у Новом Саду
Правни факултет у Новом Саду
Lj.Stajic@pf.uns.ac.rs
ORCID ID: 0000-0002-7594-5741

Ненад П. Радивојевић
Универзитет у Новом Саду
Правни факултет у Новом Саду
N.Radivojevic@pf.uns.ac.rs
ORCID ID: 0000-0002-0630-0632

Владан М. Мирковић
Универзитет у Новом Саду
Правни факултет у Новом Саду
V.Mirkovic@pf.uns.ac.rs
ORCID ID: 0000-0002-9995-8598

НЕКИ АСПЕКТИ БЕЗБЕДНОСНЕ КУЛТУРЕ У ИНФОРМАЦИОНИМ ТЕХНОЛОГИЈАМА*

Сажетак: *Информационе технологије (ИТ) су, између осталог, настале како би очувале и унапредиле живот и рад човека на пољу комуникације, образовања, очувања здравља, заштите животне средине и сл. Међутим, све технолошке иновације су поред позитивних имале и оне негативне последице по само друштво (и његову безбедност). Тако је и развој ИТ праћен бројним проблемима, питањима и контроверзама који у одређеној мери и у одређеним случајевима могу довести до угрожавања (појединца, група, компанија, државе, међународне заједнице и човечанства у целини). То је наметнуло потребу ангажовања свих (постојећих и нових) друштвених потенцијала како би се идентификовали сви они проблеми и последице које по друштво остављају како развој тако и примена ИТ. Један од тих потенцијала или*

* Рад је настао као резултат рада на научно-истраживачком пројекту *„Правна традиција и нови правни изазови“* у 2023. години, а чији је носилац Правни факултет Универзитета у Новом Саду.

механизама који друштву стоје на располагању јесте и безбедносна култура (у ИТ). Безбедносна култура је апсолутно позитивна категорија, а њена основна функција јесте превенција настанка угрожавајућих појава и остваривање оптималног стања безбедности. С тим у вези, предмет овог рада јесте анализа неких аспеката безбедносне културе у ИТ (првенствено етичких, социолошких, економских и правних). Циљ рада је проширење теоријског фонда знања из области безбедносне културе у ИТ, као и практично унапређење деловања и рада свих који учествују у креирању (развоју) и примени ИТ.

Кључне речи: *безбедност, информационе технологије, безбедносна култура, безбедносна култура у информационим технологијама, информационо-безбедносна култура.*

1. УВОД

Једна од основних преокупација човека од његовог настанка до данас била је како да опстане, а онда и како да се развија и напредује, односно како да буде безбедан.[1] Данас се све више говори о тзв. четвртој индустријској револуцији која је везана за развој дигиталних и информационих технологија (у даљем тексту: ИТ), или како кажу поједини аутори, „информационе технологије врше неупитну трансформацију (информациона револуција) из индустријског у информатичко друштво, најављујући нову дигиталну еру“.[2] С тим у вези је и крилатица „Све што ради – аутоматизује се, све што вреди – дигитализује се“.[3]

Основна функција ИТ је (или би бар требало да буде) унапређење људског живота, рада, комуникације, образовања, здравља, културе, безбедности и др. Иде се чак дотле да се тврди да су кључне карактеристике савременог друштва управо развој и употреба ИТ. Због тога се све више користе термини „информационо доба“, „технолошко-информационо доба“, „дигитална ера“, „информатичко друштво“, „информационо друштво“, односно друштво чији су опстанак и развој засновани на ИТ. У академским круговима, али и пракси постављају се питања како и колико ИТ (првенствено сајбер простор, интернет, вештачка интелигенција) утичу на остваривање националне безбедности, а онда и међународних односа, као и обрнуто, који су утицаји међународних односа у сајбер домену.[4] ИТ данас све више постају елемент моћи држава,

[1] Љубомир Стајић, *Основи система безбедности – са основама истраживања безбедносних појава*, Нови Сад 2021, 38.

[2] Саша Мијалковић, Вера Арежина-Ђерић, Горан Бошковић, „Корелација информационе и националне безбедности“, *Научно-стручно саветовање ЗИТЕХ*, Београд 2010.

[3] *Ibid*.

[4] Вид. Nazli Chucri, David D. Clark, *International Relations in the Cyber Age, The Co-Evolution Dilemma*, Cambridge Massachusetts 2018.

поред моћи знања, војне моћи, економске и политичке моћи. То је између осталог и довело до својеврсне „трке“ великих сила у погледу доминације у овој сфери људске делатности.

Треба бити свестан да су све технолошке иновације у људском друштву поред позитивних имале и оне негативне последице по само друштво (и његову безбедност). Једна од највидљивијих јесте и то да ИТ данас нису подједнако доступне свима.[5] Социјално раслојавање је приметно и у овој сфери, како унутар државе тако и између држава. Врло лако и врло често ИТ могу прерасти у генератор социјалних разлика у друштву,[6] што само по себи представља извор угрожавања. С тим у вези, одговорност за то сносе како крајњи корисници ИТ, тако и компаније које раде на развоју и иновацијама у ИТ сфери. Посебно, одговорност је и на државама и међународној заједници, као и струковним удружењима (националног и међународног карактера) да својим нормативним активностима уреде основна и најважнија питања развоја и употребе ИТ.

Један од „нових“ приступа који друштву стоји на располагању када су у питању развој и примена ИТ, а који ће бити у функцији остваривања безбедности, јесте концепт безбедносне културе. Када су у питању безбедност друштва и ИТ, безбедносна култура нам указује да морамо бити свесни да колико год ИТ убрзавају и олакшавају свакодневни рад и живот човека, толико са друге стране доносе и реалну опасност њене злоупотребе, са не тако занемарљивим последицама. Због тога посебну пажњу треба посветити питањима даљег развоја ИТ, а посебно вештачке интелигенције око које постоје бројна отворена, нерешена питања и контроверзе.[7] Питање остваривања

[5] Опште је позната чињеница да ИТ и вештачка интелигенција нису подједнако развијене и у употреби у свим државама. Светски лидери у овој области су пре свега САД, Кина, Руска Федерација, Велика Британија, Јапан, Јужна Кореја, поједине државе чланице ЕУ.

[6] Поједини аутори указују управо на ову врсту изазова када је у питању примена вештачке интелигенције, а то су социјалне разлике њене примене, односно замена и потискивање људског рада. Аутоматизација појединих процеса свакако доводи до смањења трошкова и повећања добити, али ће то нужно резултовати губитком посла на хиљаде и милионе људи. Такав ток догађаја ће неминовно довести до даљег продубљења поларизације савременог друштва. Србобран Бранковић, „Вештачка интелигенција и друштво“, *Српска политичка мисао* 2/2017, 30. Занимљиво је да је на овакав развој догађаја указивао професор Радомир Лукић још давне 1976. године, истичући да савремени друштвени процеси (у овом случају роботизација) „човека претварају у ствар, а друштвене односе у односе између ствари уместо између људи“. Такође, проф. Лукић посебно указује на то да „техника није сама себи циљ него средство за остваривање једног битног циља – а то је стварање потпунијег, савршенијег и срећнијег човека и друштва“. Радомир Лукић, *Социологија морала*, Београд 1976, 590 и 594.

