ЗБОРНИК РАДОВА

ЗБОРНИК РАДОВА

Трећа меморијална научна конференција „Предраг Марић”

Проф. др Младен Милошевић
Др Ненад Стекић (ур.)

Београд,
Новембар 2024.

Зборник радова[1] са треће меморијалне научне конференције „Предраг Марић”
24. април 2024.

Издавач
Универзитет у Београду – Факултет безбедности

За издавача
Проф. др Младен Милошевић
Декан

Уредници
Проф. др Младен Милошевић
Др Ненад Стекић

Техничко уређивање
Александар Рашковић

Дизајн корице
Ненад Стекић

Тираж
100

ISBN 978-86-80144-66-5

Штампа
Академска мисао
Приморска 21, Београд

[1] Конференција и израда овог Зборника су реализовани у оквиру пројекта који финансира Фонд за науку Републике Србије у оквиру Програма „ИДЕЈЕ” – *Management of New Security Risks - Research and Simulation Development, NEWSIMR&D*, #7749151.

Програмски одбор Конференције

- Проф. др Владан Ђокић, ректор Универзитета у Београду и редовни професор Архитектонског факултета Универзитета у Београду, председник
- Проф. др Ратко Ристић, редовни професор Шумарског факултета Универзитета у Београду
- Проф. др Владимир Поповић, декан и редовни професор Машинског факултета Универзитета у Београду
- Проф. др Владимир Лојаница, декан и редовни професор Архитектонског факултета Универзитета у Београду
- Проф. др Дејан Гвоздић, декан и редовни професор Електротехничког факултета Универзитета у Београду
- Проф. др Владимир Н. Цветковић, редовни професор Факултета безбедности Универзитета у Београду
- Проф. др Владан Кузмановић, декан и редовни професор Грађевинског факултета Универзитета у Београду
- Проф. др Горан М. Роглић, декан и редовни професор Хемијског факултета Универзитета у Београду
- Проф. др Младен Милошевић, декан и редовни професор Факултета безбедности Универзитета у Београду
- Проф. др Бранислав Ђорђевић, редовни професор и директор Института за међународну политику и привреду
- Проф. др Јасмина Гачић, председник Савета и редовни професор Факултета безбедности Универзитета у Београду
- Проф. др Ненад Путник, редовни професор Факултета безбедности Универзитета у Београду
- Проф. др Петар Станојевић, редовни професор Факултета безбедности Универзитета у Београду
- Др Ненад Стекић, научни сарадник Института за међународну политику и привреду

Организациони одбор

- Проф. др Младен Милошевић, декан и редовни професор Факултета безбедности Универзитета у Београду, председник
- Др Александар Јазић, виши научни сарадник Института за међународну политику и привреду
- Мср Милош Миленковић, помоћник начелника Управе за ватрогасно-спасилачке јединице Сектора за ванредне ситуације Министарства унутрашњих послова, дипломирани инжењер организационих наука, докторанд Криминалистичко-полицијског универзитета
- Мср Данило Потпарић, докторанд Филолошког факултета Универзитета у Београду, шеф Кабинета Ректора Универзитета
- Мср Никола Савић, докторанд Факултета политичких наука Универзитета у Београду, стручни саветник и координатор пројеката Универзитета у Београду

САДРЖАЈ

ПРЕДГОВОР

Проучавање ванредних ситуација, њихово правно регулисање, као и одговор органа власти на државном и локалном нивоу представљају изузетно значајан аспект функционисања савременог друштва. Сталне промене у околини, технолошки развој и геополитички фактори често изазивају непредвидиве догађаје који остављају несагледиве последице по безбедност заједнице, имовине и природне средине. Традиционална годишња национална меморијална конференција „Предраг Марић" представља израз настојања да се на научном и стручном нивоу понуде адекватна решења за креативне стратешке одговоре на изазове проистекле умножавањем испољавања ванредних ситуација и катастрофа у Републици Србији у последње време.

Редовна годишња Конференција је посвећена успомени на прерано преминулог генерала полиције Предрага Марића, дугогодишњег помоћника министра унутрашњих послова, начелника Сектора за ванредне ситуације, предавача Универзитета у Београду - Факултета безбедности, пионира и идејног творца система смањења ризика од катастрофа у Републици Србији. Догађај су, 24. априла 2024. године, заједнички организовали Универзитет у Београду, Факултет безбедности Универзитета у Београду, Министарство унутрашњих послова Републике Србије и Институт за међународну политику и привреду.

Овај Зборник саопштења произашао је из истраживачког пројекта NEWSIMR&D - *Management of New Security Risks – Research and Simulation Development*, ког у оквиру програма „ИДЕЈЕ" финансира Фонд за науку Републике Србије. Пројекат је посвећен анализи ванредних ситуација и пружању нормативних одговора на савремене безбедносне ризике. Циљ пројекта је оснивање Националног симулационог центра у оквиру ког ће се вршити софтверско симулирање свих врста безбедносних ризика, као и израда стратегија за ефикасно управљање кризама. Својим обухватом и мултидисциплинарним приступом, пројекат доприноси развоју стратегија и софтверских симулација за ефикасно управљање безбедносним ризицима у савременом друштву.

Зборник се састоји од 17 радова организованих у четири тематске целине, свака посвећена специфичном аспекту теме конференције. Прва целина истражује правни и нормативни оквир у Европској унији за контролу и управљање ризицима повезаним са развојем и применом вештачке интелигенције (ВИ). Божидар Бановић анализира тренутне регулативе и стандарде, док Зоран Кековић и Озрен Џигурски разматрају конвергенцију критичних инфраструктурних система и ВИ, са фокусом на изазове и будуће правце. Ана Ковачевић истиче утицај ВИ на ширење лажних вести на социјалним медијима и потенцијалне ризике, док Јелена Динић и Милица Ђурчић представљају употребу ВИ у изградњи резилијентности урбаних заједница на катастрофе.

Друга целина обухвата текстове који проучавају примену виртуелне реалности и симулација у образовању и безбедности. Владимир Буквић, Душан Кесић и Петар Станојевић објашњавају употребу *XVR* софтвера као окружења за обуку и унапређење пословних процеса на Факултету безбедности. Ненад Путник истражује дигиталне алате и симулације у области енвиронменталне форензике, док Зоран Јефтић и Петар Станојевић представљају симулације употребе цивилне заштите у ратним условима.

Горан Ј. Мандић и Јана Марковић фокусирају се на планове за ванредне ситуације у приватном сектору.

Трећа целина анализира начине на које нове технологије могу побољшати кризни менаџмент. Дејан Вулетић и Марија Вукадиновић истражују примену нових технологија у овој области, док Вања Роквић и Иван Р. Димитријевић представљају алгоритме за управљање ванредним ситуацијама. Јована Бановић представља кривична дела против безбедности рачунарских података, анализирајући правне изазове савремених технологија кроз пресуде. Милош Тошовић уноси еколошку димензију, разматрајући управљање ризицима у контексту еколошке безбедности и одрживости.

Последња целина – *Нове технологије у јавним службама и управи* – истражује начине на које се нове технологије примењују у јавним службама и управи. Ана Параушић Маринковић и Милан Липовац представљају стратегије паметног града Београда за управљање ванредним ситуацијама, док Анита Кликовац анализира интернет апликације за интегрисано управљање ванредним ситуацијама. Александра Илић истражује утицај дигиталних технологија на ресоцијализацију осуђеника, а Милош Миленковић, Данијела Спасић и Никола Митровић представљају примену информационо-комуникационих технологија у раду ватрогасно-спасилачких јединица. Наташа Марковић закључује поглавље осврtом на транспарентност јавне управе у сузбијању корупције са фокусом на заштиту од пожара.

Верујемо да текстови изложени у наставку, представљају плодотворан допринос у пружању актуелних одговора на изазове са којима се суочавамо, као и да ће меморијална конференција посвећена Предрагу Марићу наставити да окупља еминентне стручњаке из различитих области уједињених у овом заједничком напору. Стога се надамо да ће Зборник уједно представљати и важан корак ка бољем разумевању и управљању ванредним ситуацијама и ризицима. Захваљујемо се свим учесницима треће конференције «Предраг Марић» на њиховом доприносу и раду који ће, надамо се, инспирисати даље истраживање и унапређење безбедности у нашем друштву.

У Београду,
октобар 2024.

Уредници
Проф. др Младен Милошевић
Др Ненад Стекић

1

ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА И ДРУШТВЕНИ РИЗИЦИ: ПРАВНИ И НОРМАТИВНИ ОКВИР

НОРМАТИВНИ ОКВИР ЕВРОПСКЕ УНИЈЕ ЗА КОНТРОЛУ И УПРАВЉАЊЕ РИЗИЦИМА РАЗВОЈА И ПРИМЕНЕ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ[1]

Божидар Бановић[2]

Апстракт: Вештачка интелигенција убрзано постаје интегрални део свакодневног живота и пословања у већини савремених држава, значајно мењајући начин на који размишљамо, радимо, комуницирамо, доносимо одлуке. Вештачка интелигенција поседује скоро несагледив потенцијал за унапређење социјалног, економског и општег благостања и квалитета живота људи широм света. Међутим, неконтролисани развој и имплементација информационо-комуникационих система заснованих на вештачкој интелигенцији носи са собом бројне изазове и ризике по основне вредности на којима се заснивају савремена друштва и државе и изазива многобројне и значајне етичке и правне дилеме. Једна од кључних дилема тиче се поузданости вештачке интелигенције, што је у корелацији са стицањем поверења јавности у њену употребу без, или са минималним степеном ризика. С обзиром да већина питања везаних за развој и употребу вештачке интелигенције до сада није била правно регулисана, правни системи држава и међународних организација налазе се пред изазовом успостављања одговарајућег нормативног оквира за ову област. Успостављање адекватних техничких, етичких и безбедносних стандарда и доношење прописа којима ће се омогућити безбедно коришћење вештачке интелигенције и обезбедити правна средстава за отклањање евентуалних штетних последица њене употребе, основни су предуслови да се вештачка интелигенција квалификује као поуздана и одговорна. У овом раду биће критички анализиран нормативни оквир за развој у коришћење вештачке интелигенције успостављен на нивоу Европске уније, пре свега Предлог Уредбе Европског парламента и Европског савета о хармонизацији правила о вештачкој интелигенцији. Овај документ, међу првима у свету, покушава да успостави свеобухватан нормативни оквир, координисан на наднационалном нивоу, за хармонизован, безбедан и одговоран развој и употребу вештачке интелигенције у свим државама чланицама Европске уније. Упркос постојећим критикама, овај документ, као и многи други прописи Европске уније, имаће глобални утицај на правно регулисање вештачке интелигенције широм света, а посебно у државама кандидатима за пријем у Европску унију, међу којима је и Србија.

Кључне речи: вештачка интелигенција, технологија, Европска унија, нормативни оквир, хармонизација, етички стандарди, људска права.

---

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

[2] Факултет безбедности, Универзитет у Београду, banovicb@fb.bg.ac.rs

Увод

Вештачка интелигенција (ВИ) је појам који је општеприсутан у савременом свету, како у научној и стручној, тако и у лаичкој јавности. Истовремено, не постоји општа сагласност о томе шта је ВИ и чиме се она бави. Упоредо са развојем и имплементацијом савремених рачунарских система заснованих на ВИ[3], модификују се и дефиниције појма ВИ (види више High-Level Expert Group on Artificial Intelligence 2019; Samoili et al. 2020; Sheikh, Prins and Schrijvers 2023), усклађујући се, пре свега, са техничким иновацијама и ширењем подручја примене ВИ.

Као самостална информатичка дисциплина ВИ први пут је промовисана 1956. године на научној конференцији одржаној у Дартмуту (САД) (The Dartmouth Summer Research Conference on Artificial Intelligence)[4], којом приликом је од стране Џона Макартија (John McCarthy) предложено и име нове научне дисциплине (McCarthy et al. 1955). За нешто мање од 70 година, упркос застоју током осамдесетих година прошлог века, које неки аутори називају и „зимом ВИ" (Јаничић и Николић 2024, 12), ВИ доживела је такав степен развоја и примене у свим областима друштвеног живота и пословања да је многи данас сматрају стубом четврте индустријске, односно дигиталне револуције (види више Chakraborty et al. 2022; Velarde 2019).

Дигиталне технологије, науке, праксе, производи и услуге, другим речима, дигитално као свеукупни феномен радикално трансформише савремену стварност, јер ствара нова окружења и нове облике деловања са којима онда ступамо у интеракцију (Floridi 2023, 7). Убрзаном развоју и примени система заснованих на ВИ допринели су, пре свега, снага и брзина савремених рачунара и величина њихове меморије, несагледива количина и све већа доступност података у дигиталном облику[5], ефекти алгоритама и статистичких алата и број *on-line* интеракција. Другим речима, ВИ је скуп технологија које се користе подацима, алгоритмима и снагом рачунара. Информатички напредак и све већа доступност података кључни су покретачи данашњег процвата ВИ (European Commission 2019). Осим тога, број дигиталних уређаја који међусобно комуницирају већ је неколико пута већи од људске популације, при чему се већина комуникација сада одвија између машина, без учешћа људи (Floridi 2023, 5). Све више људи све више живи *on-life*, комбиновано *on-line* и *of-line*, дигитално и аналогно (Floridi 2014).

---

[3] Системи ВИ су системи које је пројектовао човек и који, кад им се зада сложени циљ, делују у физичкој или дигиталној димензији опажањем околине, прикупљањем података, тумачењем прикупљених структурираних или неструктурираних података, закључивањем на темељу знања или обраде информација из тих података и одлучивањем о радњама које је најбоље учинити да се постигне задани циљ. Системи ВИ могу користити симболичка правила или научити нумерички модел и могу прилагођавати понашање анализирајући како су њихове претходне радње утиецале на околину (High-Level Expert Group on Artificial Intelligence 2019, 7). Системи ВИ могу бити софтверски – делују у виртуалном свету (нпр. гласовни асистент, софтвер за анализу слике, системи препознавања гласа и лица) и хардверски - уграђен у хардверске уређаје (нпр. напредни роботи, аутономни аутомобили, дронови или апликације за интернет ствари).

[4] Конференција је трајала месец дана и била је фокусирана ка профилисању нове научне области. Конференцију су организовали Џон Макарти (John McCarthy), Марвин Мински (Marvin Minsky), Натанијел Рочестер (Nathaniel Rochester) и Клод Шенон (Claude Shannon).

[5] О значају података за економски и општедруштвени развој говори и развој посебне гране економије „економија података". Економија података је глобални дигитални екосистем у коме се подаци прикупљају, организују и размењују од стране мреже компанија, појединаца и институција ради стварања економске вредности (Sestinoa, Kahlawib and De Mauro 2023).

ВИ поседује скоро несагледив потенцијал за унапређење социјалног, економског и општег благостања и квалитета живота људи широм света, значајно мењајући начин на који размишљамо, радимо, комуницирамо, доносимо одлуке. Захваљујући бољем предвиђању, оптимизацији операција и расподели ресурса примена ВИ би требало да допринесе бољим резултатима и унапређењу стања у здравственој заштити, пољопривреди, образовању и оспособљавању, управљању инфраструктуром, енергетици, саобраћају, логистици, јавним услугама, безбедности, правосуђу, ефикасном коришћењу ресурса и енергије, те ублажавању климатских промена.

Међутим, неконтролисани развој и имплементација информационо-комуникационих система заснованих на ВИ носи са собом бројне изазове и ризике по основне вредности на којима се заснивају савремена друштва и државе (основне слободе и права[6], заштита података о личности и приватност, недискриминација) и изазива многобројне и значајне етичке и правне дилеме (проблеми нетранспарентности, сложености, пристраности, одређеног степена непредвидивости и делимично аутономног понашања одређених система ВИ). Посебне категорије ризика повезане су са безбедношћу и одговорношћу.[7] Поменути ризици могу произаћи из недостатака у пројектовању система ВИ (укључујући недостатке у погледу људског надзора) или због употребе података без провере и исправљања могуће пристраности.[8]

Једна од кључних дилема тиче се поузданости вештачке интелигенције, што је у корелацији са стицањем поверења јавности у њену употребу без, или са минималним степеном ризика (види више Laux, Wachter, Mittelstadt 2024). Поуздана ВИ, током целог животног века, требало би да задовољи критеријуме законитости, етичности и отпорности (High-Level Expert Group on Artificial Intelligence 2019, 5). Осим тога, пред системе засноване на ВИ постављају се захтеви за људским деловањем и надзором, техничком стабилношћ и безбедношћу, приватношћу и управљањем подацима, транспарентношћу, недискриминацијом, правичношћу, општој, а посебно еколошкој добробити и одговорношћу.

С обзиром да већина питања везаних за развој и употребу ВИ до сада није била правно регулисана, правни системи држава и међународних организација налазе се пред

[6] Примена ВИ може довести до кршења основних права и слобода, попут права на слободу изражавања, слободу окупљања, људског достојанства, недискриминацију на темељу пола, расног или етничког порекла, вере или уверења, инвалидитета, узраста или полне оријентације, права на заштиту података о личности и приватног живота или права на делотворан правни лек и правично суђење, те права на заштиту потрошача (Committee of experts on internet intermediaries 2018).

[7] Ризици повезани са безбедношћу односе се на питања сајбербезбедности, употребе ВИ у критичној инфраструктури и злонамерне упоребе ВИ, док се ризици повеани са одговорношћу за употребу ВИ односе на питања ефикасне правне заштите оштећених субјеката.

[8] На грађане и правне субјекте све чешће ће се примењивати мере и одлуке које доносе системи засновани на ВИ или се доносе уз њихову помоћ, а које понекад може бити тешко разумети и оспоравати ако је потребно. Осим тога, захваљујући ВИ могуће је подробније пратити и анализирати свакодневне навике људи, па се појављује потенцијални ризик да државни органи или други субјекти употребљавају ВИ за масовни надзор, а послодавци за праћење понашања запослених, што би било кршење права на заштиту података о личности. Због способности анализирања великих количина података и утврђивања веза међу њима ВИ се може примењивати за праћење и деанонимизацију података о лицима, па су могући нови ризици за заштиту личних података чак и кад је реч о скуповима података који сами по себи не садрже личне податке (European Commission 2020, 11)

изазовом успостављања одговарајућег нормативног оквира за ову област. Успостављање адекватних техничких, етичких и безбедносних стандарда и доношење прописа којима ће се омогућити безбедно коришћење ВИ и обезбедити правна средстава за отклањање евентуалних штетних последица њене употребе, основни су предуслови да се ВИ квалификује као поуздана и одговорна.

Као и у многим другим областима, пре свих осталих субјеката, на нивоу Европске Уније (ЕУ), предузете су значајне активности ка успостављању свеобухватног и кохерентног, наднационалног, нормативног оквира за развој и примену поуздане и одговорне ВИ, односно за управљање и контролу ризицима који су иманентни овој технологији.[9] Основни мотив за доношење нове правне регулативе заснивао се на закључку да постојеће законодавство ЕУ, као и законодавство држава чланица, не могу адекватно да одговоре на ризике који настају применом система заснованих на ВИ (види више European Commission 2020, 14-15), те је потребнно увођење нових правних инструмената и унапређење постојећих. Такође, нови нормативни оквир требало би да усклади два супротстављена интереса: слободни научно-технолошки развој и примену ВИ без икаквих тржишних и регулаторних ограничења, са једне стране, и потреба за поштовањем и унапређењем достигнутог нивоа основних вредности и људских слобода и права, на којима се заснива ЕУ, са друге стране. На крају, доношење обавезујућег прописа о ВИ на нивоу ЕУ, уз већ усвојене прописе исте врсте, директно примењиве у државама чланицама, који регулишу савремену дигиталну трансформацију, заснива се на претпоставци да ће поменути прописи, попут неких ранијих, имати глобални ефекат, односно да ће већина субјеката (државе, међународне организације, приватни сектор, произвођачи, потрошачи) и ван територије ЕУ прихватити њихову обавезност и са њима ускладити своје активности[10] (Feldstein 2023; Musch, Borrelli and Kerrigan 2023).

Поменути разлози определили су нас да, у даљем тексту, анализирамо хронологију активности ЕУ у погледу правног регулисања ВИ, као и поједина, по нама, кључна нормативна решења у Предлогу Уредбе Европског парламента и Савета о утврђивању усклађених правила о ВИ (Акт о ВИ) (European Commission 2021).

Хронологија активности ЕУ у погледу правног регулисања вештачке интелигенције

Поступак успостваљања интегралног нормативног оквира ЕУ за развој и примену ВИ није био ни брз ни лак. На том путу, органи ЕУ, а пре свега Европски парламент и Европска комисија радили су више од 4 године (Прља, Гасми и Кораћ 2021, 98).

Европски парламент донео је 2017. године Резолуцију, с препорукама Европској комисији, о правилима грађанског права о роботици (*Resolution on Civil Law Rules on Robotics*), којом се констатује да је развој уз помоћ роботике оптерећен одређеним ризи-

[9] Према подацима ОЕЦД-а, до 2021. године преко 60 земаља објавило је националне стратегије ВИ (Galindo, Perset and Sheeka, 2021.). Такође, најмање 175 земаља, фирми и других организација израдило је документе који наводе етичке принципе за ВИ, наглашавајући висок ниво активности у погледу управљања, регулисања и заштите ових система (Feldstein, 2023).

[10] Ради се о тзв. „Бриселском ефекту". Овај термин први пут је употребила Anu Bradford, професорка на Правном факултету Универзитета Колумбија, анализирајући глобалну регулаторну моћ ЕУ, односно способност ЕУ да своје правне стандарде и прописе наметне као глобално прихватљиве и обавезујуће, без потребе да за такав утицај користи међународне институције или тражи сарадњу са другим државама (Bradford 2012; Bradford 2020)

цима[11] и захтева да примена робота у различитим областима друштвеног живота буде заснована на одговарајућим етичким начелима и смерницама.[12]Осим тога, резолуцијом се захтева успостављање јединственог система грађанскоправне одговорности, на нивоу ЕУ, за штету проузроковану применом робота, у корист грађана, потрошача и предузећа.

Европска комисија је у марту 2018. године основала Експертску група на високом нивоу за ВИ (*High-Level Expert Group on AI*) чији је општи циљ био подршка имплементација иницијатива ЕУ о вештачкој интелигенцији, што је укључивало препоруке о будућем развоју политике у вези са ВИ, као и о етичким, правним и друштвеним питањима у вези са ВИ, укључујући друштвено-економске изазове. Посебан задатак ове група експерата из различитих области био је да припреми нацрт смерница за етички развој и употребу ВИ, које покривају питања као што су правичност, безбедност, транспарентност, будућност рада, демократија и шире утицај на примену Повеље о основним правима (*Charter of Fundamental Rights*), укључујући приватност и заштиту личних података, достојанство, заштиту потрошача и недискриминацију.

Европска комисија донела је 2018. године стратешки документ „Вештачка интелегнција за Европу" (*Artificial Intelligence for Europe*). Као основни циљеви ове стратегије истакнути су: развој технолошких и индустријских капацитета ЕУ и прихватање ВИ у свим областима привреде, у приватном и у јавном сектору; припрема за друштвене и привредне промене које доноси ВИ модернизацијом система образовања и оспособљавања, неговањем талената, предвиђањем промена и подстицањем транзиција на тржишту рада и прилагођавањем система социјалне заштите; стварање одговарајућег етичког и правног оквира за коришћење технологија базираних на ВИ; заједничко деловање и међусобна размена искустава земаља ЕУ у вези са развојем и употребом ВИ. Када је у питању правни оквир, стратегијом се посебно инсистира на поштовању слобода и права предвиђених Повељом о основним правима, високом нивоу безбедности производа и ефикасним механизмима правне заштите оштећених лица, чиме се ствара поверење корисника и социјална прихваћеност технологија заснованих на ВИ.

Децембра 2018. године Европска комисија усвојила је Координисани план за ВИ (*Coordinated Plan on Artificial Intelligence*), који, у ставри, представља акциони план за реализацију стратегије за ВИ. Главни циљ овог плана био је да се максимизира утицај улагања у вештачку интелигенцију на нивоу ЕУ и на националном нивоу и да се подстиче синергија и сарадња, како би се дефинисао заједнички пут и остварила конкурентност на међународном нивоу (Прља, Гасми и Кораћ 2021, 103). Тим планом постављени су темељи за сарадњу, дефинисана подручја улагања и државе чланице подстакнуте да осмисле националне стратегије за ВИ. Поменути план ревидиран је 2021. године и он представља скуп заједничких мера Европске комисије и држава чланица у сврху успостављања глобалног вођства ЕУ у области поуздане ВИ. Предложене кључне мере одраз су визије да Европска комисија, државе чланице и актери из приватног сектора

[11] Ризици који се односе на безбедност, здравље и заштиту људи, слободу, приватност, интегритет и дигнитет, те самоодређење, недискриминација и заштите података о личности;

[12] Етичке смернице требале бити засноване на начелима деловања у интересу добробити, нештетности, аутономије и правде, као и на начелима и вредностима утврђенима као што су људско достојанство, равноправност, правда и једнакост, недискриминација, информирани пристанак, заштита приватног и породичног живота и података, као и на другим темељним начелима и вредностима законодавства ЕУ, попут нестигматизације, транспарентности, аутономије, индивидуалне и друштвене одговорности, те на постојећој етичкој пракси и кодексима.

морају: убрзати улагања у технологије ВИ како би подстакли привредни и друштвени опоравак потпомогнут применом нових дигиталних решења; у целости и правовремено спровести стратегије и програме за ВИ како би ЕУ био први на тржишту да би искористио све предности које то доноси, и ускладити политике у области ВИ како би се уклонила расцепканост и одговорило на глобалне изазове.

Етичке смернице за поуздану ВИ (*Ethics Guidelines for Trustworthy AI)* сачинила је и објавила Експертска група на високом нивоу за ВИ априла 2019. године.[13] Поред етичких начела и смерница, посебну вредност овог документа чини „Појмовник", у коме су дефинисани основни појмови који су употребљени у тексту смерница и који су послужили као полазна основа за дефинисање појмова у правним прописима који су уследили (High-Level Expert Group on Artificial Intelligence, 2018, 44-46). Ове смернице као основни постулат истичу поузданост ВИ[14], а поуздана ВИ заснива се на три основна начела: законитост (поштовање примарног и секундарног права ЕУ и прописа држава чланица, посебно прописа који се односе на поједине области, попут медицине и здравствене заштите), етичност (поштовање етичких начела и са њима повезаних вредности) и отпорност (са техничког и друштвеног аспекта у односу на грешке и злоупотребе). Такође, смернице наглашавају потребу да системи ВИ буду хуманоцентрични, усмерени на човека, те да њихова употреба буде искључиво у служби човечанства и општег добра, с циљем побољшања људске добробити и слободе, уз истовремено спречавање и умањење ризика иманентних технологијама ВИ.

У оквиру начела етичности смерницама се издвајају четири етичка начела: људска аутономија, спречавање настанка штете, праведност и објашњивост. Ова начела у великој мери садржана су у постојећим правним прописима и обухваћена су и „законитом ВИ". Међутим, иако многе правне обвезе одражавају етичка начела, поштовање етичких начела надилази формалну усклађеност с постојећим законима (Floridi, 2018).

Људска аутономија подразумева одсуство неоправданог подређивања, присиљавања, заваравања, условљавања и груписања људе или манипулацију њима. Системи ВИ требало би да повећавају, допуњују и оснажују људске когнитивне, социјалне и културне вештине. Такође, ово начело захтева обезбеђивање људског надзора и контроле над радним процесима система ВИ, током целог животног века.

Системи ВИ не би смели да проузрокују, нити погоршају штету или на други начин негативно утицати на људе, што подразумева заштиту људског достојанства, духовног и телесног интегритета. Такође, морају бити безбедни и заштићени, технички отпорни, а посебно не би смели бити злоупотребљени. Смерницама се захтева посебна пажња у ситуацијама када системи ВИ могу проузроковати или погоршати негативне ефекте због разлика у моћи или информисаности (између послодаваца и радника, предузећа и потрошача, држава и грађана) или када обухватају децу, особе са инвалидитетом, и остале рањиве групе.

Праведност система ВИ подразумева обезбеђивање равноправне и праведне расподеле користи и трошкова, те избегавање ситуација у којима би појединци и групе били под утицајем неправедне пристраности, дискриминације и стигматизације. Про-

[13] Први нацрт овог документа објављен је децембра 2018. и био је предмет отворених консултација са различитим субјектима из јавног и приватног сектора, из чега је произашло преко 500 повратних информација.

[14] Поузданост ВИ не односи се само на поузданост самог система ВИ, него обухвата и поузданост свих субјеката и процеса који су део социотехничког контекста система у његовом целом животном циклусу.

цедурална димензија праведности укључује могућност оспоравања и тражења ефикасне правне заштите против одлука које донесу системи ВИ и људи који њима управљају.

Објашњивост је кључно начело за стицање поверења у системе ВИ, а подразумева да процеси буду транспарентни, да се могућности и сврха система ВИ јавно саопштавају, да се одлуке које систем ВИ доноси могу објаснити онима на које директно или индиректно утичу, у мери у којој је то могуће. Без поменутих информација одлука се не би могла на одговарајући начин оспорити.

Из поменутих етичких начела, према тексту смерница, произилазе основни захтеви које системи ВИ треба да испуне током развоја и употребе: људско деловање и надзор (види више Enqvist 2023), техничка отпорност и безбедност, приватност и управљање подацима, транспарентност, разноликост, недискриминација и праведност, добробит друштва и животне околине и одговорност. Ови захтеви детаљно су анализирани и њихово значење објашњено у тексту смерница (High-Level Expert Group on Artificial Intelligence, 2018, 17-23). Посебну вредност има део текста смерница, у коме је дат веома исцрпан попис критеријума за процену поуздане ВИ, на основу кога се може проценити да ли су и у којој мери су испуњени горепоменути захтеви (High-Level Expert Group on Artificial Intelligence, 2018, 29-38).

На крају, истакнуте су и области које могу бити проблематичне, односно у којима примена ВИ доноси висок или неприхватљив ризик, као што су: идентификација и праћење појединаца применом ВИ, прикривени системи ВИ код којих људи нису свесни да су у интеракцији са ситемом ВИ, вредновање грађана системом ВИ, које може довести до губитка аутономије и дискриминације и системи смртоносног аутономног оружја.

Следећи корак у правцу правног регулисања ВИ учињен је фебруара 2020. године када је Европска комисија донела документ под насловом „Бела књига о ВИ – европски приступ изврсности и поверењу" (European Commission 2020). Овим документом као политички циљ, дефинисана је лидерска позиција ЕУ у области ВИ, који би требало да се оствари мерама за постизање „еко-система изврсности" на свим нивоима, од истраживања и иновација, до подстицање решења на бази ВИ, али и мерама за стварање обавезујућег регулаторног оквира, усклађеног са законодавством, принципима и вредностима ЕУ, уз минимизирање ризика који се односе на основна права, безбедност и одговорност. Осим тога, наглашена је и потреба прилагођавања постојећег законодавства ЕУ променама које доноси интеграција ВИ у производе и посебно услуге, односно ширење опсега његове примене на све привредне субјекте у ланцу снабдевања, који нуде производе и услуге на бази ВИ, без обзира да ли имају седиште у ЕУ или не. Нови регулаторни оквир требало би да се базира на приступу заснованом на ризику, односно да се јасно одреди који су системи ВИ, у којим областима и којим ситуацијама, високоризични са становишта безбедности, права потрошача и основних права (види више Schuett, 2023), уз наметање посебних обавеза и обавезујућих правила за такве системе ВИ.[15] Мање ризични системи ВИ били би у режиму добровољне усклађености са новим прописима, што би се манифестовало ознакама квалитета. За процену усклађености

[15] Утврђивање усклађености високоризичних система ВИ са новим регулаторним оквиром заснивало би се на два механизма. Први би био тзв „претходна усклађеност" (поступци за испитивање, контролу или сертификацију, пре стављања на тржиште, што би могло обухватити и проверу алгоритама и скупова података који се користе у фази развоја). Други би се односио на накнадну контролу (након стављања на тржиште) и обухватио би механизме континуираног надзора над тржиштем и судског обештећења за кориснике којима је систем ВИ нанео штету.

били би надлежни национални органи, уз могућност независне ревизије у центрима за тестирање на нивоу ЕУ.

Следећи логичан корак у изградњи новог нормативног оквира за развој и примену ВИ на нивоу ЕУ био је доношење Предлога Уредбе Европског парламента и Савета о утврђивању усклађених правила о ВИ (Акт о ВИ) (*Proposal for a Regulation of the European Parliament and the Council Laying Down Harmonised Rules on Artificial Intelligence* (*Artificial Intelligence Act*)). У овом акту имплементирана је већина предлога и решења предложених у документима које смо претходно анализирали у овом раду. Уз поменути предлог Уредбе, Европска комисија је објавила и радни документ „Процена утицаја Предлога Уредбе о ВИ", којим су, између осталог, апострофирани проблеми које ће решити нови нормативни оквир за ВИ[16], те предложено неколико опција за форму новог нормативног оквира[17].

Предлог Уредбе[18] о утврђивању усклађених правила о ВИ (Акт о ВИ)[19]

Према образложењу, основна сврха овог акта је да се побољша функционирање унутрашњег тржишта ЕУ, односно да се створи уједначен правни оквир за развој, стављање на тржиште, стављање у употребу и коришћење система ВИ, да се подстакне прихватања антропоцентричне и поуздане ВИ, уз истовремено гарантовање високог нивоа заштите здравља, безбедности и основних права из Повеље ЕУ о основним правима, те да се допринесе развоју демократија, владавине права и заштите животне средине, уз подстицање иновација.

Предлогом уредбе утврђују се усклађена правила за развој, стављање на тржиште и употребу система ВИ у ЕУ, на основу пропорционалног приступа који се темељи

[16] Повећан ризик по безбедност грађана, повећан разик у односу на могућност кршења основних права грађана, непостојање ресурса за контролу усаглашености ВИ са прописима, како постојеће прописе применити на системе ВИ, неповерење у ВИ које би успорило развој и глобалну конкурентност ЕУ, фрагментација регулативе, која је препрека за јединствено тржиште ЕУ и њен дигитални суверенитет.

[17] 1. Меко право – добровољно усклађивање са прописима; 2. Секторски приступ – ad hoc прописи за поједине високоризичне системе ВИ; 3. Хоризонатални законодавни инструмент ЕУ – пропорционални приступ заснован на ризику, уз обавезне захтеве за високоризичне системе ВИ – обухвата све системе ВИ који се стављају на тржиште ЕУ; 4. Проширена трећа опција – обавезни захтеви за високоризичне системе ВИ и добровољни кодекс понашања за остале и 5. Обавезни захтеви за све ситеме ВИ пропорционално процењеном ризику.

[18] Уредбе (*regulations*) имају обавезну правну снагу и директно се примењују у свим државама чланицама. Доносе се у Савету министара ЕУ, уз обавезно или саветодавно мишљење Европског парламента, при чеми није потребно доносити посебне прописе за импементацију уредби у правни систем држава чланица. Оне имају највећу правну снагу и обавезују све, како на на нивоу EU, тако и на националном нивоу. Објављују се у Службеном листу ЕУ и ступају на снагу двадесетог дана од њиховог објављивања, осим ако самом уредбом није другачије прописано (Craig, de Búrca 2011,105).

[19] Предлог Уредбе о ВИ усвојила је Европска комисија 21.04.2021. године. Европски парламент усвојио је измењени и допуњени текст предлога уредбе 13.03.2024. године и упутио га Европској комисији и парламентима држава чланица (*European Parliament legislative resolution of 13 March 2024).* Како би се поступак доношења уредбе окончао, потребно је да текст буде усвојен у Савету министара ЕУ.

на ризику. Предлаже се јединствена и дугорочно одржива дефиниција система ВИ.[20] Прописује се посебна методологија процене ризика за здравље и безбедност или основна људска права и слободе, за све системе ВИ, те њихова класификација на системе са неприхватљивим ризиком, високоризичне и нискоризичне (види више Schuett, 2023). Забрањују се одређене изузетно штетне праксе употребе ВИ које су супротне вредностима ЕУ, те се предлажу специфична ограничења и заштитне мере у погледу одређених примена система ВИ. За високоризичне системе ВИ прописују се посебна правила да би се могли оценити поузданим пре него што буду стављени на тржиште ЕУ, али је регулисана и накнадна контрола усаглашености са тим правилима током њихове употребе. Такође, уводе се прецизне обвезе за произвођаче, увознике, дистрибутере, овлашћене заступнике и кориснике високоризичних система ВИ, како би они били у складу с постојећим прописима о заштити основних права (European Commission 2021, 3). Системи ВИ који не спадају у категорију високоризичних, подлежу постојећем законодавству и имају обавезу транспарентности, а добровољно се могу усагласити са захтевима из Предлога уредбе о ВИ, на основу кодекса понашања или неке друге саморегулативне шеме.[21]

Због ограниченог обима овог рада, у даљем тексту ограничићемо се само на краће излагање о забрањеним праксама у области ВИ, односно системима ВИ чија употреба доноси неприхватљив ризик, и високоризичним системима ВИ.

Друго поглавље Акта о ВИ носи наслов „Забрањене праксе у области ВИ" и таксативно наводи ситуације у којима је забрањена употреба система ВИ. Забрањено је стављање на тржиште, стављање у употребу или коришћење система ВИ за следеће сврхе:

- праксе које имају знатан потенцијал за манипулисање људима применом субминалних техника које делују на несвесној основи или искоришћавање слабости специфичних рањивих група као што су деца, људи са инвалидитетом, или људи специфичног друштвеног или економског положаја, како би се битно променило њихово понашање, на начин који ће њима или другим људима вероватно проузроковати психолошку или материјалну штету;
- евалуација или касификација људи или група, у одређеном раздобљу, на основу њихова друштвеног понашања или познатих, изведених или предвиђених личних карактеристика, услед чега долази до штетног и неповољног поступања према њима;
- прогнозирање вероватноће да ће неко лице учествовати у извршењу кривичног дела искључиво на основу израде његовог профила или процене његових особина и карактеристика личности;
- стварање и проширење базе података за препознавање лица нециљаним прикупљањем фотографија лица с интернета или снимака са камера за видео надзор;

[20] Систем ВИ значи машински систем дизајниран за рад с различитим нивоима аутономије, који након увођења може показати прилагодљивост те који, за експлицитне или имплицитне циљеве, из улазних вредности које прима, закључује како генерисати излазне вредности као што су предвиђања, садржај, препоруке или одлуке који могу утицати на физичка или виртуална окружења (чл. 3 Акта о ВИ).

[21] Ово значи да је, што се форме тиче, прихваћена опција усвајања хоризонаталног законодавног инструмета (захтева се потпуна усклађеност са постојећим стратегијама и законодавством ЕУ, секторским законодавством, Повељом о основним правима и секундарним законодавством ЕУ о заштити података, заштити потрошача, недискриминацији и родној равноправности), који се темељи на пропорционалном приступу заснован на ризику, уз обавезне захтеве за високоризичне системе ВИ и добровољни кодекс понашања за остале.

- извођење закључака о нечијим емоцијама на радноме месту и у образовним установама, осим ако се то чини из медицинских или безбедносних разлога;
- биометријска категоризација на основу биометријских података, како би се донео закључак о нечијој раси, политичким мишљењима, чланству у синдикату, верским или филозофским уверењима, полном животу или сексуалној оријентацији;
- даљинска биометријска идентификација у реалном времену на јавним местима, у сврху кривичног гоњења, осим ако је таква употреба нужна и у мери у којој је нужна ради једног од следећих циљева[22]:
- циљане потраге за конкретним жртвама отмице, трговине људима или сексуалног искоришћавања људи, као и потраге за несталим особама,
- спречавања конкретне, знатне и непосредне претње животу или физичком интегритету неког лица, или стварне и присутне или предвидљиве претње од терористичког напада,
- лоцирања или идентификације осумњиченог лица у сврху вођења кривичног гоњења или извршења кривичне санкције за одређена кривична дела[23] која су у дотичној држави чланици кажњива казном затвора или мером одузимања слободе у трајању од најмање четири године.

Треће поглавље Акта о ВИ детаљно регулише високоризичне системе ВИ. Према Прилогу III Акта о ВИ под високоризичним системима ВИ подразумевају се они системи који се употребљавају у било којој од следећих области: биометрија, критична инфраструктура, образовање и стручно оспособљавање, запошљавање, управљање кадровима и приступ самозапошљавању, приступ и коришћење основним приватним услугама и основним јавним услугама и накнадама, кривично гоњење, ако је то дозвољено правом ЕУ или националним правом, миграције, азил и управљање надзором државне границе, правосуђе и демократски процеси (избори, референдум и сл.). За сваку од ових области наведене су ситуације, у којима се употреба система ВИ сматра високоризичном. Други део овог поглавља Акта о ВИ садржи посебна правила за високоризичне системе ВИ која се односе на: систем управљања ризицима, начин коришћења података и техничке документације, начин евидентирања рада високоризичних система, начин остваривања транспарентности и информисања корисника, контролу рада система ВИ од стране човека, те техничку отпорност и сајбер безбедност система ВИ. На крају овог поглављња дефинисане су обавезе произвођача система ВИ[24] обавезе корисника и обавезе трећих страна. Како би се осигурало прилагођавање Акта о ВИ новим применама и апликацијама система ВИ, предвиђена је могућност проширења пописа високоризичних система ВИ у наведеним областима примене.

Иако нису изричито сврстани у високоризичне, одређени системи ВИ ипак носе висок ниво ризика од манипулације корисницима, па се за њих прописују специфич-

[22] Ови изузеци подлежу додатним условима, међу којима се издваја обавеза прибављања претходног одобрења правосудног органа или независног управног органа државе чланице у којој ће се систем ВИ употребљавати, а које се издаје на образложени захтев и у складу са правилима националног права. У хитним случајевима, систем се може употребити и без одобрења, али се захтев за одобрењем мора поднети најкасније у року од 24 сата.

[23] Прилог II Акта о ВИ садржи каталог кривичних дела за која се може применити овај изузетак.

[24] Систем управљања квалитетом, обавеза састављања техничке документације, оцењивање усаглашености, аутоматско генерисање дневника догађаја, корективне мере, обавеза обавештавања, сарадња са надлежним органима, обавезе произвођача, заступника, увозника и дистрибутера.

на правила у погледу транспарентности. Ради се о ситемима ВИ који комуницирају с људима, служе за откривање емоција или одређивање повезаности са (социјалним) категоријама на основу биометријских података или стварају сликовни, аудио или видео садржаје у којима постоји знатна сличност с постојећим лицима, предметима, местима, догађајима, или манипулишу таквим садржајем (тзв. „deep fake"). Ако је неко у интеракцији с системом ВИ или се изводи аутоматизирано препознавање његових емоција или карактеристика, мора бити обавештен да комуницира са систем ВИ. Ако се ради о „deep fake" садржајима, прописана је обвеза навођења да је тај садржај створен аутоматизованим средствима, уз изузетке у законите сврхе (кривично гоњење, слобода изражавања). То људима омогућава да доносе утемељене одлуке или одустану од коришћења система ВИ.