[7] Један од најнових примера јесте да је највиши финансијски регулатор у Сједињеним Америчким Државама по први пут упозорио да употреба вештачке интелигенције представља ризик за финансијски систем. Савет за надзор финансијске стабилности (*FSOC*), тим водећих регулатора широм америчке владе, формално је класификовао вештачку интелигенцију као „рањивост у настајању“. Савет упозорава да „вештачка интелигенција има

људских права у дигиталној ери је нешто на шта посебно треба обратити пажњу.[8] Даље, довољно је навести пример да данас сви објекти и системи који чине критичну инфраструктуру[9] у једној држави функционишу и раде на платформама, програмима, софтверима и информационим системима, односно ИТ. Не треба бити толико маштовит да се замисле стравичне последице по безбедност друштва и државе, настале услед сајбер напада на објекте (електро)енергетског система,[10] нуклеарна постројења, хемијске индустрије, здравственог система, железничког саобраћаја, авиосаобраћаја и сл. Непосредне последице би осетили и сви грађани.

2. ПОЈАМ ИНФОРМАЦИОНИХ ТЕХНОЛОГИЈА И ЊИХОВ УТИЦАЈ НА БЕЗБЕДНОСТ

У најопштијем смислу, под ИТ подразумевамо рачунаре и телекомуникациону опрему за прикупљање, аутоматску обраду, складиштење и пренос података. Сматра се да се израз ИТ, у смислу у којем га данас познајемо, први пут појавио 1958. године. Наиме, синтагма ИТ се састоји из речи информација и технологија, при чему се информација дефинише као знање стечено истраживањем, проучавањем или инструкцијама, док се технологија дефинише као практична примена знања.[11] Према Међународној професионалној

потенцијал да подстакне иновације и подстакне ефикасност, али његова употреба у финансијским услугама захтева промишљену примену и надзор за управљање потенцијалним ризицима". https://euractiv.mondo.rs/ekonomija/a5281/Vestacka-inteligencija-je-opasnost-za-finansijski-sistem-upozorava-FSOC.html?utm_source=kurir_biznis&utm_medium=euractiv_widget&utm_campaign=naslovna/infobiz, 16. децембар 2023.

[8] Остваривање права на приватност и слободу изражавања, право на заштиту података о личности, ауторска и друга сродна права и др.

[9] У складу са чл. 4, ст. 1 Закона о критичној инфраструктури (*Службени гласник РС*, број 87/18), критичну инфраструктуру чине „системи, мреже, објекти или њихови делови, чији прекид функционисања или прекид испоруке роба односно услуга може имати *озбиљне последице на националну безбедност*, *здравље и животе људи, имовину*, *животну средину*, *безбедност грађана*, *економску стабилност*, односно *угрозити функционисање Републике Србије*". Чл. 6, ст, 1 су одређени сектори у којима се врши идентификација и одређивање критичне инфраструктуре. То су: *енергетика, саобраћај, снабдевање водом и храном, здравство*, *финансије*, *телекомуникационе и информационе технологије*, *заштита животне средине и функционисање државних органа*. Битно је напоменути да су управо ИТ одређене као један од сектора који чини критичну инфраструктуру. Са безбедносног аспекта је још значајније то што сви остали сектори функционишу на платформама (софтверима, хардверима и др.) који чине ИТ.

[10] Електропривреда Србије је била објекат хакерског напада 19. децембра 2023. године. Према првим извештавањима медија, у питању је био хакерски напад крипто-типа. https://www.b92.net/biz/vesti/srbija/hakeri-napali-eps-sistem-se-uspesno-oporavlja-2452512, 19. децембар 2023.

[11] Мирјана Петковић, Јелена Лукић, „Утицај информационе технологије на дизајн организације: пример организације у здравству", *Социологија* 3/2013, 441.

организацији из области информационих технологија (*ISACA*), ИТ (енгл. *information tehnology*) обухватају „хардвер, софтвер, комуникациона и друга средства која се користе за унос, складиштење, обраду, пренос и излаз података у било ком облику“.[12] ИТ се такође дефинише и као „изучавање, дизајн, развој, имплементација и подршка или управљање у рачунарским информационим системима, софтверским апликацијама и хардвером“. Међутим, треба рећи да појам ИТ често обухвата и знатно шире поље области технологије, почев од свега онога чиме се ИТ професионалци баве, односно инсталација апликативних програма, њихово пројектовање, умрежавање и инжењеринг рачунарских хардвера, дизајнирање софтвера и база података као и управљање и администрација информационим системом,[13] па све до развоја и употребе вештачке интелигенције.

Треба напоменути да су у употреби и термини информационо-комуникационе технологије (ИКТ) или информационо-телекомуникационе технологије (ИТТ), чији је циљ да се укаже на значај ИТ у остваривању комуникације која се одвија путем телефона (данас „паметних“ телефона), каблова, интернета, рачунара и др. Њихов првенствени значај за друштво јесте могућност скупљања и обраде великих количина података и информација, а онда и њихова употреба путем истих ИТ. Ово су уједно и једни од највећих бенефита по друштво. Треба напоменути да у савременом друштву, у великим системима који функционишу на бази великог броја података и информација, време и континуитет остваривања пословања или делатности је кључан фактор опстанка и развоја. Типичан пример тога јесте остваривање неких од права грађана пред државним органима, јавним службама, привредним субјектима, образовним и здравственим установама. Не тако давна пандемија КОВИД-19 је указала на значај одржавања континуитета образовног процеса у образовном систему или пословања привредних субјекта, а све у условима физичке изолованости која је требало да спречи ширење вируса.

Свему томе треба додати и до скоро незамисливе могућности развоја и употребе вештачке интелигенције која је у функцији олакшања и унапређења људског рада у индустрији, лечења појединих болести,[14] инвалидитета,

---

[12] ISACA, Glossary. Доступно на: https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/glossary/glossary.pdf, 25. октобар 2023.

[13] https://sr.wikipedia.org/wiki/Informaciona_tehnologija, 20. септембар 2023.

[14] Уз помоћ вештачке интелигенције научници Брод института (*Broad Institute*) у Масачусетсу испитали су и тестирали милионе хемијских једињења и пронашли нови тип антибиотика, који је у стању да онеспособи две врсте бактерија које су постале имуне на постојеће антибиотике. https://zdravlje.kurir.rs/vesti/4321134/otkrivena-nova-vrsta-antibiotika-uz-pomoc-vestacke-inteligencije, 21. децембар 2023.

унапређења образовног процеса,[15] правничке професије,[16] екологије и заштите животне средине, пољопривреде, метеорологије и др. Међутим, треба бити свестан и уважити и одређена ограничења, па и могућности злоупотреба ИТ и вештачке интелигенције.

Јасно је да је функционисање модерног друштва и човека данас незамисливо без ИТ, односно да нема области нити посла (сем простог ручног рада) где нису заступљене ИТ. Као такве, оне у великој мери утичу и на остваривање безбедности у друштву. Због тога питање развоја и употребе ИТ и остваривања информационе безбедности постају доминантна питања националне,[17] али и осталих нивоа безбедности. Свакодневно смо сведоци све већег броја безбедносних проблема у вези са ИТ,[18] што је у већини држава покренуло бројне иницијативе ка новим приступима (правним, безбедносним, политичким, етичким и др.) њеном даљем развоју и употреби.

3. КЛАСИФИКАЦИЈА ПОСЛЕДИЦА РАЗВОЈА И УПОТРЕБЕ ИНФОРМАЦИОНИХ ТЕХНОЛОГИЈА ПО ДРУШТВО

Узимајући у обзир да последице развоја и употребе (коришћења) ИТ може имати различите последице по развој и функционисање друштва, неопходно је извршити класификацију тих последица. Уважавајући научни приступ, последице могу бити класификоване у складу са следећим критеријумима:

I. Према исходу последица:
   1) Позитивне и
   2) Негативне.
II. Према области друштвеног живота у којима се последице испољавају:
   1) Безбедност (систем безбедности);

---

[15] О променама у образовању које генериште Четврта индустријска револуција вид. Јован Базић, „Трендови промена у друштву и образовању које генерише Четврта индустријска револуција“, *Социолошки преглед* 4/2017, стр. 526-546.

[16] О алатима за подршку правничкој професији који користе технике вештачке интелигенције вид. Марко Марковић, Стеван Гостојић, Драго Инђић, „Вештачка интелигенција и право: преглед техника и алата за аутоматизацију задатака“, *Инфо М* 73/2021, 42-48.

[17] О утицају ИТ на националну безбедност вид: Kamran Yeganegi, Zahra Arbabi Asma Ibrahim Hussein, „The role of information technology in national security“ *Journal of Physics: Conference Series* 1/2020; Dušan Proroković, Marko Parezanović, „Artificial Inteligence and Psyhological – Propaganda Operations in the Context of Threat to National Security”, *The Policy of National Security* 2/2023, 13-32; Ненад Путник, *Сајбер рат и сајбер мир*, Београд 2022; Драган Младеновић, *Међународни аспекти сајбер ратовања*, Београд 2012.

[18] Ту свакако убрајамо све бројније појавне облике сајбер криминала, сајбер нападе на државне органе и јавне службе и установе, лажне дојаве о подметнутим бомбама у образовним и другим установама, могућности вођења сајбер ратовања, вршњачког насиља у сајбер (дигиталном) окружењу, интернет преваре и крађе идентитета и сл.

2) Економија;
3) Финансије;
4) Здравство;
5) Екологија (животна средина);
6) Наука и образовање;
7) Политика;
8) Право;
9) Морал и др.

III. Према субјектима на којима се последице испољавају:
1) Појединац (деца, стари, радници и др.);
2) Привредни субјекти (организација, корпорација);
3) Држава и државни органи;
4) Јавне службе и установе;
5) Друштво;
6) Међународна заједница.

IV. Према простору у којем се последице испољавају:
1) Сајбер простор (дигитални свет) и
2) Физички простор (реални свет).

V. Према предвидљивости последице:
1) Последице које се могу предвидети и
2) Последице које се не могу предвидети.

VI. Према последицама које настају с обзиром на медијум из палете ИТ:
1) Интернет;
2) Друштвене мреже;
3) Електронска средства информисања, алати за електронска плаћања и трговину и др.;
4) Паметни телефони, таблети, рачунари, рутери;
5) Електронска пошта;
6) Виртуелни системи, вештачка интелигенција и др.

VII. Према директности утицаја на безбедност друштва:
1) Директне (непосредне) последице и
2) Индиректне (посредне) последице.

VIII. Према намери изазивања последице:
1) Намерно изазване;
2) Случајне (ненамерне) и
3) Мешовите.

IX. Према ефектима које последице изазивају:
1) Краткорочне;
2) Средњорочне и
3) Дугорочне.

4. БЕЗБЕДНОСНА КУЛТУРА У ИНФОРМАЦИОНИМ ТЕХНОЛОГИЈАМА

Како би се друштво заштитило од негативних последица развоја и употребе ИТ, у сваком друштву треба радити на развоју и унапређењу безбедносне културе. Безбедносна култура као релативно нов концепт развијен у оквиру науке безбедности, врло брзо је нашао своју примену и у области ИТ.[19] Наиме, примена безбедносне културе у ИТ предмет је научне и стручне анализе како у свету[20] тако и код нас.

Постало је јасно да је за питање заштите информационе безбедности неопходно присуство значајног нивоа појединачне и колективне свести о потреби заштите, односно о потреби постојања и развоја безбедносне културе свих учесника у процесу развоја и примене ИТ. Основу безбедносне културе у ИТ чини пре свега свест[21] о постојању безбедносне претње, односно знања о изворима, облицима и носиоцима угрожавања у информационој сфери (ИТ и информациона безбедност), као и знања и вештине о одговарајућим механизмима правне, организационе, техничке и безбедносне заштите. То значи да безбедносна свест, као и знања и вештине из области безбедности морају бити присутни како у процесу конципирања, иновација и развоја ИТ (изражених пре свега у процесу предвиђања могућих негативних импликације те технологије приликом њене примене у друштву, а услед којих може доћи до угрожавања безбедности појединца или неког другог нивоа безбедности), тако и приликом њене употребе (примене). Са друге стране, безбедносна свест, знања[22] и вештине корисника ИТ указују на то да поред заштите

---

[19] Када су у питању ИТ, у питању је тзв. информациона култура, односно информационо-безбедносна култура као интегрална компонента безбедносне културе. Примена безбедносне културе је између осталог изражена и у следећим областима друштвеног живота и деловања: нуклеарна безбедносна култура, здравствена безбедносна култура, саобраћајна безбедносна култура, еколошка безбедносна култура и др.

[20] О различитим аспектима, дефиницијама и приступима информационо-безбедносној култури вид. Mohammed Alnatheer, „A Conceptual Model to Understand Information Security Culture“, *International Journal of Social Science and Humanity* 2/2014, 104-108; Adela da Veiga, Nico Martins, „Defining and identifying dominant information security cultures and subcultures“, *Computers & Security* 70/2017, 72-94; Betsy Uchendu, Jason Nurse, Maria Bada, Steven Furnell, „Developing a cyber security culture: Current practices and future needs“, *Computers & Security* 109/2021, Article 102387.

[21] Или како поједини аутори кажу „безбедносна свест“. Она подразумева схватање и разумевање ризика који ИТ са собом носе. Слободан Петровић, „Безбедносна свест, обука и едукација – критичне компоненте заштите кибер-простора“, *Научно-стручно саветовање ЗИТЕХ*, Београд 2006.

[22] Када су у питању знања, потребно је споменути спроведено емпиријско истраживање о факторима везаним за понашање у сајбер безбедности код средњошколаца у нашој земљи. Истраживањем је утврђено да *ученици немају потребна знања нити адекватну свест о прет-*

интереса и потреба корисника ИТ треба да се заштите и сва хардверска и софтверска материјална добра како корисника тако и свих оних са којима корисник ступа у контакт путем ИТ. Само тада можемо говорити о безбедности свих и за све, о безбедности где сваки члан друштва поред тога што брине о себи брине и о безбедности других чланова друштва. Управо та свест о значају да се брине о туђој као и о сопственој безбедности (у информационој сфери), чини основу безбедносне културе у ИТ.