Закључак

Вештачка интелигенција у последњих седамдесетак година доживела је такав степен развоја и примене у свим областима друштвеног живота и пословања да је многи данас сматрају стубом четврте индустријске револуције, са несагледивим потенцијалом за унапређење социјалног, економског и општег благостања и квалитета живота људи широм света. Међутим, неконтролисани развој и примена ВИ могу довести до значајних изазова и ризика за основне вредности на којима се заснивају савремена друштва и државе, што проузрокује бројне етичке и правне дилеме. Једна од основних дилема је како успоставити баланс између слободног научно-технолошког развоја и примене ВИ без икаквих тржишних и регулаторних ограничења, са једне стране, и потребе за поштовањем и унапређењем достигнутог нивоа основних вредности и људских слобода и права, са друге стране.

Одговор на поменуту дилему тражи се у успостављању адекватних техничких, етичких и безбедносних стандарда и доношењу прописа којима ће се омогућити безбедно коришћење ВИ и обезбедити правна средстава за отклањање евентуалних штетних последица њене употребе, што би ситеме засноване на ВИ квалификовало као поуздане и вредне поверења. Иако су многе државе и међународне организације учиниле почетне кораке у нормативном регулисању ВИ, на нивоу ЕУ већ је при крају процес успостављања свеобухватног и кохерентног, наднационалног, нормативног и институционалног оквира за развој и примену поуздане и одговорне ВИ. Завршни корак у овом правцу је усвајање Уредбе о ВИ, којом се успостављају јасни и строги стандарди за развој, имплементацију и коришћење система ВИ. Уредба о ВИ темељи се на приступу заснованом на ризику, класификујући системе ВИ у различите категорије ризика, забрањујући оне који представљају неприхватљив ризик и намећући специфичне захтеве за високоризичне апликације, укључујући безбедност, транспарентност, квалитет података, људски надзор и одговорност.

Имплементација ових правила, уз надзор националних органа и строге казне за непоштовање, има за циљ да успостави ЕУ као глобалног лидера у области етичке, безбедне и поуздане ВИ. Истовремено, овакав нормативни оквир довољно је флексибилан да се може прилагодити технолошким променама и повратним информацијама, осигуравајући динамичан и одговоран приступ развоју технологија ВИ у будућности.

Србија је, пратећи процес нормативног регулисања ВИ и усвајајући решења из релевантних стратешких и правних докумената донетих на нивоу ЕУ, међу првима у југоисточној Европи, крајем 2019 године усвојила Стратегију развоја вештачке

интелигенције у Републици Србији за период 2020–2025. године. Следећи корак у овом правцу било је доношење Етичких смерница за развој, примену и употребу поуздане и одговорне ВИ, чији је основни циљ увођење превентивног механизма за одговоран развој ВИ. Примена ових смерница препоручена је свим органима државне управе и имаоцима јавних овлашћења. На тај начин, Србија се, барем на декларативном нивоу, ускладила са стратешким циљевима и етичким стандардима за развој и примену ВИ, успостављеним на нивоу ЕУ.

Библиографија

Bradford Anu. 2012. „The Brussels Effect". *Northwestern University Law* Review 107(1): 1-68.

Bradford Anu. 2020. *The Brussels Effect: How the European Union Rules the World*. New York. Oxford University Press.

Velarde Gissel. 2019. „Artificial intelligence and its impact on the fourth industrial revolution: A review". *International Journal of Artificial Intelligence & Applications* 10(6):41-48.

Galindo Liliana, Perset Karine and Sheeka Francesca. (2021), "An overview of national AI strategies and policies", Going Digital Toolkit Note, No. 14, https://goingdigital.oecd.org/data/notes/No14_ToolkitNote_AIStrategies.pdf.

Enqvist Lena. 2023. „Human oversight in the EU artificial intelligence act: what, when and by whom?", *Law, Innovation and Technology*, 15(2):508-535.

Етичке смернице за развој, примену и употребу поуздане и одговорне вештачке интелигенције. Службени гласник Републике Србије 23/2023.

European Parliament. 2017. „Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics". Strasbourg. P8_TA(2017)0051.

European Parliament legislative resolution of 13 March 2024 - P9_TA(2024)0138. https://www.europarl.europa.eu/doceo/document/TA-9-2024-03-13_EN.html#title2_2

European Commission. 2018. „Artificial Intelligence for Europe". Brussels. COM (2018) 237 final. https://eurlex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN

European Commission. 2018. „Coordinated Plan on Artificial Intelligence". Brussels. COM (2018) 795 final. https://digital-strategy.ec.europa.eu/en/policies/plan-ai

European Commission. 2020. *White Paper on Artificial Intelligence A European approach to excellence and trust*. Brussels. COM (2020) 65 Final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0065

European Commission. 2021. *Proposal for a Regulation of the European Parliament and the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*. Brussels. COM (2021) 206 Final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

Јаничић Предраг, Николић Младен. 2024. *Вештачка интелигенција*. 4 издање. Београд. Математички факултет, Универзитет у Београду.

Laux Johann, Wachter Sandra and Mittelstadt Brent. 2024. „Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk". *Regulation & Governance* 18:3-32.

Musch Sean, Borrelli Michael and Kerrigan Charles. „The EU AI Act As Global Artificial Intelligence Regulation (August 23, 2023)". Available at SSRN: http://dx.doi.org/10.2139/ssrn.4549261

McCarthy John, Minsky Marvin, Rochester Nathaniel, Shannon Claude. 2006. „A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence", August 31, 1955". *AI Magazine*, 27(4):12-14.

Прља Драган, Гасми Гордана, Корać Вања. 2021. *Вештачка интелигенција у правном систему ЕУ*. Београд. Институт за упоредно право.

Samoili Sofia, López-Cobo Montserrat, Gómez Emilia, De Prato Giuditta, Martínez-Plumed Fernando, Delipetrev Blagoj. 2020. *AI Watch - Defining Artificial Intelligence-Towards an operational definition and taxonomy of artificial intelligence*. Luxembourg. Publications Office of the European Union.

Sestinoa Andrea, Kahlawib Adham, De Mauro Andrea. 2023. „Decoding the data economy: a literature review of its impact on business, society and digital transformation". *European Journal of Innovation Management*. https://doi.org/10.1108/EJIM-01-2023-0078.

Стратегија развоја вештачке интелигенције у Републици Србији за период 2020–2025. година. Службени гласник Републике Србије 96/2019.

Sheikh Haroon, Prins Corien, Schrijvers Erik. 2023. „Artifcial Intelligence: Defnition and Background". In: *Mission AI - Research for Policy*, edited by Sheikh Haroon, Prins Corien, Schrijvers Erik. Cham. Springer.

Schuett Jonas.2023. „Defining the scope of AI regulations". *Law, Innovation and Technology* 15(1):60-82.

Schuett Jonas. 2023. „Risk Management in the Artificial Intelligence Act". *European Journal of Risk Regulation*. Published online by Cambridge University Press 08 February 2023:1-19. doi:10.1017/err.2023.1

Feldstein Steven. 2023. „Evaluating Europe's push to enact AI regulations: how will this influence global norms?". *Democratization*. 1-18. Published online: 27 Apr 2023. https://doi.org/10.1080/13510347.2023.2196068

Floridi, Luciano. 2014. *The Onlife Manifesto Being Human in a Hyperconnected Era*. New York. Springer.

Floridi, Luciano. 2018. „Soft Ethics and the Governance of the Digital". *Philosophy& Technology* 31:1-8.

Floridi, Luciano. 2023. *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities*. Oxford University Press.

High-Level Expert Group on Artificial Intelligence. 2018. „A definition of AI: Main capabilities and scientific disciplines". Brussels. European Commission.

High-Level Expert Group on Artificial Intelligence. 2019. „Ethics guidelines for trustworthy AI". Brussels. European Commission.

Committee of experts on internet intermediaries. 2018. *Algorithms and Human Rights - Study on the human rights dimensions of automated data processing techniques and possible regulatory implications*. Strasbourg. Council of Europe. https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5

Craig Paul, de Búrca Gráinne. 2011. *EU Law: Text, Cases, and Materials -Fifth Edition* . New York. Oxford University Press.

Chakraborty Utpal, Banerjee Amit, Kumar Saha Jayanta, Sarkar Niloy, Chakraborty Chinmay. 2022. *Artificial Intelligence and the Fourth Industrial Revolution*. Singapore. Jenny Stanford Publishing.

Charter of Fundamental Rights of the European Union. 21016. Official Journal of the European Union, C 202, 7 June 2016.

NORMATIVE FRAMEWORK OF THE EUROPEAN UNION FOR CONTROL AND MANAGEMENT OF RISKS IN THE DEVELOPMENT AND IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE

Abstract: Artificial intelligence is rapidly becoming an integral part of everyday life and business in most modern countries, significantly changing how we think, work, communicate, and make decisions. Artificial intelligence has an almost incalculable potential to improve people's social, economic, and general well-being and quality of life worldwide. However, the uncontrolled development and implementation of information and communication systems based on artificial intelligence brings numerous challenges and risks to the fundamental values on which modern societies and states are based and causes numerous and significant ethical and legal dilemmas. Ensuring the reliability of artificial intelligence is critical to gaining public confidence in its use, with minimal risk. As there are no established legal regulations concerning the development and usage of artificial intelligence, it presents a challenge for countries and international organizations to establish an appropriate normative framework for this area. Establishing adequate technical, ethical, and safety standards and adopting regulations that will enable the safe use of artificial intelligence and provide legal means to eliminate possible harmful consequences of its use are the essential prerequisites for artificial intelligence to be qualified as reliable and responsible. This paper will critically analyze the normative framework for the development and use of artificial intelligence established at the European Union level, primarily the Proposal for a Regulation of the European Parliament and the European Council laying down harmonised rules on artificial intelligence. This document, among the first in the world, attempts to establish a comprehensive normative framework, coordinated at the supranational level, for the harmonized, safe, and responsible development and use of artificial intelligence in all European Union member states. Despite existing criticisms, this document, like many other European Union regulations, will have a global impact on the legal regulation of artificial intelligence worldwide, especially in countries that are candidates for admission to the European Union, such as Serbia.

Keywords: artificial intelligence, technology, European Union, normative framework, harmonization, ethical standards, human rights.

КОНВЕРГЕНЦИЈА КРИТИЧНИХ ИНФРАСТРУКТУРНИХ СИСТЕМА И ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ: ИЗАЗОВИ, МОГУЋНОСТИ И БУДУЋИ ПРАВЦИ

Зоран Кековић[1], Озрен Џигурски[2]

Апстракт: Конвергенција критичних инфраструктурних система са вештачком интелигенцијом (ВИ) представља истовремено ванредне могућности и ризике. Овај рад истражује комплексни однос између критичних инфраструктурних система и ВИ, фокусирајући се на њихову конвергенцију, као и користи и ризике које настају због тога. Анализира се тренутно стање критичних инфраструктурних система, објашњава се улога ВИ у повећању њихове ефикасности, резилијентности и безбедности, и разматрају се изазови који јављају у при интегрисању ВИ технологија у ове комплексне системе. Додатно, наводе се потенцијални истраживачки правци и разматрају се друштвени аспекти који омогућавају одговорну примену ВИ у доменима критичне инфраструктуре. Поред тога, приказане су квантитативне процене квалитета интеграције система критичне инфраструктуре и вештачке интелигенције, на основу савременог нивоа технологије, знања и имплементације. На основу тога, може се закључити да је квалитет интеграције система критичне инфраструктуре и вештачке интелигенције умерено напредан, и да постоји више проблема који треба да буду решени, како би се постигло шире усвајање и максимизовале потенцијалне користи ВИ. У Додатку, приказан је пример примене вештачке интелигенције у системима за дистрибуцију воде у паметним градовима.

Кључне речи: критична инфраструктура, вештачка интелигенција, ризици, безбедност, резилијентност, паметни градови.

Увод

Критични инфраструктурни системи, укључујући транспортне системе, енергетске мреже, системе за снабдевање водом и телекомуникационе мреже, чине кичму модерног друштва. Њихове поуздане операције су од изузетног значаја за постизање националне безбедности, економске стабилности и друштвене сигурности. Истовремено, напредак у области вештачке интелигенције отворио је нове могућности за анализу, оптимизацију и управљање овим комплексним системима. Повезивање критичних инфраструктурних система и ВИ нуди нове могућности за побољшање ефикасности, резилијентности и безбедности ових система. Међутим, ова интеграција такође уводи нове ризике и проблеме, укључујући сајбер безбедносне ризике, етичке аспекте и регулаторне оквире. Овај рад пружа преглед могућих интеграција критичних инфраструктурних система и ВИ, истражујући њихове импликације и предлажући стратегије за превазилажење проблема у овом комплексном домену.

[1] Факултет безбедности, Универзитет у Београду, zorankekovic@yahoo.com

[2] Факултет безбедности, Универзитет у Београду, odzigurski@gmail.com

Примена вештачке интелигенције у системима критичне инфраструктуре

Примена вештачке интелигенције има кључну улогу у побољшању ефикасности, резилијентности и безбедности система критичне инфраструктуре у различитим секторима, (Laplante at al. 2020). Ево неколико кључних примена ВИ у системима критичне инфраструктуре.

Предиктивно функционисање

Системи предиктивног функционисања заснованим на ВИ анализирају податке са разних сензора као и податке функционисања из прошлости, како би предвидели кварове опреме пре него што се они догоде. Раним идентификовањем потенцијалних проблема, ВИ помаже у спречавању неочекиваних периода обуставе рада и смањује трошкове одржавања компоненти система критичне инфраструктуре, као што су енергетски системи, транспортни системи, нафтоводи итд.

Сајбер безбедност

Решења за сајбер безбедност заснованим на ВИ штите системе критичне инфраструктуре од сајбер претњи. ВИ алгоритми могу открити аномалије у понашању, идентификовати потенцијалне угрожености и реаговати на сајбер нападе у реалном времену. Ови системи играју кључну улогу у заштити енергетских мрежа, мрежа за дистрибуцију воде, транспортних система и комуникационих мрежа.

Оптимизовано управљање енергијом

ВИ може да оптимизује производњу, дистрибуцију и потрошњу енергије у критичној инфраструктури као што су електромреже и системи обновљиве енергије. ВИ алгоритми анализирају податке у реалном времену да би усагласили понуду и потражњу, управљали стабилношћу мреже и ефикасно интегрисали изворе обновљиве енергије.

Управљање саобраћајем и транспортом

ВИ може да унапређује управљање саобраћајем и системима транспорта, оптимизацијом тока саобраћаја, предвиђањем транспотног застоја и побољшањем распореда јавног превоза. Паметни семафори на бази ВИ, аутономна возила и предиктивно одржавање за инфраструктуре транспорта доприносе безбеднијој и ефикаснијој урбаној мобилности.

Паметне мреже и дистрибуција енергије

ВИ омогућава развој паметних енергетских мрежа које динамично реагују на промене у тражњи и понуди енергије. ВИ алгоритми могу да оптимизују дистрибуцију енергије, управљају изворима обновљиве енергије и омогућавају програмиране одговоре на захтев у потрошњи, што доводи до побољшање стања мреже и енергетској ефикасности.

Одговор на катастрофе и резилијентност

ВИ може да помогне у одговору на катастрофе и опоравак анализом података у реалном времену са сензора, социјалних мрежа и удаљених извора информација ради

процене штете, предвиђања утицаја и ефикасне алокације ресурса. Системи за подршку одлука засновани на ВИ помажу хитним службама у доношењу одлука и обавештавање за време криза.

Даљински надзор и контрола

ВИ омогућава даљински надзор и контролу система критичне инфраструктуре, омогућавајући операторима да оптимизују операције са контролних локација. Контролни системи на бази ВИ побољшавају ефикасност, смањују људске грешке и осигуравају благовремен одговор на оперативне захтеве.

Планирање инфраструктуре и управљање ресурсима

ВИ подржава планирање инфраструктуре и управљање ресурсима анализом великих скупова података ради оптимизације реализације, одржавања и побољшавања инфраструктурних пројеката и система. Предиктивна аналитика на бази ВИ помаже у приоритетизацији инвестиција и продужавању трајања животног циклуса средстава критичне инфраструктуре.

Наведене примене показују како ВИ технологије доприносе поузданости, безбедности и одрживости система критичне инфраструктуре, што у крајњем доприноси јавној безбедности и квалитету живота. Како ВИ наставља да се развија, њена улога у управљању критичном инфраструктуром постаће суштинска за суочавање са комплексним ризицима, као и за оптимизацију употребе ресурса.

Који су проблеми при примени вештачке интелигенције у системима критичне инфраструктуре?

Иако вештачка интелигенција нуди значајне предности за оптимизацију система критичне инфраструктуре, постоје више проблема и ризика које треба узети у обзир при увођењу ВИ у ову област, (US Department of Energy 2024).

Квалитет и доступност података

Модели вештачке интелигенције знатно се ослањају на висококвалитетне и разноврсне скупове података за анализу и вредновање стања. Међутим, системи критичне инфраструктуре често генеришу комплексне и хетерогене податке из више извора, који могу да варирају по питању квалитета, формата и конзистентности. Осигуравање поузданости и доступности података од суштинског је значаја за ефикасност примене ВИ.

Интерпретабилност и веродостојност

Алгоритми вештачке интелигенције, посебно модели дубоког учења, често се сматрају „црним кутијама" због своје комплексне природе и недостатка интерпретабилности. У системима критичне инфраструктуре, где одлуке имају значајне последице, битно је разумети како ВИ модели доносе своје закључке и осигурати да њихови резултати буду поуздани и веродостојни.

Безбедност и поузданост

Уводење вештачке интелигенције у системе критичне инфраструктуре ствара потенцијалне проблеме у безбедности и поузданости функционисања. Системи

управљани ВИ морају функционисати у оквиру стриктних безбедносних ограничења и стандарда како би се спречиле неочекиване последице или нефункционалност система. Резилијентност на непријатељске нападе и неочекивани злонамерни сценарији такође представљају проблем који захтева ургентно решавање.

Регулаторна и етичка разматрања

Примена вештачке интелигенције у критичној инфраструктури подлеже регулаторним оквирима и етичким смерницама како би се обезбедила усаглашеност, одговорност и траспарентност. Поштовање регулатива о приватности података, етичких принципа и индустријских стандарда од суштинске је важности за изградњу поверења и минимизирање ризика повезаних са употребом ВИ.

Интеграција са старим технологијама

Многи системи критичне инфраструктуре функционишу на старим технологијама и архитектурама које нису увек компатибилне са модерним ВИ решењима. Интеграција ВИ у постојећу инфраструктуру захтева пажљиво планирање, укључујући разматрања у вези интероперабилности, скалабилности и минимизације поремећаја у току функционисања.

Сарадња између људи и ВИ

ВИ се често примењује да би се допунили процеси људских одлука у операцијама критичне инфраструктуре. Ефикасна сарадња између ВИ система и људских оператера од суштинске је важности за искоришћавање предности обе стране, док се истовремено мора водити рачуна о одрживости, контроли и одговорности у функционисању система критичне инфраструктуре.

Трошкови и ограничења ресурса

Увођење ВИ у системе критичне инфраструктуре укључује значајне трошкове за примену нове технологије, прикупљање нових података, развој ВИ модела и функционисање комплетног система. Ограничени буџети и ресурси могу представљати проблем за организације које желе да примене ВИ у већем обиму.

Ризици сајбер безбедности

Системи на бази ВИ су осетљиви на сајбер безбедносне претње, укључујући лажне податке, злонамерне нападе и манипулацију ВИ моделима. Безбедност ВИ алгоритама, система за пренос података и комуникационих канала од суштинске је важности за заштиту система критичне инфраструктуре од сајбер претњи.

Решавање наведених проблема захтева интердисциплинарну сарадњу између експерата из разних области, аналитичара за обраду података и информација, професионалаца за сајбер безбедност, креатора политика и регулаторних правила. Развој резилијентних ВИ решења која постављају безбедност, поузданост, транспарентност и етичка разматрања на прво место, омогућава системима критичне инфраструктуре да искористе ВИ за оптимизацију перформанси и минимизацију ризика у функционисању.

Како решавати проблеме у примени вештачке интелигенције у системима критичне инфраструктуре?

За решавање проблема повезаних са применом вештачке интелигенције у системима критичне инфраструктуре, организације могу применити више стратегија и принципа добре праксе. Ево главних приступа за решавање ових проблема и осигуравање успешне примене ВИ у критичној инфраструктури, (Gerstein and Erin 2024).

Квалитет *и* доступност података

- Увођење праксе управљања подацима да би се осигурао квалитет, конзистентност и доступност података.
- Инвестирање у алате за интеграцију и нормализацију података како би се убрзало предпроцесирање и припрема података.
- Сарадња са експертима у домену процесирања података да би се идентификовали критични извори података и приоритизовали поступци за прикупљање података.

Интерпретабилност *и* веродостојност

- Коришћење интерпретабилних ВИ модела и техника које пружају увиде у моделе предвиђања (нпр. системе одлучивања, системи базирани на правилима, итд).
- Увођење метода објашњивости ВИ (XAI) да би се генерисала транспарентна објашњења за одлуке ВИ.
- Инкорпорирање процеса валидације и тестирања модела да би се осигурало да резултати добијених применом ВИ одговарају очекиваним понашањима.

Безбедност *и* поузданост

- Развој ВИ модела са уграђеним механизмима за безбедност и ограничењима да би се спречило небезбедно понашање.
- Обављање строгих тестова, симулација и валидација како би се оценила поузданост ВИ система у различитим условима.
- Увођење механизма безбедности у критичне инфраструктурне системе и обезбеђивање резервних активности ради ограничавања потенцијалних недостатака уграђених ВИ модела.

Регулаторна *и* етичка разматрања

- Придржавање прописа о заштити података (нпр. GDPR, HIPAA) и етичких ВИ принципа (нпр. поштење, одговорност, транспарентност).
- Ангажовање регулаторних тела и других актера како би се испунили правни захтеви и захтеви усаглашености.
- Успостављање управних оквира и етичких смерница за развој и примену ВИ у критичној инфраструктури.

Интеграција са старим системима

- Вршење комплетне процене постојеће инфраструктуре да би се идентификовали проблеми интеграције и проблеми компатибилности.
- Развој модуларних и скалабилних решења у области ВИ која могу комуницирати са старим системима преко стандардних интерфејса и протокола.

- Планирање стратегије фазне имплементације ВИ да би се минимизирали прекиди у раду и олакшала интеграција са старим технологијама.

Сарадња између људи *и* машина

- Пројектовање ВИ система са интерфејсима прилагођеним за кориснике и операторе и са одговарајућим интерактивним контролним панелима да би се омогућила ефикасна сарадња између људи и машина.
- Обезбеђивање обука и образовање оператерима и доносиоцима одлука о томе како ефективно комуницирати са уграђеним ВИ системима.
- Развој културе поверења и сарадње између система ВИ и људских оператера путем транспарентне комуникације и механизама за повратне информације.

Трошкови *и* ограничења ресурса

- Извршити анализе односа трошкова и потенцијалне добити како би се оцениле дугорочне предности примене ВИ у критичној инфраструктури.
- Истраживање партнерства са научним институцијама, индустријским корпорацијама и другим институцијама да би се делили ресурси и омогућило вршење експертиза.
- Употреба ВИ платформи базиране на облаку (*cloud*) и преношењу управних услуга, како би се смањили трошкови инфраструктуре и оперативни трошкови.

Безбедносни ризици *у* виртуелном окружењу

- Имплементирање јаких безбедносних мера, укључујући енкрипцију, аутентификацију и контролу приступа, да би се заштитили ВИ системи и подаци.
- Редовно изводити безбедносне ревизије и процене рањивости како би се идентификовале и смањиле потенцијалне сајбер претње.
- Подстицати културу свести о безбедности у оквиру организације путем обука и програма за запослене и остале актере.
- Применом ових стратегија и добрих пракси, организације могу превазићи изазове повезане са применом вештачке интелигенције у системима критичне инфраструктуре. На тај начин, може се осигурати поузданост, безбедност и ефикасност путем ВИ примењених решења, у оптимизацији операција и повећању резилијентности критичне инфраструктуре. Сарадња међу одговарајућим актерима, континуирано праћење и постојано усавршавање су од кључног значаја за успешну интеграцију ВИ технологија у системима критичне инфраструктуре.

Будући правци развоја у области интеграције система критичне инфраструктуре и вештачке интелигенције

Интеграција система критичне инфраструктуре са вештачком интелигенцијом има значајни потенцијал за унапређење ефикасности, безбедности и резилијентности у различитим секторима. У блиској будућности, могу се очекивати неки од следећих кључних праваца развоја у овој области, (INTEGRITI 2024).

Напредно предиктивно функционисање

Предиктивно функционисање помоћу вештачке интелигенције постаће све софистицираније, омогућавајући критичним инфраструктурним системима као што су електричне мреже, транспортне мреже и системи за снабдевање водом да предвиде неисправности пре него што се они догоде. Ово може да минимизира време застоја у раду, смањи трошкове и повећа општу поузданост.

Аутономни системи управљања

Аутономни системи управљања помоћу вештачке интелигенције имаће све већу улогу у управљању критичном инфраструктуром. Ово укључује саморегулишуће електричне мреже, аутономна возила у транспортним мрежама и системе за дистрибуцију воде који користе вештачку интелигенцију. Ови системи ће оптимизовати операције и реаговати у реалном времену на променљиве услове и ризике.

Побољшање сајбер безбедности*:*

Вештачка интелигенција биће од суштинског значаја за јачање сајбер безбедности критичне инфраструктуре. Алгоритми вештачке интелигенције могу континуирано да надгледају и анализирају трансфер података како би открили аномалије или потенцијалне сајбер претње, обезбеђујући превентивну одбрану од сајбер напада.

Интероперабилност и интеграција

Будући развоји ће бити усмерени на ефикасно укључивање и интероперабилност између различитих система критичне инфраструктуре. Вештачка интелигенција ће олакшати расподелу података, координацију и одлучивање између повезаних система, омогућавајући ефикаснију употребу ресурса и одговор на акциденте.

Резилијентност и адаптивност

Вештачка интелигенција ће омогућити критичној инфраструктури да постане адаптивнија и резилијентнија на динамичне услове околине, као што су екстремни временски услови или неочекивани акциденти. Алгоритми вештачке интелигенције могу оптимизовати алокацију ресурса и стратегије одговора у реалном времену како би се минимизирали поремећаји због прекида у раду система.

Етичка примена вештачке интелигенције

Интеграцијом вештачке интелигенције у критичну инфраструктуру, јављају се повећани захтеви за етичком применом вештачке интелигенције. Ово укључује решавање проблема сагласности, транспарентности, одговорности и приватности како би се осигурало одговорна примена ВИ технологија.

Дистрибуирано рачунарство и вештачка интелигенција

Примена дистрибуираног рачунарства у комбинацији са вештачком интелигенцијом омогућиће критичним инфраструктурним системима да обрађују податке локално у реалном времену, смањујући кашњења и зависност од централизованих центара за податке. Ово ће бити посебно корисно за апликације које захтевају ургентна одлучивања.

Сарадња између човека и машине

Будући развоји ће бити усмерени на унапређење сарадње између људи и машина у операцијама критичне инфраструктуре. ВИ системи ће помагати људским операторима у одлучивању, обезбеђујући неопходне увиде и препоруке на основу комплексне анализе података и појава.

ВИ и одрживост система

Вештачка интелигенција ће допринети да критични инфраструктурни системи постану одрживи и прилагоднији за животну средину. Ово укључује оптимизацију потрошње енергије, смањење штетних емисија и побољшање ефикасности употребом стратегија којима управља вештачка интелигенција.

Регулаторни и политички оквири

Управни органи и регулаторна тела ће морати да развијају одговарајуће препоруке и стандарде за безбедно и одговорно примењивање вештачке интелигенције у критичној инфраструктури. Ово ће укључивати решавање правних, етичких и друштвених импликација повезаних са интеграцијом вештачке интелигенције.

Укратко, будућност интеграције вештачке интелигенције са системима критичне инфраструктуре носи огромни потенцијал за промену начина обезбеђивања, управљања и заштите основних функција и операција. Будућа истраживања, иновације и сарадње биће од суштинског значаја за остваривање многих предности вештачке интелигенције у овом критичном домену, истовремено се суочавајући са новим изазовима и ризицима.

Процена квалитета интеграције система критичне инфраструктуре и вештачке интелигенције, на основу савременог нивоа технологије, знања и имплементације

Оцењивање квалитета интеграције система критичне инфраструктуре и вештачке интелигенције је комплексна област истраживања и праксе. Да би се детаљно истражила ова тема, мора се приступити различитим изворима који укључују научне радове, извештаје, књиге и студије случаја, (McMillan and Varga 2022).

За пружање квантитативне оцене квалитета интеграције система критичне инфраструктуре и вештачке интелигенције на основу савременог нивоа технологије, знања и имплементације, могу се размотрити неколико кључних фактора, расположивих глобално, и на основу тога доделити оцену на скали од 0 до 100.

Ниво имплементације (40/100)

Многи сектори критичне инфраструктуре су започели пројекте интеграције вештачке интелигенције, али ниво имплементације значајно варира. Неки сектори као што су енергетика и транспорт су постигли значајан напредак, док су други као што су здравство и управљање водом још у раним фазама.

Ефикасност (50/100)

Примена вештачке интелигенције у критичној инфраструктури показује обећавајуће резултате у побољшању ефикасности. На пример, предиктивно одржавање у електричним мрежама и оптимизација саобраћаја у транспортним мрежама приказују конкретне

користи. Међутим, потребно је шире усвајање ВИ технологије и оптимизација примене како би се у потпуности остварили потенцијалне добити.

Квалитет и доступност података (30/100)

Квалитет и доступност података остају значајни изазови у интеграцији вештачке интелигенције. Критична инфраструктура генерише огромне количине података, али проблеми као што су лажни подаци, контрола квалитета и доступност ограничавају ефикасност алгоритама вештачке интелигенције. Потребно је више инвестирања у управљање подацима.

Сајбер безбедност и одрживост (40/100)

Вештачка интелигенција може да побољша сајбер безбедност у критичној инфраструктури, али такође уводи и нове облике угрожавања. Тренутне мере сајбер безбедности захтевају унапређење како би се процесирали нови облици претњи повезане са интеграцијом вештачке интелигенције. Такође, одржање резилијентности против сајбер напада је од кључног значаја.

Регулаторни и етички аспекти (35/100)

Регулаторни оквири и етичке препоруке за вештачку интелигенцију у оквиру критичне инфраструктуре су још увек у развоју и разликују се по разним регионима. Обрада транспарентности, одговорности и приватности захтева заједничке напоре од стране законодаваца и представника различитих привредних и других сектора.

Интероперабилност и интеграциони изазови (30/100)

Интеграција вештачке интелигенције са постојећим системима критичне инфраструктуре је сложена због изазова интероперабилности и ограничења старе технологије. Ефикасна интеграција између више инфраструктурних система и платформи са ВИ је од суштинског значаја, али постоје и даље значајни проблеми.

Недостатак експерата и изградња капацитета (40/100)

Недостатак експертских стручњака за вештачку интелигенцију способних за развој, примену и одржавање решења вештачке интелигенције за критичну инфраструктуру представља ограничавајући фактор. Потребно је више инвестиција у обуку и изградњи капацитета за примену ВИ, како би се убрзао напредак у овој области.

Утицај примене ВИ (45/100)

Интеграција вештачке интелигенције показала је конкретне утицаје на операције критичне инфраструктуре, али обим и обухват тих утицаја могу бити различити. Потребни су континуирани напори како би се схватио значај примене технологије вештачке интелигенције за повећање опште користи, укључујући побољшање перформанси, повећање безбедности и смањење трошкова.

Укратко, квалитет интеграције система критичне инфраструктуре и вештачке интелигенције је умерено напредан, (средња оцена је 37.85) али још увек постоји више проблема који треба да буду решени, како би се постигло шире усвајање и максимизовале потенцијалне користи. Додељене оцене одражавају текуће стање напретка, као и области које захтевају додатну пажњу и инвестиције.

Додатак

Примена вештачке интелигенције у системима за дистрибуцију воде у паметним градовима

У контексту паметних градова, примена вештачке интелигенције у системима за дистрибуцију воде постаје критична због потребе за обезбеђивање ефикасног и одрживог управљања градском водом. Различити научни и стручни извори покривају разне могућности примене вештачке интелигенције у системима дистрибуције воде, у контексту паметних градова, од теоријских оквира до практичних имплементација и студија случаја, (Krishnan at al. 2022). Ево неколико начина како се ВИ може користи у системима за дистрибуцију воде у паметним градовима.

Мониторинг и контрола у реалном времену

Вештачка интелигенција омогућава континуирано надгледање квалитета воде и параметара расподеле користећи сензоре распоређене по граду. Анализом података у реалном времену, системи вештачке интелигенције могу открити аномалије, застоје у испоруци и промене у квалитету воде, омогућавајући одговоре у реалном времену за обезбеђивање испоруке воде и интегритета система.

Прогностичка аналитика

ВИ алгоритми могу анализирати претходне моделе потрошње, демографске податке и спољне факторе (на пример, временске услове) да би се предвидели захтеви за испоруку воде. Ове информације помажу контролним центрима да оптимизују расподелу воде, предвиде периоде највеће потрошње и планирају надоградњу инфраструктуре у складу са тим.

Откривање и спречавање губитака у дистрибуцији воде

Системи за откривање губитака воде на бази вештачке интелигенције, могу да анализирају податке са сензора притиска, мерача протока и акустичних сензора да би идентификовали губитке и потенцијалне слабе тачке у мрежи расподеле воде. Рано откривање губитака минимизира недостатак воде, смањује трошкове сервисирања и спречава прекиде у пружању услуга дистрибуције воде.

Оптимизација потрошње енергије

Вештачка интелигенција може оптимизовати рад пумпи и других компоненти инфраструктуре за дистрибуцију воде како би се минимизирала потрошња енергије. Разматрајући факторе као што су претходни захтеви, цене енергије и ефикасност система, системи вештачке интелигенције прилагодиће операције дистрибуције воде у реалном времену, како би се постигла уштеда енергије без угрожавања квалитета услуге.

Интеграција са *IoT*

Вештачка интелигенција у паметним системима за расподелу воде често се интегрише са *IoT* уређајима и платформама за анализу података у облаку (*cloud*). Ова интеграција омогућава удаљени мониторинг, агрегацију података и предиктивно одржавање компоненти водне инфраструктуре.

Надгледање квалитета воде

Алгоритми вештачке интелигенције анализирају податке о квалитету воде из различитих извора, укључујући удаљене сензоре и јавне извештаје, како би открили загађења или измене у квалитету воде. Рано откривање проблема са квалитетом воде омогућава брз одговор и мере за смањење ризика ради заштите јавног здравља.

Мерење потрошње воде

ВИ може да анализира податке са паметних водомера да би се обезбедило прецизно мерење и тачно фактурисање на основу стварне потрошње воде. Ово помаже у смањењу губитака воде и омогућава потрошачима да прате своју употребу у реалном времену, што подстиче минимизацију потрошње воде.

Ургентно реаговање и резилијентност у кризним ситуацијама

Системи за подршку одлукама на бази ВИ доприносе сценаријима ургентног одговора и повећању резилијентности за реаговање у кризним ситуацијама, као што су поплаве или кварови у инфраструктури. Анализом података у реалном времену и догађаја у прошлости, ови системи могу препоручити оптималне акције за смањење последица и брзо поновно успостављање система за дистрибуцију воде.

У паметним градовима, интеграција ВИ технологија у системе за дистрибуцију воде доприноси доношење квалитетних одлука на основу података, побољшава оперативну ефикасност и повећава резилијентност на доминантне ризике. Ове примене доприносе стварању одрживих и безбедних урбаних окружења у сврху да се ресурсима воде управља ефикасно и одговорно.

Закључак

Интеграција критичних инфраструктурних система и вештачке интелигенције доноси велике могућности за напредак ефикасности, резилијентности и безбедности у овим системима. Међутим, да би се ове потенцијалне могућности реализовале, неопходно је суочити се са многобројним техничким, етичким и друштвеним ризицима.

Квалитет интеграције система критичне инфраструктуре и вештачке интелигенције је умерено напредан, али још увек постоји више проблема који треба да буду решени, како би се постигло шире усвајање и максимизовале потенцијалне користи. Интеграција вештачке интелигенције показала је конкретне позитивне утицаје на операције критичне инфраструктуре, али обим и обухват тих утицаја могу бити различити.

Један од већих проблема је интероперабилност, тј. интеграција опреме претходних технолошких генерација са новим системима базираним на ВИ. Многе оперативне функције у критичним системима су реализоване на бази претходних технологија, а прелазак на нове ВИ технологије представља напредак, али истовремено је и веома сложен поступак трансформације.

Из тог разлога, потребни су континуирани напори како би се схватио значај примене технологије вештачке интелигенције за повећање опште користи, укључујући побољшање перформанси, повећање безбедности и смањење трошкова у критичним инфраструктурним системима. Подстичући сарадњу између различитих дисциплина и чинилаца, може се искористити трансформативна моћ вештачке интелигенције да се изграде напредни и одрживи критични инфраструктурни системи за општи добитак у друштву.

Библиографија

Laplante P., Milojicic D., Serebryakov S., Bennett D. 2020. "Artificial Intelligence and Critical Systems: From Hype to Reality", *Computer*, Nov. 2020, pp. 45-52, vol. 53.

US Department of Energy, 2024."Potential Benefits and Risks of Artificial Intelligence for Critical Energy Infrastructure". https://www.energy.gov/sites/default/files/2024-04/DOE CESER_EO14110-AI Report Abstract_4-26-24.pdf.

Gerstein, Daniel M. and Erin N. Leidy. 2024. "Emerging Technology and Risk Analysis: Artificial Intelligence and Critical Infrastructure". *Homeland Security Operational Analysis Center operated by the RAND Corporation*, 2024. https://www.rand.org/pubs/research_reports/RRA2873-1.html.

INTEGRITI, 2024. "The Role of AI and Automation in Critical Infrastructure"
https://itegriti.com/2024/cybersecurity/the-role-of-ai-and-automation-in-critical-infrastructure/

McMillan Lauren and Varga Liz. 2022. "A Review of the Use of Artificial Intelligence Methods in Infrastructure Systems", *Engineering Applications of Artificial Intelligence*, Volume 116, 2022.

Krishnan S. R., Nallakaruppan M. K., Chengoden R., Koppu S., Iyapparaja M., Sadhasivam J., Sethuraman S. 2022. "Smart Water Resource Management using Artificial Intelligence - A Review", *Sustainability* ,Volume 14, Issue 20, 2022.

CONVERGENCE OF CRITICAL INFRASTRUCTURE SYSTEMS AND ARTIFICIAL INTELLIGENCE: CHALLENGES, OPPORTUNITIES AND FUTURE DIRECTIONS

Abstract: The convergence of critical infrastructure systems with artificial intelligence (AI) presents both unprecedented opportunities and formidable risks. This paper explores the complex relationship between critical infrastructure and AI, focusing on their convergence and its implications. We analyze the current state of critical infrastructure systems, elucidate the role of AI in enhancing their efficiency, resilience, and security, and discuss the risks inherent in integrating AI technologies into these complex systems. Furthermore, we outline potential research directions and policy considerations to facilitate the responsible deployment of AI in critical infrastructure domains. Further, quantitative assessments of the quality of integration between critical infrastructure systems and artificial intelligence have been presented, based on the current level of technology, knowledge, and implementation. Based on this, it can be concluded that the quality of integration between critical infrastructure systems and artificial intelligence is moderately advanced, and there are several issues that need to be resolved to achieve wider adoption and maximize the potential benefits of AI. In the Appendix, an example of the application of artificial intelligence in water distribution systems in smart cities is shown.

Keywords: critical infrastructure, artificial intelligence, risks, security, resilience, smart cities.

ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА И ЛАЖНЕ ВЕСТИ НА СОЦИЈАЛНИМ МЕДИЈИМА: МОГУЋНОСТИ И РИЗИЦИ[1]

Ана Ковачевић[2]

Апстракт: У данашњем дигиталном добу, свеприсутни социјални медији, засновани на веб технологији, олакшавају креирање садржаја путем платформи као што су социјалне мреже, блогови, микроблогови, интернет форуми, онлине заједнице, апликације за инстант поруке**.** Ови дигитални канали, који прелазе границе традиционалне комуникације, све чешће служе као извор информација и у ванредним ситуацијама. Међутим, широка доступност информација на социјалним медијима доноси изазове повезане с њиховом аутентичношћу, тачношћу и тумачењем. Брз раст броја корисника социјалних медија, као и експлозиван раст количине објављених информација, доводи до све већег проблема лажних вести, што може имати озбиљне последице по појединца и друштво, нарочито у ванредним ситуацијама. Поред тога, секундарни ефекат лажних вести може утицати на губитак поверења у поуздане изворе вести. Појавом генеративне вештачке интелигенције, проблем се додатно компликује због потенцијала за генерисање све веће количине дезинформација, што отежава традиционалну анализу и детекцију поузданих вести. У одговору на ове изазове, имплементирани су алгоритми на социјалним медијима за детекцију лажних вести, односно класификацију информација по веродостојности и дистрибуцију садржаја релевантним корисницима. Ова технолошка решења нуде бројне предности у борби против лажних вести, али истовремено намећу се питања о транспарентности и поузданости алгоритама великих корпорација, ризику од нетачне класификације, што може довести до пропуштања легитимних информација, и потенцијалној цензури. Додатно, неопходно је осмислити механизме који ће омогућити већу транспарентност и одговорност у имплементацији ових алгоритама, како би се осигурала њихова ефикасност и праведност. Истовремено, важно је радити на образовању корисника о критичком приступу информацијама на социјалним мрежама, чиме се додатно јача прву линију одбране против лажних вести.Топ оф Форм

Кључне речи: вештачка интелигенција, социјални медији, лажне вести, ризици, ванредне ситуације.

Увод

Брзи раст броја корисника социјалних медија, као и експлозиван раст количине објављених информација, доводи до све већег проблема лажних вести, што може имати озбиљне последице по појединца и друштво, нарочито у ванредним ситуацијама.

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

[2] Факултет безбедности, Универзитет у Београду, kana@fb.bg.ac.rs

Поред тога, секундарни ефекти лажних вести могу утицати на губитак поверења у поуздане изворе вести. Појавом генеративне вештачке интелигенције, проблем се додатно компликује због потенцијала за генерисање све веће количине нових лажних информација, што отежава традиционалну анализу и откривање поузданих извора. Социјалне мреже играју кључну улогу у ширењу лажних вести, често маскираних као веродостојне. Вештачка интелигенција, док доноси многе предности, такође може бити коришћена за креирање софистицираних лажних информација. Због брзине којом се информације шире, лажне вести могу брзо постати виралне и изазвати изузетно велике последице у друштву. Ово представља изазов за кориснике који морају бити пажљивији и критичнији према информацијама које конзумирају. Едукација о препознавању лажних вести постала је кључна за очување истинитости и поузданости информација. Изузетно је важно имати на уму важност овог проблема, како бисмо сачували интегритет и поузданост информација које делимо и конзумирамо.

У раду ће бити представљено коришћење социјалних медија у ванредним ситуацијама, улогу вештачке интелигенције у креирању и ширењу лажних вести, и могућности борбе против овог проблема. Разумевање механизама који стоје иза ширења лажних вести помаже нам да развијемо ефикасне стратегије за њихову детекцију и сузбијање.