Безбедносна култура у ИТ или информациона-безбедносна култура подразумева и одређену активност или понашање, а која су заснована на претходно наведеним знањима и вештинама. Поред индивидуалног нивоа, ово је нарочито битно у организацијама, па се у том смислу информационо-безбедносна култура схвата као интегрални део организационе културе.[23] Томе у прилог говоре и ставови страних аутора који културу информационе безбедности (информационо-безбедносну културу) дефинишу као претпоставку о томе који се тип понашања у области безбедности информација прихвата и подстиче како би се инкорпорирале карактеристике безбедности информација као начин на који се ствари раде у организацији.[24] Слично томе, поједини домаћи аутори информационо-безбедносну културу одређују као „јединство знања, перцепције, уверења и ставова запослених о информационој безбедности организације и потреби примене мера и поступака (дефинисаних политиком информационе безбедности и формализованих процедурама) и њиховог усклађеног поступања у свакодневној примени тих мера, као и способност препознавања претњи, минимизирања ризика и доношења одлука из домена сопствене одговорности у вези са безбедношћу ИКТ система“.[25]

На крају, у покушају да сублимирамо претходно наведено, безбедносну културу у ИТ можемо дефинисати као скуп усвојених ставова, знања, вештина и правила из области (информационе) безбедности, испољених као понашање и процес, о потреби, начинима и средствима заштите личних, корпоративних,

---

њама у сајбер простору. Иако постоје значајни ресурси на интернету, као и бројни туторијали, они се нису показали као ефикасна средства за учење ученика. Како аутори истраживања истичу, ово може бити сигнал образовним институцијама да активније приступе побољшању знања о сајбер безбедности на структурални начин и да науче ученике да се заштите од сајбер напада. Практичне импликације истраживања су да ученици треба да имају ефективну обуку у средњој школи о безбеднијем понашању. Ana Kovačević, Nenad Putnik, Oliver Tošković, „Factors Related to Cyber Security Behavior“, *IEEE Access* 8/2020, 125140-125148.

[23] О организационој култури, а нарочито у безбедносним организацијама вид. Chad Whelan, „Organisational culture and cultural shange: A network perspective”, *Australian & New Zeland Journal of Criminology* 4/2016, 583-599.

[24] Adele Martins, Jan Eloff, „Information Security Culture“, *Security in the Information Society – Visions and Perspectives* (eds. M. Adeeb Ghonaimy, Mahmoud T. El-Hadidi, Heba K. Aslan), IFIP Advances in Information and Communication Technology 86/2022, 205-206.

[25] Анђелија Ђукић, Дејан Вулетић, „Основи информационо-безбедносне културе у организацији“, *Безбедност* 3/2022, 146.

државних, националних и међународних вредности од свих извора, облика и носилаца угрожавања информационе безбедности без обзира на место или време њиховог испољавања.[26]

5. НЕКИ АСПЕКТИ БЕЗБЕДНОСНЕ КУЛТУРЕ У ИНФОРМАЦИОНИМ ТЕХНОЛОГИЈАМА

Значај ИТ, а онда и развоја безбедносне културе у ИТ можемо сагледати из више различитих углова, гледишта или аспеката. Овим питањем се баве различите науке и научне дисциплине и свака од њих полази од свог предмета истраживања. Наиме, добробити безбедносне културе у ИТ можемо сагледати кроз више различитих аспеката и то: етички, организациони, социолошки, економски, политички, научно-образовни, правни, психолошки, антрополошки, културолошки, филозофски, војни и други.[27] Наведено нам указује да је приликом анализирања питања развоја и употребе ИТ, а онда и улоге и значаја безбедносне културе у ИТ потребан мултидисциплинаран и холистички приступ. Наравно, неопходно је и указати на то да се поједини аспекти преклапају, прожимају и допуњују, што само још једном потврђује став да је у истраживању ових феномена неопходан мултидисциплинаран и холистички приступ. Узимајући у обзир потребе и обим овог рада, ми ћемо се у овом раду осврнути на следеће аспекте безбедносне културе у ИТ: етички, социолошки, економски и правни.

5.1. Етички аспекти безбедносне културе у ИТ

Као што смо раније напоменули, ИТ у значајној мери мењају стил живота савременог човека, мењају друштвене обичаје и обрасце понашања. Због тога је неопходно одређена етичка питања разматрати као део развоја и употребе ИТ на начин да не дође до угрожавања. Та етичка питања су данас доминантна како на међународном,[28] тако и националном, државном нивоу.

---

[26] Љубомир Стајић, Саша Мијалковић, Светлана Станаревић, *Безбедносна култура*, Нови Сад 2013, 43; Љ. Стајић, 76.

[27] Упор. Љ. Стајић et al., 51-68.

[28] Етичка питања у области ИТ на међународном плану су данас нарочито заступљена у области вештачке интелигенције. Наиме, на Самиту о управљању вештачком интелигенцијом Светског економског форума у Сан Франциску, чији је домаћин био Центар за четврту индустријску револуцију (*C4IR*), Србија се као 33. држава придружила Алијанси управљања вештачком интелигенцијом. Циљ Самита, који је окупио лидере и стручњаке из преко 200 водећих светских компанија, организација, био је *да се промовишу одговорне иновације вештачке интелигенције*, стављајући *етичке смернице* као *приоритет у технолошком напретку.*

Када је у питању развој ИТ, постојање и развијеност безбедносне културе у великој мери зависи од постојања и развијености моралних вредности и моралних правила једног друштва, моралних начела и принципа којима се појединици и компаније, које се баве развојем ИТ,[29] руководе у свом свакодневном раду и пословању. Етичко процењивање вредности у смислу шта је добро, а шта лоше, директно се одражава на (безбедносно) понашање и реаговање које настаје у процесу развоја и иновација ИТ.[30] То значи да од тога шта друштво, али и компаније и њихови инжењери – програмери, девелопери прихватају као добро, а шта лоше кад је у питању развој ИТ, директно зависи и каква ће бити безбедносна култура. Због тога је неопходно пре свега сагледати све оне негативне аспекте (даљег) развоја ИТ, јер поставља се питање да ли ће већ увелико одмакао процес развоја ИТ (а нарочито вештачке интелигенције) моћи да се заустави и спречи настанак неких будућих проблема изражених кроз угрожавање читавог друштва. Због тога је неопходно развијати професионалну етику у ИТ компанијама. Поштовање норми професионалне етике је индикатор развијене безбедносне културе.

Код безбедносне културе у примени ИТ од стране индивидуалних корисника је веома важно да човек сам себи издаје одређену моралну заповест. Та заповест мора бити заснована на свести о значају безбедносних правила и проце-

---

https://www.kurir.rs/vesti/drustvo/4295068/za-brzi-razvoj-vestacke-inteligencije-srbija-se-na-samitu-u-san-francisku-pridruzila-alijansi-upravljanja-ai, 19. новембар 2023. Такође, На пленарној седници конференције „AI Journey“ у Москви, која је посвећена вештачкој интелигенцији, руски председник Владимир Путин је нагласио да технолошки свет будућности треба да буде вишеполарни, те да је човечанство дужно да изради механизме и правила у сфери коришћења вештачке интелигенције који су прихватљиви за све. Путин је истакао да руско искуство у коришћењу вештачке интелигенције може бити употребљено и приликом утврђивања *међународних етичких стандарда* у тој области, како би се дошло до уравнотеженог система *који је у интересима свих, а не само одређених земаља*. https://sputnikportal.rs/20231124/putin-tehnoloski-svet-buducnosti-mora-biti-visepolarni-covecanstvo-pocinje-novo-poglavlje-1164202018.html?fbclid=IwAR3srVnaqouiWSiU58oCvV9AgoWBG8Sif_70hEXc7xhjuKvRdd-PyhVPYcM, 24. новембар 2023. УНЕСКО је дефинисао први глобални универзални стандард за етику вештачке интелигенције у чијој изради је учествовала Србија са својим стручњацима. Овај етички оквир који садржи бројне препоруке за „здрав“ развој и коришћење вештачке интелигенције усвојиле су 193 земље чланице УНЕСКА у новембру 2021. године. У питању је Препоруке о етици система вештачке интелигенције (*Recommendation on the Ethics of AI*). Принципи из Препорука садржани су и у Етичким смерницама за развој, примену и употребу поуздане и одговорне вештачке интелигенције у нашој земљи. Етичке смернице доступне на: https://www.ai.gov.rs/tekst/sr/586/eticke-smernice.php, 14. децембар 2023.