Социјални медији

Социјални медији су интернет-зависне апликације које омогућавају креирање и размену кориснички дефинисаног садржаја (Kaplan & Haenlein 2010). Социјални медији обухватају сајтове друштвених мрежа, блогове, викије, подкастове, форуме, микро блогове, апликације за слање порука, заједнице за дељење садржаја и друге платформе. Интеракција на социјалним медијима се може обављати путем текстуаних порука, гласновних порука, слика и/или видеа. Основне карактериситке социјалних медија укључују партиципацију корисника, могућност повратне информације, двосмерну комуникацију, брзо креирање заједница, ефикасно комуницирање и повезивање са другим сајтовима, ресурсима и људима. Поред тога, социјални медији омогућавају комуникацију више-према-више, што је различито од традиционалних медија.

Сингер & Брукингс (Singer & Brookings 2018) наводе да не постоји ништа слично платформама социјалних медија што је тако брзо преплавило свет. Постоји више од 4,88 милијарди активних корисничких налога на социјалним медијима, што представља око 60,6% посто светске популације (Kemp 2023). Пре само осам година овај проценат је био дупло мањи, односно износио је 30%. Треба имати на уму да број активних корисника је већи него број људи који користе те налоге, односно да неки људи имају више активних корисничких налога. Према наводима Кемп-а (Kemp 2023), корисник у просеку проводи 2 часа и 26 минута на социјалним медијима. У Србији, преко 81% интернет популације има налог на социјалним мрежама, док 83,5% испитаника (или 100% испитаних студената) користи интернет (Ковачевић и др. 2022). Такође, сваке године се бележи раст броја активних корисника социјалних медија (Kemp 2023). Највише активних корисника има на социјалној мрежи Фејсбук (Facebook), преко 3 милијарде активних корисника (Kemp 2023). Експлозивни раст социјалних медија утиче на различите аспекте друштва: социјлане, економске, културне и политичке.

Примена социјалних медија у ванредним ситуацијама

Социјални медији су омогућили грађанима да генеришу садржај, па свако са паметним телефоном и са интернетом може да креира, дистрибуира и шаље информације. Социјални медији могу да се примењују у различитм фазама управљања ванредним ситуацијама. На пример, у фази превенције могу се користити за едуковање о ризицима и подизање свести. Тако је на страници Asian Disaster Preparedness Center (ADPC) социјална мрежа Фејсбук коришћена је као платформ за ширење знања. Коришћењем различитих форми социјалних медија, људи ће бити спремнији да приме подршку која им је потребна током и након катастрофа. Пријатељи и породице угрожених могу тражити информације и помоћ о својим ближнима.

Током ванредних ситуација, изузетно важно је праћење социјалних медија у реалном времену. На пример, у случају поплаве важно је знати кључне информације за процену штете, нестанак струје, секундарну заштиту становништва, као и утврђивање ефикасног одговора на инцидент. Велику количину генерисаних података, немогуће је манулно анализати, па је потребно је коришћење алата за структурирано праћење.

Постоје бројне апликације које су се примениле у ванредним ситуацијама и користиле су социјалне медије, попут платформе Усхахиди (Ushahidi). Ова платформа отвореног кода користи *crowdsourcing* за аутоматско прикупљање информација и веб 2.0 технологије за интеграцију података из више извора (друштвене мреже, телефони, е-пошта). Платформа Усхахиди је прво примењена у Африци за кризно мапирања, а затим у неколико интернационалних катастрофа. Информације прикупљене преко ове платформе могу се директно проследити онима којима су најпотребније.

Један од велих изазова је преоптерећеност непровереним информацијама. Апликација Сахана (Sahana), систем отвореног кода за управљање катастрофама, омогућава координацију током катастрофе: од налажења несталих људи, управљања волонтерима, помоћи до ефикасног праћења владиних јединица, невладиних организација и жртва.

Микроблогинг попут Твитера (Twitter) је добро проучаван у академским истраживањима. Подаци са Твитера се користе као „сензори" за прикупљање геопросторних информација о угроженим областима, са позитивном корелацијом између активности на Твитеру и угрожености становника. Анализа социјалне мреже може открити утицај корисника, релевантност теме и ставова према темама. Ова анализа утиче на правилну перцепцију догађаја, предикцију развоја догађаја и трендова, као и правовремено доношење правих одлука. Такође, кроз анализу социјалне мреже може се вршити анализа сентимента кроз процену емоционалне реакције корисника.

Након напада који се десио у Паризу 2015.године у року 15 минута од инциднета на Твитеру се појавило већ 2% порука, док први твит добијен од званичног налога (општине Паризе), у коме су упозоравали људе да остану у својим становима и чекају званичне инструкције, био објављен неколико сати касније (Santoni & Rufat 2021). Авенути (Avvenuti) et al. (2016) су показали да уз помоћ алата за семантичку анализу и корпоративне базе знања могу да се открију информације о локацији и величини штете, које се користе за израду интерактивне кризне мапе.

Бројни су примери коришћења социјалних медија у ванредним ситуацијама у опоравку од катастрофа, попут блога www.sarvodaya.org, који је креиран преко ноћи и који се показао одличан за прикупљање донација (прикупљено је преко милион долара за неколико недеља). Гугле (Google) и Епл (Apple) су упућивали на овај блог.

Након серије терористичких напада и лажних узбуна, француски национални мобилини телефон за рано упозорење је укинут 2017. године због низа неуспеха у кашњењу и слању упозорења, а Француска влада је потписала споразум са Твитером, Фејсбуком и Гуглом за развој кризне комуикације (Santoni& Rufat 2021).

Према истраживању које су спровели Сантони и Руфат (2021), највећи проблем са подацима на социјалним медијима је да су загушени шумом, гласинама и лажним вестима, као и нетачне географске локације и накнадно ретвитована „бука". Један од механизамам самоисправљања је и да сами корисници уочене неправилности коригују на друштвеним медијима.

Лажне вести

Лажне вести нису нов феномен, но са појавом социјалних медија доживљавају невероватну експанзију. Социјални медији због својих карактеристика имају предност у ширењу вести: јефтини су и омогућавају брзо ширење информација.

Са порастом броја корисника социјалних медија и могућностима генерисања садржаја, долази до експлозивног раста количине објављених информација, што може имати озбиљне последице по појединца и друштво, нарочито у ванредним ситуацијама. Још пре више од десет година, Светски економски форум је проблем масовне дигиталне дезинформације означио као значајан технолошки ризик (Howell 2013).

Бројни су примери дезинформација на социјалним медијима током скорашње пандемије, попут лажне листе медицинских препорука угледном америчког универзитета Стенфорд (Statt 2020), или током председничких избора у Сједињеним америчким државама (САД). Пример са претходних председничих избора у САД-у показао је колики је утицај лажних вести био на изборе. Анализом 171 милиона твитова у последњих пет месеци пред изборе у САД-у, 17% садржало је линк са вестима, од чега је четвртина (7,5 милиона твитова) делила лажне или екстремно пристрасне вести (Boveta & Makse 2019).

Интересантни су наводи лажне вести имају више дељења и реакција: у последња три месеца председничких избора у САД-у 2016. године, двадесет најуспешпешнијих лажних вести на изборима је изазвало више дељења и реакција на Фејсбуку него двадесет најуспешних вести из новинарских извора (Hughes & Waismel-Manor 2020). Дизајкс (Dizikes 2018) наводи да лажне вести имају 70% већу вероватноћу да буду поново подељене у поређењу са тачним вестима и достижу десет поновних дељења двадесет пута брже од тачних вести.

Са великим напредком у обради природног језика и доступношћу генеративне вештачке интелигенције, креирање лажних вести постаје поље изузетне експанизеје са неисцрпним могућностима. Ако бисмо написали промпт код ChatGPT4 „Напиши ми три новинска чланка, са по четири реченице у којима се препоручује употреба рузмарина за заштиту од електромагнетног зрачења, на екавици, уз навођење референци, и уз то креира слику" добићемо одговор као што је представљано на Слици 1. За изузетно кратко време добијамо генерисане вести које наводе измишљене респектабилине изворе,да би поткрепили своје тврње. Уобичајени синтаксне грешке које су до скора се биле присутне код генератора језика су исправљене.

Слика 1: Резултат генерисаних новинских текстова за задати промпт

Примена алгоритама вештачке интелигенције за детекцију лажних вести

Са енормно великим бројем корисника вештачке интелигенције и великом количином података која се генерише, поставља се проблем како дистрибуирати садржај релевантним корисницима и класификовати информације према веродостојности. Овај проблем је посебно значајан у области као што су ванредне ситуације, где су правовремене и веродостојне информације од изузетне важности. Једно од могућих решења овог проблема је примена вештачке интелигенције. Иако доноси бројне предности, такође доноси изазове и потенцијалне проблеме. Ови алгоритми морају имати двоструку функцију: класификацију информација према веродостојности и дистрибуцију садржаја релевантним корисницима. Иако ово решење нуди бројне предности у борби против лажних вести, постављају се питања о транспарентности и/или праведности алгоритама које користе социјални медији.

Универзитет у Стенфорду је 2023. године спровео истраживање о транспаретности великих језичких модела (Wheatley 2023). Користећи преко сто индикатора, показано је да компаније које користе велике језичке моделе нису довољно транспарентне; чак и велики језички модели отвореног кода користе нетранспарене податке за обучавање. Према овом истраживању, Метин Лама 2 (Metin Llama 2) se pokazo kao najtransparentiji sa 54% (Wheatley 2023).

Заговорници алгоритма сматрају да је боље постојање алгоритама вештачке интелигенције, јер би у супротном информације корисника који објављују највише постова биле видљивије, што не значи да су то најрелевантније информације. Нетачна класификација вести може довести до пропуштања легитимних информација и

потенцијалне цензуре (Ковачевић & Демић 2023). Неопходно је користити алгоритме, али је изузетно важно да имамо поуздане алгоритме којима можемо веровати, чије су пристрасности исправљене, чије закључке, ограничења и начин обучавања разумемо.

Поред покушаја повећавања транспарентности алгоритама великих компанија социјалних медија, један од начина борбе против лажних вести је и едукација. Да бисмо установили полазну тачку и прилагодили боље курикуиме, урадили смо испитивање студената о постојању алгоритама за детекцију лажних вести на социјалним медијима. Показало се да значајан број испитаника није чуо или је мало чуо о алгоритимама на социјалним медијима за проналажење лажних информација (Ковачевић и Демић, 2023). Поређење старијих и млађих студената указује на то да старији студенти више читају о овим програмима и сматрају их корисним за друштво. Већина испитаника верује да алгоритми за откривање лажних вести олакшавају проналажење поузданих информација, али и да долази до погрешног уклањања вести и цензуре политичких ставова; такође, испитаници сматрају да би се у процесу детекције лажних вести требало користити комбинација алгоритама вештачке интелигенције и људске експертизе (Ковачевић и Демић, 2023).

Закључак

Проблем лажних вести није нов, али са експанзијом социјалних медија кроз велики број корисника и објава, представља огроман изазов. Социјалне мреже су постале главни канал за ширење ових неистина, често примењујући и генеративну вештачку интелигенцију за креирање садржаја. Вештачка интелигенција, иако доноси бројне предности укључујући детектовање лажних вести, може бити злоупотребљена за креирање и дистрибуцију дезинформација. Неопходно је развијати софистицираније алате за детекцију лажних вести у чију правичност и транспарентност имамо увида. Поред тога, изузетно је важна и едукација јавности о препознавању лажних вести, јер она игра кључну улогу у борби против дезинформација. Важно је радити на образовању корисника о критичком приступу информацијама на социјалним мрежама, чиме се додатно јача прва линија одбране против лажних вести.

Такође, одговорност лежи и на платформама друштвених медија да имплементирају ефикасне мере за сузбијање лажних вести, а које неће бити употребљене за цензуру. Заједнички напори технолошких компанија, законодаваца и корисника интернета су неопходни за креирање безбедног дигиталног окружења. Само уз координисану акцију можемо смањити негативне ефекте лажних вести на друштво. Улога медијске писмености никада није била важнија него данас. На крају, свако од нас мора преузети одговорност за проверу извора информација пре него што их поделимо даље.

Библиографија

'ADPC'. Accessed 30 June 2024. https://www.facebook.com/adpc.thailand.

Avvenuti, Marco, Mario G. C. A. Cimino, Stefano Cresci, Andrea Marchetti, and Maurizio Tesconi. 'A Framework for Detecting Unfolding Emergencies Using Humans as Sensors'. *SpringerPlus* 5, no. 1 (December 2016): 43. https://doi.org/10.1186/s40064-016-1674-y.

Bovet, Alexandre, and Hernán A. Makse. 'Influence of Fake News in Twitter during the 2016 US Presidential Election'. *Nature Communications* 10, no. 1 (2 January 2019): 7. https://doi.org/10.1038/s41467-018-07761-2.

Dizikes, Peter. 'Study: On Twitter, False News Travels Faster than True Stories'. *MIT News* 8 (2018): 2018.

Howell, Lee. 'Digital Wildfires in a Hyperconnected World', 2013. https://www.weforum.org/reports/world-economic-forum-global-risks-2013-eighth-edition/.

Hughes, Heather C., and Israel Waismel-Manor. 'The Macedonian Fake News Industry and the 2016 US Election'. *PS: Political Science & Politics* 54, no. 1 (January 2021): 19–23. https://doi.org/10.1017/S1049096520000992.

Kaplan, Andreas M., and Michael Haenlein. 'Users of the World, Unite! The Challenges and Opportunities of Social Media'. *Business Horizons* 53, no. 1 (1 January 2010): 59–68. https://doi.org/10.1016/j.bushor.2009.09.003.

Kemp, Simon. 'Digital 2023: Global Overview Report'. DataReportal – Global Digital Insights, 26 January 2023. https://datareportal.com/reports/digital-2023-global-overview-report.

Kovačević, Ana, and Emir Demić. 'Veštačka inteligencija za otkrivanje lažnih vesti na socijalnim medijima – ispitivanje stavova'. *Међународни ūроблеми* LXXV, no. 4 (2023): 685–710.

Ковачевић, Миладин, Владимир Шутић, Урош Рајчевић, and Ивана Минаева. 'Употреба Информационо-Комуникационих Технологија у Републици Србији, 2022.' Републички завод за статистику, Београд, 2022. https://www.stat.gov.rs/publikacije/publication/?p=14856.

Sahana. 'Sahana Foundation'. Sahana Foundation, 24 November 2021. https://sahanafoundation.org/.

Santoni, Victor, and Samuel Rufat. 'How Fast Is Fast Enough? Twitter Usability during Emergencies'. *Geoforum* 124 (1 August 2021): 20–35. https://doi.org/10.1016/j.geoforum.2021.05.007.

Sarvodaya. 'Sarvodaya'. Accessed 30 June 2024. https://www.sarvodaya.org/.

Singer, Peter Warren, and Emerson T. Brooking. *Likewar: The Weaponization of Social Media*. Houghton Mifflin Harcourt, 2018.

Statt, Nick. 'Major Tech Platforms Say They're "Jointly Combating Fraud and Misinformation" about COVID-19'. The Verge, 17 March 2020. https://www.theverge.com/2020/3/16/21182726/coronavirus-covid-19-facebook-google-twitter-youtube-joint-effort-misinformation-fraud.

Ushahidi. 'Crowdsourcing Solutions to Empower Communities'. Ushahidi. Accessed 30 June 2024. https://www.ushahidi.com//.

Wheatley, Mike. 'Stanford's AI Transparency Index Shows Foundational Models Are Shrouded in Secrecy'. *SiliconANGLE* (blog), 18 October 2023. https://siliconangle.com/2023/10/18/stanfords-ai-transparency-index-shows-foundational-models-shrouded-secrecy/.

ARTIFICIAL INTELLIGENCE AND FAKE NEWS ON SOCIAL MEDIA: OPPORTUNITIES AND RISKS

Abstract: In today's digital age, the pervasive nature of social media, powered by web technology, facilitates content creation through platforms such as social networks, blogs, microblogs, internet forums, online communities, and instant messaging applications. These digital channels, which go beyond traditional communication boundaries, increasingly serve as sources of information, even in emergencies. However, the widespread availability of information on social media brings challenges related to authenticity, accuracy, and interpretation. The rapid growth in the number of social media users, along with the explosive increase in the volume of published information, has led to the escalating problem of fake news, which can have serious consequences for individuals and society, particularly during emergencies. Moreover, the secondary effect of fake news can lead to a loss of trust in reliable news sources. The emergence of generative artificial intelligence further complicates this issue by increasing the potential for generating large amounts of disinformation, making traditional analysis and detection of reliable news more challenging. In response to these challenges, social media platforms have implemented algorithms to detect fake news, classify information based on credibility, and distribute content to relevant users. These technological solutions offer numerous advantages in combating fake news, but they also raise questions about the transparency and reliability of algorithms used by large corporations, the risk of inaccurate classification leading to the omission of legitimate information, and potential censorship. Additionally, mechanisms need to be devised to ensure greater transparency and accountability in the implementation of these algorithms to guarantee their effectiveness and fairness. Simultaneously, it is crucial to educate users on critically assessing information on social media, thereby strengthening the first line of defense against fake news.

Keywords: Social media, fake news, generative artificial intelligence, disinformation, algorithmic detection

УПОТРЕБА ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ У ПРОЦЕСУ ИЗГРАДЊЕ РЕЗИЛИЈЕНТНОСТИ УРБАНИХ ЗАЈЕДНИЦА НА КАТАСТРОФЕ

Јелена Динић[1], Милица Ћурчић[2]

Апстракт: Природне катастрофе у савременим градовима генеришу далекосежне последице у хуманој, економској, еколошкој и инфраструктурној димензији урбаног простора. Употреба вештачке интелигенције (AI) у сегменту управљања катастрофама има потенцијал да унапреди процес изградње резилијентности у свакој каскадној компоненти, почевши од антиципирања потенцијалних претњи и проактивног деловања, реактивног деловања у виду апсорпције нежељеног стресора, адаптације на измењене околности и процеса опоравка система. Оптимизација и аутоматизација, два основна процеса која се налазе у сржи вештачке интелигенције, чине обраду података бржом и ефикаснијом. У контексту управљања катастрофама, поменути процеси дају значајан допринос у унапређењу функционисања система за рано упозорење и подизање нивоа спремности грађана посредством анализе индикатора догађаја са деструктивним потенцијалом. Употреба вештачке интелигенције у одговору на катастрофе има посебан значај због могућности генерисања мапа догађаја и настале штете, чиме се унапређује ситуациона свесност и олакшава рад спасилачких тимова на терену. Ресторативни капацитет урбаних заједница суочених са катастрофама огледа се у синергетском дејству институционалних и ванинституционалних актера. Применом вештачке интелигенције, унапређује се временска димензија опоравка заједнице у виду смањења броја временских јединица потребних за ресторативну фазу као и кроз израду планова за опоравак, праћење регенеративних процеса, причињене материјалне штете и новчаних средстава намењених обнови. У наличју употребе савремених технолошких достигнућа опажа се потенцијално компромитовање резилијентности урбаних заједница употребом вештачке интелигенције. Приоритизација ефикасности подстакнуте вештачком интелигенцијом може умањити атрибуте редундантности и диверзитета које систем суочен са стресором манифестује у циклусу резилијентности без високотехнолошких утицаја. Етички и правни аспекти употребе вештачке интелигенције захтевају посебну пажњу научне и стручне јавности због могућих злоупотреба и несавесне примене технолошких иновација у процесу управљања катастрофама.

Кључне речи: вештачка интелигенција, резилијентност, урбане заједнице, природне катастрофе, етички аспекти.

---

[1] Универзитет Сингидунум, jdinic@singidunum.ac.rs

[2] Институт за нуклеарне науке „Винча", Институт од националног значаја за Републику Србију, milica.curcic@vin.bg.ac.rs;

Истраживање је реализовано уз финансијску подршку Министарства за науку, технолошки развој и иновације Републике Србије, у оквиру финансирања научноистраживачког рада Универзитета у Београду, Института за нуклеарне науке Винча (Уговор бр. 451-03-66/2024-03/200017 од 05.02.2024.)

Увод

По подацима Уједињених нација, до 2050. године две трећине светске популације живеће у урбаним срединама (UN, 2018). Последице рапидне урбанизације и динамика глобалног окружења намећу потребу за употребом савремених технолошких решења у унапређењу безбедности становника у урбаним срединама. Савремене урбане заједнице одликује велика густина насељености на ограниченом простору. Појава природних катастрофа у градовима има потенцијал да угрози велики број људских живота, причини значајну материјалну штету и компромитује функционалност урбаног простора. Емергентне технлогије и њихов прогресивни развој током Пете индустријске револуције[3] отвориле су бројне могућности за унапређење процеса изградње резилијентности урбаних заједница на природне катастрофе. Појавне форме вештачке интелигенције попут модела са надзором и без надзора, дубоког учења, подстицајног дубоког учења и оптимизације података (Sun et al., 2020) могу дати значајан допринос у проактивном деловању институционалних и ванинституционалних актера, њиховом правовременом одговору на катастрофе, адаптацији на измењене околности функционисања града као и процесу опоравка. Подизање нивоа ефикасности рада система цивилне заштите, посебно у сегменту доношења одлука (Ghaffarian et al., 2023), представља кључни допринос у имплементацији емергентних технолошких решења у изразито комплексан процес изградње резилијентности урбаних заједница на катастрофе. Употреба емергентних технологија у различитим фазама процеса управљања катастрофама генерише одређене ризике и отвара бројна питања у контексту етичких аспеката употребе датих иновативних решења. Комплексност и недовољна транспарентност начина рада вештачке интелигенције (ВИ) као интегралног дела емергентних технологија намеће захтеве за успостављањем атрибута објашњивости, чиме је омогућена јасна интерпретација, дубинско разумевање одлука и изградња поверења у перформансе вештачке интелигенције (Ghaffarian et al., 2023). Питања везана за заштиту људских права, посебно права на приватност, упитна поузданост података на којима се заснима доношење одлука вештачке интелигенције и дискриминација појединих категорија становника као крајњих корисника бенефита емергентних технологија захтевају мултидисциплинаран приступ научне и стручне јавности у адресирању стејкхолдера са капацитетом за осмишљавање одговора на постављене етичке дилеме.

Резултати малобројних експлоративних студија спроведених на тему утицаја напредне технологије на различите функционалне аспекте урбаних заједница указали су на постојање ниског нивоа свести и знања грађана о бенефитима и ризицима употребе дигиталне технологије последње генерације у процесу изградње атрибута rezilijenntosti grada na природне катастрофе (Yigitcanlar et al., 2021; Kankanamge et al., 2021). Дисеминацијом знања у форми пријемчивој широј јавности о употреби емергентних технологија у области цивилне заштите постиже се неопходан услов за неутралисање негативних ефеката утицаја дигиталних технологија на различите димензије резилијентности урбаних заједница.

[3] Пета индустријска револуција означава период од 2020. године обележен интеракцијом између хумане и вештачке интелигенције

Употреба емергентних технологија у превенцији катастрофа у урбаним заједницама

Коришћење технологије која „имитира" когнитивне функције људских бића попут процеса учења или вештина решавања проблема (Konar, 2018) има апликативну функцију у изградњи резилијентности савремених урбаних заједница на природне катастрофе. Технолошка достигнућа последње генерације, тзв. емергентне технологије (Mijić, 2023) своју примену налазе у области метеорологије, геологије, сеизмологије и екологије (Xu, 2023). Анализом научне и стручне публицистике уочава се заступљеност технолошких достигнућа последње генерације у сегменту раног упозорења јавности, индикатора о непосредној близини катастрофе и припрема за евакуацију, док у симулацијама и показним вежбама примена вештачке интелигенције није заступљена у великој мери (Sun et al., 2010). Вештачка интелигенција је од посебног значаја у сфери раног мониторинга поплава, земљотреса и вулканских ерупција (Xu et al., 2023). Предиктивне анализе у реалном времену извршене од стране вештачке интелигенције могу детектовати локације на којима ће се катастрофа десити, проценити потенцијалне застоје у раду критичне инфраструктуре, динамику кретања масе у процесу евакуације (Sun et al, 2024, 13). У ту сврху најчешће се користе неуралне мреже, подстицајно дубоко учење и алгоритми за оптимизацију (Sun et al, 2024, 13). Допринос вештачке интелигенције у сегменту превенције катастрофа у урбаним заједницама може се представити у склопу неколико кластера (Xu et al., 2023, 2):

- брзом обрадом велике количине података унапређује прецизност предвиђања катастрофа и правовремено реаговање, посебно у сегменту превенције геолошких, метеоролошких и еколошких катастрофа;
- успостављањем прецизног система раног упозорења редукује се могућност лажних узбуна становника, подстиче се кредибилитет система за рано упозорење као и поверење грађана;
- савремена технолошка достугнућа омогућила су трансмисију велике количине података у реалном времену чиме су унапређени капацитети за мониторинг катастрофа;
- емергентне технологије, посебно велики скупови података (eng. *big data*) и рачунарство у облаку (eng. *cloud computing*), дају импулс у унапређењу паметног доношења одлука у оквиру проактивног управљања катастрофама;
- паметне технологије унапређују процес едукације и подизања свести грађана о потенцијалним катастрофама.

Ингресијом четбот технологије засноване на вештачкој интелигенцији (eng. *Chatbot GPT*) у различите друштвене сфере покренуто је питање имплементације овог технолошког решења у области управљања у ванредним ситуацијама (Xue et al., 2023). Изразито висок потенцијал четбот технологије огледа се у могућности мимикрије језика људских бића и способности вођења конверзације (Xue et al., 2023:557). У складу са наведеним могућностима, поменуто технолошко решење има апликативну сврху у обасти превенције катастрофа. Посебно драгоцену улогу четбот технологија има у контексту пружања објашњења из области управљања катастрофама популацији која не разуме стручну терминологију (Xue et al., 2023). Такође, четбот технологија може дати изузетан допринос у контексту информација о превентивним мерама, систему за рано упозорење, интерпретирати сигнале за упозорење и усмерити на евакуационе путеве и склоништа (Xue et al., 2023, 559). Ова иновативна технологија, поред набројаних

предности, поседује и мањкавост у виду недовољне поузданости и прецизности (Tao, 2023). С тим у вези, потребно је додатно усавршити њене капацитете за примену у проактивном одговору на катастрофе у урбаним заједницама. У Јапану је конструисан систем заснован на вештачкој интелигенцији за извештавање о локацијама земљотреса под називом „*Torreter*", чија брзина и прецизност надилазе потенцијале надлежних служби за обавештавање јавности (Munawar et al., 2022, 5). Примена алата вештачке интелигеније у електроенергетском систему има огроман потенцијал у области детекције потенцијалних прекида снабдевања електричном енергијом, дајући допринос у унапређењу рада овог сегмента критичне инфратсруктуре рањивог на различите појавне облике катастрофа (Munawar et al., 2022).

Појава земљотреса у градовима изазива велику забринутост због великог броја потенцијалних жртава и материјалне штете, посебно на објектима критичне инфратсруктуре. Новија генерација истраживача доводи у питање конвенционалне сеизмолошке методе попут детекције радиоактивног гаса радона из микропукотина чији настанак претходи масивном померању тектонских плоча (Riggio et al., 2015). Машинско учење као подпоље вештачке интелигенције има доказану успешност у детекцији земљотреса посредством алгоритама заснованих на тумачењу комплексних сеизмолошких образаца, метеоролошких података и великој брзини прикупљања истих (Pwavodi et al., 2024). У Гватемали, комбиновањем вештачке интелигенције и машинског учења врше се предикције локалитета на којима се налазе зграде подложне рушењу током земљотреса (Sharifi & Allam, 2023, 13). Идентификацијом подручја рањивих на катастрофе посредством анализе сателитских снимака урађених уз помоћ вештачке интелигенције и машинског учења даје се додатни подстицај у унапређењу превентивног капацитета резилијентности урбаних заједница на кататсрофе.

Табела 1: Примена ВИ у фази превенције катастрофа
(адаптирано по узору на: Kankanamge et al., 2021, 3).

Примена технологије ВИ	Методе ВИ
Детекција кризног догађаја	Линеарне регресије, дубоко учење
Разумевање реакције јавности, подстицање свести о могућим катастрофама	Нелинеарне регресије, логистичке регресије; дубоке неуралне мреже
Процена рањивости	Разумевање слика на нивоу објекта; машине за векторску подршку
„озбиљне игре"/апликације за симулацију	К-најближи суседи, неуронске мреже, хијерархијско груписање, К-кластери (алгоритам за учење без надзора)
Претрага података у контексту катастрофа управљање знањем и анализа великих група података са интернета и друштевних мрежа	Груписање на основу заједничких карактеристика (eng. *fuzzy clustering*); анализа главних компоненти; Chatbot GPT

Имплементација иновативних технологија у одговору на катастрофе у урбаним срединама

Апсорпциони и адаптивни капацитет урбане заједнице суочене са одређеним појавним обликом катастрофе рефлектује се у способности институционалних и ванинстицуционалних актера да пруже адекватан одговор и прилагоде се на измењене услове функционисања унутар урбаног простора без нарушавања идентитетних обележја и функционалности виталних система (Schintler & McNeely, 2022; Dinić, 2023). Првих 12 часова од тренутка наступања катастрофе (eng. *standard relief hours*) представљају кључни временски период за спашавање угроженог становништва и допремање помоћи (Farazmehr & Wu, 2023). Имплементација емергентних технологија у процесу одговора на катастрофу унутар урбане заједнице је од изузетног значаја због чињенице да адекватан и правовремен одговор може бити одлучујући фактор у спашавању великог броја лица угрожених катастрофом (Sun et al., 2020).

Мапе догађаја и потенцијалне штете генерисане од стране вештачке интелигенције подстичу развој ситуационе свести, утичу на ефикаснији одговор спасилачких служби и расподелу ресурса у заједници (Sun et al., 2020, 14). Ефикасан и правовремен одговор додатно унапређује употреба роботике, друштвених мрежа и података прикупљених уз помоћ паметних телефона (Takashi et al., 2015). У контексту података прикупљених са друштвених мрежа поставља се питање њиховог кредибилитета и поузданости (Sun et al., 2020, 15). Заступљеност роботике у процесу одговора на катастрофе добија на значају због великих потенцијала да служе као платформе за даљинско надгледање подручја погођених катастрофом пружајући обиље података надлежним службама, посебно у сегменту мапирања терена, гашења пожара у опасним условима, претраге за преживелим лицима и евидентирању причињене материјалне штете (Schneider & Wildermuth, 2017; Hu et al., 2019; Lattanzi & Miller, 2015).

Временске јединице унутар којих се одвија непосредан одговор на катастрофу и адаптација на измењене услове функционисања у урбаном простору одликује интензиван телекомуникациони саобраћај и процес евакуације становништва. Машинско препознавање образаца и кључних речи у комуникацији и употреба алгоритама за обраду природних језика доприносе унапређењу ситуационе свести што у крајњој инстанци доводи до ефикасније расподеле људских и материјалних ресурса надлежних служби (Sun et al., 2020, 15). Егзактно лоцирање угроженог подручја и допремање опреме и залиха хране, воде и медицинских средстава у кратком временском року је од есенцијалног значаја у процесу заштите и спашавања (Farazmehr & Wu, 2023). Употреба вештачке интелигенције у сврху анализе садржаја профила на друштвеним мрежама непосредно након кататсрофе стиче се увид у потребе пружања психолошке потребе угроженим грађанима и допремања хуманитарне помоћи (Sun et al., 2020, 16).

Обрада природних језика (eng. *NLP*) и компјутерски вид као подпоље вештачке интелигенције користе метаподатке преузете са друштвених мрежа попут текстуалних порука, видео записа и слика у циљу побољшања одговора на катастрофе (Imran et al., 2020). Процена преовладавајућег сентимента у реакцији јавности на катастрофу посредством обраде података преузетих са друштвених мрежа може бити од изузетног значаја и служити као корективна смерница властима у правцу побољшања институционалног одговора (Imran et al., 2020, 2). Такође, подаци са друштвених мрежа могу бити од велике користи у идентификацији сведока који на основу непосредног искуства могу проценити ниво причињене штете и указати на обим ангажовања надлежних служби у процесу

спашавања повређених и несталих лица (Zahra et al., 2018). Постојање дезинформација и гласина на друштвеним мрежама у тренуцима након катастрофе има потенцијал да компромитује ефикасност одговора надлежних служби (Imran et al., 2020, 3).

Интегрисана употреба вештачке интелигенције, дронова и гео-информационог система (eng. *geographic information system- GIS*) у поступку ваздушног извиђања локације погођене катастрофом представља изузетно моћну алатку у процесу изградње резилијентности урбаних заједница на катастрофе (Iqubal et al, 2021).

Табела 2: Примена ВИ у фази одговора на природне катастрофе (адаптирано по узору на: Kankanamge et al., 2021, 3).

Примена технологије ВИ	**Методе ВИ**
Симулација препознавања	Сакривени Марков модел, неуралне мреже (конволуционе, рекурентне, рекурзивне);
Разумевање реакције јавности, идентификација сведока, кризно коуницирање	Вишеслојна перцепција;
Активности пружања помоћи током катастрофа, употреба дрона у детекцији преживелих	Q-учење; градијенти прописа, генетички алгоритми;
Употреба *Chatbot* технологије за унапређење менталног здравља	Оптимизација роја честица; симулирани подстицаји;
Евакуација масе	Конволуциона неуралнa мрежа; вештачка неуралнa мрежа.

Примена вештачке интелигенције у процесу опоравка урбаних заједница од катастрофа

Ресторативна фаза циклуса резилијентности урбаних заједница на катастрофе рефлектује се у капацитету институционалних и ванинституционалних актера да се у кратком временском периоду опораве од последица стресора, уз демонстрацију очуваног идентитета и функционалности урбаног простора (Dinić, 2023). Опоравак физичких компоненти урбане заједнице од последица катастрофе је комплексан и дуготрајан процес који захтева синергетско залагање стејкхолдера из различитих интересних сфера у циљу процене штете, обезбеђивања буџета за санацију као и планирања изградње. Технолошка решења последње генерације у форми вештачке интелигенције дају допринос у редукцији времена потребног за опоравак, праћењу процеса и финансијских токова обнове (Sun et al., 2023, 19).

Брза и тачна процена физичке штете је од есенцијалног значаја за отпочињање ресторативне фазе циклуса резилијентности, и поменути процес може бити унапређен уз помоћ слика прикупљених различитим технолошким средствима (дроновима, сензорима за мерење података и сл.) (Sun et al., 2023, 19). Технике оптимизације података нашле су примену у области израде планова за опоравак заједнице, паралелно са дубоким учењем и подстицајним учењем примењеним у креирању стратегија опоравка заједница од катастрофа (Joo et al, 2019). Неометан проток информација је од

есенцијалног значаја у процесу одговора и опоравка од кататсрофа. У складу са наведеним, машинско учење може имати примену у процесу детекције лажних пријава штете и сличних преварних радњи (Gilmour, 2019). Методе вештачке интелигенције попут неуралних мрежа, случајне шуме (eng. *Random Forest*), одлучивања у једном покушају (eng. *One-shot learning*) и машина за векторску подршку (eng. *Support Vector Machine*) користе се у детекцији штете настале под утицајем катастрофа (Munawar et al., 2022). Улога фотограметрије засноване на вештачкој интелигенцији је од изузетног значаја у прикупљању квантитативних података о обиму и врсти оштећења физичких објеката (Iqubal et al, 2021, 12).

Потешкоћа примене технологије последње генерације у области реконструкције урбаних заједница огледа се у одсуству стандардизованих метода за прикупљање и обраду информација чиме се ствара неусаглашеност у резултатима процене економских губитака (Sun et al., 2023, 20). Такође, примена истоветних алатки вештачке интелигенције за процену штете на објектима грађених од различих грађевинских материјала и различитим методама градње указује на потребу развоја стандарда за крајње кориснике из различитих области (Munawar et al., 2022, 5).

Табела 3. Примена ВИ у фази опоравка од катастрофа
(адаптирано по узору на: Kankanamge et al., 2021, 3).

Примена технологије ВИ	Методе ВИ
Детектовање штете и социоекономског опоравка	Обрада природних језика (eng. *Natural Language Processing*)
Разумевање реакција јавности, процена штете	
Процена изгубљених људских живота	

Изазови и ризици употребе вештачке интелигенције у процесу управљања катастрофама

Доба Пете индустријске револуције генерисало је бројне друштвене и економске бенефите. Истовремено, примена савремених технолошких решења, нарочито у процесу изградње резилијентности савремених урбаних заједница на катастрофе, изнедрила је бројне изазове и ризике. У контексту изазова, могу се издвојити следеће појаве (Xu et al., 2023, 3):

- потреба за унапређењем обуке и квалитета људских ресурса, у циљу подизања нивоа знања и вештина потребних за коришћење технологије засноване на вештачкој интелигенцији;
- дељење података захтева посебну пажњу због могућег компромитовања приватности грађана;
- неизвесност као једна од особености вештачке интелигенције, као и карактеристике „црне кутије [4]";

[4] „*Black box*" karakteristike veštačke inteligencije odnose se na odsustvo uvida šire javnosti u ulazne i izlazne operacije (eng. *input, output*) na kojima je zasnovan rad sistema (Black box AI, 2024).

- примена вештачке интелигенције у земљама у развоју представља својеврстан изазов због чињенице да технолошка решења последње генерације изискују значајна материјална улагања; доступност вештачке интелигенције и потенцијално стварање социјеталне асиметрије због немогућности приступа високотехнолошким решењима или услед недостатка знања и вештина потребних за коришћење;
- потребно је уложити додатне напоре у циљу популаризације вештачке интелигенције и едуковања шире јавности о начинима примене и бенефитима.

Нормативна регулатива употребе вештачке интелигенције углавном је заснована на препорукама и смерницама, односно документима без обавезујуће правне снаге. Одсуство увида у начин рада технолошких система заснованих на раду вештачке интелигенције довело је до развоја атрибута објашњивости (eng. *Explainable AI – XAI*).

Наведени појам имплементиран је у препоруке и етичке смернице којима се указује на препоручени смер решавања „невидљивих ризика" употребе емергентних технологија (Roca et al., 2017). Разлика између легалне и етичке употребе вештачке интелигенције представљена је у Табели 4.:

Табела 4: Разлика између легалне и етичке употребе вештачке интелигенције (адаптирано по узору на: Qian et al., 2024, 2)

	„Легална" ВИ	**„Етичка" ВИ**
Дефиниција	Сет правила створених од стране административних власти друштва у циљу обезбеђивања развоја и коришћења ВИ у складу са позитивним прописима;	Скуп моралних принципа који контролошу рад ВИ или конфликте везане за развој и коришћење ВИ;
Сврха	Стварање правно усклађеног развоја и употребе ВИ;	Обезбеђивање етике као централног принципа развоја и коришћења ВИ;
Последице	Развој правних оквира за обезбеђење надзора и упутства за развој и употребу ВИ;	Усвајање и адаптација постојећих моралних принципа за управљање развојем и употребом ВИ, као и формулација нових етичких принципа.

Кључно етичко питање у контексту употребе вештачке интелигенције у социјеталној сфери тиче се дискриминације и пристрасности проистекле из технолошког и хуманог аспекта коришћења ове врсте емергентних технолошких решења (Qian et al., 2024, 3). Атрибути „црне кутије" отежавају детекцију наведених проблема унутар система вештачке интелигенције, док са друге стране недовољно развијена свест твораца вештачке интелигенције о социјеталним аспектима употребе може довести до различитих облика дискриминације (Qian et al., 2024).

Разумевање начина на који функционише вештачка интелигенција је од виталног значаја за целокупно друштво. С тим у вези, неопходно је унапредити објашњивост ВИ, поузданост и транспарентност (Qian et al., 2024, 3). Важно је истаћи да компаније које се баве креирањем вештачке интелигенције пружају отпоре смештању емергентних технологија у законске оквире јер правно обавезујућа снага наведене нормативне

регулативе успорава прогресиван напредак технолошких решења последње генерације и поседује потенцијал да угрози компетитивну предност (Siau, 2003). Улагање у образовне профиле из области вештачке интелигенције уз континуирано унапређење „меких вештина" отвара простор за ефикасно супротстављање широкој лепези изазова насталих као последица употребе емергентних технологија (Qian et al., 2024). Ера изразитих динамичних промена у технолошкој сфери намеће потребу јачања „квоцијента адаптибилности" (eng. *adaptability quotient - AQ*) који се рефлектује у континуираном прилагођавању образовног система потребама детектованим на актуелном тржишту рада (Qian et al., 2024, 4).

Посебну забринутост шире јавности изазива потенцијално угрожавање приватности од стране различитих технолошких форми вештачке интелигенције. Колекција, обрада и дисеминација података прикупљених у циљу превенције катастрофа у урбаном простору, пружања адекватног одговора институционалних и ванинституционалних актера као и брзог опоравка заједнице захтева посебан приступ у циљу заштите основних људских права, посебно права на приватност. Било који облик угрожавања приватности грађана представља синоним за угрожавање њихове безбедности (Rizi & Seno, 2022, 12). Заштита приватности грађана обухвата (Rizi & Seno, 2022, 12):

- спацијалну (просторну) компоненту (просторно-временске податке, праћење, прогнозирање);
- комуникације (телефонске позиве, поруке, е-маил корсподенцију);
- физичку и менталну компоненту (мишљења, веровања);
- понашања и активности (навике, интересовања, понављајуће обрасце понашања);
- друштвени живот грађана;
- облике удруживања (групе за подршку, чланство у организацијама);
- мултимедијалне садржаје (аудио и видео записе, фотографије).

Подаци о здравственом и финансијском стању имају епитет посебно осетљивих (Rizi & Seno, 2022, 21) и као такви захтевају посебну заштиту. Одсуство универзалних смерница и протокола о употреби вештачке интелигенције у области управљања у ванредним ситуацијама као и аката са правно обавезујућом снагом попут закона намеће потребу нормативног уређења и усклађивања дате области у циљу заштите основних људских права и етичког поступања уз симултану изградњу резилијентности урбаних заједница на катастрофе.

Закључна разматрања

Савремени градови представљају генераторе привредног и технолошког развоја. Подложност градова стресорима и претурбацијама у виду пандемија, климатских промена, природних катастрофа, опасних догађаја изазваних антропогеним утицајем и политичког насиља указује на потребу за досезањем атрибута резилијентног и одрживог урбаног система. Учесталост природних катастрофа и њихов деструктивни потенцијал у савременим урбаним заједницама захтевају свеобухватан приступ у циљу унапређења превентивних механизама и реактивних капацитета изложених у форми адекватног и правовременог одговора, прилагођавања на измењене услове функционисања и рапидног опоравка целокупне заједнице. Концентрација великог броја становника на географски лимитираном простору намеће потребу израде планова и стратегија за унапређење резилијентности урбаних заједница подложних катастрофама.

Опсежним прегледом научне литературе у форми најеминентнијих светских часописа уочава се тренд примене вештачке интелигенције првенствено у сегменту превенције и непосредног одговора на катастрофе. Примена емергентних технологија у одговору на катастрофе и процесу опоравка је у повоју. Огроман потенцијал вештачке интелигенције захтева примену опсежних мера у стварању нове генерације стручњака који ће поред неопходних знања и вештина имати развијену свест о изазовима употребе технолошких решења последње генерације, посебно у погледу етичких аспеката примене. Узевши у обзир чињеницу да вештачка интелигенција улази у све сфере социјеталног битисања, мултидисциплинарни приступ решавању изазова и ризика постаје императив. Синхронизацијом рада доносилаца политичких одлука, невладиног сектора, научно-истраживачких институција, привредног сектора и грађана у погледу решавања изазова и ризика примене емергентних технологија ствара се плодно тло за унапређење резилијентности урбаних заједница на катастрофе посредством примене различитих технолошких форми вештачке интелигенције.

Библиографија

Black box AI. Accessed 8th April 2024. https://www.techtarget.com/whatis/definition/black-box-AI

Dinić, Jelena. 2023. „Rezilijentnost urbanih zajednica na opasnosti izazvane požarima". Fakultet bezbednosti, Univerzitet u Beogradu (doktorska disertacija).

Farazmehr, Shima and Wu, Yong. 2023. "Locating and deploying essential goods and equipment in disasters using AI-enabled approaches: A systematic literature review". *Progress in Disaster Science*, 100292.

Ghaffarian, Saman, Taghikhah, Firouzeh Rosa and Maier, R. Holger. 2023. "Explainable artificial intelligence in disaster risk management: Achievements and prospective futures". *International Journal of Disaster Risk Reduction*, *98*, 104123.

Gilmour, Paul Michael. 2019. "The application of photography in investigating fraud". *The Imaging 1258 Science Journal* 67(4):215–223.

Hu Da, Li Shuai, Chen Junjie, Kamat R. Vineet. 2019. "Detecting, locating, and characterizing voids in 1376 disaster rubble for search and rescue". *Advanced Engineering Informatics* 42:100974.

Imran, Muhammad, Ofli, Freda, Caragea, Doina and Torralba, Antonio. 2020. "Using AI and social media multimodal content for disaster response and management: Opportunities, challenges, and future directions". *Information Processing & Management*, *57*(5), 102261.

Iqbal, Umair, Perez, Pascal and Barthelemy, Johan. 2021. "A process-driven and need-oriented framework for review of technological contributions to disaster management", *Heliyon* 7 e08405

Joo, Soo-hyun, Ogawa, Yoshiki and Sekimoto, Yoshihide. 2019. "Decision-making system for road-recovery considering 1452 human mobility by applying deep Q-network". In: *The 2019 IEEE International Confer1453 ence on Big Data, IEEE.*

Kankanamge, Nayomi, Yigitcanlar, Tan and Goonetilleke, Ashantha. 2021. "Public perceptions on artificial intelligence driven disaster management: Evidence from Sydney, Melbourne and Brisbane". *Telematics and Informatics*, *65*, 101729.

Konar, Amit. 2018. *Artificial intelligence and soft computing: behavioral and cognitive modeling of the human brain*. CRC press.

Lattanzi, David and Miller, R. Gregory. 2015. "3D scene reconstruction for robotic bridge inspection". *Journal of Infrastructure Systems* 21:04014041.

Mijić, Jelena. 2023. Jaz u odgovornosti u informatičkoj eri. *Изазови дигиталне трансформације: између свакодневице и трансхуманизма: зборник радова са научног скупа» Друштво и политика», Бања Лука, 2023*, *4*(4), 25-38.

Munawar, Hafiz Suliman, Mojtahedi, Mohammad, Hammad, W. Ahmed, Kouzani, Abbas, and Mahmud, M. Parvez. 2022. "Disruptive technologies as a solution for disaster risk management: A review". *Science of the total environment*, *806*, 151351.

Pwavodi, Joshua, Ibrahim, Abdullahi Umar, Pwavodi, Pwadubashiyi Coston, Fadi, Al-Turjman and Mohand-Said, Ali. 2024. "The role of artificial intelligence and IoT in prediction of earthquakes". *Artificial Intelligence in Geosciences*, 100075.

Qian, Yuzhou, Siau, L. Keng L, & Nah, F. Fiona. 2024. Ž2Societal impacts of artificial intelligence: Ethical, legal, and governance issues". *Societal Impacts*, *3*, 100040.

Riggio, Ana, Santulin, Marco. 2015. "Earthquake forecasting: a review of radon as seismic precursor". *Bollettino Di Geofisica Teorica e Applicata* 56 (2), 95–114.

Rizi, Mohammad Hosein Panahi Rizi and Seno, Seyed Amin Hosseini. 2022. "A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city". *Internet of Things*, *20*, 100584.

Roca, Jaime Bonnin, Vaishnav, Parth, Morgan, M. Granger, Mendonça, Joana and Fuchs, Erica. 2017. "When risks cannot be seen: Regulating uncertainty in emerging technologies". *Research Policy*, *46*(7), 1215-1233.

Schintler, A. Laurie and McNeely, L. Connie. 2022. "Artificial intelligence, institutions, and resilience: Prospects and provocations for cities". *Journal of Urban Management*, *11*(2), 256-268.

Schneider, E. Frank and Wildermuth, Dennis. 2017. "Using robots for firefighters and first responders: 2129 scenario specificaton and exermplary system description". *In: Proceedings of the 18th 2130 Carpathian Control Conference*, pp 216–221.

Sharifi, A. and Allam, Zaheer. 2023. *Contributions of smart technologies to disaster resilience. Book Chapter, Urban Climate Adaptation and Mitigation*, Elsevier.

Keng, Siau. 2003. "Interorganizational systems and competitive advantages–lessons from history". *J. Comput. Inf. Syst.* 44 (1)33–39.

Sun, Wenjuan, Bocchini, Paolo and Davison, D. Brian. 2020. "Applications of artificial intelligence for disaster management". *Natural Hazards*, *103*(3), 2631-2689.

Takahashi Bruno, Edson C. Tandoc and Carmichael Christine. 2015. "Communicating on Twitter during a disaster: 2254 An analysis of tweets during Typhoon Haiyan in the Philippines". *Computers in Human Behavior* 50:392–398.

Tao, Xin. 2023. *Exploring Trustworthiness Issues About Disaster-Related Information Generated by Artificial Intelligence* (Doctoral dissertation, University of South Carolina).

UN DESA, 2018. Accessed 3rd April 2024. https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html

Xu, Chong. 2023. "An introduction to "application of novel high-tech methods to geological hazard research". *Natural Hazards Research* 3 (2), 353–357

Xu, Chong and Xue, Zhiwen. 2023. "Applications and challenges of artificial intelligence in the field of disaster prevention, reduction, and relief". *Natural Hazards Research*.

Xue, Zhiwen, Xu, Chong and Xu, Xiwei. 2023. "Application of ChatGPT in natural disaster prevention and reduction". *Natural Hazards Research*, *3*(3), 556-562.

Yigitcanlar, Tan, Corchado, M. Juan, Mehmood, Rashid, Li, Rita Yi Man, Mossberger, Karen and Desouza, Kevin. 2021. "Responsible urban innovation with local government artificial intelligence (AI): A conceptual framework and research agenda". *Journal of Open Innovation: Technology, Market, and Complexity*, *7*(1), 71.

Zahra, Kiran, Imran, Muhammad, Ostermann, O. Frank. 2018. "Understanding eyewitness reports on twitter during disasters". In: *15th International Conference on Information Systems for Crisis Response and Management ISCRAM*, Rochester (USA), 21 May 2018 - 23 May 2018. ISCRAM, 687-695.

THE USE OF ARTIFICIAL INTELLIGENCE IN BUILDING RESILIENCE OF URBAN COMMUNITIES TO DISASTERS

Abstract: Natural disasters in contemporary cities generate far-reaching consequences in the human, economic, ecological and infrastructural dimensions of urban space. The use of artificial intelligence (AI) in the segment of disaster management has the potential to improve the process of building resilience in each cascade component, starting from the anticipation of potential threats and proactive action, reactive action in the form of absorption of unwanted stressors, adaptation to changed circumstances and the process of system recovery. Optimization and automation, two fundamental processes at the core of artificial intelligence, make data processing faster and more efficient. In the context of disaster management, the aforementioned processes make a significant contribution to improving the functioning of the early warning system and raising the level of preparedness of citizens through the analysis of indicators of events with destructive potential. The use of artificial intelligence in disaster response is of particular importance due to the ability to generate maps of events and resulting damage, thereby improving situational awareness and facilitating the work of rescue teams in the field. The restorative capacity of urban communities faced with disasters is reflected in the synergistic effect of institutional and non-institutional actors. By applying artificial intelligence, the temporal dimension of community recovery is improved in the form of a reduction in the number of time units required for the restorative phase, as well as through the development of recovery plans, monitoring of regenerative processes, material damage and funds intended for reconstruction. In contrast to the use of modern technological achievements, there is a potential of compromising resilience of urban communities through the use of artificial intelligence. Prioritizing AI-enhanced efficiency can diminish the attributes of redundancy and diversity that a system facing a stressor manifests in a cycle of resilience without high-tech influences. Ethical and legal aspects of the use of artificial intelligence require special attention from the scientific and professional public due to possible abuses and negligent application of technological innovations in the process of disaster management.

Keywords: artificial intelligence, resilience, urban communities, natural disasters, ethical aspects.

2

ОБРАЗОВАЊЕ, ВИРТУЕЛНА РЕАЛНОСТ И СИМУЛАЦИЈЕ

СПЕЦИФИЧНОСТИ ПРИМЕНЕ XVR СОФТВЕРА: ВИРТУЕЛНА РЕАЛНОСТ КАО ОКРУЖЕЊЕ ЗА ОБУКУ И УНАПРЕЂЕЊЕ ПОСЛОВНИХ ПРОЦЕСА НА ФАКУЛТЕТУ БЕЗБЕДНОСТИ[1]

Владимир Буквић[2], Душан Кесић[3], Петар Станојевић[4]

Апстракт: Примена виртуелне реалности у области образовања и едукације може се подвести под симулацију и експлорацију животних ситуација које не би могле бити другачије реализоване, односно у случајевима када би се нешто могло реализовати али би носило са собом изразито велики ризик по безбедност учесника. Под образовањем и едукацијом у смислу виртуелне реалности посебно се истиче могућност тренинга и обуке појединаца у различитим областима. Симулације омогућавају ученицима да искусе одређену ситуацију на безбедан начин и тиме стекну нове вештине у професијама које укључују ризике, нарочито у случајевима када присутни ризици представљају препреку за достизање жељених циљева обуке. Последњих година симулациони модели и виртуелна реалност бивају инкорпрорани у стратегију образовања и обуке као елемент који комплементира стандардни програм. У овом раду акценат је стављен на примену виртуелне реалности и симулација у процесу обуке припадника ватрогасно-спасилачких јединица. Како се чланови ватрогасно-спасилачке јединице у свакодневном раду сусрећу са веома ризичним и по живот опасним ситуацијама, њихова обука се не може реализовати креирањем таквих услова за потребе тренинга. Са друге стране, виртеулна технологија омогућава да припадници ватрогасно-спасилачке јединице стекну непосредно искуство у односу на кризне ситуације, без последица по њихов живот и здравље. У оквиру припрема симулација виртуелне реалности, специфичност примене ове области на Факултету безбедности се огледа у пројектовању оптималног одговора на акцидентну ситуацију. Оптимални одговор се дефинише усвајањем и алгоритмизацијом знања и искуства експерата из области кризне ситуације и њихова имплементација у оквиру XVR окружења.

Кључне речи: виртуелна реалност, XVR, симулациона вежба, оптимизација, кризна ситуација.

Увод

Током последње деценије дошло је до популаризације употребе компјутерских софтверских и хардверских технологија у различитим индустријским областима

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

[2] Факултет безбедности Универзитет у Београду, vladimir.bukvic@mod.gov.rs

[3] Факултет безбедности Универзитет у Београду, dusan.kesic@fb.bg.ac.rs

[4] Факултет безбедности Универзитет у Београду, petstano45@gmail.com

пословања за потребе тренинга запослених и приправника у областима производње, грађевине и војске. У поређењу са традиционалним приступом образовању и методама тренинга, примена тренинга заснованог на виртуелној реалности има своје предности у уштеди новца, унапређењу безбедности и ефективности, смањењу времена потребног за реализацију тренинга итд. (Shen 2019). Симулације омогућавају ученицима да искусе одређену ситуацију на безбедан начин и тиме стекну нове вештине у професијама које укључују ризике, нарочито у случајевима када присутни ризици представљају препреку за достизање жељених циљева обуке. Симулациони сценарији се користе као једна од стратегија образовања и обуке која комплементира стандардни програм. Њихова употреба показала се ефективном у достизању образовних циљева (Blazauskas & Gudoniene 2020). Виртуелна реалност нуди широк спектар могућности у примени на област образовања. Примена виртуелне реалности јесте ново средство које омогућава ефективније и непосредније ступање у контакт са ученицима. Са једне стране, виртуелна реалности подстиче, мотивише и ситимулише ученике да се непосредно укључе у процес учења, док са друге стране омогућава избегавање низа ризика скопчаних са практичним процедурама едукације (Getso 2017). Дакле, данас се систем образовања, а потом и бројни едукативни програми, не могу замислити без примене нових технолошких достигнућа, која могу бити искоришћена у сврху унапређења искуства, знања или способности појединаца.

У вези са тим, акценат у овом раду стављен је на примену виртуелне реалности и симулација у процесу обуке припадника ватрогасно-спасилачких јединица. Како се чланови ватрогасно-спасилачке јединице у свакодневном раду сусрећу са веома ризичним и по живот опасним ситуацијама, њихова обука се не може реализовати креирањем таквих услова за потребе тренинга. Са друге стране, виртеулна технологија омогућава да припадници ватрогасно-спасилачке јединице искусе из прве руке ризичне ситуације, без последица по њихов живот и здравље. Уједно, модерни програми обуке и тренинга припадника ватрогасно-спасилачких јединица у свету еволуирају ка примени симулационих модела уз помоћ виртуелне реалности, како би се постигли бољи резултати уз смањење мање трошкова. Следствено томе, у раду је приказана употреба софтвера XVR On-Scene на Факултету безбедности у сврху развој симулационог модела намењеног обуци и тренингу чланова ватрогасно спасилачке јединице. Конкретно, приказан је процес осмишљавања сценарија акцидентне ситуације, који је обухватио специфичности кризног догађаја, улоге и задатке чланова ватрогасно-спасилачке јединице, као и сам процес поступања и доношења одлука у складу са особеностима конкретног догађаја или ситуације.

Виртуелна реалност: образовање, обука и тренинг

Развој и примена симулација и виртуелне реалности своју претечу налази у области комерцијалне авио индустрије, свемирских програма и различитих намена у оквиру војске. На пример, симулатор за летење постали су неизоставни део функционисања комерцијалних авио компанија током 60-их година 20. века. Више се није сматрало практичним да се обука реализује у правим авионима, како због безбедносних фактора тако и због унапређења ефективности тренинга пилота. Током 70-их развој технологије рачунара омогућио је њихову примену у области симулације летења (Page 2000). Могућности виртуелне реалности у примени на развој вештина и компетенција за специфичне потребе имају широку употребу, нарочито у случајевима када је реч о опасним ситуацијама

(Daniela & Aierken 2020). Дигиталне технологије, а нарочито технологија виртуелне реалности може плодотворно бити употребљена у сврху образовања, имплементацијом активног учења и непосредног искуства кроз руковање овом технологијом. Основна предност учења посредством виртуелне реалности огледа се у томе што омогућава студентима да се укључе у виртуелно окружење, сценарије и симулације на начин који је истовремено и инклузиван и едукативан. Поред тога, једна од кључних предност симулација у виртуелној реалности тиче се безбедног окружења за тестирање експеримената који би били веома опасни у реалности (Rossoni 2024, 259).

Виртуелна реалност је технологија која омогућава имерзивности у вештачки свет, који може бити у потпуности имагинаран или репродукција стварног света. Искуство у виртуелном свету може бити визуелно, звучно а некада и додирно. Имерзија се остварује коришћењем опреме или сета за главу који користи бинокуларни стереоскопски дисплеј, по један за свако око корисника. Популарност виртуелне реалности везује се за 80 године 20. века. Међутим, она није остварила значајнији успех током наведеног периода јер технологије везане за виртуелну реалности нису биле познате широј јавности тог времена. Ипак, тек од 2012. године виртуелна реалност постаје доступнија и интересантнија широј публици, пре свега захваљујући технолошким и комперцијалним искорацима који су обезбедили довољно комфора у употреби и задовољење интереса свих заинтересованих страна. Посматрано од 2014. године виртуелна реалност постепено налази ширу примену, са појавом опреме и сетова за главу који су били ефективнији и ценовно приступачнији (Noureddine 2019, 236).

Технологија виртуелне реалности пружа бројне могућности које сведоче о изванредним технолошким достигнућима. Њен напредак одвија се релативно брзо, креирајући нове могућности које се могу плодотворно применити за стварање нових пракси и искустава у области образовања и едукације. Ипак, треба имати у виду да технологија, а тиме и технологија виртуелне реалности, представља само средство које не може само од себе реализовати активности учења или едукације појединаца. Стога је потребно да ова технологија буде ефективно употребљена како би могла бити од користи за образовни процес (Chen 2009). Предности виртуелне реалности огледају се превасходно у повећању инволвираности студената у наставни процес; обезбеђивању активног, конструктивистичког учења; повећању аутентичног искуства учења; омогућавању студентима да испоље креативност; пружању оквира за визуализацију апстрактних концепата. Једна од важних карактеристика виртуелне реалности тиче се могућности конструктивистичког учења, односно омогућавња студентима да изграде своје знање на основу релевантног искуства. У овим случајевима искуства, студенти се сусрећу са аутентичним проблемима, истражујући решења и могућности заједничког рада са другима (Hu-Au & Lee 2017, 216-219).

Свеукупно, примена виртуелне реалности у области образовања и едукације може се подвести под симулацију и експлорацију животних ситуација које не би могле бити другачије реализоване, односно у случајевима када би се нешто могло реализовати али би носило са собом изразито велики ризик по безбедност учесника. Под образовањем и едукацијом у смислу виртуелне реалности посебно се истиче могућност тренинга и обуке појединаца у различитим областима. Употреба виртуелног окружења као средине за стицање нових вештина била је једна од првих намена ове технологије. Пример тога јесте употреба симулатора за летење који су коришћених за обуку пилота. Дакле, у овом случају акценат је на трансферу вештина а не искључиво знања (Кеванах (Sam Kavanagh) и сарадници истичу да је најчешћи случај примене симулација и виртуелне реалности

у области образовања и едукације, чак 58% идентификованих симулационих програма намењено је тренинга особља (Kavanagh et al. 2017, 92). Како у свом истраживању учења уз помоћ виртуелне реалности наводе Буха и сарадници (2011, 53), Блумова (Benjamin Bloom) таксономија образовних циљева обухвата и три нивоа исхода учења:

1. когнитивни ниво – разумевање, примена, знање, анализа, синтеза, евалуација.
2. афективни ниво – ставови, интереси, вредности, схватања, намере,
3. психомоторни ниво – вештине, кретање, писање, руковање.

Оно што је специфично за ову Блумову таксономију јесте и постојање низа поднивоа учења унутар сваког од наведених нивоа учења, који теку од базичнијих, површинских нивоа ка комплекснијим, дубљим нивоима учења (Hogue 2017, 45). Когнитивни ниво учења усмерен је на стицање вештина усресређених предоминатно на менталне процесе. Унутар овог домена учења пажња је усмерена на хијерархију вештина које укључују обраду информација, изградњу размевања, примену знања, решавање проблема и спровођење истраживања. Афективни домен учења подразумева да учење није искључиво когнитивни, ментални процес. Напротив, овај домен имплицира да је могуће је учење осећања, емоција и ставова. Најзад, психомоторни ниво учења обухвата одређене физички кодиране информације, односно природне аутономне рефлексе и реакције. Дакле, психомоторни ниво учења усмерен је на коришћење моторичких способности и њихову координацију(Hogue 2017, 46-50). Употреба виртуелне реалности омогућава синтезу наведених нивоа учења, што додатно аргументује њену примену у процесу образовања и едукације. Како истиче Чен (Chew Jen Chen), виртуелна реалност пружа бројне могућности у погледу њене примене у области образовања и едукације. Специфичне могућности виртуелне реланости огледају се у: могућности појединаца да визуализују и интерреагују са тродимензионалном виртуелном представом; могућности да искусе виртуелно окружење у реалном времену; могућности визуализацију апстрактних концепата; артикулацији разумевања феномена кроз конструисање или манипулисање виртуелним окружењем; изградња неограниченог броја перспектива у односу на виртуелно окружење; пружање могућности појединцима да остваре интеракцију у колаборативном виртуелном окружењу; као и да учествују у догађајима који су недоступни или неизводљиви услед временске и просторне дистанце, трошкова или безбедносних фактора (Chen 2009, 71).

Предности виритуелне реалности чине се изузетно погодним за случајеве обуке и тренина припадника хитних служби (тј. војске, полиције, ватрогасаца, медицинског особља итд.) управо због веома сложених и ризичних задатака које они обављају у свакодневном поступању на радном месту. Симулације догађаја или ситуација из делокруга њиховог рада омогућавају стицање искуства и знања у безбедном окружењу. Нарочито се истиче предност стицања знања и искуства кроз активно учење, непосредним искуством у решавању проблема и доношењу одлука на бази какрактеристика кризног догађаја обухваћеног кроз симулациони модел. Искуство кроз виртуелну реалност подразумева како визулене и звучне, тако и додирне аспекте, што омогућава аутентично искуство и развој знања, вештина и ставова потребних за успешно извршавање задатака.

XVR - специфичности примене на Факултету безбедности

Софтвер XVR On Scene представља моћно средство за учење и обуку припадника хитних служби (тј. ватрогасаца, полицајаца, медицинског особља итд.). Флексибилност XVR платформе омогућава креирање замишљеног сценарија, који ће усклађен са осо-

беностима конкретне ситуација којом се жели управљати. Услед флексибилности платформе присутан је велики број дидактичких опција (тј. учење, тренинг и процене), као и скалабилних опција (тј. самовођени или тренинг са више учесника). XVR платформа обезбеђује корисницима есенцијални сценарио тренинга. Учесници тренинга укључени су у безбедну ситуацију која је у потпуности контролисана, која се веома лако може поновити и анализирати, што омогућава неопходно самопоуздање у суочавању са кризним ситуацијама. Уједно, намена овог програма тиче се унапређења компетенција и експертизе хитних служби у управљању кризним ситуацијама (XVR Simulation 2024). Примена овог софтвера налази широку употребу, док су приступи изради симулационих модела у овом софтверу углавном засновани на репродукцији процедура у виртуелно окружење. Поред тога, присутни су и покушаји да се одговарајући концепти и варијабле искористе као окосница за израду симулационог модела за евалуацију нивоа спремности или специфичних способности. На пример, ситуационо резоновање идентификовано је као кључни фактор за успешно управљање кризним ситуацијама у зависности од контекста и персоналних фактора. Генерално, могуће је разликовати три категорије ситуационог резновања. Прва категорија обухвата перцепцију командира ватрогасно-спасилачких јединица, односно њихову способност да прикупе потребне информације постављајући питања правим особама у правом тренутку. Друга категорија способност разумевања командира кроз прикупљање информација и њихово обједињавање у сврху добијања кохерентне оперативне слике одређене ситуације. На крају, трећу категорију чини предикција, односно способност да се прогнозира шта ће уследити у кризној ситуацији која се динамички развија када се употребе ресурси како би се спречило ширење хазарда и смањили ризици. Разумевање и предикција су кључни за ефективну употребу ресурса у ограничном временском интервалу (Polikarpus et al. 2023).

У Естонији су за потребе тренинга одабрали софтвер XVR On-Scene за тестирање три нивоа ситуационог резоновања командира. Провера знања командира ватрогасно-спасилачких јединица у Естонији је до 2016. године била заснована на тесту са питањима која имају понуђене одговоре. Временом се показало да ова врста тестирања није нарочито интересантна нити мотивишућа за командире. Стога је развијен нови програм тренинга који је намењен вежбању и мерењу динамичког одлучивања, што укључује и ситуационо резоновање. Нови програм заснован је на три приниципа, први је подразумевао да сваки командир ватрогасно-спасилачке јединице треба да има прилику да командује акцидентом у виртуелној симулацији. Предност употребе виртуелне симулације састоји се у могућности креирања временског притиска у веома ризичним ситуацијама за командире, обезбеђујући тиме искуство учења у које су непосредно инволвирани. Други приницип овог програма састојао се у томе да се процесу доношења одлука сваког командира треба бити евалуирано на основу његовог командовања у виртуално симулираној акцидентној ситуацији. Како би наведено било имплементирано у тренинг програм састављен је програм Ефективног командовања (Effective Command) као средство процене њиховог поступања. И на крају, трећи приницип обухватио је постојање е-платформе за све командире у Естонији, како би се објединили теорија, документација и компјутерски засновано тестирање знања (Polikarpus 2020). Провера знања и способности управљања кризним ситуацијама за командире почива на уверењу да они морају поседовати добро ситуационо резоновање. Доношење одлука командира у кризним ситуацијама као што су пожари, саобраћајне незгоде или цурење штетних хемикалија, мора бити ефективно и правовремено како би адекватно проценили хазарде и ризике за становништво и животну средину. Међутим, мерење

њиховог ситуационог резоновања није могуће остварити у реалном времену када они треба да реагују у веома ризичним ситуацијама као што су кризне ситуације. Поред свих тешкоћа које карактеришу тренинг и процену рада командира ватрогасно-спасилачких јединица, провера ситуационог резоновања је веома тежак задатак за лица задужена за спровођење обуке и провере знања и способности. Решење за тестирање ситуационог резоновања нуде виртуелне симуалције, које се могу дефинисати као сценарио презентован ученику употребом софтвера и харедвера како би се креирало виртуелно окружење за кризне ситуације окарактерисане динамичким променама. Услед тога неопходно је адекватно кризно одлучивање, односно динамичко одлучивање, као доношење серије независних одлука у стално променљивом окружењу услед предузети одлука или аутономних промена у окружењу. Стога, тренинг и евалуација командира ватрогасно-спасилачких јединица засновани на виртуелним симуалцијама представљају услов тренинга динамичког одлучивања у безбедном окружењу без штетних последица (Polikarpus et al. 2023).

Изграда симулације подразумевала је сарадњу више субјеката кроз неколико фаза. Као прво, неопходно је написати сценарио ванредне симулације, уз спецификацију врсте акцидента, наратива догађаја и специфичних изазова који захтевају доношење одлука. Други корак обухвата додатни развој сценарија догађаја и изградњу симулације у XVR софтверу. Трећи корак обухвата тестирање симулације од стране проценитеља у складу са критеријумима Ефективне команде. Наведено подразумева да виртуелну симулацију ванредне ситуације тестира експерт. Четврти корак тиче се финализације сценарија кризне ситуације у складу са сугестијама из фазе тестирања од стране експерта. На крају, проценитељи се обучавају како да презентују акцидент у форми виртуелне симулације на истоветан начин свим командирима ватрогасно-спасилачких јединица који ће проћи обуку (Polikarpus et al. 2023, 27). Свеукупно, процес израде симулационог модела захтева неколико комплексних корака, од осмишљавања ситуације или догађаја који ће се симулирати, до развоја сценарија и осмишљавања различитих елемената ситуације који захтева одгогварајуће резновање, доношење одлука и правилно поступање командира.

Аналогно наведеним настојањима, да се употребом виртуелне реалности развију симулације које ће омогућити тренинг и обуку припадника ватрогасно-спасилачких јединица, на Факултету безбедности у оквиру Националног симулационог центра за безбедносне ризике реализована је израда једне такве симулације. У оквиру припрема симулација виртуелне реалности, специфичност примене ове области на Факултету безбедности се огледа у пројектовању оптималног одговора на кризну ситуацију. Оптимални одговор се дефинише усвајањем и алгоритмизацијом знања и искуства експерата из области кризне ситуације и њихова имплементација у оквиру XVR окружења. У конкретном случају, сарадња са припадницима Сектора за ванредне ситуације и Београдске ватрогасне бригаде омогућила је потребне елементе за израду сценарија кризне ситуације. Односно, на основу искуства у досадашњем раду одабран је случај поступања ватрогасно-спасилачке јединице који је био веома комплексан и изазован, и који је захтевао доношење низа исправних одлука које су определиле крајњи исход интервенције у смислу ефективног сузбијање пожара и минимализовања последица. Израда симулационе вежбе подразумева и одговарајуће предулове када је реч о условима виртуелне реалности. У оквиру ове припреме за вежбу помоћу виртуелне реалност мора бити унапред дефинисан циљ вежбе (обучавање, евалуација - оцена), ниво и састав који је обухваћен сценаријем, односно организацијско-формацијска структура вежбајућег састава са личном и материјалном формацијом. Морају бити дефинисани учесници,

од којих су неки по природи ствари – аватари – наиме иза одређених улога - учесника постоји човек, а други учесници имају унапред дефинисано програмирано понашање. Приликом развоја симулационог модела, кроз сарадњу са припадницима Сектора за ванредне ситуације, дефинисани су приоритети у погледу циљева симулационе вежбе – обука руководилаца, командира чете и шефа смене (Слика 1. Демонстрација првог симулационог модела). Друга фаза развоја симулационог модела обухватила обуку чланова навалног и водног тима.

Слика 1: Демонстрација првог симулационог модела

Наиме, кризна ситуација у виртуелној реалности се дефинише сценаријем и одговарајућим скриптовима – по улогама, просторно и временски. Улоге - учесници могу бити аутоматизованог – програмираног понашања или представљају аватаре – стварне учеснике, стварне људе који активно учествује у симулационој вежби. У контексту израде одабраног симулационог модела главне улоге додељене су командиру чете и шефу смене. Када је реч о програмираном понашању, на пример са XVR објектом Task – задатак детаљно се описује физичке промене стања, низ активности – радње, са привременим извршиоцем/извршиоцима (yellow dummy*). Ко ће извршити овај низ промене стања, радњи и активности одређује се* накнадно. У току вежбе овај низ радњи могу се додељивати различитим извршиоцима у складу са одлукама играјућих учесника (представљених аватарима) – у оквиру дефинисаних улога. С друге стране Event – догађај је такав објекат којим се предефинише логика понашања, низ повезаних активности једног или више аутоматизованих учесника. У циљу потпуног дочаравања стварности постоје и други типови објеката као што су Path, Locations и Triggers.

Дефиниција кризне – инциденте ситуација се утврђује дефинисањем различитих супозиција, поступним развојем кризне ситуације. Овај опис развоја инцидентне, кризне ситуације је садржан у сценарију и скрипту сценарија. У току припреме за симула-

циону вежбу на Факултету безбедности се обавезно анализира оптимални одговор на кризне ситуације. Имајући у виду услове виртуелног окружења кризна ситуација се анализира кроз елементе лексичке и семантичке анализе. У оквиру задатих елемената (особине инцидента, укључени учесници, нормативни документи и дефинисане процедуре) оптимизује се очекивано понашање у разрешавању захтева кризне ситуације. Ово је посебно важно када се увежбавају руководиоци. Тада је могуће унапред припремити извршавања вербалних наредби играјућих руководиоца као учеснике вежбе који одлучују о начину извршења интервенције. У овој фази посебно је важно укључивање експерата са знањем и искуством адекватног одговора на инцидентну ситуацију која се проиграва. Оптимизовано понашање непосредних извршиоца се аутоматизује кроз расположиве концепте XVR као што су улоге (Role) и процедуре дефинисане било као Task – задатак, Event – догађај или Triggers – окидач или други расположиви објекти у XVR окружењу. Оптимизација одговора се може проверити адекватним другим софтверским алатима којима располаже Факултет безбедности, било потпуно математичким, статистичким или другим аналитичким симулационим алатима као што је AnyLogic. Тиме се ствара фонд знања о оптималним реакцијама на инцидентне ситуације. Ово је посебно важно када је потребно анализирати оптималне одговоре у условима нових изазова и претњи, односно нових или сложених кризних ситуација. И коначно, самим играјућим учесницима кроз пост-анализу вежбе омогућава боље сагледавање поступака у одређеним кризним ситуацијама.

Закључак

Током последње деценије, захваљујући развоју технологије, виртуелна технологија наишла је на ширу примену. Предности виртуелне технологије у образовању и тренингу особља огледају се у уштеди времена и новца, као и безбедном окружењу за остваривање непосредног искуства. Штавише, употреба симулационих модела омогућава репродукцију стварних догађаја или ситуација које омогућавају инклузиван и едукативан оквир за активно учење и стицање потребних знања и вештина у безбедном окружењу. Управо последње наведено указује на предност употребе виртуелне технологије и симулација у тренингу припадника полиције, војске, ватрогасно-спасилачких јединица и медицинског особља. Наиме, обављање ових послова скопчано је са високим ризиком по безбедност, што онемогућава спровођење тренинга у реалним условима. У таквој ситуацији могућности виртуелне реалности долазе до свог пуног изражаја, као допуна традиционалним програмима обуке. Наиме, развој симулационих модела који репродукују одређене стварне догађаје или ситуације у раду омогућава активно учење и стицање непосредног искуства, као и потребних знања и вештина лица укључених у тренинг.

Примена симулација и виртуелне реалности на Факултету безбедности заснивају пројектовању оптималног одговора на кризну ситуацију. Дефинисање оптималног оддговора подразумева претходну анализу одабране кризне ситуације у сарадњи са експертима, како би се детаљно разрадили сви аспекти дате ситуације који захтевају одговарајуће одлучивање руководећих нивоа – командира четее и шефа смене. Након опсежне анализе кризне ситуације следи иднетификовање оптималних одговора у односу на изазове које са собом доноси кризна ситуација. Након тога следи следи алгоритмизација знања и искуства експерата у XVR окружење, чиме се креира сценарио кризне ситуације са јасно постављеним премисама у погледу ефективног поступања

приликом руковођења. Према томе, специфичност се огледа не само у комбинацији примене различитих алата, већ и ослонца на специфична знања експерата из области кризне ситуације која се симулира у виртуелној реалности. Основни искорак је управо у еклектицизму, споју математичких и аналитичких модела, позивања на искуство и знања експерата, и на крају, имплементација наведеног кроз сценарио или скрипту сценарију виртуелне реалности као тренутно најбољег система за пренос знања и искуства на појединце укључене у симулацију, слушаоце и студенте.

Библиографија

Blazauskas, Tomas, and Daina Gudoniene. 2020. "Virtual reality and augmented reality in educational programs" In: Linda, Daniela. *New perspectives on virtual and augmented reality*, pp. 82-94. London: Routledge.

Buha, Vesna, Radmila Janičić, Vinka Filipović, and Mirjana Gligorijević. "Virtuelna realnost u obrazovanju na daljinu i marketinškim komunikacijama." *Management-časopis za teoriju i praksu menadžmenta* 16, no. 60 (2011): 51-59.

Chen, Chwen Jen. 2009. "Theoretical bases for using virtual reality in education". *Themes in science and technology education* 2 : 71-90.

Daniela, Linda, and Yipaer Aierken. 2020. "The educational perspective on virtual reality experiences of cultural heritage". In: Linda, Daniela. *New perspectives on virtual and augmented reality*, pp. 82-94. London: Routledge.

Elmqaddem, Noureddine. 2019. "Augmented reality and virtual reality in education. Myth or reality?". *International journal of emerging technologies in learning* 14, no. 3.

Getso, Muhammad Mannir Ahmad, and Kinn Abass Bakon. 2017. "Virtual reality in education: the future of learning". *International Journal of Information System and Engineering* 5, no. 2: 30-39.

Hoque, D. M. 2016. "Three Domains of Learning: Cognitive." *Affective and Psychomotor* 2.

Hu-Au, Elliot, and Joey J. Lee. "Virtual reality in education: a tool for learning in the experience age". *International Journal of Innovation in Education* 4, no. 4 (2017): 215-226.

Kavanagh, S., Luxton-Reilly, A., Wuensche, B., & Plimmer, B. 2017. "A systematic review of virtual reality in education". *Themes in science and technology education*, *10*(2), 85-119.

Polikarpus, Stella, Ley, Tobias, and Katrin Poom-Valickis. 2020. "Developing the situational awareness of incident commanders: evaluating a training programme using a virtual simulation". Proceedings Estonian Academy of Security Sciences, 19: 195-226.

Page, Ray L. 2000. "Brief history of flight simulation". *SimTecT 2000 proceedings*: 11-17.

Polikarpus, Stella, Edna Milena Sarmiento-Márquez, and Tobias Ley.2023 "Creation and Use of Virtual Simulations for Measuring Situation Awareness of Incident Commanders." In: Gjøsæter, Terje, Jaziar Radianti, and Yuko Murayama. *International Conference on Information Technology in Disaster Risk Reduction*, pp. 23-38. Cham: Springer Nature Switzerland.

Rossoni, Marco, Elena Spadoni, Marina Carulli, Chiara Barone, Giorgio Colombo, and Monica Bordegoni.2024. "Virtual reality in education to enable active learning and hands-on experience". *Computer-Aided Design and Applications* 21, no. 2: 258-269.

Shen, Haosheng, Jundong Zhang, Baicheng Yang, and Baozhu Jia. 2019. "Development of an educational virtual reality training system for marine engineers". *Computer Applications in Engineering Education* 27, no. 3: 580-602.

XVR Simulation. 2024. "Why XVR". Acessed on 22 June 2024. https://www.xvrsim.com/en/

SPECIFICS OF XVR SOFTWARE APPLICATION: VIRTUAL REALITY AS A TRAINING ENVIRONMENT FOR ENHANCING BUSINESS PROCESSES AT THE FACULTY OF SECURITY STUDIES

Abstract: The application of virtual reality in education and training can be classified under the simulation and exploration of life situations that could not otherwise be realized, or in cases where something could be realized but would involve significant safety risks for participants. In the context of virtual reality, education and training particularly emphasize the potential for training individuals in various fields. Simulations allow trainees to experience a specific situation in a safe manner, thus acquiring new skills in professions that involve risks, especially in cases where present dangers are an obstacle to achieving the desired training goals. In recent years, simulation models and virtual reality have been incorporated into education and training strategies as a complementary element to standard programs. This paper focuses on the application of virtual reality and simulations in the training of members of fire and rescue units. As these units regularly face highly risky and life-threatening situations in their daily work, their training cannot be conducted by creating such conditions for practice. On the other hand, virtual technology enables fire and rescue unit members to gain direct experience with crisis situations without endangering their lives and health. Within the preparation of virtual reality simulations, the specificity of the application of this field at the Faculty of Security Studies lies in the design of an optimal response to an emergency situation.

Key words: virtual reality, XVR, simulation exercise, optimization, crisis situation

ДИГИТАЛНИ АЛАТИ И СИМУЛАЦИЈЕ У ОБЛАСТИ ЕНВИРОНМЕНТАЛНЕ ФОРЕНЗИКЕ[1]

Ненад Путник[2]

Апстракт: Деградација животне средине, климатске промене, али и илегална трговина биљним и животињским врстама, као облик транснационалног организованог криминала, остављају тешко поправљиве последице по животно окружење, природу, али и здравље људи. Процењује се да су поједини процеси у природи, као последица девастације животне средине и еколошког криминала постали нереверзибилни. Проблематика еколошког криминала и одрживог развоја високо је позиционирана не само на глобалној политичкој сцени, већ и у агендама и активностима држава и компанија на националном нивоу. Развој технологије, дигиталних алата и симулатора олакшао је истраге у области енвиронменталне форензике, али и предвиђању последица евентуалних еколошких акцидената. Агрегација географски распоређених техничких ресурса, омогућила је креирање симулација и перформанси високог квалитета и разноврсности. Уз технике теренске енвиронменталне форензике, симулациони модели дали су значајан допринос откривању и процесуирању починилаца дела еколошког криминала, али и предвиђања будућих промена у природним токовима. У овом раду биће описане поједине технике енвиронменталне форензике, као и значај дигиталних алата у симулацији догађаја, њиховом објашњењу и предвиђању.

Кључне речи: еколошки криминал, форензика, сензори, симулације, модели.

Увод

Питања заштите животне средине, очувања биодиверзитета и природних богатстава, добила су заслужену пажњу светске јавности, што због нивоа угрожености и девастације, што због значаја који природа има по опстанак и функционисање друштва. Свест јавности, али и доносилаца одлука подигнута је на много виши ниво, последицама климатских промена, нарушавања природних токова и постепеним, али сигурним нестанком делова флоре и фауне. Многе европске земље међу приоритете своје политике поставиле су питање заштите животне средине, а здраво природно окружење промовисано је од стране Уједињених нација (УН) као једно од основних људских права. Поред свакодневног немара људи према животном окружењу и постојања великих индустријских извора загађења, дела еколошког криминала су она која све више угрожавају животну средину. Према УН Програму за Животну средину (United Nations Environment program – UNEP), „еколошки криминал је нарастајућа глобална претња" (UNEP, 2018). Притом, посебну опасност представља транснационални организовани еколошки криминал.

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

[2] Факултет безбедности, Универзитет у Београду, nputnik@fb.bg.ac.rs

Постоји велики број фактора који утичу на развој овог облика транснационалног криминала и формирања црног тржишта производа везаних за природу. Неки од узрока леже у потражњи, у различитим земљама, за ретким производима за које замене нису доступне или легално прихваћене, недостатку свести и бриге о животној средини, и недовољно јакој правној и казненој регулативи. Укупна вредност главних облика међународног еколошког криминала, нелегалне сече, риболова, нелегалне трговине дивљим животињама и супстанцама које оштећују озонски омотач, као и нелегалног одлагања опасног отпада мери се износом од 20 до 40 милијарди долара годишње, што је око 5-10% од величине износа светске трговине дрогом (Brack, 2004, A80). Од 1996. године, Самити Г8 позивају на ефикасније и боље координисане акције у борби против међународног еколошког криминала, а Интерпол, Светска царинска организација и Програм Уједињених нација за животну средину (UNEP), су почели да улажу веће напоре у супротстављању овом изазову - успостављене су различите мреже агенција за спровођење закона о животној средини, укључујући Међународну мрежу за поштовање и спровођење закона о животној средини и Европску мрежу за имплементацију и спровођење закона о животној средини. Посебан проблем у борби против еколошког криминала јесте чињеница да он није увек „јасно видљив и виктимизација често има одложен карактер" (Makela et al., 2023). Утицаји и безбедносне последице транснационалног еколошког криминала могу се сврстати у категорије штетности по природу, људе и економију.

Последице по природу огледају се у: обилнијим поплавама услед неконтролисане и нелегалне сече шума; даљем утицају на озонски омотач; ремећењу ланца исхране у природи; променама у популацији, попут инвазије предатора и/или повећања или смањења других врста; нестанку појединих екосистема.

Последице по становништво и државе видљиве су у: девастацији земљишта; све катастрофалнијим природним непогодама, као последици еколошког криминала и климатских промена; појави зооноза; грађанским сукобима услед лоших животних услова.

Последице по економију очитују се кроз: трошкове опоравка нарушених екосистема; губитке у туристичкој индустрији; губитке у буџету услед неплаћених такси и пореза. Повећање броја еколошких деликата, њихових узрока, појавних облика и последица, захтева унапређење и усавршавање метода и техника за откривање починиоца ових дела (Бошковић, 2007, 132). Озбиљност дела еколошког криминала условила је развој специфичних знања, метода и техника за њихово откривање и доказивање, а који су данас утемељени као дисциплина енвиронменталне форензике.