[29] Једна од најновијих области примењене етике јесте компјутерска етика. Вид. Драгана Ћорић, „Увод у компјутерску етику“, *Зборник радова Правног факултета у Новом Саду* 4/2015, 1813-1830 и D. Mika Hester, Pol Dž. Ford, *Kompjuteri i etika u sajber dobu*, Beograd 2009.

[30] Треба напоменути да су етичке вредности променљива категорија, односно како поједини аутори наводе да „етика није једном дато схватање доброг и лошег; њена садржина је променљива јер се базира на променљивом, друштвено прихватљивом схватању доброг и лошег.“ Д. Ћорић, 1814.

дура, знању, вештинама и технологији заштите, а не да она долази као осећање наметања од стране неког другог, споља, у виду неке императивне норме.

Одређујући свој морални однос према другима, целом друштву или самом себи, појединац тај однос мора сагледати и кроз призму безбедносног деловања. Основни услов морално прихватљивог безбедносног деловања када су у питању ИТ јесте да се претходно усвоји систем вредности ка коме је то деловање усмерено. Тај систем вредности се односи и на потребу заштите информационе безбедности како појединца, тако и пословних субјекта, државе и читавог друштва. Узимајући у обзир наведено, етички аспект безбедносне културе у ИТ се између осталог огледа у:[31]

- обављању функције информационе безбедности поштовањем етичких принципа (у смислу прихватања оног позитивног и исправног када је у питању развој ИТ – развој ИТ који је у функцији развоја и безбедности човека; када је у питању примена ИТ, да се она користи на начин да се други корисници и њихове вредности не угрозе);
- ширењу позитивног стања информационе безбедности у систему: грађанин-грађанин, грађанин-организација/корпорација, грађанин-држава, држава-међународна заједница и обрнуто;
- деловању на савест и свест свих припадника друштва о томе шта је морално (не)исправно када су у питању развој и употреба ИТ, као и њиховог утицаја на остваривање безбедности друштва;
- познавању система моралних вредности одређених категорија носилаца угрожавања информационе безбедности (хакери, организоване криминалне групе, компаније које се баве производњом вируса, терористичке организације и др.);
- инкорпорирању етичких стандарда из области ИТ у одговарајуће законске, подзаконске и друге акте у области информационе безбедности;
- промени моралних (етичких) начела у сфери ИТ, што треба да доведе и до промене понашања како креатора тако и корисника ИТ, али и читавог друштва;
- изградњи и поштовању кодекса професионалне етике у ИТ индустрији, којих ће се придржавати сви запослени.

5.2. Социолошки (друштвени) аспект безбедносне културе у ИТ

Када су у питању ИТ и могућности њене (зло)употребе у друштву, можемо рећи да је на настанак безбедносне културе као нове дисциплине утицао:

- постигнут степен информационо-технолошког напретка, праћених свешћу, знањима, али и потребама друштва и човека да добробити ИТ подреди

[31] Упор. Љ. Стајић et al., 52-53.

својим потребама у свакодневном личном, пословном, политичком и уопште друштвеном животу;
- потреба друштва да сопствену (информациону) безбедност подигне на виши ниво, нарочито код тако масовне и значајне сфере друштвеног живота као што је употреба ИТ;
- потреба да се теоријска и практична знања о безбедносној култури у ИТ на систематизован начин, учине доступним већем броју грађана, привредних субјеката и државних органа.

Као што смо навели, безбедносна култура је своју примену у друштву пронашла и у области ИТ – информационо-безбедносна култура. Оправдање за тим проналазимо у све бројнијим и деструктивнијим појавама у сфери информационе безбедности, која захтевају нове приступе промишљању о ИТ у друштву, као и нове механизме заштите. Ако се однос друштво-безбедносна култура схвата као допуњујући однос, у коме је безбедносна култура интегрални део друштва, онда је информационо-безбедносна култура интегрални део савременог (информационог) друштва, односно саставни део његовог живљења.

У друштву се формирају одређене виталне вредности, од којих је даљи развој ИТ (који ће бити у функцији остваривања безбедности) свакако један од њих. С тим у вези, у друштву се идентификују и сви они, са аспекта безбедности, негативни обрасци понашања који ће као такви бити санкционисани моралним и(ли) правним нормама. Због тога се каже да од способности друштва да идентификује и анализира све оне последице развоја и примене ИТ са негативним предзнаком, зависи и његова безбедност.[32] То значи идентификацију свих оних извора, облика и носилаца угрожавања информационе безбедности. Након тога следи друштвена реакција у виду нових политика безбедности у информационој сфери која укључује усвајање правних аката, стратешких докумената и (ре)организацију система националне безбедности, праћених перманентним развојем безбедносне културе како на нивоу појединца тако и на нивоу читавог друштва.

Од развијености безбедносне културе у ИТ код свих чланова друштва зависи и остваривање оптималног стања (информационе, као интегралног дела индивидуалне, националне, корпоративне и међународне) безбедности. Јасно је да ниво развијености безбедносне културе у ИТ није подједнако развијен у свим друштвима као и међу њеним члановима. Посебну пажњу

[32] Још је давних дана академик Михајло Марковић упозоравао на то да „када говоримо о благодетима *друштва информатике*, треба бити критичнији према тамним његовим странама“. Он даље наводи да ће „електронска револуција све више појединце излагати притиску порука и сугестија које ће свесно, и, још више, несвесно обликовати ставове и аспирације грађана и на тржишту роба и на тржишту идеја“. Михајло Марковић, „Етички проблеми науке“, *Проблеми науке у будућности – искуства и виђења* (ур. академик Милош Мацура, академик Драгомир Виторовић), Београд 1991, 146.

треба посветити развоју информационо-безбедносне културе корисника, а нарочито деце и младих као лица која данас највише користе ИТ. Као најподложнији различитим облицима сајбер угрожавања, на развоју њихове безбедносне културе треба највише радити. Највећу улогу у томе имају и најзначајније друштвене институције: породица, васпитно-образовни систем, медији и др.

Да би безбедносна култура у ИТ имала позитивне ефекте у друштву неопходно је:[33]

- јасно разграничити прихватљиве од неприхватљивих мотива и циљева развоја ИТ, као и образаца рада и понашања приликом коришћења ИТ;
- правовремено реаговати на девијације, проблематичне појаве настале услед развоја и почетне примене ИТ,[34] као и проблематично и непожељно понашање појединих запослених/службеника (непрофесионално и небезбедно понашање у раду и непоштовање основних принципа безбедносне културе);[35]
- промовисати оне законе, стандарде и правила понашања у области ИТ које треба да разуме, а онда и прихвати већина људи који користе ИТ;
- прихватити чињеницу да различите друштвене групе имају различите ставове, захтеве и потребе по питању информационе безбедности, што се директно рефлектује и на садржај њихове безбедносне културе;
- утицати на то да одређене друштвене групе (деца и млади), институције (привредни сектор, јавне службе, установе и предузећа, полиција, службе безбедности и други професионални субјекти система националне безбедности и др.) али и компаније из сфере ИТ имају виши ниво развијености безбедносне културе;
- константно радити на унапређењу и прилагођавању безбедносне културе савременим безбедносним проблемима у области угрожавања информационе безбедности, користећи све расположиве друштвене ресурсе.