Енвиронментална форензика – значај, технике и примена

Енвиронментална форензика своју експанзију добила је у последњих 20 година, „развијајући се настојањима да се специјализовне анализе података фокусирају на аналитичку хемију, као и мултидисциплинарну примену хемијских, геоспатијалних, историјских, хидрогеолошких и геохронолошких података у комбинацији са статистиком и различитим облицима моделовања" (Boehm and Murphy, 2015, 4). Основна питања на које дисциплина и практична примена енвиронменталне форензике треба да одговоре јесу: шта?, где?, када? и ко? је починио. Попут других форензичких дисциплина и енвиронментална форензика треба да одговори или помогне утврђивању одговора на претходно наведена питања о идентитету починиоца, карактеру и методи учињеног дела еколошког криминалитета (Бошковић, 2010, 105). Форензичке истраге

имају тенденцију да буду холистичке, оне укључују више дисциплина, различите познате алате али и оне нове, који се развијају у духу времена и нових ризика, креиране као продукт техничких и софтверских достигнућа. У пракси, делатност енвиронменталне форензике састоји се од три основне и повезане компоненте:

- Синтеза сазнања о штетној материји која је регистрована у животној средини и сагледавање обима контаминације (земље, воде или ваздуха) – карактеризација станишта,
- Успостављање историјског контекста и временског одређења испуштања загађујуће материје и
- Утврђивање починиоца дела (намерног или ненамерног) угрожавања животне средине, односно могућег еколошког криминала (Бошковић, 2010).

Карактеризација станишта је први корак у свакој истрази из домена енвиронменталне форензике и представља прву процену стања животне средине. Основна сврха ове процене јесте:

- Одређивање природе контаминације, врсте и састава штетне материје (најчешће хемикалије)
- Одређивање обима контаминације у тродимензионалној сфери
- Процена ризика по здравље људи и природне токове и односе и
- Процена потреба и обима уклањања штетне материје и контаминираног дела животне средине.

Штетне материје за чије детектовање се најчешће користе методе енвиронменталне форензике јесу „хлорисани раствори, диоксини, пестициди, метали (жива, арсен и други), метан, хидрокарбонати" (Sandau, 2006, 10).

Успостављање историјског контекста и временског одређења испуштања загађујуће материје подразумева, пре свега, сагледавање квалитета животне средине пре доспевања загађујуће материје у њу (на основу постојеће базе података, претходних фотографских снимака, сведочења и слично), затим тродимензионално снимање терена употребом сателитске опреме и ГИС технологије, као и узимање узорака. Неке од метода и алата које се користе у овој фази, која је позната и као хронолошка студија станишта јесу:

- „Временске серије фоторафија из ваздуха,
- Мапе ватрогасних служби,
- Геохронолошки подаци о станишту и узорковање загађујуће материје
- Одређивање времена доспевања загађујуће материје на локацији која се истражује" (Boehm and Murphy, 2015, 7).

Исход истраге у великој мери зависи од адекватног спровођења ове фазе. Прецизност анализа хемијских супстанци, изотопа, токсиколошких извештаја, тродимензионалних снимака „хроматографије и методе отисака (fingerprint) треба да недвосмислено укажу на детектовани проблем у животној средини и дају одговор на питање како се акцидент десио" (Taylor, 2004, A88). Идентификација извора хемијских загађивача је уобичајен проблем у форензичкој истрази загађења животне средине (Johnson et al., 2015, 610). Успешно откривање извора загађења (загађивача), зависи од дизајна плана узорковања, прикупљања узорака, процедуре, методе хемијске анализе и познавања историјских индустријских процеса на датом станишту и широј области.

Од коришћења адекватних метода и мултидисциплинарних резултата и закључака претходне две фазе, зависи и успех треће – утврђивање починиоца (извора угрожавања – физичког или правног лица), фомулисање доказа за даље процесуирање, али и проце-

на ресурса, могућности и времена за опоравак погођеног станишта. Нарочито у процесима откривања извора загађења, где је потребно извршити реверзибилни приступ (од тренутног стања доћи до почетног), као и прављењу планова опоравка животне средине, симулациони модели представљају значајно средство енвиронменталним форензичарима и уопште свима који се баве заштитом и опоравком природе. Многе студије су доказале да су моделовање и симулације ефикасни начини да се истраже динамични феномени и процеси у циљу подршке даљим истраживањима и одлукама у политици решавања питања животне средине (Nourani et al., 2019; Wang et al., 2019). Бројни алати моделовања конструисани су за потребе праћења стања и промена у атмосфери, на и у земљишту и у воденим токовима. Међутим, сложеност процеса и међуодноса у природи по себи, а нарочито у случају њиховог нарушавања присуством загађујуће материје, чини да није сваки модел применљив у свакој студији случаја.

Моделовање у енвиронменталној форензици

Пред креаторе модела и симулација се постављају изазови за дизајнирањем софтверског алата који би био применљив на највећи број случајева еколошког криминала и истрага енвиронменталне форензике. Дељење и поновна употреба ресурса симулације постали су основни предуслови за истраживаче да састављају моделе, податке и серверске ресурсе за задатке симулације животне средине (Zhang et al., 2020).

Основу програмирања чинили су познати програми попут Modular Modeling Language (MML), The Open Model Interface (OpenMI), Component Modeling Interface (CMI) и Basic Modeling Interface (BMI) проистекао из Community Surface Dynamic Modeling System (CSDMS) (Pecham et al, 2013; Peckham, 2014). Са развојем интернета и web платформи, дељење података, али и резултата симулација, значајно је олакшано. Платформе попут Web Services Description Language (WSDL), Open Geospatial Consortium Web Processing Service (OGC WPS), као и The Cloud Services Innovation Platform (CSIP), поставиле су основе дељења извора података и закључака (Zhang et al., 2020). Ипак, свако станиште и његове нише и микро-клима имају своје специфичности и модели и симулатори који уско прате те карактеристке, специјализовани су за поједине појаве и процесе. На пример, дељење такозваних „component-based" конструкција омогућени су за Landlab моделе, the Storm Water Management Model (SWMM), као и основне моделе за мониторинг шумских подручја, али нису применљиви код такозваних „black box" симулатора, попут Ground Water System (GMS) и MIKE11. Неки од њих су велики системи са много суб-симулатора, попут модела Soil and Water Assessment Tool (SWAT) модел и Weather Research Forecast (WRF), а неки су једноставни модели базирани на процесуирању података и алгоритама, попут Random Forest model (Zhang et al., 2020). Једно од решења јесте дизајнирање неколико врста интерфејса који ће задовољити потребе енвиронменталне истраге, у зависности од тога који специфичан елемент је кључан у конкретном случају. У том смислу, могуће је дизајнирати следеће врсте интерфејса:

- Модел описног интерфејса, који омогућава свим учесницима размену описа,
- Модел инкапсулационог интерфејса, који омогућава размену података о коришћеном материјалу,
- Интерфејс управљања сервером, који омогућава провајдерима да размењују базичне информације са различитих сервера и
- „Sim-task" оперативни интерфејс, који подржава модел размене података и њихових извора, и поновно моделирање (Zhang et al., 2020)

Осим за потребе истрага енвиронменталне форензике, симулатори процеса и промена у животној средини имају значајну улогу и у активностима и пословима управљања ванредним ситуацијама изазваним природним непогодама. Замајац који је развој такозваних Internet of Things (IoT) доживео, условио је усавршавање сензора за потребе мониторинга животне средине (Sun et al., 2019, 1). Сензори у склопу IoT омогућавају истовремено прикупљање великог броја различитих података са станишта, њихову анализу и презентовање у такозваном реалном времену: „Постоји велики потенцијал да се омогући моделовање у реалном времену спајањем IoT технологија и еколошких модела преко интернета. Ова достигнућа омогућавају моделима животне средине да тренутно приступају континуираним записима са сензора и олакшавају ефикасну и благовремену испоруку резултата симулације" (A.Y. Sun et al., 2019, 1).

Једна од водећих компанија која ради на развоју интероперабилних стандардизованих геоспатијалних web сервиса јесте The Open Geospatial Consortium (OGC). Тако, на пример, OGC Web Processing Service (WPS) даје могућност да се традиционалне аналитичке функције користе кроз стандардизовани web интерфејс. Овај приступ изазвао је велику пажњу академске и стручне јавности (Qiao et al., 2019; Zhang et al., 2019). Даљи развој web сервиса специјализованих за ову намену (WPS) омогућио је интеграцију овог система и сензора за мониторинг животне средине у активност геопроцесуирања у реалном времену. Лианг и сарадници (Liang et al., 2016), представили су OGC SensorThings API – модел који омогућава унифицирани начин интерконекције IoT апаратуре, података и апликација на web-u. Ово омогућава флексибилан, али на стандардима заснован интерфејс за обраду података са различитих IoT сензора и комплетних сензорних система. Интегрисање SensorThings API и WPS може, уз предности стандарда оба система, да побољша интероперабилност на web платформама заснованог моделовања у реалном времену (Zhang et al., 2023).

Закључак

Незаконита трговина дивљим животињама (Illegal Wildlife Trading - IWT) спада у такозване зелене злочине или еколошке злочине, који се дефинишу као илегалне активности које штете животној средини и које имају за циљ да донесу профит од експлоатације, штете, трговине или крађе природних ресурса, појединцима, групама или компанијама. IWT се сматра једном од најпрофитабилнијих илегалних индустрија на свету, са процењеном годишњом зарадом од 7 до 23 милијарди долара (Mozer and Prost, 2023, 1). С обзиром на природу незаконите трговине, последице се некада тешко могу потпуно проценити. Предвиђа се да ће прекомерна експлоатација природних ресурса, која укључује и дивљу флору и фауну, превазићи чак и климатске промене у својим штетним ефектима на биодиверзитет. Транснационални организовани криминал који се врши на мору, такозвани „плави криминал" (Blue crime), тек је недавно препознат као значајно безбедносно питање које захтева пажњу доносилаца политичких одлука. Злочини као што су поморска пиратерија, незаконита трговина људима, наркотицима, оружјем или отпадом на мору, и злочини у вези са животном средином, као што су илегални риболов или загађење, све су важније димензије управљања океанским водама и са њим повезаног програма поморске безбедности. Такви злочини имају различите појавне облике широм светских поморских региона и утичу на људске животе, политичку стабилност и економске интересе на различите начине, у распону од њиховог утицаја на обалне заједнице до међународног бродарства, па чак и нацио-

налне безбедности. Поморски криминал добија све већу пажњу на највишим нивоима креирања међународних политика. Савет безбедности УН одржао је своју прву дебату о овом питању у фебруару 2019. године под насловом „Транснационални организовани криминал на мору као претња међународном миру и безбедности". Ова и друга, не само еколошка већ и високо безбедносна питања и изазови, указују на то да су пред истражним органима у области еколошког криминала велики изазови: истраге и борба против организованих криминалних група и успешно процесуирање осумњичених. Поред еколошког криминала, последице климатских промена, све више девастирају природу, односећи, при томе и бројне животе људи и остављајући читава насеља без извора хране или воде за пиће. Енвиронментална форензика, својом мултидимензионалношћу и мултидисциплинарношћу, треба да пружи тачне и брзе одговоре на све сумњиве штетне појаве у животној средини. Осим тога, моделовање које из активности енвиронменталне форензике произилази, помаже не само сагледавању размера девастације и откривању извора, већ даје и предикцију будућих дешавања на станишту и могућности ресторације. Имајући све изнето у виду, симулатори и модели праћења промена мораће да развијају све детаљније облике интерфејса. Напредак и развој научних дисциплина, као и њихова сазнања, постају врло значајни за усавршавање техника енвиронменталне форензике и моделовања. Комплекснија структура симулатора омогућила би вишеструко примењиве апликације, како за различите појаве и станишта, тако и ситуације – од евидентирања дела еколошког криминала до управљања ванредним ситуацијама.

Библиографија

Boehm, P.D. and Murphy, B.L. 2015. "Introduction to Environmental Forensics". In: Murphy and Morrison (Eds.) *Introduction to Environmental Forensics*. Elsevier Ltd.

Bošković, M. 2007. "Forenzika životne sredine - identifikacija dokaza počinjenih dela ekološkog kriminala". *Bezbednost* 49 (3): 132-143.

Bošković, M. 2010. *Izazovi industrijskog društva: Nove tehnologije i ekološka bezbednost*. Beograd: Univerzitet u Beogradu - Fakultet bezbednosti.

Johnson, G.W., Ehrlich, R., Full, E.W. and Ramos, S. 2015. "Principal Components Analysis and Receptor Models in Environmental Forensics.". In: Murphy and Morrison (Eds.) *Introduction to Environmental Forensics*, 609-653. Elsevier Ltd.

Mäkelä, T., Huhtala, S., Lindqvist, M. and Bucht, R. 2023. "The Current Status of Environmental Forensic Science in the member Institutes of the European network of Forensic Science Institute (ENFSI)". *Forensic Science International* 348: 1-8.

Mozer, A. and Prost, S. 2023. "An introduction to illegal wildlife trade and its effects on biodiversity and society". *Forensic Science International: Animals and Environments* 3: 100064.

Nourani, V., Gökçekuş, H. and Umar, I. K. 2020. "Artificial intelligence based ensemble model for prediction of vehicular traffic noise". *Environmental research* 180: 108852.

Peckham, S.D., Hutton, E. and Norris, B. 2013. "A component-based approach to integrated modeling in the geosciences: The design of CSDMS". *Computers & Geosciences* 53: 3-12.

Peckham, S.D. 2014. "The CSDMS standard names: Cross-domain naming conventions for describing process models, data sets and their associated variables". In: *International Congress on Environmental Modelling and Software* 12, 67-74.

Qiao, X., Li, Z., Ames, D., Nelson, J. and Swain, N. 2019. "Simplifying the deployment of OGC web processing services (WPS) for environmental modelling – Introducing Tethys WPS Server". *Environmental Modelling & Software* 115 (7): 38-50.

Sandau, C. 2006. "Environmental Forensics as a Tool for Environmental Liability Management". Remtech, Trium: Environmental Solutions Ltd: 1-34.

Sun, Y.A., Zhong, Z., Jeong, H. and Qian, Y. 2019. "Building complex event processing capability for intelligent environmental monitoring". *Environmental Modelling & Software* 116 (3): 1-6.

Taylor, D.A. 2004. "Innovative technologies. Environmental Forensic Files". *Environmental Health Perspectives* 112 (2): 88.

UNEP. 2018. The State of Knowledge of Crimes that have Serious Impact on the Environment. Accessed 17 May 2024. https://www.unep.org/resources/publication/state-knowledge-crimes-have-serious-impacts-environment

Wang, X., Huang, R., Li, L., He, S., Yan, L., Wang, H., Wu, X., Yin, Y. and Xing, B. 2019. "Arsenic removal from flooded paddy soil with spontaneous hygrophyte markedly attenuates rice grain arsenic". *Environment International* 133, Part A: 105159.

Zhang, F., Chen, M., Ames, D., Shen, C., Yue, S., Wen, Y. and Lü, G. (2019). "Design and development of a service-oriented wrapper system for sharing and reusing distributed geoanalysis models on the web". *Environmental Modelling & Software* 111: 498-509.

Zhang, F., Chen, M., Yue, S., Wen, Y., Lü, G. and Li, F. 2020. "Service-oriented interface design for open distributed environmental simulations". *Environmental Research* 191: 110225.

DIGITAL TOOLS AND SIMULATIONS IN THE FIELD OF ENVIRONMENTAL FORENSICS

Abstract: Environmental degradation, climate change, but also illegal trade in plant and animal species, as a form of transnational organized crime, leave hard-to-repair consequences for the living environment, nature, and people's health. It is estimated that certain processes in nature have become irreversible as a result of environmental devastation and environmental crime. The issue of environmental crime and sustainable development is highly positioned not only on the global political scene, but also in the agendas and activities of states and companies at the national level. The development of technology, digital tools and simulators has facilitated investigations in the field of environmental forensics, but also the prediction of the consequences of possible environmental accidents. The aggregation of geographically distributed technical resources enabled the creation of simulations and performances of high quality and variety. Along with the techniques of field environmental forensics, simulation models made a significant contribution to the detection and prosecution of the perpetrators of environmental crimes, but also to the prediction of future changes in natural flows. This paper will describe certain techniques of environmental forensics, as well as the importance of digital tools in the simulation of events, their explanation and prediction.

Keywords: environmental crime, forensics, sensors, simulations, models.

СИМУЛАЦИЈА УПОТРЕБЕ ЦИВИЛНЕ ЗАШТИТЕ У РАТУ[1]

Зоран Јефтић[2], Петар Станојевић[3]

Апстракт: Да би се национална стратегија у области смањења ризика од катастрофа оживотворила и могла подржати глобалну и регионалну политику у области смањења ризика од катастрофа, потребно је развити оптималне националне ресурсе за супростављање свим потенцијалним ризицима, што је и препорука Међународне организације цивилне заштите (ICDO). Полазећи од те чињенице постоји потреба израде реалних процена угрожености од елементарних непогода, техничко-технолошких несрећа ратних разарања, као и њихове провере кроз симулационе моделе. Рад под наведеним називом даће садржај и анализу елабората за практичан задатак употребе цивилне заштите у рату у урбаној средини. Анализа ће се односити пре свега на: Програм рада за израду документа; Мере приправности; Мобилизацију; Организацију и спровођење мера заштите и спасавања; Употребу јединица цивилне заштите и Руковођење. Посебан део односиће се на израду већег броја супозиција у односу на процењено стање, као предуслова за формирање симулационог модела и његову имплементацију у програм рада Симулационог центра Факултета безбедности.

Кључне речи: национална стратегија, цивилна заштита, процена угрожености, симулациони модели.

Увод

У свим земљама света планирање, супротстављање и санирање последица ванредне ситуације[4] представља организован одговор друштва на опасности које угрожавају становништво, материјалниа добара и животну средину. Све активности усмерене на адекватан одговор на ванредне ситуације могу се садржајно профилисати кроз систем заштите и спасавања, и у највећем број земаља Европе препознаје се кроз термин цивилне заштите (civil protection), управљање у ванредним ситуацијама (civil emergency planninig, disaster management), а у неким земљама и кроз термин цивилна одбрана (civil defence). Без обзира на терминолошко одређење, та врста активности државе представља целовит

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

[2] Факултет безбедности, Универзитет у Београду, jefticz@ymail.com

[3] Факултет безбедности, Универзитет у Београду, petstano45@gmail.com

[4] „Ванредна ситуација је стање које настаје проглашењем од надлежног органа када су ризици и претње или настале последице по становништво, животну средину и материјална и културна добра таквог обима и интензитета да њихов настанак или последице није могуће спречити или отклонити редовним деловањем надлежних органа и служби, због чега је за њихово ублажавање и отклањање неопходно употребити посебне мере, снаге и средства уз појачан режим рада" Закон о смањењеу ризика од катастрофа и управљањзу ванредним ситуацијама,, Члан 2., СЛ.Гласник РС" бр. 87/2018. (РС 2018).

систем и најшири облик организовања, припремања и учешћа становништва у заштити и спасавању у случају елементарних непогода, техничко-технолошких несрећа и ратних разарања. Она је делатност која данас функционише у миру и рату, пре у време и након извршења задатака из области одбране, односно оружане борбе, као њеног ужег дела. Стога је категоријални појам са јасним приоритетима, модалитететима функционисања у заштити јавног интереса - људских живота, материјалних добара и животне средине.

Ова хуманитарна делатност уређена је међународним правом, Женевском конвенцијом из 1949. године и Допунским протоколом уз Женевску конвенцију из 1977. године. Оба документа ратификовала је Скупштина СФРЈ 1950. и 1977. године и данас их Република Србија прихвата као сукцесорски легат. Израз цивилна заштита према међународном праву представља вршење хуманитарних активности са циљем заштите цивилног становништва од свих облика опасности и обезбезбеђења потребних услова за преживљавање.

Уочавајући значај заштите и спасавања становништва и материјалних добара 1965. године УН, у Резолуцији Генералне скупштине број 2034, позвале све земље да успоставе одговарајуће механизме за планирање интервенција и спасилачких операција, односно да свака земља према својој сопственој процени дефинише обим и тип помоћи која јој може бити потребна у случају природних непогода, техничких несрећа и ратних разарања.

У вези са том иницијативом формирана је у Женеви Међународна организација цивилне заштите **ICDO (International Civil Defence Organisation),** која представља кишобран националним структурама цивилне заштите и уједно допринси њиховом стварању и снажењу. Поред тога **ICDO** има и улогу савеза који кроз универзално признате и прихваћене вредности обједињује капацитете националних структура свих чланица и партнера за постизање заједничких циљева у заштити и спасавању. **ICDO** је једина међувладина организација која има мандат за деловање у области заштите и спасавања и заснива се на Конститутивном акту (1966) и декларацијама из Амана и Пекинга, усвојеним на Десетој (1994) и Једанаестој (1998) Светској конференцији о цивилној заштити (Зоран Јефтић 2001.).

Полазећи од одредби Женевске конвенције и допунског протокола, као и својих сопствених потреба, створене су организације цивилне заштите у свим развијеним земљама света. Највећи број земаља види приоритет у организовању и припремању за мирнодопско ангажовање (у случају елементарних непогода, техничко технолошких несрећа и других опасности) и укључивању у одбрамбени систем земље у случају рата.

Конкретна решења у државно-правној пракси појединих земаља су различита. Један број земаља има самосталну организацију цивилне заштите, директно одговорну највишем органу власти у држави у облику министарства или дирекције или агенције, у другим земљама, која се налази у надлежности МУП-а заједно са ватрогаством, као окосницом сваке ефикасно конципиране организације цивилне заштите, док је код једног броја земаља управно смештена у Министарство одбране.

Цивилна заштита у савременом смислу, егзистира на територији бивше СФРЈ од 1955. године. Протекли период, као и НАТО агресија, пружили су довољно могућности за промену постојећих решења у области заштите и спасавања у случајевима елементарних непогода, техничко технолошких несрећа али и у условима рата. Данас су послови цивилне заштите у Републици Србији организационо смештени у Министартсво унутрашњих послова у оквиру Сектора за ванредне ситуације - Управе за управљање ризиком.

Да би цивилна заштита у нашим условима успешно функционисала мора пре свега: (1) постојати ваљана процена угрожености становништва у оквиру које треба развијати организацију, опремање, финансирање и обуку припадника цивилне заштите, (2) усмерити развој снага цивилне заштите на квалитативној компоненти, (3) одговарајућа предузећа која се по природи своје основне делатности баве заштитом и спасавањем оспособљавати и укључивати у планове деловања цивилне заштите, (4) цивилну заштиту приоритетно развијати у великим градовима и индустријским центрима, (5) обезбедити планску изградњу склоништа са оријентацијом на вишенаменска склоништа, (6) материјалну опремљеност цивилне заштите довести до нивоа који омогућава успешно спровођење како личне и узајамне заштите тако и свих мера заштите и спасавања, (7) функционално повезати цивилну заштиту са системом за рано упозоравање.

Обзиром да тема рада није анализа тренутног организационог модела и ситуирања цивилне заштите задржаћемо се на констатацији њеног управног одређења и поћи од става да се цивилна заштита у Србији суочава се с различитим изазовима, укључујући потребу за модернизацијом опреме, подизање капацитета за превенцију ризика те јачањем капацитета за одговор на све сложеније катастрофе уз развијање јавне свести о потреби система заштите и спасавања. Као посебан захтев истиче се и потреба изградње симулационих модела који се односе на њено ангажовање како у миру тако и у ратним условима.

Улога и значај организовања цивилне заштите у миру и рату

Различите врсте опасности као последице узроковане елементарним непогодама, техничким, технолошким акцидентима, и ратним дејствима, свакако представљају највеће ризике који прете човеку и његовој околини. Оптимално сагледавање значаја цивилне заштите није могуће посебни посматрати кроз мирнодопско и ратно стање. Угроженост од разноврсних, мирнодопских катастрофа и одговор на њих, добија још више на значају у далеко комплекснијим ратним условима. То се посебно односи на градови, индустријске центре и велике привредне системе критичне инфраструктуре. Стога морамо из основа мењати наше схватање о спремности целокупног друштва за спровођење превентивних и оперативних мера заштите и спасавања.

Поред опасности од елементарних непогода, техничких и других несрећа у миру, ратне опасности и последице које би биле узроковане дејством агресора на нашу земљу из ваздуха, и са копна, нужно условљава потребу адекбатним развојем квалитетне организације заштите и спасавања људи и материјалних добара.

Савремени борбени системи, а посебно оружје за масовно уништавање са својом разорном моћи, али и психолошким дејством, уводе нову физиономију рата. У таквој ситуацији становништво, градови, привредни (посебно индустријски комплекси великих система), политички, културни и други објекти могу бити уништени у већој мери него снаге и средства оперативне армије, што потврђују и досадашња искуства рата у Украјини. Нагли и квалитетно нови развој ратне технике, и све савршеније нуклеарно и конвенционално оружје у случају агресије на нашу земљу, могу да ставе под истовремени удар и дејство комплетну њену територију.

Све чињенице указују на то да би се евентуални будући рат знатно разликовао од ратова у прошлости, што може битно изменити услове живота и рада, начин вођења оружане борбе и других облика отпора агресору. Иако нису устројени јасно дефинисани доктринарн ставови о цивилној заштити, припрема за одбрану, заштиту и

спасавање становништва у свим условима мира и рата, представља значајан фактор укупне организованости за одбрану и заштиту у току рата. Способност нашег друштва за успешну одбрану земље, а посебно за вођење рата, у великој мери зависи и од отпорности свих његових делова на разне врсте опасности. Заштитом становништва и материјалних добара од мирнодобских опасности и ратних дејстава, смањују се губици у људству и материјалним добрима и стварају предуслови за ефикасније и организованије функционисање државе у рату.

Ово указује на потребу за одговарајућим системом заштите и спасавања, посебно са аспекта превентиве за ефикаснију заштиту људства и материјалних добара друштва од последица које могу настати од елементарних непогода, техничких и технолошких акцидената, као и од ратних разарања, а могу имати катастрофалне размере и битан утицај на ефикасност одбрамбено-заштитног механизма државе.

Значај функције заштите и спасавања људи и материјалних добара, која је у нашој земљи кодификована као цивилна заштита, мора произилазити из оцене и сагледавања физиономије и начина вођења рата у савременим условима, и могуће визије агресије на нашу земљу. Наиме, услови и захтеви за успешно вођење оружане борбе и различитих облика отпора агресору битно претпостављају неодложан захтев организовања, припремања и функционисања заштите и спасавања становништва и материјаних добара и у мирнодопским условима. Цивилна заштита је интегрални и незаменљив део одбране у рату, намењен спасавању људи и материјалних добара са којима се планира и реално рачуна у свим могућим ратним ситуацијама у којима се наше друштво може наћи..

Улога и значај цивилне заштите, отуда, нису садржани само у њеном појмовном дефинисању - заштита и спасавање људи и материјалних добара од елементарних непогода и других несрећа и ратних разарања - већ и у њеном месту и значају међу бројним чиниоцима њене спремности и способности за успешно супротстављање агресији. Порастом губитака цивилног становништва и нестајањем границе између фронта и позадине, увећавају значај и улогу цивилне заштите као организоване друштвене делатности за заштиту и спасавање становништва и материјалних добара.

Стога припрема за успешно фунционисање цивилне заштите представља задатак од прворазредног значаја, како би се у највећој могућој мери смањили људски и материјални губици, и брзо и успешно санирале последице, ратних разарања. Цивилна заштита захтева већу бригу и мора постати предмет интересовања свих субјеката друштва од грађанина до надлежних институција.

Истовремено савремени ратови постају комплекснији, опаснији, без јасних граница, циљева, сфера интереса. Све је више актера на глобалној сцени, од међународних војних организација (НАТО, ШОС), економских и политичких унија (ЕУ, АСЕАН, БРИКС), финансијских институција (ММФ, ВБ, ЕИБ) до појединачних држава, терористичких организација (Ал Кида, Боко Харам) и интернет група (Анонимуси, Викиликс). Комплексност мултиполарног света, нови изазови савремених начина ратовања, недовољно природних ресурса и недефинисане сфере утицаја воде у хаос великих размера. Покушај Друштва народа, затим Уједињених нација да светски поредак успоставе на миру са јасним међународним правилима у оружаним сукобима, довео је до манипулације системима вредности прокламованих Повељом УН и разним декларацијама и резолуцијама. Уосталом и ова организација претрпела је последице трансформације светског поретка, због чега данас нема улогу глобалног „полицајца", већ је више постала легитимна арена дипломатских сукоба великих сила.

Промене које су захватиле државе, однос војне и економске моћи, мултипликовање и преплитање интереса, није променило узроке (ресурси, енергенти, геостратешки положај), али јесте природу сукоба. Немогуће је уочити јасне циљеве (а сигурно их има), нити правце деловања великих сила (финансирање час једне, час друге стране, војно интервенисање, па повлачење, склапање споразума, па поништавање (као у случају САД-Иран)). Са војног становишта, може се извући закључак да војске данашњице и сутрашњице морају да се припреме за три врсте сукоба: 1) са великим силама или коалицијама земаља, да би их одвратиле од намере преузимања њихових националних ресурса, 2) грађанске ратове и сличне унутар државне територије, односно сукобе који постају доминантан облик ратовања великих против малих и 3) рат у сајбер и информационој сфери. За прву групу сукоба треба изградити снаге одвраћања, за другу свакако треба ојачати обавештајно-безбедносне и војнополицијске снаге, а за трећу се мора створити нов организационо-технолошки подсистем оружаних снага. Све ово подразумева успостављање одговарајућих организационо-технолошких приоритета, али и значајно оснажење система цивилне заштите, што у пракси потврђује и актуелни сукоби у Украјини и Гази (З.Јефтић и др. 2018)

Потреба за вежбама и симулацијама

Развој система цивилне заштите мора ићи у три смера: организациони развој, материјално опремање и развој кадра. Под организационим развојем подразумева се доношење стратегијских, планских, доктринарних и других неопходних докумената и смерница уз креирање организационе структуре, њену попуну кадром и успостављање линија и начина комуникација и преношења информација. Под материјалним развојем се подразумева опремање неопходним материјално-техничким средствима и успостављање система резерви. Претходна два смера имају улогу формирања и изградње система који без школованог, увежбаног и мотивисаног особља (кадрова) неће моћи ни у ком случају да функционише.

Припрема кадрова подразумева њихово одговарајуће школовање, одржавање и увежбавање. Данас су потребна знања све обимнија и специфичнија. Истовремено, није више уобичајено да се спроводе велике вежбе цивилне заштите са учешћем значајног броја људи ради провере доктринарних ставова и увежбавања људства. Таква пракса је била присутна у време хладног рата, док је данас мање уобичајена. Истовремено, захтеви за ниво обучености су све виши, јер се организација цивилне заштите мора ослањати како на високо специјализоване јединице и појединце, тако и на масовну примену људства и опреме. Из претходног разлога, потребно је ослонити се на методе које омогућавају обуку и увежбавање најближе реалним условима, а које истовремено не подразумевају увек велике и скупе вежбе на терену.

Вежбе и симулације су незамењиви алати за проверу планских докумената, процедура и поступака у тачно дефинисаним и контролисаним условима ангажовања снага цивилне заштите (ЦЗ) како у рату тако и у миру. Оне представљају најсложенији облик примењеног обучавања припадника ЦЗ и проверавања њихових способности за извршавање планираних задатака у ратним и мирнодопским условима. Најчешће се вежбе и симулације дела на теренске и виртуелне.

Теренске вежбе подразумевају стварно ангажовање снага и средстава у реалном времену и простору. Оне представљају организовани облик обучавања у којем су доминантне практичне и теренске методе обучавања. Виртуелне симулације као основу ко-

ристе посебну информатичку опрему и софтвере за симулацију разноврсних сценарија у виртуалном окружењу, што значајно олакшава и појефтињује симулирање стварних догађаја.

Поред наведенога, вежбе и симулације можемо делити према учесницима (штабови, јединице, садејство појединачних учесника и јединица у активностима ЦЗ), према садржају и општим условима за деловање (спровођење мера приправности, мобилизацијске вежбе, отклањање последица ратних дејстава и сл.), према месту извођења и према организационом облику.

У општем случају вежбе и симулације можемо поделити на:

- Симулације доктринарних начела, процеса и планова,
- За увежбавање појединаца и јединица цивилне заштите,
- За увежбавање штабова.

Симулације доктринарних начела, процеса и планова су симулације којима се преко креираног модела проверава неко организационо, доктринарно или техничко-технолошко решење. Циљ је да се пронађе најбоље решење или провере ефекти и претпоставке, као и да се одреде могућа ограничења примене.

Увежбавање штабова (команди) се првенствено изводи кроз командно-штабне игре. Ова врста симулације је у основи хибридна где се део вежбе изводи кроз уобичајену „штабну игру", односно физичку симулацију уз употребу карте и израду потребних докумената, а део вежбе се обавља преко рачунара којим се приказује терен и моделује ситуација, израчунавају последице нежељених догађаја и слично.

Појединци и јединице се увежбавају да тачно и по процедури извршавају радње из домена њихове намене и конкретних задатака. Циљ је да се коришћењем рачунаром подржаних метода омогући максимална сличност виртуалне реалности са стварном и максимални број понављања вежби, до аутоматизма извршавања радњи и процедура.

У оквиру Националног симулационог центра на Факултету безбедности Београдског Универзитета постоји више софтвера који се могу искористити у сврху симулација процеса и планова (видети више на сајту факултета (Факултет Безбедности, Национални симулациони центар n.d.)). То су првенствено ADMS и ANYLOGIC. Постоји и озбиљно истраживачко искуство у креирању модела и истраживању појава из безбедносног домена (Stanojevic Petar 2019.). За увежбавање појединаца и јединица цивилне заштите намењен је софтвер XVR који омогућава креирање симулационих вежби за обуку професионалаца и јединица ЦЗ. Овај софтвер се може користити у комбинованим или хибридним симулацијама намењеним за обуке штабова и команди. Такође, овај софтвер има могућност да ситуацију прикаже на начин „виртуелне реалности", што додатно повећава ниво обуке, јер се увежбава и ситуационо сналажење, орјентација и деловање.

Увежбавање штабова је донекле сложеније и захтевније, јер подразумева изучавање докумената, формирање претпоставки о могућим и потребним дејствима, креирање организације, израду планских докумената, рад по супозицијама и сл. Због сложености свих претходно наведених поступака и мера, није их могуће све приказати кроз софтверска решења (или би то захтевало веома много времена и ресурса). Из тог разлога прибегава се хибридним симулацијама где се део изводи израдом планских докумената и цртањем карти, део се изводи на терену, као што су командантска извиђања или инспекције организација и опреме, а за део се могу применити рачунари посебно када се ради о приказу ситуације на карти или виртуелним сликама објеката и терена. Рачунарима се могу симулирати последице појединих одлука како би учесници вежби могли брзо да се увере у сврсисходност урађеног. Рачунарска техника се може користити

и као средство комуникација међу учесницима и као веза са дроновима или другим сензорима на терену.

Успешним спровођењем вежби и симулација могу се пре свега уочити недостаци и слабости постојећих планских докумената, процедура и поступака руководећих органа цивилне заштите и створити услове за подизање нивоа обуке и координацију свих учесника у превенцији и одговору на удес или ратна разарања. Посебно је значајно да се подиже ниво јавне свести о потреби обучавања припадника цивилне заштите, као и изградња поверења свих актера система заштите и спасавања.

Како би се сачинио оптималан елаборат и практични задатак за вежбу и симулацију употребе цивилне заштите у урбаној средини у рату, потребно је као основу узети план функционисања цивилне заштите и на његовој основи сачини све остале потребне елементе.

Елаборат би у основи требао да садржи четири целине са већим бројем супозиција.

Први део обухвата: Практични задатак; Стање на територији града (насељеност, капацитети болница, смештаја, привредних организација, возног парка и сл.); Карта градске територије и План града.

Други део се односи на: Програм и динамику рада на изради документа плана одбране за употребу ЦЗ; Процену угрожености и повредљивости од ратних дејстава и Одлуку о организовању, припремању и функционисању ЦЗ на градској територији

Трећи део обухвата: Мере приправности; Мобилизација – активирање цивилне заштите са прилозима за мобилизацију, Употребу ЦЗ у рату која садржи Организацију и спровођење мера заштите о спасавања са прилозима по свакој мери заштите и спасавања; Употреба јединица и снага које се ангажују на задацима ЦЗ, шема распореда и правци употребе са прилозима; Извод из организације везе, руковођења и криптозаштите за потребе ЦЗ; Дневник употребе.

Четврти део се односи на практични задатак и најмање пет различитих Супозиција са пратећим очекујућим решењима.

Сви појединачни сегменти елаборта, а посебно они који се односе на трећи део захтевају висок степен ажурности плана функционисања цивилне заштите и реалне процене угрожености становништва и материјалних добара, расположивих ресурса и начина употребе снага и средстава цивилне заштите. Актуелност података условљава и израду већег броја реалних супозиција и проверу система цивилне заштите у најсложенијим ратним условима.

Закључак

У овом раду покушали смо да укажемо на важност развоја оптималних националних ресурса за супростављање свим потенцијалним ризицима из области цивилне заштите. Незаобилазна је потреба обуке и увежбавања кадрова цивилне заштите као и потреба израде реалних процена угрожености од елементарних непогода, техничко-технолошких несрећа ратних разарања, као и њихове провере кроз симулационе моделе.

Рад је указао на садржај и анализу елабората за практичан задатак употребе цивилне заштите у рату у урбаној средини. Анализа ће се односила на могућности реалне примене симулација као методе развоја и унапређења цивилне заштите, као и на практичне садржаје, а пре свега на: Програм рада за израду документа; Мере приправности; Мобилизацију; Организацију и спровођење мера заштите и спасавања; Употребу јединица цивилне заштите и Руковођење. Указано је на нужност израде већег броја

супозиција у односу на процењено стање, као предуслова за формирање симулационог модела и његову имплементацију.

Кроз опис Симулационог центра Факултета безбедности и софтвера које поседује, дат је преглед могућности примене, овог савременог ресурса, у будућности као његово место и значај у систему цивилне заштите.

Библиографија

Stanojevic Petar, Mirjana Misita, Jeftic Zoran, Milosevic Mladen, Miskovic Vasilije, Bukvic Vladimir. 2019. „Organizational design based on simulation modeling.“ *The International Journal of Advanced Manufacturing Technology* 104 (9-12): 3251-3.

Зоран Јефтић. 2001. *Међународна орīанизација цивилне заштите-заштита и ūомоћ за све, ūревод са енīелескоī језика.* Београд: ЈП ПТТ Србија.

Зоран Јефтић, Гордана Мишев, Жарко Обрадовић, Петар Станојевић. 2018. „ Савремени конфликти и њихове тенденције .” *Војно дело* 38.

РС, Службени Гласник. 2018. Верз. 87/2018. Република Србија.

Факултет Безбедности, Национални симулациони центар. n.d. *https://nsc.fb.bg.ac.rs/OCentru.html.*

SIMULATION OF CIVIL PROTECTION USAGE IN WAR

Abstract*:* In order for the national strategy in the area of disaster risk reduction to come to life and be able to support the global and regional policy in the area of disaster risk reduction, it is necessary to develop optimal national resources for confronting all potential risks, which is also the recommendation of the International Civil Protection Organization (ICDO). Based on this fact, there is a need to make realistic assessments of the threat from natural disasters, technical-technological accidents and war destruction, as well as their verification through simulation models. The work under the mentioned title will provide the content and analysis of the study for the practical task of using civil protection in war in an urban environment. The analysis will primarily refer to: Work program for the preparation of the document; Preparedness measures; Mobilization; Organization and implementation of protection and rescue measures; Use of civil protection units and Management. A special part will refer to the development of a larger number of assumptions in relation to the estimated situation, as a prerequisite for the formation of a simulation model and its implementation in the work program of the Simulation Center of the Faculty of Security Studies.

Keywords: National strategy; civil protection; Vulnerability assessment; Simulation models.

ПЛАНОВИ ЗА ВАНРЕДНЕ СИТУАЦИЈЕ У ПРИВАТНОМ СЕКТОРУ[1]

Горан Ј. Мандић[2], Јана Марковић[3]

Апстракт: Организације приватног (али и јавног) сектора, попут држава у целини или њених локалних јединица нису имуне на несреће. Било да су природне, изазване техничко-технолошким акцидентима или проузроковане људским чињењем (или нечињењем), несреће проузрокују одређене последице. Обим последица, на здравље и живот људи, имовину, пословање или животну средину зависан је како од карактеристика саме несреће, тако и од карактеристика, у првом реду отпорности, организације или заједнице. Са једне стране, када овакве несреће погоде заједницу и достигну извесни обим, оне прерастају у ванредну ситуацију. Тада је реаговање релевантних субјеката (на државном нивоу или нивоу федералних или локалних јединица) по правилу нормативно регулисано. Са друге стране, када овакве несреће погоде организацију, онда се она третира као ванредна ситуација, ситуација која одудара од оне „редовне". За овакве ванредне ситуације, за организацију је боље да има адекватне планове за реаговање. Аутори праве кратак осврт на ванредне ситуације доводећи их у везу за појмом „контингентност", затим на управљање ванредним ситуацијама и планирање за деловање у случају њиховог остваривања. С обзиром на тему, аутори даље указују на правце деловања приватног сектора у случају ванредних ситуација. Централни део рада јесте уједно и део који је у функцији циља рада, а то је представљање карактеристика и оквирних елемената планова за ванредне ситуације. На крају, аутори представљају одређена ограничења планова и отварају дискусију о могућностима коришћења софтвера у функцији унапређења планова и поспешивања свеукупне припреме за реаговање у случају ванредних ситуација.

Кључне речи: контингентност, ванредне ситуације, планирање у ванредним ситуацијама, планови за ванредне ситуације, приватни сектор.

Приватни сектор контролише 85 одсто критичне инфраструктуре у земљи. Заиста, осим ако мета терориста није војна или друга безбедносна државна установа, „први" који први реагују ће скоро сигурно бити цивили. Национална безбедност и припремљеност нације стоје често почињу од приватног сектора.

– The 9/11 Commission Report (2004)

Увод – контингентност и ванредне ситуације

Можда не уобичајено, али за разумевање ванредне ситуације могуће је користити појам „контингентност". Она се може разумети као тродимензионални концепт који укључује неодређеност (може се догодити или не), неизвесност (будућност је непредвидива) и

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

[2] Факултет безбедности, Универзитет у Београду, goran.mandic@fb.bg.ac.rs.

[3] Факултет, безбедности Универзитет у Београду, markovicfb22@gmail.com, jana.markovic@fb.bg.ac.rs.

условљеност (зависи увек од нечега) (Schedler 2007, 57). Односи се на оно што би се могло десити у будућности, што обично изазива проблеме или чини неопходним даљи аранжман (Cambridge Advanced Learner's Dictionary & Thesaurus n.d.). Кроз наставак текста, уочиће се карактеристике које су заједничке и за контингентност и за ванредне ситуације.

Када се дискутује о ванредним ситуацијама (енг. *emergency*), треба имати на уму да постоје различита одређења исте. Најпре, можемо разликовати две врсте дефиниција: академске дефиниције настале од стране научника и у научно-образовне сврхе и административне дефиниције формулисане од стране институција и организација а за њихову сврху и потребе (нпр. легислативна документа – видети табелу 1, FEMA, UNDRR)[4].