---

[33] Упор. Љ. Стајић et al., 56.

[34] Ово се нарочито односи на бројна упозорења светске стручне и научне јавности која се односе на даљи развој вештачке интелигенције. Једна од области забринутости када је у питању вештачка интелигенција јесте појава дубоке лажи (енгл. *deepfake*). Наиме, у питању је компјутерска манипулација чији је резултат опонашање стварних личности и догађаја, а која је, захваљујући све развијенијим способностима вештачке интелигенције, омогућила да се без много муке праве компромитујући видео-клипови или аудио-снимци. Могућности које је на овај начин отворила вештачка интелигенција донеле су нове страхове и потрагу за оним што је аутентично или јединствено, изворно. https://www.nin.rs/drustvo/vesti/41852/ima-li-razloga-za-strah-od-vestacke-inteligencije, 6. децембар 2023.

[35] Примера ради, непрофесионално и небезбедно понашања приликом употребе ИТ обухвата оне случајеве у којима запослени службене рачунаре користе у приватне сврхе, преко њих посећују бројне недозвољене, пиратске сајтове, при чему са њих „скидају“ одређене садржаје (филмове, музичке материјале, софтверске програме и сл.).

5.3. Економски аспект безбедносне културе у ИТ

ИТ су данас један од главних генератора економског раста и развоја, што утиче и на остваривање економске безбедности.[36] То се директно одражава и на промене у радном процесу у виду механизације, компјутеризације, роботизације, аутоматизације, који су засновани на ИТ. Перманентност иновација у ИТ је императив даљег развоја појединих држава, али и привредних субјеката чији се организација и пословање заснива на тим истим технологијама.[37] Због тога је на међународном плану све израженија „трка" за водећом позицијом светског лидера у области ИТ, а нарочито када је у питању вештачка интелигенција.[38] Са друге стране, успех пословања бројних компанија у условима све бржих иновација у ИТ зависи од развијености безбедносне културе на свим нивоима (од топ менаџера, преко највишег нивоа до свих запослених). То значи да се ИТ користе уз поштовање одређених образаца безбедносног понашања, односно поштовањем одређених принципа и правила изражених кроз безбедносне процедуре.

Економски аспект безбедносне културе у ИТ има више позитивних утицаја на остваривање безбедности друштва, а то су:[39]

- усвајањем основних, а онда и специјализованих знања и вештина из области ИТ и информационе безбедности, спречава се и смањује број сајбер угрожавања, чиме се чине значајне економске уштеде (како за појединца, тако и организацију и систем безбедности), а чиме се остварује економска безбедност;
- развијена безбедносна култура у ИТ утиче на усвајање ставова и доношење правних прописа о развоју, коришћењу, поступању и извозу ИТ и знања које могу имати безбедносне импликације (пре свих ИТ у војној индустрији и за потребе других безбедносних органа);
- земље са развијеном безбедносном културом у ИТ имају мање шансе да постану жртве сајбер угрожавања, а чије последице се мере у милијардама долара и повећавају из године у годину;[40]

---

[36] О економској безбедности вид. Горан Милошевић, Љубомир Стајић, *Економска безбедност*, Нови Сад 2022.

[37] ИТ утичу и на остваривање организационе структуре компанија или појединих јавних установа. Вид. Миленко Мацура, „Утицај информационих технологија на дизајн организације", *Инфо М* 39/2017, 15-18; М. Петковић, Ј. Лукић, 439-460.

[38] Што наравно ни у ком случају, са аспекта безбедности и безбедносне културе, не би требало да буде и средство за остваривање доминације над неким државама.

[39] Упор. Љ. Стајић et al., 63.

[40] У 2020. укупни економски трошкови сајбер криминала се процењују на око 1000 милијарди америчких долара годишње, у односу на 600 милијарди америчких долара годишње у 2018. КОВИД-19 и све већа употреба дигиталних технологија у свету након пандемије додатно су повећали економску важност сајбер ризика. Eling Martin, Elvedi Mauro, Falco Greg,

– земље са развијеном безбедносном културом у ИТ имају веће шансе за страна улагања, односно страни капитал захтева поштовање одређених међународних безбедносних стандарда где је безбедност у информационим технологијама незаобилазна и одмах иза физичке безбедности.

5.4. Правни аспекти безбедносне културе у ИТ

Угрожавања информационе безбедности су данас све заступљенија и све деструктивнија и прете да ставе у други план све оне позитивне аспекте које ИТ са собом носе. У том новом информационом (дигиталном, сајбер) окружењу право добија нову друштвену функцију. Због тога се као један од најактуелних правних изазова данашњице наводи правно регулисање најважнијих питања развоја и примене ИТ у друштву. Оно постаје императив времена, као и околности и потреба технолошког развоја у којем живимо. Право као скуп норми и правила којима се уређује понашање људи поводом односа у које ступају, представља један од главних инструмената који треба да омогући спречавање могућих злоупотреба ИТ. Правне норме (националне или међународне), исто као и моралне, морају пратити развој свих оних људских делатности које су од виталног значаја за друштво, како би биле ефикасна брана свим могућим угрожавајућим појавама.

Када су у питању развој употреба ИТ данас, право има двоструки задатак. Прво је да правним субјектима (физичким и правним лицима) омогући да остварују одређени интерес у друштву, ступајући у одређене односе.[41] У овом случају би то било наставак даљих иновација и развоја, а онда и употребе ИТ у различитим сферама друштва. Други задатак се односи на усмеравање или ограничавање понашања и деловања физичких и правних лица на начин да их спречава или санкционише за непоштовање унапред одређених правила понашања. То значи да су унапред предвиђена правила понашања која уређују развој и употребу ИТ, као и санкције за њихово непоштовање.

Област употребе ИТ је регулисана нормама различитих грана права (управног, кривичног, грађанског, привредног и др.). Приметне су тенденције развоја нових грана права попут права информационе или информационо-комуникационе технологије које обухватају правне норме које регулишу друштвене односе у вези са употребом информационе и комуникационе технологије. Битно је напоменути да ове правне норме нису систематизоване у једном закону већ су, као што смо рекли, расуте у бројним другим правним областима (грађанско, кривично, управно, трговинско, привредно и др.) и налазе се у бројним општим и специјалним законима. Заједничко им је то што

„The Economic Impact of Extreme Cyber Risk Scenarios“, *North American Actuarial Journal* 3/2023, 1-15.

[41] Али интерес који је у складу са друштвеним потребама и етичким принципима.

регулишу односе људи поводом употребе ИТ.[42] Правни субјекти који подлежу овим нормама су физичка лица (грађани, појединици) и правна лица (компаније и друге организација јавног или приватног карактера).

Како сам појам безбедносне културе у ИТ обухвата и скуп правила (па и правних правила), правни аспект безбедносне културе у ИТ пре свега треба посматрати управо у том контексту. То је постојања правила која се испољавају кроз понашање које је у складу са правном нормом и које је у функцији заштите одређених вредности (у овом случају су то информација, право на заштиту податка о личности, право на приватност, ауторска и друга сродна права, право на информисаност, право на слободу изражавања и др.).

Правно уређење ИТ представља основ за сва друга деловања у информационој сфери, па и безбедносно. Оно обухвата понашања и деловања људи почев од развоја ИТ (које се пре свега односи на ИТ компаније) па све до њене употребе код крајњих корисника. Због тога су нека од ових питања постала предмет уређености и бројних стратешких и правних докумената како на националном нивоу тако и у оквиру Европске уније.[43]

Правни аспект безбедносне културе у ИТ има више позитивних утицаја на остваривање безбедности друштва, а то су:

- јасно и прецизно одређење циљева развоја ИТ, као и њиховог (безбедног) коришћења;
- регулисање права и обавеза учесника на тржишту ИТ;
- јасно и прецизно регулисање права, обавеза и одговорности правних и физичких лица када су у питању развој и употреба ИТ;
- јасно и прецизно регулисање различитих области примене ИТ у друштву;
- јасно и прецизно идентификовање и одређење безбедносних ризика у ИТ;
- устројавање система националне безбедности (одређивање субјеката, уређење њихове надлежности, овлашћења, одговорности, контроле и др.) који ће бити у могућности да се ефикасно супротстави безбедносим ризицима у ИТ сфери;
- регулисање мера (техничке, организационе, правне, безбедносне) заштите и одређење носилаца за њихово спровођење како у јавном тако и у приватном сектору;
- регулисање надлежности појединих државних органа као субјеката који ће спроводити надзор над применом правне и друге регулативе и стандарда у ИТ индустрији, као и свим другим елементима ИТ које користе сви грађани као крајњи корисници;

---

[42] Предраг Димитријевић, *Право информационе технологије*, Ниш 2011, 10.

[43] Једно од њих је свакако и вештачка интелигенција. Вид. Стефан Андоновић, „Стратешко-правни оквир вештачке интелигенције у упоредном праву“, *Страни правни живот* 3/2020, 111-123.

- јасно и прецизно регулисање области критичне инфраструктуре (која обухвата и сектор ИТ[44] која је у директној међузависности са осталим секторима);
- формирање националног тела[45] које ће се бавити питањима превенције (укључујући и развој и примену безбедносне културе у ИТ) и координације свих активности из области заштите информационе безбедности.

6. ЗАКЉУЧАК

ИТ су постале саставни део развоја савременог друштва. Данас је готово назамисливо обављање неког посла, делатности без постојања и примене ИТ. Као такве, оне су у значајној мери промениле и унапредиле људски живот и рад, а самим тим и његову безбедност. Један од основних циљева развоја и употребе ИТ и јесте да побољша живот и рад човека у његовим свакодневним активностима, почев од комуникације, образовања, функционисања државних органа, јавних служби, унапређења безбедности животне средине и сл. Међутим, као и сваки технолошки развој тако је и развој ИТ праћени одређеним ограничењима, проблемима, контровезама и нерешеним питањима, који у одређеним ситуацијама и у одређеној мери могу довести до угрожавања. То се исто односи и на примену (употребу) ИТ. Због тога све више на значају добија информациона безбедност, као интегрална компонента безбедности појединца, али и корпоративне, националне и међународне безбедности.

Треба бити свестан да развој и употреба ИТ могу довести до различитих последица по друштво, као и да поред оних позитивних димензија развоја и примене ИТ, оне могу имати и негативну димензију. Друштво данас све више постаје свесно могућности да ИТ могу бити злоупотребљене, односно њене угрожавајуће димензије. То свакако пред друштвом намеће потребу изналажења „нових" друштвених ресурса, потенцијала и(ли) механизама како би се такве злоупотребе спречиле или како би се евентуалне последице свеле на минимум. Један од тих механизама јесте безбедносна култура, која све више налази своју примену у ИТ.

Основу безбедносне културе у ИТ (информационо-безбедносне културе) чини постојање свести о свим безбедносним ризицима и проблемима до којих доводи развој ИТ, као и свести о могућностима угрожавања приликом њиховог коришћења. Та свест мора бити праћена перманетним усвајањем

---

[44] Вид. Татјана Бугарски, Милана Писарић, „Правно уређење безбедности информационе критичне инфраструктуре", *Правни и безбедносни аспекти управљања ризицима од природних и антропогених катастрофа* (ур. Владимир М. Цветковић), Београд 2022, 31-41.

[45] Вид. Закон о информационој безбедности, *Службени гласник РС*, бр. 6/2016, 94/2017 и 77/2019, чл. 14 и 15.

нових и проширивањем постојећих знања и вештина из области ИТ и информационе безбедности. Поред свести, неопходно је постојање знања и вештина о изворима, облицима и носиоцима угрожавања информационе безбедности, као и начинима и средствима њене заштите. Не треба изгубити из вида чињеницу да је човек и даље кључни чинилац технолошког развоја и да од његових способности, афинитета, мотивације, карактера, емоција, моралних начела, али и свести, знања и вештина зависи у ком правцу ће се даље одвијати развој и употреба ИТ.

Посебно треба истаћи да безбедносна свест, као и знања и вештине из области безбедности морају бити присутни у свим фазама и аспектима развоја и примене ИТ. На то јасно указују и неки аспекти безбедносне културе које смо у раду анализирали, а то су етички, социолошки, економски и правни. Они свакако нису и једини. Будућа истраживања свакако треба усмерити ка различитим аспектима безбедносне културе у ИТ, узимајући у обзир последице које развој и употреба ИТ остављају на друштво. Испреплетаност, као и прожимање и допуњавање појединих аспеката безбедносне културе у ИТ указује да приступ истраживању ових феномена мора бити мултидисциплинаран и холистички. С тим у вези, како би се развој и примена ИТ у друштву наставили, а друштво остало безбедно, непходно је наставити са даљим истраживањима улоге и значаја који безбедносна култура има у тим процесима.

ЛИСТА РЕФЕРЕНЦИ

Adele Martins, Jan Eloff, „Information Security Culture“, *Security in the Information Society – Visions and Perspectives* (eds. M. Adeeb Ghonaimy, Mahmoud T. El-Hadidi, Heba K. Aslan), IFIP Advances in Information and Communication Technology 86/2022.

Adela da Veiga, Nico Martins, „Defining and identifying dominant information security cultures and subcultures“, *Computers & Security* 70/2017.

Ana Kovačević, Nenad Putnik, Oliver Tošković, „Factors Related to Cyber Security Behavior“, *IEEE Access*, vol. 8, 2020.

Анђелија Ђукић, Дејан Вулетић, „Основи информационо-безбедносне културе у организацији“, *Безбедност* 3/2022.

Betsy Uchendu, Jason Nurse, Maria Bada, Steven Furnell, „Developing a cyber security culture: Current practices and future needs“, *Computers & Security* 109/2021.

Горан Милошевић, Љубомир Стајић, *Економска безбедност*, Нови Сад 2022.

D. Mika Hester, Pol Dž. Ford, *Kompjuteri i etika u sajber dobu*, Beograd 2009.

Драган Младеновић, *Међународни аспекти сајбер ратовања*, Београд 2012.

Драгана Ћорић, „Увод у компјутерску етику“, *Зборник радова Правног факултета у Новом Саду* 4/2015.