Ванредна ситуација представља „непредвиђену комбинацију околности или настало стање које захтева хитну акцију", односно, ствара „хитну потребу за помоћи или олакшањем" (Merriam-Webster n.d.). Анализом дефиниција датих од стране међународних организација, дефиниција која би могла да се понуди на овом месту је следећа: ванредна ситуација је 1) изненадна и обично непредвиђена појава 2) изазвана природним догађајем или догађајем који је проузроковао човек (укључујући и комбинацију наведеног)[5], 3) која проузрокује људску патњу и губитке по погођену заједницу и животну средину 4) тако да последице превазилазе капацитете погођене заједнице и захтевају тражење помоћи (Марковић 2023, 300). Међутим, „ванредна ситуација је појам који се може користити истовремено или упоредо са појмом катастрофа у контексту биолошких и технолошких опасности везаних за здравље људи, али се појам ванредне ситуације може односити *и* на опасне догађаје који не резултирају озбиљним поремећајима *у* функционисању заједнице *и* друштва" (UN General Assembly 2016). Све наведене карактеристике одговарају дефиницијама ванредне ситуације (или инцидента) које су приложене у Табели 1. Ипак, ове дефиниције се односе на ниво државе или њене територијалне јединице.

Под ванредном ситуацијом подразумевамо и „неповољан скуп фактора и догађаја који угрожавају животе људи, нарушавају услове за њихов нормалан рад, онемогућавају производњу, привреду и друге врсте делатности и свакодневни живот" (Белокапић-Шкунца 2005). Ванредна ситуација је свака изненадна ситуација која може да изазове смрт или значајне повреде запослених, корисника или шире популације; да прекине посао или операцију; да битно оштети материјална или природна добра; да угрози финансијско стање или углед организације (Wahle & Beaty 1993, 5). То је ситуација угрожавања структуре, делатности и вредности организације под околностима које карактерише нестабилност, оскудност информација, временски притисак и ургентно доношење круцијалних одлука и спровођење активности у циљу одговора и опоравка организације од последица ванредне ситуације.

Важно је нагласити да иако се ванредна ситуација најчешће односи на државу, њене грађане и територију, ванредна ситуација схваћена на овај начин може постојати на нивоу организације са или без могућности ескалације ван њених граница[6]. То су ситуације изазване природним појавама попут земљотреса, поплава, урагана или цунамија, ситуације активног пожара, нестанка струје. То могу бити и ситуације попут дојаве о

[4] Видети више у: (Млађан и Кекић 2007); (Ковачевић, Бабић и Ковач 2020).

[5] Врло детаљан списак могућих штетних догађаја може се пронаћи у: (NFPA 1600 2019, 65-66).

[6] Напомена: У раду се не користи одређење ванредне ситуације матичног Закона о смањењу ризика од катастрофа и управљању ванредним ситуацијама (члан 2, став 1, тачка 7) Републике Србије које је специфично и не представља догађај, већ стање које настаје проглашењем од надлежног органа.

постављеном минско-експлозивном средству, експлозије, отмице, претње или употребе оружја, недостатка робе за организацију која се бави снадбевањем, пандемијом изазваног изостанка кључних људи у организацији и слично. Све ове ситуације захтевају хитан и високоструктуриран одговор који се заснива на релативно добро дефинисаном ризику, способностима надлежних да схвате шта се догађа (обим и природа инцидента) и шта треба да раде (ефективна стратегија), укључујући и могућности употребе расположивих средстава у складу са процедурама које су прописане у одговарајућим плановима (Ђукић 2017, 342). Према написаном:

- надлежни могу бити надлежни органи и лица из надлежних органа државне структуре, али и надлежна лица унутар организације у приватном сектору (главни извршни директор (CEO), корпоративни председник или друго више руководство);
- расположива средства могу се односити на државне ресурсе или ресурсе организације[7] и
- планови могу бити донесени како за национални, (регионални) и локални ниво, тако и за микрониво организације.

Табела 1: Неке дефиниције ванредне ситуације

Дефиниција	Извор
У Руској федерацији, ванредна (изванредна, изузетна) ситуација дефинише се као „стање на одређеној територији које је настало као последица удеса, опасне природне појаве, катастрофе, ширења болести, која представља опасност за друге, природне или друге непогоде која може да настане или је проузроковала последице у виду људских жртва, оштећењу здравља људи или животне средине, значајних материјалних губитака и нарушавања услова живота људи".	Федеральный закон от 21.12.1994 N 68-ФЗ (ред. от 14.04.2023) „О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера" (Статья 1)
У легислативи Кине, одређује се ванредни инцидент који се односи „природну катастрофу, изненадну катастрофу, инцидент у јавном здравству или инцидент у сфери социјалне сигурности, који се догодио случајно, проузроковао је или би могао проузроковати озбиљну друштвену штету и захтева доношење мера хитног реаговања.	Emergency Response Law of the People's Republic of China (Article 3)
У Републици Србији, ванредна ситуација дефинише се као „стање које настаје проглашењем од надлежног органа када су ризици и претње или настале последице по становништво, животну средину и материјална и културна добра таквог обима и интензитета да њихов настанак или последице није могуће спречити или отклонити редовним деловањем надлежних органа и служби, због чега је за њихово ублажавање и отклањање неопходно употребити посебне мере, снаге и средства уз појачан режим рада".	Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама (члан 2, став 1, тачка 7)

Извор: Аутори.

[7] Ресурси правних лица (организација), као и физичких лица могу бити стављени на располагање држави и коришћени за потребе државе, а под условима који су прописани легислативом.

План који се израђује за поступање у ванредним ситуацијама, које су неодређене, неизвесне, изазивају проблеме и захтевају конкретне мере, осим што се назива планом за ванредне ситуације може се назвати и „контингентни план" (енг. *contingency plan*). Одатле, могло би се говорити о контингентном планирању које може бити сегмент проактивног кризног менаџмента. С тим у вези, реч је о планирању које „осигурава организацију у односу на могуће, али ипак не и вероватне догађаје и кретања који су критични за опстанак организације" (Кешетовић 2008, 134). Схваћено на овај начин, контингентно планирање је ограничено на само један скуп потенцијалних поремећаја занемарујући оне који су могући и исто тако вероватни. Зато, контингентност треба разумети на начин који је већ описан, као ситуације које су неодређене, неизвесне, изазивају проблеме и захтевају конкретне мере. Важно је на овом месту нагласити да ванредне ситуације не морају нужно да доведу до последица по живот и здравље људи, материјална добра или животну средину. Једноставно, реч је о ситуацији који излази изван оквира „нормалног" и има потенцијала да изазове негативни ефекат у мањем или већем обиму. Ради поједностављења наведеног, контингентност ће се разумети као ванредна ситуација[8]. Контингентно планирање стога ће се разумети као планирање за поступање у ванредним ситуацијама (енг. *emergency*), а чији је производ план који ћемо означити као „план за ванредне ситуације".

Планирање као сегмент управљања ванредним ситуацијама

Када се ванредне ситуације разумеју „шире", тада управљање ванредним ситуацијама није у искључивој надлежности државе и њених органа већ је и у надлежности приватног сектора[9]. То нарочито бива важно у заштити критичне инфраструктуре. Најрањивија инфраструктура сваке државе јесте њена критична инфраструктура, односно, системи, објекти или њихови елементи чије би угрожавање, односно, оштећење или уништење, имало значајне последице по функционисање државе и њене грађане. Неретко су кључни инфраструктурни сектори у власништву приватног сектора или њима управља приватни сектор. Поред тога, не само да је приватни сектор често примарни пружалац критичних услуга, већ је реч о сектору који поседује знање и ресурсе значајне за управљање ванредним ситуацијама без обзира на њихов обим.

Управљање ванредним ситуацијама може се разумети као непрекидан процес за планирање, спречавање, припрему, реаговање (ограничавање, ублажавање и отклањање), одржавање континуитета операција (владе) и опоравак од последица. Циљ (система) управљања ванредним ситуацијама јесте „задржавање квалитета управљаног система и у условима реализације ванредног догађаја, а критеријуми су минимални губици (људски и материјални), минимална улагања у реализацију превентивних мера и минимално време за реализацију оперативних мера" (Мићовић 2014, 294). Управљање ванредним ситуацијама увек обухвата превенцију и реаговање. Превенција би се могла одредити као скуп мера које се унапред спроводе и имају за циљ да што више смање

[8] Уколико се ипак инсистира на повлачењу паралеле, рећи ћемо да за разлику од контингентности, ванредну ситуацију карактерише већа озбиљност последица и већа хитност у пружању одговора.

[9] На пример, у Анексу за подршку координацији приватног сектора одређено је да приватни сектор има обавезе да одговори на ванредну ситуацију било да је 1) погођен ванредном ситуацијом, 2) ресурс за реаговање, 3) одређена и/или одговорна страна или 4) члан Државне организације за управљање ванредним ситуацијама (Homeland Security 2008, 53).

ризик од ванредних ситуација, али и очувају здравље људи, смање штету по животну средину и материјалне губитке уколико до њих дође. Реаговање, са друге стране, обухвата спасавање и друге хитне послове који за циљ имају очување здравља људи, смањење штете по животну средину и материјалних губитака, односно, локализацију зона ванредних ситуација и спречавање ширења ефеката (Федеральный закон от 21.12.1994 N 68-ФЗ (ред. от 14.04.2023)).

Све чешће, приватни сектор је припремљен да одржи свој континуитет пословања и заштити запослене кроз усвајање регулаторних захтева и међународних индустријских стандарда. Тако, приватни сектор све чешће користи могућности „које се нуде", а које им омогућавају развој планова за целокупни менаџмент, па самим тим и онај „безбедносни" у који свакако да спадају и планови за ванредне ситуације. Када не постоји обавеза израде ове врсте планова (без обзира на то који је њихов тачан назив), тада приватни сектор на добровољној основи може да сачини квалитетан план и тиме заштитити своје вредности, али и вредности другога. Самим тим, државе могу и треба да користе планове развијене од стране приватног сектора за допуну планова државног (и локалног) карактера. У даљем раду, фокус се ставља на приватни сектор и планове који се доносе у приватном сектору (иако се неке карактеристике и елементи плана у појединим деловима односе и на планове државног карактера). Као што је наглашено, деловање приватног сектора је од посебне важности и оно се одвија у два правца:

1) јачање интерне припремљености на ванредну ситуацију:
   – континуирано проактивно деловање,
   – идентификовање и процена ризика[10],
   – развијање планова за ванредне ситуације,
   – планирање капацитета за реаговање, одржавање материјалних ресурса и повећање спремности запослених,
   – континуирана комуникација и координација са надлежним државним органима и службама, другим заинтересованим странама о узајамној сарадњи и помоћи,
2) поступање када наступи ванредна ситуација
   1. у оквиру организације приватног сектора:
   – поступање по претходно развијеном плану за ванредне ситуације,
   2. ван организације приватног сектора:
   – размена информација са свим релевантним субјектима, а у складу са законом и међусобним споразумима или на добровољној основи,
   – пружање добара и услуга или помоћ при пружању добара и услуга, а у складу са законом и међусобним споразумима или на добровољној основи.

У основи, свако планирање јесте одређивање циљева и начина на који ти циљеви могу или треба да се остваре. Планирање за ванредне ситуације јесте процес 1) усвајања и имплементације процедура за идентификацију предвидивих ванредних ситуација коришћењем системске анализе и 2) припреме, тестирања и ревизије плана одговора на ванредну ситуацију (Petrović i Tivković 2010, 453). Такво планирање састоји се из два аспекта: 1) проактивно (институционализација, едукација, одржавање и заштита, надзор и кон-

[10] Процена ризика се најчешће сматра свеукупним процесом идентификације ризика (процес проналажења, препознавања и описивања ризика), анализе ризика (процес схватања природе ризика и одређивање нивоа ризика) и вредновања ризика (процес поређења резултата анализе ризика са критеријумима за ризик да би се утврдило да ли је ризик и/или величина ризика прихватљива или се може толерисати) (SRPS A.L2.003:2017, Термини и дефиниције).

трола процеса) и 2) реактивно (активности на ограничавању, ублажавању и отклањању ефеката и последица ванредне ситуације). Смит (Smith) сугерише да планирање никако не сме да се сведе на питање „Шта се дешава ако?" већ да се заснива на превентивним елементима (1990, 270), питањима попут „Шта учинити да до нечега не дође?".

Мере које су предложене након 11. септембра 2001. године а које се односе на припремљеност за спасавање, поновно покретање и опоравак операција: 1) план за евакуацију, 2) адекватне комуникационе капацитете и 3) план за континуитет операција (9/11 Commission Report 2004) и више су него оскудне. Рецимо да план за ванредне ситуације треба да садржи:

- Идентификацију стања, сагледавање ситуације и стварних околности;
- Прогнозу развоја ванредне ситуације;
- Процену капацитета неопходних за ограничавање, ублажавање и отклањање ефеката и последица;
- Развој стратегије спречавања ескалације ванредне ситуације и њених последица;
- Одређивање просторних и временских параметара поступања, односно, извршавања задатака и послова;
- Одређивање приоритетних задатака и послова, одређивање надлежних организационих јединица са описом задатака које треба извршити и одговорних лица (нарочито оних лица која врше контролу и координацију). Утврђивање улога и одговорности унутрашњих и екстерних субјеката, њихових овлашћења и услове и начин делегирања овлашћења;
- Логистичку подршку и расподелу ресурса (људски ресурси, стручно знање, обука, објекти и постројења, средства и опрема, материјали, технологија, финансије, подаци и информације и временски оквир у којима ће бити потребни);
- Спровођење оперативних неопходних мера (ако их је могуће спровести, а до доласка надлежних служби или заједно са њима);
- Континуирану комуникацију, прикупљање, анализу и размену информација уз вођење рачуна о њиховој заштити. Важно је одредити које су информације потребне, њихов обим, субјекте и начин прикупљања и обраде и услове за дељење истих.
- Уз наведене елементе наводимо следеће:
- Сваки план треба да буде израђен уз максимално уважавање свих нормативних аката, стандарда и принципа добре праксе који омогућавају развијање што ефикаснијег плана. Уз то, веома је значајно за онога ко план израђује да током или непосредно након израде плана затражи и уважи, ако је то оправдано, мишљења других интерних и/или екстерних лица и/или тимова која могу унапредити квалитет плана.
- Сваки план треба да има дефинисан циљ и да служи остварењу тог циља.
- Сврха сваког плана јесте да послужи као корисно средство за поступање свих релевантних субјеката (списак релевантних државних органа које треба укључити у решавање ванредне ситуације уз списак лица из служби за хитне случајеве, списак организација приватног сектора које су у обавези или могу да допринесу решавању ванредне ситуације) у обиму и на начин који је прописан, а у циљу ограничавања последица на најмању могућу меру и елиминације истих. Сврха плана треба да одговара циљевима који су постављени, јер се тако спречава расипање ресурса (новца, људи, опреме и средстава за рад, времена).
- Сваки план треба да садржи регулаторну основу (стратегије, закони, подзаконски акти, усвојени међународни стандарди, потписани споразуми о узајамној или

другој помоћи и/или сарадњи, интерни акти организација, као и други документи који представљају основ израде и доношења/усвајања плана).

- Сваки план треба да садржи одељак о карактеристикама организације у оквиру које се израђује (величина организације; њена делатност, опис активности, процеса, производа и услуга; компетентност запослених).
- Сваки план треба да уважи карактеристике екстерног окружења за које се израђује: потенцијалне опасности, њихову вероватноћу испољавања и могуће последице; подручје које је угрожено и посебно критичне објекте на том подручју, њихову евентуалну повезаност; дистрибуцију запослених; комуникацију и кореспонденцију са заинтересованим странама; раније усвојене и предузете стратегије[11].
- Сваки план треба да експлицитно наведе обим реаговања у ванредним ситуацијама – који субјекти су одговорни, на који начин и на којим подручјима.

Сваки план треба да буде саставни део обуке, предмет редовне евалуације, ревизије и ажурирања. Услови ажурирања плана треба да буду јасно дефинисани у самом плану или неком другом документу (обично су то годишња ажурирања или када наступи нека значајна промена која утиче на план). У вези са овим квалитетом, план карактерише флексибилност.

Компоненте плана могу се сагледати и кроз неколико основних елемената који обухватају до сада изнете елементе и карактеристике. Најпре, сваки план треба да има циљ који ће усмеравати све напоре који се чине у случају ванредне ситуације. Сваки план треба да има препознат ризик или „окидач" када се ставља у потребу, као и један или неколико одговора који се могу предузети када се „окидач активира". Обично постојање више од два потенцијална одговора значи да се одговорнима за спровођење плана оставља избор једног одговора у зависности од карактеристика саме ванредне ситуације. На крају, увек постоји временски оквир и кључни људи и средства чије је ангажовање, односно, употреба неопходна у датом временском оквиру.

По правилу, планирање за ванредне ситуације се повезује са управљањем континуитетом пословања. Реч је о процесу „идентификације претњи којима је организација изложена, одређивања критичних ресурса који су неопходни организацији за функционисање и процену могућих последица тих претњи по критичне ресурсе, као и одређивање ресурса (стратегија, капацитета, мера и временских оквира) неопходних за превазилажење последица поремећаја" (Марковић 2023, 21-22). У литератури се може пронаћи став да је план континуитета пословања ширег обима, те да често укључује план за ванредне ситуације (Fernandes and da Gama 2008). Овакав став може бити прихватљив уколико се узме да су планови за ванредне ситуације конкретнији и фокусирани на одређене сценарије или ванредне ситуације, док планови за континуитет пословања покривају шири спектар потенцијалних поремећаја и обухватају стратегије опоравка дугорочног карактера. Можда је ипак прихватљивији другачији став да планирање за ванредне ситуације има четири основна аспекта: анализу утицаја на пословање, план реаговања на инциденте, план опоравка од катастрофе и план континуитета пословања (Clark 2010).

[11] Ако се говори о плану који се доноси на национално, регионалном или локалном нивоу, неке карактеристике би биле другачије (географско подручје које је угрожено и критичне објекте на том подручју (вртићи, школе, старачки домови, болнице, критична инфраструктура); повезаност критичних објеката; диструбуција становништва; комуникација и кореспонденција са релевантним друштвеним субјектима; раније усвојене и предузете активности на спречавању наступања штетног догађаја, или ванредне ситуације).

Ограничења планова и како софтвери могу да помогну?

Поседовање плана за ванредне ситуације омогућава бржи опоравак од последица, даје до знања да организација води бригу о својим интересима и интересима својих запослених, као и другим заинтересованим странама и у служби је заштите имица и репутације организације. Како указују Ериксон и Меконел (Eriksson and McConnell), не треба да чуди то што академски стручњаци, консултанти за управљање кризама и владе упућују на развој детаљних планова за различите ситуације (2011, 90). Ипак, постоји и друга страна, а то је питање реалних могућности примене планова. Уколико су усвојени форме ради, онда је њихова функционална употребљивост врло мала или чак никаква[12]. Није редак случај, укључујући Републику Србију, да се различита акта доносе ради испуњавања законских норми или услова прописаних стандардима. Даља проблематика јесте:

- квалитет тих аката (стварна стручност лица која акте израђују и израда акта тако да стварно испуни функцију ради које је написан),
- целокупан систем контроле усвајања, примене и ажурирања тих аката од стране надлежних органа (приватног и јавног сектора),
- питање ревизије и ажурирања планова у складу са новонасталим променама и „наученим лекцијама" и
- едукација особља које планове треба да спроведе.

Уз све наведено, треба имати на уму да некада и врхунско израђен план уз континуирану едукацију не може произвести жељене резултате. Планирање за ванредне ситуације само је један од многих фактора који утиче на исходе целокупног управљања кризом. Једноставно, „планирање и успех се не поклапају, већ су лабаво повезани или чак потпуно одвојени" (Clarke 1999, 57).

Како је изнето у претходном тексту, значајан део планова за ванредне ситуације односи се на поступање одређених лица или група лица. Да би та лица/запослени знали како да поступе у случају неке одређене ванредне ситуације неопходно је да буду упознати са активностима које су одређене и по којима треба да поступају. У организацији, то се постиже тако што се сваком запосленом (уколико је одређен планом да поступа у случају ванредне ситуације) обезбеђује извод из плана који садржи све информације које су запосленом потребне за поступање. Наредни корак јесте обука запосленог и периодичне провере како би се осигурало да сваки запослени буде спреман за деловање када наступе околности које то захтевају. Та обука значи теоријску едукацију и практично увежбавање. За практично увежбавање, односно, спровођење вежби, најбоље је исценирати ванредну ситуацију (или неки њен део) створивши реалне услове под којима запослени треба да делује онако како је претходно научио кроз теоријска предавања. Међутим, када се не могу обезбедити реални услови за извођење неке вежбе[13], што може бити поприлично често, тада се као вредни ресурс издвајају софтвери који омогућују спровођење вежбе у виртуелном окружењу које може верно да „ослика" реалну ситуацију и услове. Наравно, „жива" обука не може бити до краја замењена обуком преко софтвера, али да треба користити све могућности у едукацији – без икакве сумње, треба.

Софтвери попут XVR софтвера, омогућавају креирање симулација чија се вредност огледа у могућностима које пружа корисницима. Неке од предности коришћења софтвера су следеће:

[12] Видети више у: (Clarke 1999); (Boin and Lagadec 2000); (Kapucu 2008).

[13] Интересантан је податак да отприлике 12% свих повреда у ватрогасно-спасилачкој служби у САД настаје током обуке (National Fire Protection Association 2021).

- Корисници могу да доживе различите инцидентне ситуације у безбедном окружењу чији се параметри могу мерити, контролисати и мењати;
- Корисници могу да стекну практична знања и вештине пролазећи/доживљавајући/увежбавајући сценарије чиме се оспособљавају за ефикасније поступање у инцидентним ситуацијама када се оне догоде у реалности;
- Могуће је развити велики број сценарија који се могу накнадно мењати и прилагођавати другачијим ситуацијама. Стварање таквих ситуација у (физичкој) реалности захтевало би велике ресурсе и остављало би реалне и „скупе" последице, те зато и није честа одлука. Софтвери за стварање виртуелне стварности та ограничења отклањају;
- Сценарији се могу увежбавати већи или мањи број пута, колико год да је потребно током обуке;
- Софтвер даје могућност и индивидуалног рада и тимског рада у њему;
- XVR софтвер један је од ретких који имају интегрисани комуникациони програм који бележи сву комуникацију у симулацији (Barta et al. 2016, 79).
- Ипак, на крају, не треба заборавити да коришћење било ког софтвера укључујући и XVR има и одређена ограничења, а у првом реду:
- набавка и коришћење софтвера захтева одређена новчана средства (Организација може набавити софтвер за своје потребе или може користити – изнајмити софтвер који је набавила нека друга организација. У сваком случају, да би се софтвер користио потребно је набавити не само софтвер већ и пратећу опрему попут хардвера који ће моћи да подржи карактеристике софтвера или лица која ће бити компетентна да подесе и користе функције које софтвер има);
- коришћење софтвера захтева и одређена знања и развијене вештине (Као и у сваком другом случају, опрема без обучених лица нема сврху. Без лица која су компетентна за коришћење софтвера, функције које софтвер нуди неће бити искоришћене у потпуности).
- коришћење софтвера не може да симулира психолошке елементе попут панике (Иако ниједна симулација, било да се изводи уживо или преко софтвера не може у потпуности да испуни све елементе ванредне ситуације, укључујући и ове, ипак се део њих може постићи када се симулације изводе уживо).

Дакле, софтвер ипак остаје „алат" само за оне који могу и желе исти да набаве и уложе у његово коришћење. У највећој мери, то су јавне службе или научно-образовне установе. 2015. године, процењено је да овај софтвер користи преко 150 хитних служби у Великој Британији и широм света. Такође, у току 6 година које су претходиле овој години, компетенција кандидата се побољшала захваљујући раду у овом софтверу (Lamb et al. 2015, 237).

Уместо закључка

Иако је у раду акценат стављен на приватни сектор, те поступање приватног сектора у ванредним ситуацијама, оправдано је проширити контекст и ван овог сектора. У вези са тим, резултати рада се могу посматрати са аспекта свих правних лица, као правно признатих организација, без обзира да ли припадају приватном или јавном сектору, профитном или непрофитном. Не постоји разлог да се планови за ванредне ситуације не израде, на пример, за јавне (државне) образовне или здравствене установе, као што могу да се израде за ове врсте приватних организација. Вредности правних лица је потребно штитити у сваком случају.

Када организација одговорно приступи континуираној заштити свих својих вредности (лицима, имовини и пословању), неизоставни део таквог приступа засигурно је дефинисање политика, процедура и планова како за поступање у редовном стању, тако и за поступање у случају ванредних ситуација. Тек са свешћу и одговорним приступом менаџмента организације, квалификованим лицима, разумевању циљева организације може се говорити о одговорном бављењу безбедношћу организације. На темељу наведеног, организација не би требало да има проблем када је реч о идентификовању ризика по организацију, њиховој процени и планирању поступања са идентификованим ризицима укључујући планирање у случају ванредних ситуација. Како план за ванредне ситуације треба да обезбеди смернице за поступање онда када ванредна ситуација наступи, он делује као „водиља". Није погрешна претпоставка да што је план детаљнији, то је организованији одговор на ванредну ситуацију; што више потенцијалних ризика или развијених сценарија обухвати, то је организација спремнија да делује. У крајњој линији, план обезбеђује дугорочни успех за посао, а са адекватним плановима организације раде далеко безбедније и ефикасније. Тиме, она дугорочно обезбеђује своје пословање. Планови за ванредне ситуације могу имати различит обим или форму. Они ће се разликовати свакако и у зависности од организације за коју се израђују, укључујући и различите ризике који се идентификују. Ипак, циљеви ових планова су увек исти – заштити вредности и наставити пословање.

Библиографија

9/11 Commission Report. 2004. Washington DC: National Commission on Terrorist Attacks Upon the United States.

Barta, Jiri, Michaela Vaskova, and Jiri J. Urbanek. 2016. „Evaluation of Simulation Programs Applicable to the Support of Decision-Making Processes in Crisis Management of Critical Infrastructure“. *International Journal of Education and Learning Systems*, 1: 74-80.

Белокапић-Шкунца, Вера. 2005. „Руковођење у ванредним ситуацијама”. Безбедност, 47 (5): 893-902.

Boin, Arjen and Lagadec, Patrick. 2000. „Preparing for the future: Critical challenges in crisis management“. *Journal of Contingencies and Crisis Management* 8 (4): 185–191.

Ђукић, Станимир. 2017. „Кризни менаџмент и ванредна ситуација”. Војно дело 69 (2): 333-355.

Cambridge Advanced Learner's Dictionary & Thesaurus. n.d. *Contingency*. Cambridge University Press. Приступљено 03.03.2024. са

Clarke, Lee. 1999. *Mission improbable: Using fantasy documents to tame disasters*. Chicago: University of Chicago Press.

Emergency Response Law of the People's Republic of China. Доступно на: https://www.lawinfochina.com/display.aspx?looktype=3&lib=law&Cgid=96791

Eriksson, Kerstin and McConnell, Allan. 2011. „Contingency planning for crisis management: Recipe for success or political fantasy?“. *Policy and Society* 30 (2): 89-99.

Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама. 2018. Службени гласник РС, бр. 87/2018-3.

Институт за стандардизацију Србије. 2017. Безбедност и отпорност друштва — Процена ризика, SRPS A.L2.003:2017.

Федеральный закон от 21.12.1994 N 68-ФЗ (ред. от 14.04.2023) “О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера”. Доступно на: https://www.consultant.ru/document/cons_doc_LAW_5295/bb9e97fad9d14ac66df4b6e67c453d1be3b77b4c/

Fernandes, Leão José, and F. Saldanha da Gama. 2008. „Contingency planning–a literature review“. In: *SCM Competitiveness* (pp. 457-467). India: Macmillan.

Homeland Security. 2008. *Overview: ESF and Support Annexes Coordinating Federal Assistance In Support of the National Response Framework*. FEMA.

Kapucu, Naim. 2008. „Planning for disasters and responding to catastrophes: Error of the third type in disaster policy and planning“. *International Journal of Public Policy* 3 (5–6): 313–327.

Кешетовић, Желимир. 2008. Кризни менаџмент. Београд: Факултет безбедности; Службени гласник.

Ковачевић Ненад, Бабић Бранко и Ковач Митар. 2020. „Појмовно одређење ванредних ситуација“. У: *15. Међународна конференција „Ризик и безбедносни инжењеринг”* (стр. 296-302). Копаоник.

Lamb, Katherine, Martijn Boosman, and Jim Davies. 2015. „Introspect Model: Competency Assessment in the Virtual World”. In: *ISCRAM2015 Conference Proceedings*, edited by Leysia Palen, Monika Büscher, Tina Comes and Amanda Hughes (pp. 235-243).

Марковић, Јана. 2023. „Безбедност информација у функцији управљања континуитетом пословања”. Савремене студије безбедности 1: 11-28.

Марковић, Јана. 2023. „Улога службеника обезбеђења у ванредним ситуацијама". У: Зборник радова: Друга меморијална научна конференција „Предраг Марић", уредили Н. Стекић и М. Милошевић, 299-310. Београд, Универзитет у Београду-Факултет безбедности.

Merriam-Webster. n.d. *Emergency*. In Merriam-Webster.com dictionary. Приступљено 03.03.2024. са https://www.merriam-webster.com/dictionary/emergency.

Мићовић, Марија. 2014. „Концепција сложености управљања у ванредним ситуацијама". У: Супротстављање савременом организованом криминалуи тероризму, уредили С. Мијалковић, О. Лајић, З. Кесић, М. Поповић, 291-305.

Млађан, Драган. и Кекић, Далибор. 2007. „Ванредна ситуација – прилог концептуалном одређењу безбедности". НБП – Журнал за криминалистику и право (3): 61-83.

National Fire Protection Association. 2019. *NFPA 1600, Standard on continuity, emergency, and crisis management.*

National Fire Protection Association. 2021. *United States firefighter injuries in 2020: 2*.

Petrović, Pero, i Ţivković, Aleksandar. 2010. „Sistem upravljanja i planiranje u vanrednim situacijam". U: *Međunarodna naučna konferencija „Menadžment 2010"* (str. 451-457). Kruševac.

Philip Clark. 2010. „Contingency planning and strategies". In: *2010 Information Security Curriculum Development Conference (InfoSecCD '10)* (pp. 131–140). New York: Association for Computing Machinery.

Schedler, Andreas. 2007. „Mapping contingency". In: *Political contingency: Studying the unexpected, the accidental, and the unforeseen,* edited by I. Shapiro, S. Bedi, pp. 54–78. New York: New York University Press.

Smith, Denis. 1990. „Beyond contingency planning: towards a model of crisis management". *Industrial Crisis Quarterly* 4 (4), 263–275.

UN General Assembly. 2016. *Report of the open-ended intergovernmental expert working group on indicators and terminology relating to disaster risk reduction (A/71/644)*. United Nations. Приступљено 03.03.2024. са https://reliefweb.int/report/world/report-open-ended-intergovernmental-expert-working-group-indicators-and-terminology

Wahle, Thomas and Gregg Beatty. 1993. *Emergency Management Guide for Business & Industry*. Federal Emergency Management Agency (FEMA).

EMERGENCY PLANS IN PRIVATE SECTOR

Abstract: Organizations of the private (but also public) sector, such as the state as a whole or its local units, are not immune to accidents. Whether they are natural, caused by technical-technological accidents or caused by human action (or inaction), accidents cause certain consequences. The extent of the consequences, on the health and life of people, property or the environment, depends both on the characteristics of the accident itself, and on the characteristics, primarily of resilience, of the organization or community. On the one hand, when such disasters hit the community and reach a certain scale, they turn into an emergency situation. Then the reaction of the relevant entities (at the state level or at the level of federal or local units) is as a rule normatively regulated. On the other hand, when such accidents hit the organization, then it is treated as an emergency situation, a situation that deviates from the "regular" one. For such emergency situations, it is better for the organization to have adequate response plans. The authors make a brief overview of emergencies, linking them to the term "contingency", then to the management of emergencies and planning for action in case of their realization. With regard to the topic, the authors further indicate the directions of action of the private sector in case of emergencies. The central part of the work is also the part that serves the purpose of the work, which is the presentation of the characteristics and framework elements of plans for emergencies. In the end, the authors present certain limitations of the plans and open a discussion about the possibilities of using the software in the function of improving the plans and enhancing the overall preparation for responding in case of emergencies.

Keywords: contingency, emergencies, emergency planning, emergency plans, private sector.

3

УПОТРЕБА НОВИХ ТЕХНОЛОГИЈА У УПРАВЉАЊУ КРИЗАМА

ПРИМЕНА НОВИХ ТЕХНОЛОГИЈА У КРИЗНОМ МЕНАЏМЕНТУ[1]

Дејан Вулетић[2], Марија Вукадиновић[3]

Апстракт: Модерне технологије обухватају широк спектар напредних алата, техника и система који се користе за решавање одређених проблема или побољшање процеса у различитим областима. Оне имају значајан утицај на све друштвене процесе односно на свакодневни живот људи. У првом делу рада анализирају се најновија технолошка достигнућа (вештачка интелигенција, друштвене мреже, рачунарство у облаку, мобилне апликације и слично). Истраживање нових технологија и њихов утицај на кризни менаџмент је кључан корак ка бољем разумевању и повећању способности за реаговање на кризне ситуације. У другом делу рада обрађене су основе кризног менаџмента, пре свега теоријско одређење, циљеви и фазе. У научној заједници превладавајуће мишљење је да се кризни менаџмент може поделити на четири фазе: фаза превенције, фаза припреме, фаза реаговања и фаза опоравка. Истраживање је имало за циљ анализу нових технологија које могу донети корист у управљању кризама по фазама кризног менаџмента, пружајући тако додатну ефикасност и поузданост у процесима решавања кризних ситуација. На основу анализе релевантне литературе, студија случаја и стручних радова који се баве применом нових технологија у кризном менаџменту, у трећем делу рада идентификоване су области примене одређених, нових, технологија у различитим фазама кризног менаџмента. Нове технологије могу бити кључни алати у побољшању ефеката и брзине реакције. Овај рад представља допринос бољем разумевању како технолошки напредак може трансформисати начин на који се управља кризним ситуацијама, али истовремено указује на то да аспекти примене нових технологија у области управљања кризама нису довољно обрађени. Резултати истраживања представљају основ за даљу анализу комплексности примене нових технологија у кризном менаџменту, имајући у виду да је реч о новом, па самим тим и недовољно истраженом феномену.

Кључне речи: нове технологије, кризни менаџмент.

Увод

Нова технолошка достигнућа постају неизоставан део свакодневног живота људи па самим имају значајну улогу и у кризном менаџменту. Нове технологије могу да помогну у превазилажењу кризних ситуација и минимизовању њихових последица. Историјски гледано, кроз различите фазе у развоју рачунарских система, приметан је континуитет

[1] Рад је настао у оквиру пројекта који финансира Фонд за науку Републике Србије у оквиру програма „ИДЕЈЕ" – Management of New Security Risks – Research and Simulation Development, NEWSIMR&D, #774951.

[2] Институт за стратегијска истраживања, Београд, dejan.vuletic@mod.gov.rs

[3] Институт за стратегијска истраживања, Београд, marija.vukadinovic@mod.gov.rs

у напретку технологије који обликује нашу свакодневну стварност (Attali 2011; Herman T. Tavani 2013, 6-9). Прелазак на 5G мрежу представља одличан пример високог нивоа технолошког умрежавања и приступности нових уређаја у свакодневном животу и ова транзиција не само да унапређује мобилне комуникације и пренос медијских садржаја, већ и има значајан утицај на различите аспекте савременог друштва (Mamta, Navrati & Abhishek 2019, 192). Развој 5G и најава 6G мрежа наговештавају да ће будућност донети још дубљу интеграцију технологије у наше животе, стварајући потпуно нове облике комуникације и интеракције у „паметним" окружењима (Kaur, Kumar & Baliyan 2018). Савремена технолошка достигнућа представљају бројне изазове и могућности, од приватности и сигурности информација до етичких питања у вези са употребом нових технологија. Акценат у раду биће на одређеним, често примењиваним, новим технологијама које се користе у различитим фазама кризног менаџмента.

Нове технологије

Одређене, нове, технологије су од посебног значаја за кризни менаџмент - вештачка интелигенција (*Artificial Intelligence - AI*), друштвена мрежа Твитер, рачунарство у облаку (*Cloud Computing*) и мобилне технологије (GAO-22-104714 2022, 24-48).

Вештачка интелигенција је грана информатике, специјализована за дизајнирање и развој интелигентних рачунарских система, способних да самостално обављају задатке које су некада извршавали људи. Као таква, она представља сложену и динамичну област коју карактерише константан развој и чије крајње домете је тешко предвидети. Главни циљеви развоја вештачке интелигенције су производња и усавршавање рачунара који могу обављати задатке уз достизање високог нивоа компетентности и самосталности, као и подстицање развоја технологије способне да подражава и унапреди људску интелигенцију (Morley et al., 2023 420). Кроз алгоритме вештачке интелигенције, могуће је анализирати огромне количине података и идентификовати узорке који указују на могуће кризе, чиме се значајно унапређује брзина и ефикасност реакције у кризним ситуацијама (Morley et al. 2023, 421). Осим што постоји велики потенцијал за примену вештачке интелигенције у побољшању квалитета живота људи, могућност злоупотребе и развоја у деструктивне сврхе представља значајан безбедносни изазов. Вештачка интелигенција има значајан утицај на управљање кризама (Ayub et. al. 2023, 223).

У области аутоматског препознавања и обраде информација, вештачка интелигенција може брзо и ефикасно обрађивати велике количине података из различитих извора, укључујући сателитске снимке, снимке са беспилотних летелица и информације примљене са различитих врста сензора, али и праћење и анализу објава на друшвеним мрежама. Ова функција вештачке интелигенције унапређује способности за праћење кретања и активности на терену, чиме омогућава боље разумевање ситуације и доношења оптималних одлука. У области унапређења комуникације, вештачка интелигенција доприноси развоју сигурних и брзих средстава за комуникацију.

Комуникација је изузетно важна, а друштвене мреже су постале кључни канал комуникације због своје широке доступности и утицаја на колективну свест (Watson & Rodrigues 2017). Бројни извори указују на велики утицај друштвених медија (мрежа) и ефеката брзе дистрибуције информација. Друштвена мрежа Твитер (лого ове друштвене мреже је средином 2023. године промењен у велико, рестилизовано, слово „X") је једна од главних, најчешће коришћених, платформи друштвених медија (Marwick & Lewis 2017). Интеракција између корисника Твитера није заснована на односима из стварног живота

и тако лабаво повезане везе омогућавају дистрибуцију нових информација, што чине ову платфору погодном не само за дистрибуцију информација већ и за манипулације, а означен је и као плодно тло за злонамерне кориснике (Caldarelli et. al. 2020).

Рачунарство у облаку је једна од нових, често коришћених, технологија. То је модел пружања услуга који омогућава приступ рачунарским ресурсима попут рачунарских система, података, или апликација преко Интернета. Уместо да корисници одржавају властите физичке сервере или рачунарску инфраструктуру, они могу користити ресурсе који су доступни путем „облака" (енг. *cloud*). Рачунарство у облаку представља значајан инструмент у управљању кризним ситуацијама због своје ефикасности, доступности и могућности дељења информација између различитих организација (Velev & Zlateva 2011, 119). Хостовање сервера у облаку омогућава рад на безбедном удаљеном месту од било ког догађаја или катастрофе, што је кључно за омогућавање приступа и рада у неповољним условима (Velev 2014, 70). Коришћење апликација базираних на рачунарство у облаку омогућава корисницима да буду ефикасни са било ког места и са било ког уређаја, што је од велике важности у кризним ситуацијама када је брз и ефикасан приступ информацијама неопходан (Velev 2014, 70).

Поред наведених, нових, технологија, веома важан ресурс представљају мобилне апликације. Оне омогућавају брз и лак приступ информацијама, упутствима за поступање у кризним ситуацијама, као и могућност за праћење и координацију активности током кризних догађаја (Klaufhold 2021, 70). Овај вид технологије игра кључну улогу у управљању кризама пружајући правовремене информације, ресурсе и алате појединцима и организацијама које се суочавају са кризним ситуацијама (Klaufhold 2021, 70). Мобилне апликације представљају дигитални мост између корисника и кључних услуга, нудећи функционалности попут ажурирања у реалном времену, комуникационих канала и упозорења у кризним ситуацијама (Boulos et. al. 2011). Мобилне апликације су одиграле кључну улогу током пандемије COVID-19 пружајући корисницима информације о актуелним мерама заштите, статистике о броју заражених и преминулих, упутстава за поступање у случају појаве симптома, као и приступ виртуелним консултацијама са здравственим стручњацима (Zhou 2021). Ове апликације су омогућиле корисницима да буду информисани, да брзо реагују на променљиве услове и да претпузму превентивне мере како би заштитили себе и своје заједнице.

Кризни менаџмент

Не постоји домен који је имун на кризе, и тиме се артикулише суштина кризног менаџмента - способност организације да се суочи са изазовима и ефикасно управља кризама које могу да наруше нормално функционисање. Области безбедности и управљања ризиком примарно су усмерене на природне катастрофе, за разлику од кризног менаџмента који се фокусира на кризе које су производ човекових активности или су директно изазване људским фактором (Каровић 2015, 79). Такав приступ открива јасну специфичност кризног менаџмента и његову релевантност у савременом друштву. Кризни менаџмент представља кључни сегмент управљања организацијом у ситуацијама које могу довести до озбиљних последица по њен опстанак, углед или ефикасност пословања базирајући се на процес сачињен од четири фазе: превенције, припреме, реаговања и фаза опоравка од кризне ситуације (Каровић 2015, 80-81; Bundy at al. 2017). Кешетовић и Милашиновић сматрају да је једна од основних разлика између кризног менаџмента и других сродних концепата попут управљања ризицима (*risk*

management) је усмерен на идентификацију потенцијалних ризика и њихово смањење или елиминацију пре него што се криза деси, док кризни менаџмент се бави управљањем кризом када се она већ догодила (Кешетовић, Милашиновић 2008).

Фазе кризног менаџмента, које укључују превенцију, припрему, реаговање и опоравак, представљају темељне кораке у ефикасном управљању кризом (Mitroff, Shrivastava & Udwadia 1987, 285.) Фаза превенције је почетна тачка у кризном менаџменту, где организација користи различите системе упозорења како би идентификовала потенцијалне ризике и претње (Zamoum & Gorpe 2018). Рачунарски системи контроле процеса, системи за праћење, омогућавају рано откривање проблема пре него што се они ескалирају у озбиљне кризне ситуације (Jaques 2007, 150). Ова фаза обухвата систематско и свеобухватно спречавање или припрему за кризе које су већ идентификоване (Mitroff, Shrivastava & Udwadia 1987, 285). Припрема за кризне ситуације, развој планова за односе с јавношћу, формирање тимова за управљање кризама су само неки од корака који се предузимају како би се минимизовали негативни утицаји кризе на организацију (McConell 2003, 363–409). Када се криза догоди, организација улази у фазу реаговања.

У тој фази се поступа по плановима, тимови за управљање кризом преузимају контролу ситуације, а стратегије за односе с јавношћу се примењују како би се очувала репутација организације (McConell 2003, 370). Након што се криза смири, организација улази у фазу опоравка. Ово је време за детаљну анализу оно га што је организација научила из претходних криза. Евалуација ефикасности стратегија за управљање кризом, идентификација области за унапређење способности за управљање кризом и развој бољих планова за будућност су клучни кораци у тој фази (McConell 2003, 404). У наредном потпоглављу биће вршена анализа о томе како се могу, одређене, нове технологије примењивати у кризном менаџменту.