Dušan Proroković, Marko Parezanović, „Artificial Inteligence and Psyhological – Propaganda Operations in the Context of Threat to National Security”, *The Policy of National Security* 2/2023.

Eling Martin, Elvedi Mauro, Falco Greg, „The Economic Impact of Extreme Cyber Risk Scenarios“, *North American Actuarial Journal* 3/2023.
ISACA, Glossary. Доступно на: https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/glossary/glossary.pdf
Јован Базић, „Трендови промена у друштву и образовању које генерише Четврта индустријска револуција“, *Социолошки преглед* 4/2017.
Kamran Yeganegi, Zahra Arbabi, Asma Ibrahim Hussein, „The role of information technology in national security“, *Journal of Physics: Conference Series* 1/2020.
Љубомир Стајић, Саша Мијалковић, Светлана Станаревић, *Безбедносна култура*, Нови Сад 2013.
Љубомир Стајић, *Основи система безбедности – са основама истраживања безбедносних појава*, Нови Сад 2021.
Марко Марковић, Стеван Гостојић, Драго Инђић, „Вештачка интелигенција и право: преглед техника и алата за аутоматизацију задатака“, *Инфо М* 73/2021.
Миленко Мацура, „Утицај информационих технологија на дизајн организације“, *Инфо М* 39/2017.
Мирјана Петковић, Јелена Лукић, „Утицај информационе технологије на дизајн организације: пример организације у здравству“, *Социологија* 3/2013.
Михајло Марковић, „Етички проблеми науке“, *Проблеми науке у будућности – искуства и виђења* (ур. академик Милош Мацура, академик Драгомир Витровић), Београд 1991.
Mohammed Alnatheer, „A Conceptual Model to Understand Information Security Culture“, *International Journal of Social Science and Humanity* 2/2014.
Nazli Chucri, David D. Clark, *International Relations in the Cyber Age, The Co-Evolution Dilemma*, Cambridge Massachusetts 2018.
Ненад Путник, *Сајбер рат и сајбер мир*, Београд 2022.
Предраг Димитријевић, *Право информационе технологије*, Ниш 2011.
Радомир Лукић, *Социологија морала*, Београд 1976.
Саша Мијалковић, Вера Арежина-Ђерић, Горан Бошковић, „Корелација информационе и националне безбедности“, *Научно-стручно саветовање ЗИТЕХ*, Београд 2010.
Слободан Петровић, „Безбедносна свест, обука и едукација – критичне компоненте заштите кибер-простора“, *Научно-стручно саветовање ЗИТЕХ*, Београд 2006.
Србобран Бранковић, „Вештачка интелигенција и друштво“, *Српска политичка мисао* 2/2017.
Стефан Андоновић, „Стратешко-правни оквир вештачке интелигенције у упоредном праву“, *Страни правни живот* 3/2020.
Татјана Бугарски, Милана Писарић, „Правно уређење безбедности информационе критичне инфраструктуре“, *Правни и безбедносни аспекти управљања ризицима од природних и антропогених катастрофа* (ур. Владимир М. Цветковић), Београд 2022.
Chad Whelan, „Organisational culture and cultural shange: A network perspective”, *Australian & New Zeland Journal of Criminology* 4/2016.

ПРАВНИ ИЗВОРИ

Закон о критичној инфраструктури, *Службени ɪласник РС*, бр. 87/18.
Закон о информационој безбедности, *Службени ɪласник РС*, бр. 6/16, 94/17 и 77/19.

ИНТЕРНЕТ ИЗВОРИ

Amerika prvi put upozorava! Veštačka inteligencija je opasnost za finansijski sektor, https://euractiv.mondo.rs/ekonomija/a5281/Vestacka-inteligencija-je-opasnost-za-finansijski-sistem-upozorava-FSOC.html?utm_source=kurir_biznis&utm_medium=euractiv_widget&utm_campaign=naslovna/infobiz
Hakeri napali EPS: Sistem se uspešno oporavlja, https://www.b92.net/biz/vesti/srbija/hakeri-napali-eps-sistem-se-uspesno-oporavlja-2452512
Informaciona tehnologija, https://sr.wikipedia.org/wiki/Informaciona_tehnologija
Otkrivena nova vrsta antibiotika uz pomoć veštačke inteligencije: Uništava one bakterije koje su postale otporne, https://zdravlje.kurir.rs/vesti/4321134/otkrivena-nova-vrsta-antibiotika-uz-pomoc-vestacke-inteligencije
Za brži razvoj veštačke inteligencije: Srbija se na Samitu u San Francisku pridružila Alijansi upravljanja AI, https://www.kurir.rs/vesti/drustvo/4295068/za-brzi-razvoj-vestacke-inteligencije-srbija-se-na-samitu-u-san-francisku-pridruzila-alijansi-upravljanja-ai
Путин: Технолошки свет будућности мора бити вишеполаран, човечанство почиње ново поглавље, https://sputnikportal.rs/20231124/putin-tehnoloski-svet-buducnosti-mora-biti-visepolarni-covecanstvo-pocinje-novo-poglavlje-1164202018.html?fbclid=IwAR3srVnaqouiWSiU58oCvV9AgoWBG8Sif_70hEXc7xhjuKvRdd-PyhVPYcM
Etičke smernice za razvoj, primenu i upotrebu pouzdane i odgovorne veštačke inteligencije, https://www.ai.gov.rs/tekst/sr/586/eticke-smernice.php
Ima li razloga za strah od veštačke inteligencije, https://www.nin.rs/drustvo/vesti/41852/ima-li-razloga-za-strah-od-vestacke-inteligencije

Ljubomir S. Stajić
University of Novi Sad
Faculty of Law Novi Sad
Lj.Stajic@pf.uns.ac.rs
ORCID ID: 0000-0002-7594-5741

Nenad P. Radivojević
University of Novi Sad
Faculty of Law Novi Sad
N.Radivojevic@pf.uns.ac.rs
ORCID ID: 0000-0002-0630-0632

Vladan M. Mirković
University of Novi Sad
Faculty of Law Novi Sad
V.Mirkovic@pf.uns.ac.rs
ORCID ID: 0000-0002-9995-8598

Some Aspects of Security Culture in Information Technologies

Abstract: *Information technologies (IT), among other things, were created to preserve and improve human life and work in the field of communication, education, health preservation, environmental protection, etc. However, all technological innovations, in addition to positive ones, can have negative consequences for society itself (and its security). Thus, the development of IT is accompanied by numerous problems, questions and controversies that to a certain extent and in certain cases can lead to endangerment (individuals, groups, companies, states, the international community and humanity as a whole). This imposed the need to engage all (existing and new) social potentials in order to identify all the problems and consequences that the development and application of IT can leave for society. One of those potentials or mechanisms available to society is the security culture (in IT). Security culture is an absolutely positive category, and its basic function is to prevent endangerment and to provide an optimal state of safety and security. In this regard, the subject of this work is the analysis of various aspects of security culture in IT (primarily ethical, sociological, economic and legal). The aim of the work is to expand the theoretical fund of knowledge in the field of security culture in IT, as well as to practically improve the actions and work of all those who participate in the creation (development) and application of IT.*

Keywords: *security, information technologies, security culture, security culture in information technologies, information security culture.*

Датум пријема рада: 25.12.2023.
Датум достављања коначне верзије рада: 18.01.2024.
Датум прихватања рада: 18.01.2024.