Улога нових технологија у кризном менаџменту

Нове технологије нуде низ предности и могућности при чему је важно истаћи да анализа њихове примене има битну улогу у кризном менаџменту. „Научене лекције" помажу организацији да постане отпорнија на будуће кризе и да ефикасније управља ризицима. Анализа претходних кризних ситуација могу бити корисне у предвиђању и управљању будућим кризама (Jarrahi, 2018). Проучавање кризних ситуација које су се већ десиле могу открити обрасце који се понављају и омогућиће боље суочавање са новим изазовима. Услед све веће зависности од информационо-комуникационих технологија, ризик од сајбер напада постаје све израженији (Вулетић, Миленковић & Ђукић 2021, 2). Ове претње могу компромитовати критичне информационе инфраструктуре, што може имати катастрофалне последице током кризе (Guembe et al. 2022).

Улога нових технологија у фази превенције кризе

Када је реч о унапређивању фазе превенције кризе, оперативни кризни план са адекватном проценом ситуације је кључан за успешну превенцију потенцијалне кризе (Каровић 2015, 132). Нове технологије могу значајно унапредити способност организације да препозна потенцијалне кризне ситуације или претње пре него што се оне развију у кризу. Нове технологије омогућавају организацијама да анализирају велике количине података како би идентификовали узроке, трендове или неправилности које могу указивати на потенцијалне кризне ситуације. Ово може укључивати анализу финансијских података, друштвених медија, интерних извештаја и других релевантних

извора информација. Вештачка интелигенција се може користити за анализу података и идентификацију аномалија које могу указивати на потенцијалне кризне ситуације. Ови системи могу аутоматски препознавати неправилности или промене у подацима и упозоравати одговорне особе на потенцијалне проблеме.

Увођење нових технологија, интеграција вештачке интелигенције и квантног компјутинга (*quantum computing*), представља основу система за предвиђање (Hallaq at. al. 2017). Када су се 2019. године појавиле прве анализе Пентагона на тему развоја вештачке интелигенције, констатовано је да би такав напредак на пољу нових технологија довео не само до промене карактера рата, већ и до потпуне промене његове природе. Пример примене вештачке интелигенције се може видети у одлуци Владе Канаде која је развила „алгоритамску процену утицаја" (*Algorithmic Impact Assessment - AIA*), као алат за подршку својој „Директиви о аутоматизованом доношењу одлука" (Trilateral Research 2021, 16).

Криза у САД 2012. године изазвана ураганом „Сенди" (*Sandy*) представља добар пример како друштвене мреже доприносе бољој координацији превенције али и реакцији у кризним ситуацијама и да последице буду што мање (Eriksson & Olsson 2016). У случају кризе као што је природна катастрофа (нпр. ураган, шумски пожар или велике поплаве), авионских несрећа, саобраћајних несрећа на аутопуту, терористичког напада или великих јавних немира који укључују уништавање имовине, коришћењем мобилних апликација грађани су у могућности да примају релевантне, поуздане и правовремене информације (Svrdlin & Cvetković 2019, 169). Друштвене мреже и мобилне апликације омогућавају дистрибуцију важних информација о превентивним мерама, упутствима за поступање и контактима за хитну помоћ што је посебно важно у случају природних катастрофа, терористичких напада или других хитних ситуација где је брза реакција кључна за спашавање живота и заштиту имовине. Одређене апликације за кризне ситуације, као што су „*KATWARN*" и „*NINA*" у Немачкој, имају информативну и упозоравајућу функције што је веома значајно са аспекта превенције и информисаности грађана о могућим кризама (Kaufhold, Haunschild, Reuter 2020, 2).

Рачунарство у облаку, такође, омогућава организацијама да користе напредне технологије и ресурсе како би идентификовале, анализирале и реаговале на потенцијалне кризне ситуације пре него што ескалирају. Ова технологија може побољшати ефикасност, скалабилност и сигурност превентивних стратегија, помажући организацијама да се припреме за изазове који би могли довести до кризе.

Улога нових технологија у фази припреме

У фази припреме кризног менаџмента, нове технологије имају кључну улогу у омогућавању организацијама да ефикасно планирају и да се припреме за потенцијалне кризне ситуације. Добар пример представља систем компаније „Гоогле" (*Google*) за одговор на кризне ситуације (*Google Crisis response*). Како се наводи на званичном сајту, „од лансирања СОС упозорења у јесен 2017. године, алати које је развио тим за реаговање у кризним ситуацијама активирани су током више од 200 криза широм света, а информације о кризним ситуацијама које пружају упозорења прегледане су више од 1,5 милијарди пута" (Google Crisis Response). Примена ове технологије у фази припреме омогућавају дистрибуцију информација о кризним ситуацијама о затварању путева и мостова преко државних граница, што је од суштинске важности током кризних ситуација.

Виртуелна обука омогућава организацијама да ефикасно обуче своје особље за различите сценарије кризних ситуација. Виртуелна обука може укључивати симулације,

интерактивне тренинге и тестирања која помажу особљу да стекне практично искуство и вештине за реаговање у стварним ситуацијама. Напредни софтвери за планирање и симулацију омогућавају организацијама да развијају и тестирају различите сценарије кризних ситуација како би идентификовали слабости у њиховим плановима и процедурама. Ови алати омогућавају организацијама да боље разумеју како ће се њихови планови понашати у стварним ситуацијама и да их оптимизују пре него што дође до кризе (Murakami at al. 2002).

Европска комисија (*European Commission*) је 2018. године уочила промену у начину на који људи реагују на кризне ситуације. Уместо да одмах зову службе за спасавање, људи се често фокусирају на друштвене мреже да би делили информације и затражили помоћ (Red Cross 2024). Таква тенденција је покренула разматрање о томе како дигиталне платформе могу бити коришћене за боље управљање кризама и брже реаговање на кризне ситуације (European Commission 2018). Један од пројеката финансираних од стране Европске уније је управо развој система безбедности који повећава комуникацију између грађана и служби које реагују у кризним ситуацијама, као што су терористички напади или природне катастрофе (European Commission 2018).

У циљу ефикасне припреме користе се одређене мобилне апликације као што је нпр. апликација *READI* у Аустралији, доприноси информисаности, активном укључивању и непрекидном унапређењу мера за одговор. Нове технологије, као што су апликације за мобилне уређаје, платформе за рачунарство у облаку и алати за видео конференције, омогућавају организацијама да одрже ефикасну комуникацију са особљем, партнерима, властима и другим релевантним субјектима током кризе. Коришћење ових технологија у фази припреме кризног менаџмента омогућава организацијама да ефикасно планирају, оспособе особље и оптимизују своје процесе како би биле спремне за потенцијалне кризне ситуације. Ово омогућава бржу и ефикаснију реакцију када се криза догоди, што може значајно смањити штету и последице.

Улога нових технологија у фази реаговања

У фази реакције кризног менаџмента, нове технологије могу бити кључне за брзу и ефикасну координацију, комуникацију и решавање проблема. Примена вештачке интелигенције у фази реакције кризног менаџмента може значајно побољшати брзину, прецизност и ефикасност реакције организација на непредвиђене ситуације.

Употреба платформи за виртуелну комуникацију као што су *Skype, Zoom, Microsoft Teams* или *Slack* за брзу координацију тимова, без обзира на њихову локацију. Ове платформе омогућавају организацијама да одрже контакт и координирају активности у реалном времену. Мобилне апликације омогућавају брзу дистрибуцију важних информација, упутстава и упозорења члановима тима и другим заинтересованим странама. Ове апликације омогућавају корисницима да пријаве кризне ситуације или да пруже важне информације у реалном времену. У фази реаговања, друштена мрежа „X", може бити примењена за за праћење и идентификацију потенцијалних нових претњи (Garay-Tamajon & Roelofsen 2024).

Имајући у виду различите инфраструктуре рачунарства у облаку, као и велики број организација у приватном сектору које промовишу коришћење одређеног «клауда» због чињенице да је координација и доношење одлука током кризе најтежи и најважнији захтев за постигање успешних исхода у хитним ситуацијама, издваја се рачунарство у облаку Кејмбриџ (Cambridge International Systems Inc. 2024). Како се наводи на њиховом званичном сајту , Кејмбриџ пружа скалирани, јавно доступан систем за управљање

хитним ситуацијама и овај систем омогућује многим „федералним агенцијама, државним, локалним, племенским и територијалним владама, као и невладиним организацијама, сарадњу ради побољшања доношења одлука у одговору на кризу" (Cambridge International Systems Inc. 2024).

Рачунарство у облаку, као нова технологија, може бити корисна у фази реаговања. Једна од главних препрека за имплементацију ових система, посебно за државне органе јесте недостатак заштите података тј. безбедносни ризици употребе ове технологије (Jaeger et al. 2008). Коришћење софтверских алата за управљање пројектима које се ослањају и на рачунарство у облаку као што је нпр. *Trello* за праћење и управљање активностима везаним за реакцију на кризне ситуације омогућавају тимовима да делегирају задатке, прате напредак и идентификују проблеме који се могу појавити. Имплементација система за управљање информацијама који омогућавају организацијама да брзо прикупе, анализирају и деле кључне информације о кризној ситуацији. Ови системи могу интегрисати различите изворе података и омогућити корисницима да приступе релевантним информацијама у реалном времену.

Улога нових технологија у фази опоравка

Употреба нових технологија у фази опоравка може помоћи организацијама да брзо и ефикасно обнове своје операције, минимизирају штету и поврате нормално стање фонкционисања што је пре могуће након кризе (DesJardine, Bansal & Yang 2019). Вештачка интелигенција може значајно допринети у фазама опоравка након кризе, идентификацијом области где су потребне додатне инвестиције или унапређења како би се убрзао процес опоравка (Banasik & Pikiewicz 2023).

Коришћење рачунарства у облаку омогућава организацијама да брзо обнове инфраструктуру и ресурсе након кризне ситуације. Рачунарство у облаку пружа практично неограничен капацитет за рачунање, складиштење и мрежне услуге. Подаци и сервиси морају бити лако доступни у овој фази ради што бржег опоравка да би се обезбедио континуитет функционисања организације.

Према наводима агенције Брајтпатх (Bryghtpath), америчка агенција за управљање кризама, непрекидности пословања и комуникацијама у кризним ситуацијама је од суштинског значаја у свакој фази кризног менаџмента (Bryghtpath, Rethinking Disaster Recovery). Предност коришћења наведене технологије огледа се у брзом приступу и враћању података, што смањује време прекида рада и минимизира утицај на операције, могућност репликације целокупне инфраструктуре у облаку, обезбеђујући да се сви системи и апликације могу брзо опоравит у случају кризне ситуације (Bryghtpath, Rethinking Disaster Recovery). Различити алати за анализу података могу се користити за процену штете и утврђивање приоритета током процеса опоравка. Ови алати омогућавају организацијама да идентификују кључна подручја која захтевају хитну интервенцију и планирају ресурсе.

Закључак

Примена нових технологија, попут вештачке интелигенције, друштвених мрежа, рачунарства у облаку и мобилних апликација, у кризном менаџменту доноси значајне предности које могу побољшати способност организација у циљу превенције кризних ситуација, припреме, реаговања и опоравка. Кроз анализу података, брзу комуникацију, аутоматизацију процеса и оптимизацију ресурса, разматране технологије омогућују

организацијама да буду агилније, ефикасније и отпорније на кризне ситуације. Међутим, како би се максимално искористиле предности нових технологија, важно је континуирано улагати у обуку особља, осигурати транспарентност и одговорност у коришћењу те пажљиво размотрити сигурносне и етичке импликације. Примена нових технологија у кризном менаџменту може трансформисати начин на који организације препознају и управљају кризама, пружајући им алате и ресурсе потребне за брзу, координирану и ефикасну реакцију у тешким ситуацијама.

Важно је напоменути да примена нових технологија није сама по себи решење за све изазове у кризном менаџменту. Нове технологије могу да пруже значајну подршку у анализи података, праћењу трендова, прогнозирању ризика, и управљању ресурсима у случају кризних ситуација. Међутим, не треба занемарити улогу човека у том процесу. Нове технологије имају потенцијал да значајно допринесу ефикасности и успешности кризног менаџмента, али је њихова ефикасна примена најбоље остварљива кроз колаборацију човека и технологије, са фокусом на етичким и моралним аспектима.

Библиографија

Agiwal, Mamta, Navrati Saxena, & Abhishek Roy. 2018. "Towards Connected Living: 5G Enabled Internet of Things (IoT)." *IETE Technical Review* 36 (2): 190–202. doi:https://doi.org/10.1080/02564602.2018.1444516.

Australian Institute for Disaster Resilience. n.d. "READI - National Crisis Management Mobile Application." www.aidr.org.au. Accessed May 23, 2024. https://www.aidr.org.au/news/readi-national-crisis-management-mobile-application/.

Ayub, Al, Arumugam Mahalakshmi, K. ArulRajan, Joel Alanya Beltran, & Mohd Naved. 2022. "Integrated Artificial Intelligence Effect on Crisis Management and Lean Production: Structural Equation Modelling Frame Work." *International Journal of Systems Assurance Engineering and Management* 14 (1). Springer Science+Business Media: 220–27. doi:https://doi.org/10.1007/s13198-022-01679-1.

Banasik, Arkadiusz, & Piotr Pikiewicz. 2023. "Application of AI in Crisis Management." *Zeszyty Naukowe - Politechnika Śląska. Organizacja I Zarządzanie* 2023 (186): 9–19. https://doi.org/10.29119/1641-3466.2023.186.1 .

Boulos, Maged, Steve Wheeler, Carlos Tavares, & Ray Jones. 2011. "How Smartphones Are Changing the Face of Mobile and Participatory Healthcare: An Overview, with Example from ECAALYX." *BioMedical Engineering OnLine* 10 (1): 24. https://doi.org/10.1186/1475-925x-10-24.

Brygthpath, Navagating Resilience. n.d. "Rethinking Disaster Recovery: The Impact of Cloud Computing." Bryghtpath. Accessed May 23, 2024. https://bryghtpath.com/resources/whitepapers/rethinking-disaster-recovery-the-impact-of-cloud-computing/ .

Bundy, Jonathan, Michael D. Pfarrer, Cole E. Short, & W. Timothy Coombs. 2016. "Crises and Crisis Management: Integration, Interpretation, and Research Development." *Journal of Management* 43 (6): 1661–92. https://doi.org/10.1177/0149206316680030.

Caldarelli, Guido, Rocco De Nicola, Fabio Del Vigna, Marinella Petrocchi, & Fabio Saracco. 2020. "The Role of Bot Squads in the Political Propaganda on Twitter." *Communications Physics* 3 (1). doi:https://doi.org/10.1038/s42005-020-0340-4.

Cambridge International Systems, Inc. 2018. "About Cambridge International". Accessed May 23, 2024. https://cbridgeinc.com/about/

DesJardine, Mark, Pratima Bansal, & Yang Yang. 2017. "Bouncing Back: Building Resilience through Social and Environmental Practices in the Context of the 2008 Global Financial Crisis." Journal of Management 45 (4): 014920631770885. https://doi.org/10.1177/0149206317708854 .

Eriksson, Mats, & Eva-Karin Olsson. 2016. "Facebook and Twitter in Crisis Communication: A Comparative Study of Crisis Communication Professionals and Citizens." Journal of Contingencies and Crisis Management 24 (4): 198–208. https://doi.org/10.1111/1468-5973.12116 .

European Commission. 2018. "Real-Time Crisis Communications System Helps Save Lives | Research and Innovation." Projects.research-And-Innovation.ec.europa.eu. 2018. https://projects.research-and-innovation.ec.europa.eu/en/projects/success-stories/all/real-time-crisis-communications-system-helps-save-lives.

Google Crisis Response. n.d. "Chicago Crisis Response." Accessed May 24, 2024. https://crisisresponse.google/

Guembe, Blessing, Ambrose Azeta, Sanjay Misra, Victor Chukwudi Osamor, Luis Fernandez-Sanz, & Vera Pospelova. 2022. "The Emerging Threat of Ai-Driven Cyber Attacks: A Review." Applied Artificial Intelligence 36 (1): 1–34. https://doi.org/10.1080/08839514.2022.2037254.

Hallaq, Bilal, Tiia Somer, Anna-Maria Osula, Kim Ngo, & Timothy Mitchener-Nissen. 2017. "Artificial Intelligence within the Military Domain and Cyber Warfare." In Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS 2017), Dublin, Ireland, 29-30 June 2017.

Jacques, Attali. 2009. *A Brief History of the Future.* Reprint. Sydney: Allen and Uwin.

Jaeger, Paul T., Jimmy Lin, & Justin M. Grimes. 2008. "Cloud Computing and Information Policy: Computing in a Policy Cloud?" *Journal of Information Technology & Politics* 5 (3): 269–83. https://doi.org/10.1080/19331680802425479 .

Jaques, Tony. 2007. "Issue Management and Crisis Management: An Integrated, Non-Linear, Relational Construct." *Public Relations Review* 33 (2): 147–157. https://doi.org/10.1016/j.pubrev.2007.02.001.

Jarrahi, Mohammad Hossein. 2018. "Artificial Intelligence and the Future of Work: Human-AI Symbiosis in Organizational Decision Making." Business Horizons 61 (4): 577–86. https://doi.org/10.1016/j.bushor.2018.03.007.

Kaufhold, Marc-André, Jasmin Haunschild & Christian Reuter. 2020. "Warning the Public: A Survey on Attitudes, Expectations and Use of Mobile Crisis Apps in Germany." Paper presented at the Twenty-Eighth European Conference on Information Systems (ECIS2020), Marrakesh, Morocco.

Kaufhold, Marc-André. 2021. "Information Refinement Technologies for Crisis Informatics: User Expectations and Design Principles for Social Media and Mobile Apps". Springer Nature. https://doi.org/10.1007/978-3-658-33341-6.ž

Kaur, Ketanpreet, Shailesh Kumar, & Anupam Baliyan. 2018. "5G: A New Era of Wireless Communication." *International Journal of Information Technology*, May. doi:https://doi.org/10.1007/s41870-018-0197-x.

Lewis, Becca, & Alice E. Marwick. 2017. "Media Manipulation and Disinformation Online." Data & Society. https://datasociety.net/library/media-manipulation-and-disinfo-online/ .

Lluís Alfons Garay-Tamajón, & Maartje Roelofsen. 2024. "Tourism Content on Twitter (X) during a Crisis." *Annals of Tourism Research Empirical Insights* 5 (2): 100132–32. https://doi.org/10.1016/j.annale.2024.100132 .

McConnell, A. 2003. "Overview: Crisis Management, Influences, Responses and Evaluation." *Parliamentary Affairs* 56 (3): 363–409. https://doi.org/10.1093/parlij/gsg096.

Mitroff, Ian I., Paul Shrivastava, & Firdaus E. Udwadia. 1987. "Effective Crisis Management." *Academy of Management Perspectives* 1 (4): 283–92. https://doi.org/10.5465/ame.1987.4275639.

Morley, Jessica, Libby Kinsey, Anat Elhalal, Francesca Garcia, Marta Ziosi, & Luciano Floridi. 2021. "Operationalising AI Ethics: Barriers, Enablers and next Steps." *AI & SOCIETY*, November. doi:https://doi.org/10.1007/s00146-021-01308-8.

Murakami, Yasukazu, Kazutomo Minami, Tomoyuki Kawasoe, & Toru Ishida. 2002. "Multi-Agent Simulation for Crisis Management." *Proceedings. IEEE Workshop on Knowledge Media Networking*. https://doi.org/10.1109/kmn.2002.1115175 .

Red Cross, Talks. 2024. "Tech Talk: More Americans Using Mobile Apps - Canadian Red Cross Blog." *Red Cross Canada*. Accessed May 23. https://www.redcross.ca/blog/2012/9/tech-talk-more-americans-using-mobile-apps

Roche, Stephane, Eliane Propeck-Zimmermann, & Boris Mericskay. 2011. "GeoWeb and Crisis Management: Issues and Perspectives of Volunteered Geographic Information." GeoJournal 78 (1): 21–40. https://doi.org/10.1007/s10708-011-9423-9.

Svrdlin, Maja, & Vladimir Cvetković. 2019. "Mobilni Komunikacioni Sistemi i Aplikacije od značaja za integrisano upravljanje katastrofama." Vojno Delo 71 (7): 164–77. https://doi.org/10.5937/vojdelo1907164s.

Tavani, Herman T. 2012. *Ethics and Technology, Binder Ready Version*. Wiley.

Trilateral Research. 2022. "A Survey of AI Risk Assessment Methodologies." https://www.trilateralresearch.com/wp-content/uploads/2022/01/A-survey-of-AI-Risk-Assessment-Methodologies-full-report.pdf 19.4.2024

U. S. Government Accountability Office. 2022. "Information Environment Opportunities and Threats to DOD's National Security Mission". GAO-22-104714 Report to Congressional Addressees

Velev, Dimiter. 2014. "Challenges and Opportunities of Cloud-Based Mobile Learning." International Journal of Information and Education Technology 4, br. 1, 49-53.

Watson, Hayley, & Rowena Rodrigues. 2017. "Bringing Privacy into the Fold: Considerations for the Use of Social Media in Crisis Management." *Journal of Contingencies and Crisis Management* 26 (1): 89–98. doi:https://doi.org/10.1111/1468-5973.12150.

Zamoum, Khaled, & Tevhide Serra Gorpe. 2018. "Crisis Management: A Historical and Conceptual Approach for a Better Understanding of Today's Crises." Crisis Management - Theory and Practice, June. https://doi.org/10.5772/intechopen.76198.

Zhou, Sophia L., Jia, Xianhan, Skinner, Samuel P., Yang, William, & Claude, Isabelle. (2021). "Lessons on Mobile Apps for COVID-19 from China." Journal of Safety Science and Resilience 2, 40-49.

Вулетић, Дејан, Миленковић, Милош & Ђукић, Анђелија. 2021. „Сајбер простор као подручје сукобљавања: Случај САД – Иран и Северна Кореја". Војно дело LXXIII (1): 1-14.

Каровић, Самед. 2015. «Кризни менаџмент.» Београд: Медија Центар Одбрана. ISBN 978-86-335-0439-3 70-80.

Кешетовић, Желимир, & Срђан Милашиновић. «Кризни менаџмент и слични концепти - покушај разграничења.» Безбедност 50, br. 1-2 (2008): 37-58. ISSN 0409-2953.

APPLICATION OF NEW TECHNOLOGIES IN CRISIS MANAGEMENT

Abstract: Innovative technologies encompass a wide range of advanced tools, techniques, and systems used to solve certain problems or improve processes in different areas. They have a significant impact on all social processes, i.e., on people's everyday lives. This paper analyzes the latest technological achievements (artificial intelligence, social networks, cloud computing, mobile applications, etc.) and their impact on crisis management. The second part of this research focus with the basics of crisis management, primarily theoretical definitions, goals, and phases. The prevailing opinion in the scientific community is that crisis management can be divided into four phases: prevention phase, preparation phase, response phase, and recovery phase. The research aimed to analyze new technologies that can bring benefits to crisis management according to the phases of crisis management, thus providing additional efficiency and reliability in crisis situation resolution processes. Based on the analysis of relevant literature, case studies and professional works dealing with the application of new technologies in crisis management, in the third part of the paper, the areas of application of certain new technologies in different phases of crisis management were identified. New technologies can be key tools in improving the effects and speed of response. This paper contributes to a better understanding of how technological progress can transform the way crisis situations are managed, while also indicating that aspects of applying new technologies in crisis management are not sufficiently addressed. The research results provide a basis for further analysis of the complexity of applying new technologies in crisis management, considering that this is a new and therefore insufficiently researched phenomenon.

Keywords: innovative technologies, crisis management.

АЛГОРИТАМ ЗА УПРАВЉАЊЕ ВАНРЕДНИМ СИТУАЦИЈАМА[1]

Вања Роквић[2], Иван Р. Димитријевић[3]

Апстракт: Потреба за развојем и употребом алата вештачке интелигенције (ВИ) у области управљања ванредним ситуацијама све је већа имајући у виду константан раст природних катастрофа и њихових последица у погледу људских и материјалних губитака. Због тога су многе државе и организације почеле с увођењем алата ВИ, како би се повећали постојећи капацитети за предвиђање катастрофа и адекватног одговора на исте. На пример, ови алати користе се за рано откривање шумских пожара, за мапирање угрожености од поплава и клизишта, предикцију земљотреса, мапирање оштећених зграда након катастрофа или за правовремену припрему хитних обавештења и упозорења. Имајући у виду разноврсност алата ВИ и њихову вишеструку примену, аутори предлажу могућност њиховог обједињавања појмом „алгоритам за управљање ванредним ситуацијама" и пружају дефиницију истог. Под наведеним појмом аутори подразумевају алгоритме вештачке интелигенције изражене компјутерским кодом, који су спроведени кроз савремене технологије и способни да делују у свим фазама процеса управљања ванредним ситуацијама. На основу дате дефиниције, анализе релевантне литературе и одабраних критеријума у раду је пружен преглед одбраних алата. Посебан фокус стављен је на интерактивни алат Радар технологија будућности за смањење ризика од катастрофа, који омогућава систематско праћење и разумевање технологија будућности, као и на Humanitarian Openstreetmap Team, Ushahidi, Вештачка интелигенција за дигитални одговор и Фондација отворених извора геопросторних података. У раду је закључено да постоје многобројне предности у употреби алата ВИ, али исто тако и извесни ризици. Стога је наглашено да је неопходно да се препознају сви могући ризици како би се одговорило на њих, и уједно искористиле и унапредиле предности ових алата. Али, како је у раду закључено, увек се мора имати у виду да је човек у центру сваког система и да ови алати не могу да замене људско искуство, емоције и знање неопходно за доношење одлука у комплексним и непредвидивим ситуацијама, какве су природне и друге катастрофе.

Кључне речи: нове технологије, вештачка интелигенција, природне катастрофе, отворени извори података, управљање у ванредним ситуацијама.

---

[1] Рад је настао у оквиру научноистраживачког рада НИО за 2024. годину, које финансира Министарство науке, технолошког развоја и иновација Републике Србије. Погледи изнети у чланку одражавају личне ставове аутора, а не институције у којој су запослени.

[2] Факултет безбедности, Универзитет у Београду, vanjarokvic@fb.bg.ac.rs, https://orcid.org/0000-0002-8382-4616

[3] Факултет безбедности, Универзитет у Београду, ivan.dimitrijevic@fb.bg.ac.rs, https://orcid.org/0000-0001-9485-280X

Увод

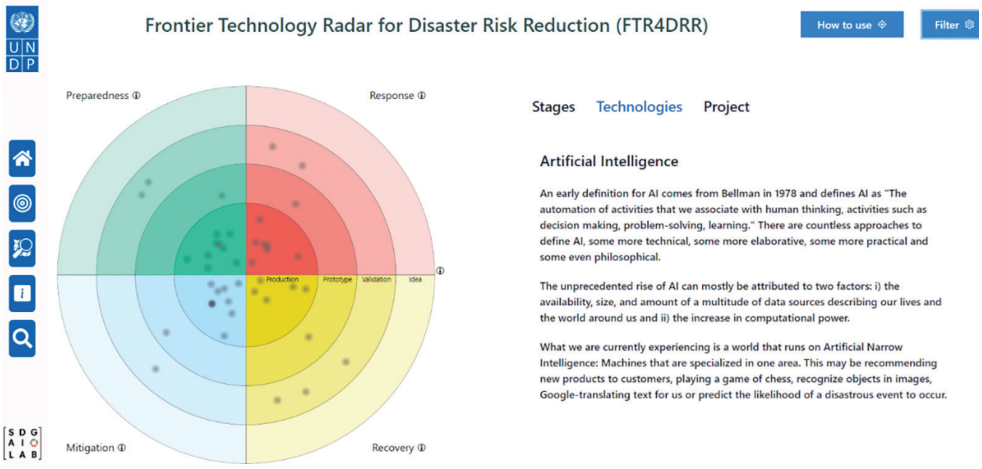
Позивајући се на податке Међународне базе података о катастрофама (The International Disaster Database, EM-DAT)[4], Канцеларија Уједињених нација за смањење ризика од катастрофа наводи да је у периоду од 1980. до 1999. године регистровано 4.212 природних катастрофа, док је та бројка у периоду од 2000. до 2019. године износила 7.348 (CRED & UNDRR 2020, 6).[5] Већи број катастрофа утицао је на веће губитке, како у људским животима, тако и у економији (слика 1), што је условило потребу за технолошким иновацијама у области управљања ванредним ситуацијама и смањењу ризика од катастрофа (UNDP & OCHA 2023).

Слика 1: Последице катастрофа (UNDRR 2020, 6)

У извештају „Иновације у управљању ванредним ситуацијама" (Innovation in Disaster Management) наводи се неколико технолошких достигнућа која су своју примену пронашла у свим фазама управљања ванредним ситуацијама (UNDP & OCHA 2023). У наведена технолошка достигнућа уврштени су 3Д штампа, вештачка интелигенција (ВИ), дронови, виртуелна стварност, географски информациони систем, интернет ствари, друштвене мреже, краудсорсинг, блекчејн технологија, комуникационе технологије, клауд технологија, сателити и сензори (UNDP & OCHA 2023, 11-12). Као резултат овог извештаја развијен је и 2022. године покренут интерактивни алат под називом Радар технологија будућности за смањење ризика од катастрофа (Frontier Technology Radar for Disaster Risk Reduction, FTR4DRR), који прати развој нових технологија и врши њихову категоризацију у односу врсту технологије, врсту катастрофе/кризе и фазу управљања ванредном ситуацијом (слика 2).

[4] База је отвореног приступа. Опширније у: (EM-DAT 2023).

[5] Из извештаја су искључени подаци о техничко-технолошким катастрофама, али се претрагом базе података може видети да их је само у периоду од 2000. до 2019. године било 5.142 (EM-DAT 2023).



Слика 2: Радар технологија будућности за смањење ризика од катастрофа (FTR4DRR 2024)

Имајући у виду растући утицај вештачке интелигенције у свим сферама друштвеног живота и рада, или како то поједини аутори кажу, будући да живимо у „златно доба вештачке интелигенције" (Alruqi and Aksoy 2023; Kaynak 2021), у овом прегледном раду фокусираћемо се на приказ алата базираних на вештачкој интелигенцији и отвореним изворима података, који су своју примену нашли у стварним кризним ситуацијама и катастрофама.

Употреба вештачке интелигенције у ванредним ситуацијама

У анализи 100 научних и стручних студија о примени алата ВИ коју су спровели Камран Абид и сарадници (Abid et al. 2021), наводи се да се алати ВИ јављају у многобројним облицима (попут машинског учења, дубоког учења, софтвера, роботике, дронова, сензора и слично) и да су „знатно повећали наше капацитете за предвиђање катастрофа и пружање подршке током катастрофа" (Abid et al. 2021, 6). Ови алати своју примену су пронашли у мапирању угрожености од поплава и клизишта, предикцији поплава и земљотреса, детекцији пожара, мапирању оштећених зграда након катастрофа и друго (Abid et al. 2021).

Слично истраживање спровели су и Сун, Бокини и Дејвисон (Sun, Bocchini and Davison 2020), који су у свом раду анализирали примену 27 алата (попут One Concern, CrissisMappers, Dataminr и других), у свим фазама управљања ванредним ситуацијама, и дошли до закључка да су анализирани алати „веома корисни" за управљање ванредним ситуацијама. Њихова корист, како наводе Гафариан и сарадници (Ghaffarian et al. 2023), огледа се у унапређењу способности за идентификацију и предикцију могућих катастрофа, мапирању угрожених подручја, процени оштећења, као и смањењу ризика од катастрофа. Уједно, алати вештачке интелигенције, захваљујући пруженим информацијама у реалном времену, утичу на процес доношења одлука, приоритизовању акција и ефикаснијем распоређивању ресурса. Као један од примера ови аутори наводе примену алгоритама машинског учења на сателитским снимцима у сврху предикције

ширења пожара, а самим тим и раног упозорења и адекватног одговора на новонасталу ситуацију (Ghaffarian et al. 2023).

Преглед доступних ВИ алата и њиховог потенцијала за ублажавање последица катастрофа изазваних климатским променама пружила је и ауторка Динева (Dineva 2023) која је мапирала досадашње напоре и пројекте у овој области. Она је у свом прегледном раду направила пресек домета употребе ВИ алата за борбу против последица климатских промена, који обухвата три кључне области – ублажавање последица, прилагођавање и развој отпорности и базична питања (истраживање климе и моделирање). Након тога је, на основу проучене доступне литературе, пре свега рада Махера и сарадника (Maher et al. 2022), пружила преглед кључних области у којима ВИ може да се користи: 1) прикупљање, комплетирање и обрада података, 2) подршка планирању и доношењу одлука, 3) оптимизација процеса, 4) подршка колаборативним екосистемима, 5) охрабривање понашања која позитивно утичу на климатске промене. Такође, код употребе ВИ у конкретним кризама као што су хуманитарне, поједини аутори предлажу алгоритме засноване на Large Language Model (LLM) и GPT-2 у контексту пружања психолошке подршке и савета жртвама ових врста криза (Aradhana et al. 2024). Поред тога, код геопросторних података које прикупља ВИ, више аутора направило је преглед доступних алгоритама и њихове употребне вредности за специфичне катастрофе и кризе (Ivić 2019; Kemper & Kemper 2020).

Поред многобројних научних и стручних радова који се баве овом тематиком, постоје и пројекти посвећени примени ВИ у управљању ванредним ситуацијама, попут **ARTION (Disaster Management Artificial Intelligence Knowledge Network), из којег је произашао портал** - Disater Managament AI Portal (ARITON 2024), затим пројекти Европске комисије (Extreme HP, TEMA, CREXDATA) (TEMA 2024), или пак отворене базе и програми попут NASA's Earth Science Data Systems (ESDS) Program, који захваљујући приступу сателитским снимцима и многобројним развијеним алатима даје вишеструке могућности у управљању ванредним ситуацијама (EARTHDATA 2023). Уједно, и анализа напред поменутог Радара пружила нам је увид у многобројне доступне алате базиране на ВИ, попут WG5 Geo-AI, Robotics for Good, Sealr, Terai Cross-Border Flood Early Warning System, C Bot ChatBot, Ignitia, ConvNetQuake, Ushahidi, 4W Wizard, DiCRA... (FTR4DRR 2024).

Имајући у виду разноврсност алата вештачке интелигенције, у овом раду определили смо се да у њиховом представљању и опису користимо заједнички именитељ - „алгоритам за управљање ванредним ситуацијама". Разлог за овај избор лежи у чињеници да се овај појам увелико примењује у оквирима наука безбедности, па се тако употреба алата вештачке интелигенције у савременим оружаним сукобима назива „алгоритмом ратовања". Аналогно постојећим дефиницијама у наукама безбедности (Lewis et al. 2016), алгоритам за управљање ванредним ситуацијама могли бисмо дефинисати као алгоритме вештачке интелигенције изражене компјутерским кодом, који су спроведени кроз савремене технологије (софтвер, веб и мобилне апликације, дрон, сензор, сателит и друго) и способни да делују у свим фазама процеса управљања ванредним ситуацијама.

Међутим, поставило се питање које критеријуме користити за анализу и представљање алата ВИ у овом раду. Након анализе релевантне литературе, доступних пројеката и програма, као критеријуме користили смо следеће: да су алати јавно доступни, да се употребљавају у различитим фазама управљања, да су примењени у стварним ситуацијама, и да их могу користити како државне институције и релевантне организације из области управљања ванредним ситуацијама, тако и појединци.

Имајући у виду и ограничења у писању рада у погледу обима, у наредном тексту представићемо следеће изабране алате: Humanitarian Openstreetmap Team, Ushahidi, Вештачка интелигенција за дигитални одговор (Artificial Intelligence for Digital Response) и Фондација отворених извора геопросторних података (Open Source Geospatial Foundation). Свакако, прво ћемо се осврнути на Радар технологија будућности за смањење ризика од катастрофа, као алат који омогућава систематско праћење и разумевање технологија будућности. Уједно, у раду ће бити представљене предности, али и недостаци алата вештачке интелигенције.

Радар технологија будућности за смањење ризика од катастрофа

Радар технологија будућности је онлајн апликација која „омогућава систематско праћење и разумевање такозваних технологија будућности (Frontier Technologies) током њиховог развоја" (FTR4DRR 2024), а у контексту праћења ванредних ситуација/катастрофа и конфликата/криза широм света. Замисао је да овај алат „охрабри размену знања и идеја међу учесницима у његовом развоју како би се технологије будућности употребљавале у контекстима катастрофичних догађаја или конфликата" (FTR4DRR 2024). Крајњи циљ употребе ових технологија је „указивање на потенцијал технолошких решења у катастрофама свима који се баве смањењем ризика, одговором на катастрофу и обновом након катастрофе" (FTR4DRR 2024). Овај алат је такође замишљен као подршка онима који су учествовали у његовом развоју, да пронађу употребну вредност постојећих и нових технологија у овој области.

Алат је развијен кроз сарадњу једне међународне организације и приватне иницијативе. У оквиру Бироа за кризе Програма за развој Уједињених нација (UNDP Crisis Bureau) постоји Тим за изградњу отпорности кроз смањење ризика од катастрофа и обнову (Disaster Risk Reduction and Recovery for Building Resilience Team) који „обезбеђује интегрисану политику и програмску подршку смањењу ризика од катастрофа и обнови након катастрофа у контексту стратегијског приступа UNDP-а спречавању криза и повећању отпорности" (FTR4DRR 2024). Посебан задатак овог тима јесте „подстицање свеобухватног увођења смањења ризика као кључног елемента одрживог развоја и опоравка након катастрофа на националном, регионалном и секторском нивоу, уз усмеравање на интегрисане приступе прилагођавању климатским променама" (FTR4DRR 2024).

Друга организација која учествује у развоју овог алата је Лабораторија за циљеве одрживог развоја и вештачку интелигенцију (SDG AI Lab) тимова Бироа за подршку политикама и програмима UNDP-а (UNDP BPPS), чија је мисија употреба технологија будућности, конкретно вештачке интелигенције (ВИ), машинског учења и географских информационих система у сврху остваривања циљева одрживог развоја (FTR4DRR 2024). Лабораторија се бави истраживањем, развојем и саветовањем у областима технологија будућности и одрживог развоја. Такође, она пружа подршку Програму за развој Уједињених нација у погледу јачања напора на унапређењу захтева за дигитална решења у овој области и у томе јој помаже група волонтера из области научне употребе података.

На крају, у развоју Радара велику улогу има иницијатива Connecting Business (CBi) која повезује приватни сектор пре, током и након катастрофа и ванредних ситуација тако што координисано унапређује обим и ефикасност одговора и процеса обнове након катастрофа. Чланице мреже ове иницијативе су у последњих осам година реаговале

на укупно 159 различитих криза и искористиле су укупно 115 милиона америчких долара и помогле 51 милиону људи током катастрофа (CBi 2023). Мрежа коју захвата ова иницијатива покрива преко 4.000 компанија које имају приступ ка више од 40.000 микро, малих и средњих предузећа (FTR4DRR 2024). Ова иницијатива такође редовно дели чланицама иновативне методе како би их информисала о томе шта су последња технолошка решења у овој области.

Радар функционише тако што се на визуализацији радара (слика 2) прелази преко тачака које представљају појединачне технологије за четири фазе смањења ризика од катастрофа – приправност, одговор, ублажавање последица и обнову након катастрофе. Након одабира жељене технологије или апликације добијају се детаљне информације о њеним могућностима тако што су представљене следеће кључне карактеристике: обухват циљева одрживог развоја, кратки опис, технологија коју користи (ВИ, ГИС итд), врста катастрофе, употребна вредност апликације, веза са Уједињеним нацијама, партнерске организације, врста података, тема коју покрива, линк ка сајту апликације и година у којој је апликација успостављена.

Такође, Радар може да се претражује и преко конкретнијих параметара како би се уштедело време због великог броја обухваћених апликација и технологија. Сужавање претраге апликација може се извршити преко опције „Stages" односно фаза, где су апликације груписане у односу на то коју фазу смањења ризика од катастрофа покривају. Након одабира фазе, корисник бира једну од четири опције у зависности од тога који ниво апстракције/конкретизације апликација покрива: идеју, валидацију, прототип или продукцију. На крају, Радар омогућава додатно сужавање претраге доступних технологија и апликација за смањење ризика од катастрофа преко опције филтрирања (Filter) која нуди претрагу технологија на основу прикупљања података, анализе података, сајбер система, ГИС-а, четбот апликација, ВИ, обраде природног језика и других релевантних категорија. Од осталих параметара, Радар нуди одабир покривеног региона, државе, врсте катастрофе, теме коју покрива, циљева одрживог развоја и типа података коју садржи. Временски период који је обухваћен Радаром је од 2005. године до данас.

Приказ одабраних алата ВИ за управљање ванредним ситуацијама

Као што смо навели у уводном делу рада, постоји мноштво алата базираних на ВИ и отвореним изворима података, али смо се у овом раду, а на основу прегледа литературе и претходно дефинисаних критеријума, определили за приказ четири алата: Humanitarian Openstreetmap Team, Ushahidi, Вештачка интелигенција за дигитални одговор и Фондација отворених извора геопросторних података.

Humanitarian OSM Team

Пројекат OpenStreetMap (OSM) настао је 2004. године са циљем формирања отворених база са геопросторним подацима и креирања дигиталних мапа. Будући да се пројекат реализује на волонтерској основи, многобројни аутори га називају и Википедија мапа (Palen et al. 2015; Herfort et al. 2021). Иницијално, овај пројекат је настао ради мапирања улица, путева, бициклистичких стаза, приступа за особе које користе инвалидска колица и слично.[6] Међутим, све већи број природних катастрофа

[6] Као што је то случај и у Србији. Видети: (Open Street Map 2024).

и последица које остављају, указао је на могућност, али и на потребу коришћења ових алата у одговору на катастрофе.

Према писању Содена и Пален (Soden and Palen 2014) прва примена OSM у хуманитарне сврхе забележена је 2009. године у одговору на тропску олују на Филипинима, да би након земљотреса на Хаитију 2010. године дошло до значајног помака у коришћењу овог алата. Он је коришћен како би се израдила основна мапа главног града Порт о Пренса, за коју се наводи да је била толико свеобухватна да су је тимови за потрагу и спасавање преузимали како би могли обавити свој посао. Након земљотреса формиран је Humanitarian OSM Team (HOT) као међународни тим волонтера који израђује мапе за област катастрофа и резилијентности на климатске промене, одрживих градова и заједница, јавног здравља, миграција и родне равноправности (HOT 2024).

Алат, односно, бесплатни и отворени софтвер који се користи за координацију волонтера и организовање група за мапирање назива се HOT Tasking Manager (Herfort et al. 2021). Након што до катастрофе дође, мобилишу се волонтери који користећи сателитске снимке са OSM, снимке начињене дроновима у оквиру HOT OpenAerialMap и геопросторне податке, креирају отворене мапе (OpenAeriallMap 2024). Оне садрже податке о инфраструктури, попут података о путевима, склоништима, зградама, путевима за евакуацију, али и податке о здравственим установама, доступности воде и хране и свим осталим подацима неопходним за планирање и координисање одговора на ванредну ситуацију. У оквиру HOT имплементирано је машинско учење као помоћ у креирању пројеката и додели задатака, као и мапирање уз помоћ ВИ. У питању је fAlr алат који на основу сателитских снимака и снимака дронова даје предлог елемената/карактеристика које треба унети у мапе. Уједно, 2018. године HOT је у сарадњи са Фејсбуком покренуо иницијативу MapWithAI, односно алат који захваљујући сателитским снимцима и RapiD алату за уређивање, предвиђа и црта потенцијалне путеве и генерише слике бољег квалитета како би их волонтери могли користити (Rapid 2024). Од 2019. године MapWithAI генерисао је мапе за готово све државе (Clark 2023).

Ushahidi

Ushahidi представља отворену веб платформу за мапирање у реалном времену, на основу информација са ознакама локације, времена и датума, које путем текстуалних порука, друштвених мрежа, имејлова, фотографија, видео и аудио записа и коментара, достављају грађани. Ова платформа настала је Top of Formca циљем мапирања информација о кршењу људских права након избора у Кенији 2008. године. Наиме, и сама реч *ushahidi* на свахилију значи „сведочење" или „сведок", а првобитна суштина платформе била је да грађани пријаве случајеве насиља које би иначе, према писању Киреа и сарадника (Kirea et al. 2018), прошло незапажено, како од стране медија, тако и од других релевантних организација. Потом би пријављени инциденти били постављени на Гугл мапама. Првобитно мапирање радила је група волонтера, да би убрзо непрофитна компанија Ushahidi Inc. развила бесплатан софтвер за прикупљање информација, њихову визуализацију и интерактивно мапирање (Ushahidi 2023a).

Своју прву примену, у контексту ванредних ситуација, Ushahidi је нашао након разорног земљотреса на Хаитију 2010. године. Једна од најзначајнијих активности ове платформе била је Мисија 4636 (Munro 2012). Ова мисија подразумевала је могућност слања бесплатних текстуалних порука путем којих би грађани указали на своје потребе и локацију, што је омогућило ефикасније пружање помоћи на терену. Група волонтера преводила је садржај порука, потом би се на основу података из локације путем ГПС

утврђивале тачне координате, а на крају, захваљујући отвореним мапама, мапирале локације и мапе постављале на haiti.ushahidi.com и достављале организацијама на терену (Norheim-Hagtun and Meier 2010).

Након 2010. године платформа се шири и примењује у великом броју држава, као нпр. у Италији где је коришћена ради спречавања и контролисања шумских пожара, након земљотреса на Новом Зеланду 2011. године, земљотреса у Непалу 2015. године, али и током катастрофалних поплава у Србији 2014. године. Наиме, сајт poplave.rs заснован је на Ushahidi платформи и пружао је велики број информација у реалном времену о ситуацији и потребама на терену (Lazarević 2017). Уједно, на захтев Центра за кризни менаџмент и пружање хуманитарне помоћи (The Center for Excellence in Disaster Management and Humanitarian Assistance), организације америчког Министарства одбране, Ushahidi је изградио платформу за припрему за катастрофе у региону Азија-Пацифик (Ushahidi 2023b).

Данас Ushahidi има широку примену, не само у контексту пружања помоћи након катастрофа, већ и за надгледање избора, пријаву сексуалног насиља, пријаву корупције, полицијске бруталности и слично. Уједно, оно што је значајно са аспекта теме овог рада, софтвер се константно унапређује и данас користи алате ВИ како би се информације брже прикупиле, анализирале и дистрибуирале корисницима.

Вештачка интелигенција за дигитални одговор (Artificial Intelligence for Digital Response, AIDR)

AIDR представља бесплатно доступну и отворену платформу „која филтрира и класификује објаве на друштвеним мрежама које се односе на ванредне ситуације, катастрофе и хуманитарне кризе" (AIDR 2024). Платформа се заснива на активности људске и машинске интелигенције која је у стању да аутоматски препозна на хиљаде релевантних објава током једног минута. Идеја која је окосница развоја ове платформе је заснована на томе да човек не може самостално да обради толику количину објава на друштвеним мрежама у кратком временском периоду, док су с друге стране, ти подаци превише комплексни и садржајни да би их рачунари успешно обрадили. У том смислу, AIDR комбинује људску и машинску интелигенцију у процесу прикупљања и филтрирања поменутих података у реалном времену. Платформу је развио Катарски институт за компјутерска истраживања (Qatar Computing Research Institute, QCRI) Универзитета Хамад Бин Калифа из Катара, уз партнерство с Канцеларијом УН за координацију хуманитарних послова (UN Office for the Coordination of Humanitarian Affairs, UN OCHA). Носилац пројекта је Патрик Мејер (Patrick Meier) из поменутог института.

Што се тиче корисника ове платформе, она је једноставна за употребу свакоме ко учествује у решавању хуманитарних криза или у реаговању на природне катастрофе, а упознат је с базичним функционисањем друштвених мрежа као што је Твитер. За просечног корисника ове друштвене мреже потребно је познавање кључних речи и израза везаних за дату кризу или катастрофу, као и прецизно филтрирање погођене географске области или конкретне државе. Након почетка прикупљања података на основу задатих параметара, потребно је додатно филтрирати прикупљене објаве – конкретно помоћу фокусирања на област од тренутног интереса – „лекови", „медицинска помоћ", „храна", „склониште" и слично, у зависности од тога чиме се корисник конкретно бави на терену.

Први корак подразумева прикупљање објава на Твитеру које се директно односе на дату кризу или катастрофу. Опција „Прикупљач" (Collector) затим филтрира објаве

на основу задатих кључних речи и израза, што је слично стандардним параметрима за претрагу Твитера (нпр. „ураган", „земљотрес" и слично). Због тога што је количина резултата у овим опште задатим појмовима огромна, укључује се и опција „Обележивач" (Tagger) која додатно фокусира претрагу на конкретне проблеме у датој кризи или катастрофи (нпр. „инфраструктура", „помоћ", „средства" и слично). Заједно, обе поменуте опције фокусирају претрагу на конкретну локацију, кризни догађај и потребе, чиме се у реалном времену мапирају најбитније и најхитније ситуације на које је потребно реаговати.

Платформа AIDR у пракси је више пута коришћена и тестирана у различитим кризама и катастрофама. Током земљотреса у Пакистану 2013. године, платформу је први пут користио сам аутор платформе, Патрик Мејер, који је користио два алата која је развио за прикупљање и филтрирање података о самом догађају са друштвене мреже Твитер (Collins 2013). Ови алати омогућили су стварање јасне слике о хитним потребама у погођеним областима и тиме демонстрирали могућности и домете платформе у катастрофама. Прва права провера платформе у реалној ситуацији одиграла се 2014. године током земљотреса и цунамија на обали Чилеа (Meier 2015:104-105). Након провере платформе у реалним ситуацијама, она је у сарадњи са УНИЦЕФ-ом коришћена за аутоматизовано пружање савета и информација младима о ширењу вируса HIV у Замбији и другим афричким државама, преко УНИЦЕФ-ове СМС апликације U-Report. Платформа AIDR је у овом случају аутоматски класификовала текстуалне поруке у реалном времену и свим групама истих порука прослеђивала брзе и релевантне одговоре (Meier 2015:108, Nowogrodzki 2016).

Фондација отворених извора геопросторних података (Open Source Geospatial Foundation - OSGeo)

OESgeo је непрофитна, невладина организација, основана 2006. године са циљем развоја отворених геопросторних технологија и података. Заправо, како наводе Котсе и сарадници (Coetzee et al. 2020, 4), OESgeo је кровна организација за „пројекте који се постали основа екосистема отвореног софтвера за геопросторне податке". Имајући у виду да су, како то пишу Гавана и сарадници (Ghawana et al. 2021, 2) „геопросторне технологије неопходан алат за све фазе управљања ванредним ситуацијама", будући да се овим технологијама добијају неопходни подаци о терену, инфраструктури, густини насељености угрожених подручја, није ни чудно то што су под окриљем ове кровне организације развијени многобројни софтвери. Могу се користити као десктоп апликације (GRASS GIS, gvSIG , Marble, Orfeo ToolBox, QGIS, Giswater, Opticks, OSGeo4W, GET-IT), мобилне апликације (Geopaparazzi и QField) или за веб мапирање (degree, GeoMoose, GeoNode, GeoServer, MapBender, MapServer, OpenLayers, pygeoapi, PyWPS, и други). Поред наведених, у оквиру организације постоје и други софтвери, иницијативе, као и базе података (OESgeo 2024).

Будући да не постоји могућност да се представе све наведене технологије, у овом раду укратко ћемо приказати GeoNode, систем за управљање геопросторним садржајем, односно платформу за управљање и објављивање геопросторних података. Другим речима, GeoNode представља веб апликацију, односно софтвер отвореног кода који омогућава корисницима приступ, дељење и визуализацију геопросторних података. Овај софтвер има широку примену у управљању ванредним ситуацијама и на његовој основи развијени су многобројни алати. Тако је на основу овог софтвера развијен Innovation Lab GeoNode, односно, отворени извори података за разумевање кata-

строфа. GeoNode је имплементиран и у GeoSafe, веб платформу која омогућава онлајн коришћење InaSAFE софтвера отвореног кода. Овај софтвер симулира реалистичне сценарије природних катастрофа и њихових последица, како би се на основу добијених информација извршило планирање, припрема и одговор на њих (GeoNode 2022).

Своју примену GeoNode је нашао и у IHP-WINS (The **Intergovernmental Hydrological Programme›s Water Information Network System), систему намењеном дистрибуцији података везаних за воду међу државама и организацијама укљученим у управљање водним системима. Поред наведених примена,** GeoNode су имплементирале и многе државе (Хаити, Малави, Шри Ланка, Јапан и друге) и региони у циљу управљања ванредним ситуацијама и смањења ризика од катастрофа. Неке од примена јесу PaRIS (Pacific Risk Information Systems), систем који обухвата највећи скуп геопросторних података за регион острвских држава у Пацифику. Основна намена овог система јесте да владама и релевантним организацијама пружи информације о вероватноћи да ће се нека катастрофа десити, попут тропског циклона (ветар, надолазеће олује и киша) и земљотреса (цунамија), како би се адекватно припремили и одговорили на њих (GeoNode 2022).

Предности и изазови примене алгоритма за управљање ванредним ситуацијама

Као што смо навели у претходним деловима рада, истраживања употребе алата ВИ у ванредним ситуацијама, као и анализа одабраних алата, указали су на многобројне предности које ови алати носе са собом. Према истраживању Гафариана и сарадника (Ghaffarian et al. 2023), алати базирани на ВИ унапредили су способност предиктивне анализе (ширења пожара, поплава и сл.) и доприносе бољој идентификацији угрожених подручја. Ови аутори даље наводе да алати ВИ доприносе процесу одлучивања кроз пружање информација у реалном времену које могу помоћи тимовима на терену да приоритизују акције и ефикасно распореде ресурсе. Уједно, потреба ВИ за анализу геопросторних података може допринети у анализи обима штете након катастрофе (Ghaffarian et al. 2023). Поред наведеног, према Велеву и Златевој (Velev and Zlateva 2023) алати ВИ доприносе и брзој и прецизној анализи велике количине података из различитих извора (сателитски снимци, друштвени медији, метеоролошки подаци и друго). Ови аутори предвиђају да ће у скоријој будућности ови алати имати важну улогу у управљању ванредним ситуацијама и одговору на катастрофе, нарочито у погледу побољшане предикције и система за рано упозорење, аутоматизоване процене оштећења, повећане употребе дронова, персонализоване комуникације са угроженим грађанима, побољшане алокације ресурса, али и сарадње и комуникације (Velev and Zlateva 2023).

Међутим, нове технологије одувек су представљале „мач са две оштрице". Поред предности које пружају у управљању ванредним ситуацијама, постоје и многобројни изазови које ове технологије носе са собом. Као један од највећих изазова аутори наводе квалитет и квантитет доступних података, али и њихове тачности (Alruqi and Aksoy 2023;Velev and Zlateva 2023). Као изазови у примени ових алата наводе се и етичка и правна питања, односно питања приватности и безбедности у контексту анализе личних података грађана. Код изазова мора се сагледати економски аспект и аспект техничке експертизе, будући да развој, одржавање и имплементација захтевају значајна финансијска средства и знање (Velev and Zlateva 2023).

Мора се узети у обзир и чињеница да ВИ алати не представљају универзална решења за свако питање и проблем у области управљања ванредним ситуацијама. Ови алати

могу бити осетљиви на контекст, па ако су тренирани на једном сету података или за одређену врсту катастрофа, они неће ефикасно радити у новим или непредвиђеним околностима. Друго, подаци којима се ови алати „хране" и „тренирају" статистички не могу да покрију апсолутно сваку могућу ситуацију, што даље имплицира да неће увек бити у стању да пруже стопостотно адекватно решење (Velev and Zlateva 2023). Оно што се морати увек имати на уму јесте чињеница да ови алати не могу да замене људско искуство, емоције и знање неопходно за доношење одлука у комплексним и непредвидивим ситуацијама. Људски фактор је кључан за интерпретацију резултата, доношење одлука и координацију активности, као и за процес надзора и контроле над употребом ових алата.

Закључак

Током година знатно се повећао број природних катастрофа што је за последицу имало и веће људске и материјалне губитке. Стога се јавила и потреба за технолошким иновацијама у области управљања ванредним ситуацијама и смањењу ризика од катастрофа. У том смислу данас су нам на располагању многобројне нове технологије попут сателита, сензора, дронова, вештачке интелигенције, друштвених мрежа и других, које су знатно повећале постојеће капацитете за предвиђање катастрофа и адекватног одговора на исте.

Имајући у виду да употреба ВИ представља својеврсни нови стандард у области управљања ванредним ситуацијама, у овом прегледном раду фокусирали смо се да на основу анализе релевантне литературе и дефинисаних критеријума, прикажемо одабране алате ВИ које смо у складу са њиховом применом у области безбедности назвали - алгоритам за управљање ванредним ситуацијама. Тако су у раду, поред изузетно значајног интерактивног алата Радар технологија будућности за смањење ризика од катастрофа, који омогућава систематско праћење и разумевање такозваних технологија будућности, представљени Humanitarian Openstreetmap Team, Ushahidi, Вештачка интелигенција за дигитални одговор и Фондација отворених извора геопросторних података.

На основу анализе одабраних алата, али и релевантне литературе и истраживања из ове области, можемо закључити да постоје многобројне предности њихове употребе у управљању ванредним ситуацијама, од предикције катастрофе, анализе велике количине података из различитих извора до олакшавања процеса одлучивања. Међутим, мора се имати у виду да нове технологије носе са собом и извесне ризике. Они се огледају у зависности од тачности података, генерализовања, осетљивости на контекст, као и разних економских, етичких и правних питања.

Стога је за њихов развој потребно приступати из више различитих научних дисциплина што увећава могућности за правовремено уочавање потенцијалних недостатака у перформансама ових алата. Важно је да се препознају сви могући изазови које алгоритми носе са собом, како би се одговорило на њих, и уједно искористиле и унапредиле њихове предности у управљању ванредним ситуацијама. На крају, оно што се увек мора имати у виду јесте да је ипак човек у центру сваког система, и да ови алати не могу да замене људско искуство, емоције и знање неопходно за доношење одлука у комплексним и непредвидивим ситуацијама, какве су природне и друге катастрофе.

Библиографија

Abid, Sheikh Kamran, et al. 2021. "Toward an integrated disaster management approach: how artificial intelligence can boost disaster management". *Sustainability*. 13(22):12560.

AIDR. 2024. "Artificial Intelligence for Digital Response". Accessed 09 May 2024. https://aidr.qcri.org/

Alruqi, Salman Asma and Sabih Mehmet, Aksoy. 2023. "The Use of Artificial Intelligence for Disasters". *Open Journal of Applied Science*. 13(5):731-738.

Aradhana, R., A. Rajagopal, V. Nirmala, and Immanuel Johnraja Jebadurai. 2024. "Innovating AI for humanitarian action in emergencies". In *First International Conference on Addressing Socioethical Effects of Artificial Intelligence*. Accessed 11 May 2024. https://openreview.net/attachment?id=CLJxxqSKNJ&name=pdf

ARITON. 2024. "Disater Managament AI Portal". Accessed 15 April 2024. https://www.kios.ucy.ac.cy/ARTION/disaster-management-ai-portal/

Clark, Ben. 2023. "Available Countries". Accessed April 29 2024. https://github.com/facebookmicrosites/Open-Mapping-At-Facebook

Coetzee, Serena, Ivana Ivánová, Helena Mitasova, and Maria Antonia Brovelli. 2020. "Open geospatial software and data: A review of the current state and a perspective into the future." *ISPRS International Journal of Geo-Information* 9(2): 90.

Collins, Katie. 2013. "How AI, Twitter and digital volunteers are transforming humanitarian disaster response". *Wired*. Accessed 10 May 2024. https://www.wired.com/story/digital-humanitarianism/

Connecting Business Initiative (CBi). 2023. Accessed 14 May 2024. https://www.connectingbusiness.org/

CRED and UNDRR. 2020. "The human cost of disasters: an overview of the last 20 years (2000-2019)". Accessed 17 April 2024. https://www.undrr.org/publication/human-cost-disasters-overview-last-20-years-2000-2019

Dineva, Snezhana. 2023. "Applying artificial intelligence (AI) for mitigation climate change consequences of the natural disasters". *Research Journal of Ecology and Environmental Sciences.* 3(1):1–8.

EARTHDATA. 2024. "Data Tools". Accessed https://www.earthdata.nasa.gov/learn/use-data/tools

EM-DAT The Internationa Disaster Database. 2023. "Inventorying Hazards & Disasters Worldwide Since 1988". Accessed 25 April 2024. https://www.emdat.be/

FTR4DRR. 2024. "Frontier Technology Radar for Disaster Risk Reduction". Accessed 13 May 2024. https://drrtechradar.org/#/radar

GeoNode. 2022. "Geo Node Gallery". Accessed 16 May 2024. https://geonode.org/gallery/

Ghaffarian, Saman, et al. 2023. "Explainable artificial intelligence in disaster risk management: Achievements and prospective futures". *International Journal of Disaster Risk Reduction*. 98:104123

Ghawana, Tarun, Lyubka Pashova, and Sisi Zlatanova. 2021. "Geospatial Data Utilisation in National Disaster Management Frameworks and the Priorities of Multilateral Disaster Management Frameworks: Case Studies of India and Bulgaria". *ISPRS International Journal of Geo-Information* 10 (9): 610

Herfort, Benjamin et al. 2021. "The evolution of humanitarian mapping within the OpenStreetMap community". *Scientific reports*. 11(1): 3037.

HOT. 2024. "Humanitarian OpenStreetMap Team". Accessed 12 April 2024. https://www.hotosm.org/

Ivić, Majda. 2019. "Artificial intelligence and geospatial analysis in disaster management". *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*. 42: 161-166.

Kayanak, Okyay. 2021. "The golden age of Artificial Intelligence". *Discover Artificial Intelligence.* 1(1):1-7.

Kemper, Hannah & Gehard Kemper, G. 2020. "Sensor fusion, GIS and AI technologies for disaster management". *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*. 43: 1677-1683.

Kirea, Abraham Njeru et al. 2018. "Contribution of social media platforms in conflict management: Case of Ushahidi Platform in Kenya". *International Academic Journal of Information Sciences and Project Management*. 3(2): 364-377.

Lazarević, Varvara. 2017. "Ushahidi platforme kao svedok vremena i građanskog aktivizma". *Infoteh Jahorina*. 16:259-264.

Lewis, A. Dustin et al. 2016. "War-Algorithm Accountability". Harv. L. Sch. Program on Int'l L. & Armed Conflict (PILAC). Accessed 04 May 2024. https://pilac.law.harvard.edu/aws#:~:text=We%20define%20%E2%80%9Cwar%20algorithm%E2%80%9D%20as,in%20relation%20to%20armed%20conflict.

Maher, Hamid et al. 2022. "How AI Can Be a Powerful Tool in the Fight Against Climate Change". Boston Consulting Group. Accessed 18 May 2024. https://web-assets.bcg.com/ff/d7/90b70d9f405fa2b67c8498ed39f3/ai-for-the-planet-bcg-report-july-2022.pdf

Meier, Patric. 2015. *Digital Humanitarians: How Big Data is Changing the Face of Humanitarian Response*. Boca Raton: CRC Press.

Munro, Rob. 2012. "Mission 4346 Report". Accessed 11 May 2024. https://www.mission4636.org/

Norheim-Hagtun, Ida, and Patrick, Meier 2010. "Crowdsourcing for crisis mapping in Haiti". *Innovations: Technology Governance Globalization.* 5(4): 81.

Nowogrodzki, Anna. 2016. "AI helps answer thousands of health queries in Zambia via SMS". *NewScientist*. Accessed 09 May 2024. https://www.newscientist.com/article/2083044-ai-helps-answer-thousands-of-health-queries-in-zambia-via-sms/

OESGeo. 2024. "The Open Source Geospatial Foundation". Accessed 11 April 2024. https://www.osgeo.org/

Open Street Map. 2024. "Srbija". Accessed 30 April 2024. https://openstreetmap.rs/?pismo=lat

OpenAeriallMap. 2024. "The open collection of aerial imagery". Accessed 20 April 2024. https://openaerialmap.org/

Palen, Leysia et al. 2015. "Success & scale in a data-producing organization: The socio-technical evolution of OpenStreetMap in response to humanitarian events". In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, pp. 4113-4122.

Rapid. 2024. "Map editing". Accessed 20 April 2024. https://rapideditor.org/

Soden, Robert, and Leysia, Palen 2014. "From crowdsourced mapping to community mapping: The post-earthquake work of OpenStreetMap Haiti". In *COOP 2014-Proceedings of the 11th International Conference on the Design of Cooperative Systems, 27-30 May 2014, Nice (France)*, pp. 311-326. Cham: Springer International Publishing.

Sun, Wenjuan, Paolo Bocchini, and Brian D. Davison. 2020. "Applications of artificial intelligence for disaster management". *Natural Hazards*. 103(3): 2631-2689.

TEMA. 2024. "AI.BIG Cluster". Accessed 15 April 2024. https://tema-project.eu/projects-cluster

UNDP and OCHA. 2023. "Innovation in Disaster Management. Leveraging Technology to Save More Lives". Accessed 02 May 2024. https://www.undp.org/sites/g/files/zskgke326/files/2024-03/innovation_in_disaster_management_web_final_compressed.pdf

Ushahidi. 2023a. "Crowdsourcing Soultion to Empower Communities". Accessed 11 April 2024. https://www.ushahidi.com/about/our-story/

Ushahidi. 2023b. "Crisis Prepadness Platform". Accessed 13 May 2024. https://www.ushahidi.com/in-action/crisis-preparedness-platform/

Velev, Dimiter and Plamena, Zlateva. 2023. "Challenges of artificial intelligence application for disaster risk Management". *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*. 48: 387-394.

ALGORITHM FOR DISASTER MANAGEMENT

Abstract: The integration of artificial intelligence (AI) tools has become a pivotal standard in the disaster management realm recent years. This shift is driven by the escalating frequency and severity of natural disasters and their profound impact on both human lives and infrastructure. Consequently, numerous nations and organizations have begun incorporating AI tools to bolster their disaster prediction capabilities and improve response protocols. For instance, these tools are instrumental in the early detection of wildfires, mapping flood and landslide vulnerability, predicting earthquakes, assessing damage to buildings post-disaster, and issuing timely emergency notifications and warnings. Given the variety of AI tools and their multiple applications the authors suggest the idea of grouping them together under the term "algorithm for disaster management" and provide a definition for it. By the stated term, the authors mean artificial intelligence algorithms expressed in computer code, implemented through new technologies and capable of operating in all phases of disaster management. Based on the provided definition, analysis of relevant literature, and selected criteria, the paper presents an overview of AI-based tools, with a specific focus on the innovative Frontier Technology Radar for Disaster Risk Reduction. This tool enables systematic monitoring and comprehension of emerging technologies. Furthermore, it sheds light on the contributions of the Humanitarian OpenStreetMap Team, Ushahidi, Artificial Intelligence for Digital Response, and the Open Source Geospatial Foundation. In conclusion, while the use of AI tools offers numerous advantages, it is crucial to recognize and address the associated risks. It is imperative to leverage and enhance the benefits of these tools while mitigating potential drawbacks. However, it must always be borne in mind that humans remain central to every system, and that these tools cannot supplant the human experience, emotions, and knowledge crucial for decision-making in intricate and unforeseeable scenarios, such as natural and other disasters.

Keywords: new technologies, artificial intelligence, natural disasters, open sources of data, disaster management.

КРИВИЧНА ДЕЛА ПРОТИВ БЕЗБЕДНОСТИ РАЧУНАРСКИХ ПОДАТАКА – ИЗАЗОВИ САВРЕМЕНИХ ТЕХНОЛОГИЈА НА ПРИМЕРУ НЕКОЛИКО ПРЕСУДА

Јована Бановић[1]

Апстракт: Поред несумњиве користи коју има, свеопшти технолошки напредак са собом носи и одређене, не тако мало ризике по човека, организације, инфраструктуру и функционисање друштва уопште. Када ти ризици поприме озбиљнију димензију, постају и кривичноправно релевантни. Отуд се високотехнолошком криминалу поклања све већа научна и стручна пажња. Парадоксално или не, у пракси домаћих правосудних органа се кривична дела против безбедности рачунарских података не појављују тако често (према подацима Републичког завода за статистику, од 2011. године наовамо, број поднетих кривичних пријава је у годишњем просеку мањи од 15, а број осуда мањи од пет). Нормативни оквир српског права, поред Кривичног законика чини и посебни процесно-организациони Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала. Поред тога, дигитална имовина као потенцијални предмет извршења кривичних дела против безбедности рачунарских података представља нови изазов за органе кривичног правосуђа. Но, без обзира на неспорни значај који имају „футуристичка" питања, фокус рада је на анализи стварног стања на примеру неколико пресуда Вишег суда у Београду - Одељења за борбу против високотехнолошког криминала. Циљ ове обраде је разматрање појавних облика најчешћих кривичних дела из 27. Главе Кривичног законика (рачунарска превара, прављење и уношење рачунарских вируса, неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података…), са посебним акцентом на радње извршења и начине њиховог предузимања. Приметићемо и да извршење ових дела често „не иде само" о чему сведочи разноликост кривичних дела у стицају каква су: фалсификовање исправе, недозвољена трговина, проневера или прање новца. Претпоставка је да разматрање пресуђених случајева може допринети ваљанијем разумевању природе и манифестације ових кривичних дела и превазилажењу непознаница које баштине нове технологије. Посебно јер је реч о делима која због „техничких особености" неретко могу бити погођена „тамном бројком" криминалитета и као таква створити ризично окружење које се може контролисати заједничким напорима стручњака из различитих области.

Кључне речи: рачунарски подаци, рачунарска превара, рачунарски вирус, неовлашћен приступ, сајбер безбедност, високотехнолошки криминал.

Уводна разматрања

Безбедност рачунарских података представља област од нарочитог значаја у дигиталној ери. Нећемо претерати ако кажемо да су електронски подаци насушна потре-

[1] Факултет безбедности, Универзитет у Београду, jovana.banovic@fb.bg.ac.rs

ба данашњице. Од свакодневних активности, попут коришћења рачунара за обављање посла, учење, куповину, заказивање услужних термина; преко неких „уноснијих" какви су креирање дигиталних садржаја, „рударење" криптовалута и сл; па до „стратешких" у виду управљања и надзора критичне инфраструктуре, различитих индустријских, технолошких постројења, али и здравства, саобраћаја…

Без обзира на несумњиве предности, употреба рачунарских технологија носи и бројне ризике. Отуда су превентивне мере заштите уређаја и података неопходне скоро колико и њихово постојање. Међутим, када ти ризици прерасту у озбиљније повреде или угрожавања, оправдана је репресивна реакција. Кривична дела против безбедности рачунарских података прописана су унутар Главе 27 Кривичног законика (КЗ). Према посебном организационо-процесном Закону о организацији и надлежности државних органа за борбу против високотехнолошког криминала (ЗВТК 2005, чл. 3-11), за кривично гоњење ових кривичних дела на целој територији Републике Србије надлежно је Више јавно тужилаштво у Београду – Посебно одељење за борбу против високотехнолошког криминала[2] које поступа пред Вишим судом у Београду – Одељењем за борбу против високотехнолошког криминала. У оквиру Министарства унутрашњих послова, формирана је и Служба за борбу против високотехнолошког криминала. Специјализација државних органа у борби против ове врсте криминалног деловања је пожељна, посебно што чак и у раду обавештајних органа спречавање и сузбијање сајбер криминала налази своје место уз нека „традиционалнија" дела усмерена против националне безбедности каква су тероризам, организовани криминал или прање новца (Bachmaier Winter 2022). У сваком случају, обликовање ових кривичних дела како са материјалног, тако и процесног, те организационог аспекта је углавном учињено у складу са преузетим међународним обавезама, особито оним предвиђеним у Конвенцији Савета Европе о високотехнолошком криминалу из 2001. године и додатним протоколима уз њу (детаљније о томе у: Делић 2021, 325-327; Милошевић 2022, 171-173).[3]

Иако одређеним питањима нећемо посветити пажњу у овом раду, вреди поменути да се са експанзијом дигиталне имовине „дигитално поље" стварног и правног деловања додатно шири и отвара простор за важна проматрања. Тако некада може бити спорна надлежност поводом кривичних дела у вези са дигиталном имовином (нпр. да ли је у питању тешка крађа или, у случају хаковања неко од кривичних дела високотехнолошког

[2] За потребе ЗВТК, надлежно тужилаштво се означава појмом „посебно јавно тужилаштво". Ипак, у смислу Закона о јавном тужилаштву (ЗЈТ), није реч о „јавним тужилаштвима посебне надлежности" каква су Јавно тужилаштво за организовани криминал и Јавно тужилаштво за ратне злочине, а како је то наведено у чл. 13 ЗЈТ.

[3] На нивоу прописа Европске уније, поменућемо неколико новијих директива које се у мањој или већој мери односе (и) на кривичноправну заштиту рачунарских података. То су: Директива 2013/40/ЕУ од 12. августа 2013. о нападима на информационе системе и о замени Оквирне одлуке Савета 2005/222/ПУП, Директива 2019/713/ЕУ од 17. априла 2019. о борби против превара и фалсификата у вези са безготовинским средствима плаћања и замени Оквирне одлуке Савета 2001/413/ПУП, као и Директива 2011/93/ЕУ од 13. децембра 2011. о сузбијању сексуалног злостављања и сексуалне експлоатације деце и дечје порнографије и замени Оквирне одлуке Савета 2004/68/ПУП. Усаглашавање домаћег права са правним тековима Европске уније је један од циљева Стратегије за борбу против високотехнолошког криминала за период 2019–2023. године (Стратегија). Не улазећи у детаљну анализу садржине нормативног усклађивања материјалног и процесног кривичног законодавства, ваља истаћи да се на инкриминисање радњи пресретања комуникације које, за разлику од међународних инструмената наше важеће право не предвиђа, указује и у теорији (Делић 2021, 327; Милошевић 2022, 171 фн. 55).

криминала), или то што кривична дела из чл. 140 и 141 Закона о дигиталној имовини (ЗДИ) не потпадају под режим високотехнолошких кривичних дела према ЗВТК, као и увек интересантна питања у вези са одузимањем имовинске користи стечене кривичним делом (примера ради, како државни орган који врши одузимање може сазнати „приватни кључ" како би средства пребацио на „буџетски дигитални новчаник" по том основу) (више о томе: Поповић 2023; Radisavljević 2023; Banović 2023). Поред тога, могућности тзв. *dark-net* мреже у трговини дрогом, оружјем, краденим уметнинама, затим фотографијама злостављане деце, па и наручивање убистава су додатни разлог за стручну и научну обраду ових тема (Reid 2018, 241).

Предмет рада биће анализа неколико пресуда Вишег суда у Београду у циљу разматрања појавних облика најчешћих кривичних дела из поменуте 27. Главе КЗ – рачунарске преваре, прављења и уношења рачунарских вируса, и у мањој мери кривичних дела из чл. 299, 302 и 304а КЗ. Посебан акценат ће бити на радњама извршења и начинима њиховог предузимања. Приметићемо и да извршење ових дела често „не иде само" о чему сведочи разноликост кривичних дела у стицају каква су: фалсификовање исправе, недозвољена трговина, проневера или прање новца. Опредељујући разлог за обраду ове теме доминантно методом анализе садржаја судске праксе је један можда и парадоксалан податак да је удео кривичних дела против безбедности рачунарских података у укупном броју кажњивих дела релативно низак. Због тога смо мишљења да извесно „осветљавање" појавних облика у досадашњој пракси органа кривичног правосуђа може дати одговор на питање зашто је то тако чак и у условима све веће употребе рачунарских технологија.

Статистички подаци

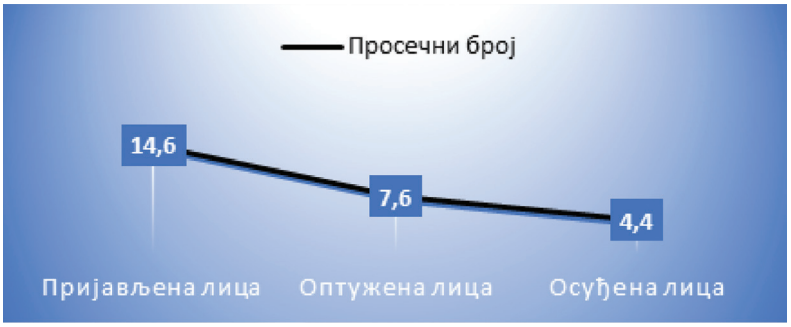
У наставку се налази табеларни приказ података о броју пријављених, оптужених и осуђених лица за кривична дела против безбедности рачунарских података у периоду од 2013. до 2022. године према подацима Републичког завода за статистику (РЗС). У табели нису садржани подаци о појединим кривичним делима из ове Главе будући да ћемо се на изречене санкције осврнути кроз анализу појединачних случајева.

Табела 1: Статистички приказ пунолетних учинилаца кривичних дела против безбедности рачунарских података у периоду од 2013. до 2022. године (подаци издвојени из Билтена РЗС, 2023)

Пунолетни учиниоци[4]										
Година	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**
Пријављени	29	9	14	16	20	11	5	14	13	15
Оптужени	6	10	3	12	13	16	4	1	5	6
Осуђени	4	8	2	7	8	3	4	1	5	2

[4] Подаци о малолетним учиниоцима нису разматрани будући да је удео кривичних дела против безбедности рачунарских података учињених од стране ових лица занемарљив и креће се од једног до (ретко) два дела годишње.

На бази статистичких података, изражено математичким просеком, у протеклој деценији је за кривична дела из Главе 27 КЗ на годишњем нивоу било око 15 кривичних пријава, око осам оптужења и просечно пет осуда.



Графикон 1: Годишњи просек броја пријављених, оптужених и осуђених лица за кривична дела против безбедности рачунарских података за период од 2013. до 2022. године

Анализа неколико пресуда Одељења за борбу против високотехнолошког криминала Вишег суда у Београду

С обзиром на изнете статистичке податке и извесни „дефицит" у пресуђењима поводом кривичних дела против безбедности рачунарских података, предмет ове сумарне анализе је седам пресуда (осуђујућих, ослобађајућих и одбијајућих) Вишег суда у Београду донетих у редовном поступку или на основу споразума о признању кривичног дела. Обрадићемо их по „количини" појављивања, односно заступљености у пракси државних органа, при чему ћемо се, према конкретном случају, уз „рачунарско дело" дотаћи и „пратећих" кривичних дела учињених у стицају.

Рачунарска превара – чл. 301 КЗ

Ово кривично дело је у обрађеном узорку пресуда најчешће, па ће му следствено бити посвећена највећа пажња. Иако по својој суштини представља посебан облик „обичне" преваре (Делић 2021, 331), од ње се ипак разликује превасходно с обзиром на заштитне објекте који се штите овим инкриминацијама. Једна од кључних дистинкција је у томе што је превара усмерена на имовину пасивног субјекта као објекта радње, а рачунарском преваром се утиче на електронску обраду података, тј. уређај, одн. средство (Милошевић 2022, 181). Кривично дело постоји уколико се на резултат електронске обраде и пренос података утиче уношењем нетачног, пропуштањем уношења тачног податка или прикривањем или лажним приказивањем података на други начин. Потоња алтернативно прописана радња представља „кишобран норму" под коју се могу подвести различите радње. Последица се огледа у проузроковању имовинске штете (што додатно сугерише на „природну везу" са преваром као општим имовинским кривичним делом). Радња мора бити предузета у намери прибављања противправне имовинске користи.

Разноврсни су начини на које се подаци „лажно приказују" и средства путем којих се врши електронска обрада. Тако је у Пресуди ВСБГ К.По3 бр. 43/16 „окривљени оглашен

кривим јер је заједно са још два лица довео у заблуду радника оштећене спортске кладионице задуженог за исплату у погледу легалности оствареног добитка на аутоматима за коцкање … који се налазе у објектима кладионице и прикривањем чињенице да су на наведеним аутоматима претходно извршили замену оригиналних чипова који су били и фискализовани налепницом и холограмом од стране Пореске управе … Замену оригиналних чипова вршили су тако што су их скидали, а на њихово место постављали лажне чипове, тзв. сијамце који представљају епром чипове (прим. аут. корисник сам уписује садржај у такву врсту меморије, при чему се тај садржај може брисати под дејством УВ светлости) … да би тако ушли у сервисни мод апарата који им омогућава добитак притиском на тастере који увек добијају, укуцавши само њима познату шифру која активира чип". У контексту „неуспешних" превентивних мера, интересантно је сагледати утицај људског фактора кроз улогу помагача у овом кривичном делу. Наиме, једно од окривљених лица је било запослено у кладионици на месту на ком се врши „осматрање објекта путем сигурносних камера, па је по претходном договору, у замену за новчани износ … пропустило да реагује и упозори раднике кладионице када је првоокривљени физички преусмеравао камеру којом су апарати били осматрани, чиме је омогућило да предузете радње не буду уочене на снимцима сигурносних камера". С обзиром на то да је окривљени „преко лажних чипова налепио претходно набављене фалсификоване контролне налепнице Пореске управе и тако лажну исправу употребио као праву", осуђен је и за кривично дело фалсификовања исправе. За кривично дело рачунарске преваре у продуженом трајању, окривљеном је по споразуму о признању кривичног дела утврђена казна затвора од пет месеци, а за фалсификовање исправе два месеца и изречена јединствена казна од шест месеци затвора. У овом кривичноправном догађају је остварен и законски опис кривичног дела из чл. 304а КЗ Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података, али ово дело није било предмет споразума, а на концу ни цитиране пресуде.

Рачунарску превару чини и окривљени који је „инсталирао четири GSM gateway уређаја (мрежни пролаз је врста хардверског уређаја чија је улога превођење из једног протокола у други, односно прилагођавање електричног сигнала једног, у електрични сигнал другог протокола) који би се могли конектовати на различите и удаљене VoIP и мобилне мреже како би вршили пребацивање долазећих и одлазећих комуникационих канала, па је преко лица у Македонији, повезао опрему ради уношења нетачних података о ИМЕИ бројевима који представљају електронске податке … и тако омогућавали обављање незаконитог телефонског саобраћаја, заобилажењем легалних мобилних оператера који нису регистровали телефонски садржај реализован на овај начин" (Пресуда ВСБГ К.По3 бр. 28/15). Практично, овде је реч о прављењу и употреби лажних сим-картица на штету регистрованих мобилних оператера. За ово кривично дело окривљеном је утврђена казна затвора у трајању од једне године и 11 месеци и изречена условна осуда, што је, како видимо, „у граничним вредностима" за изрицање ове мере упозорења.

Интернет преваре представљају један од честих појавних облика, али је симптоматично да интернет превара не представља посебно кривично дело. Уколико се врши путем рачунарске мреже, а објект радње је физичко лице, превара из чл. 208 КЗ може бити дело високотехнолошког криминала ако материјална штета прелази износ од милион динара у складу са чл. 3 ст. 2 ЗВТК. Међутим, и тада ће се радити о имовинском кривичном делу, али ће за то дело бити надлежни посебни државни органи према ЗВТК. Дакле, таква превара у материјалноправном смислу не постаје рачунарска у смислу чл. 301 КЗ

(вид. Милошевић 2022, 182). У вези са тим, интересантно је сагледати ове финесе кроз једну осуђујућу пресуду ВСБГ К.По3 61/15 за кривично дело учињено на сајту за онлајн куповину. Оно је квалификовано као рачунарска превара због утицаја на електронску обраду и пренос података. Наиме, окривљени је оглашен кривим јер је, уз остварености осталих обележја, „неовлашћено и незаконито покушао поновну регистрацију налога са корисничким именом 'Име' на веб-страни WWW са истом личном картом, али различитим подацима у њој, тако што је на већ постојећој личној карти на име 'Име и Презиме' по којој је већ једном регистровао налог, преправио податке тиме што је уносио различита презимена и потписе, док су бројеви личне карте и ЈМБГ остали непромењени". Сходно овој одлуци, утицајем на електронску обраду и пренос података сматра се, дакле, и преправљање података у налогу на штету правног лица. Поред рачунарске преваре, окривљени је осуђен и за кривично дело недозвољене трговине из чл. 243 КЗ јер се, након што је утицао на резултат електронске обраде, уз помоћ тако „прибављених" налога „бавио трговином без овлашћења за трговину нуђењем различитих предмета на продају – наочара које је у намери да обмане купце означавао туђим робним маркама … и у тако креираном налогу у обавештењу о предметима унео податке који не одговарају садржини, врсти, пореклу и квалитету производа". Иако су потенцијално компромитовани и неки лични подаци, у поступку се није поставило питање евентуалног постојања кривичног дела Неовлашћеног прикупљања личних података из чл. 146 КЗ што и није неочекивано будући да се гоњење за ово кривично дело предузима по приватној тужби, тј. зависи од воље оштећеног. Окривљеном је за рачунарску превару утврђена казна затвора од шест месеци, а за недозвољену трговину од девет месеци, те изречена условна осуда са утврђеном јединственом казном затвора од годину и два месеца.

Запосленима у једном привредном друштву је стављено на терет „уношење нетачних података којима се утиче на резултат електронске обраде података, тако што су на радним местима у више наврата продали робу која је плаћана у готовини приликом преузимања и о чему су издавани фискални рачуни, а онда, након тога, да су у рачунима које су правили у програму свог предузећа накнадно мењали рачуне и наводили да је роба плаћана чековима грађана, платним картицама или делом у готовини, делом у чековима и тако добијен новац од продаје робе присвајали за себе". Поред кривичног дела рачунарске преваре, имајући у виду да се радило о средствима која су окривљенима поверена на раду, оптужба се односила на стицај са кривичним делом проневере из чл. 364 КЗ[5]. Пресудом ВСБГ К.По3 бр. 131/11 окривљени су ослобођени оптужбе, будући да није доказано да су баш они предузимали наведене радње. Ипак, вештачењем је утврђено да јесте постојало неслагање у износима наведеним у фискалним рачунима и програму које је користило привредно друштво, те да је „мањак настао тако што су поједини рачуни који су били евидентирани у рачунарском систему предузећа у којима је било наведено да су плаћени у готовини, *касније мењани уз помоћ администраторске шифре* (прим. аут. којој је приступ имало више лица, а да није несумњиво утврђено којих) у рачуне за које је наведено да су плаћени путем чекова. Тим променама, готов новац који је наплаћен од купца делимично је задржан од стране непознатог лица, а за чекове који су у програму били наведени као средство плаћања се на крају пословне године испоставило да не постоје".

[5] У време извршења кривичног дела, током 2009. и 2010. године, и проневера „у предузећу" потпадала је под окриље кривичног дела проневере из групе дела против службене дужности. Након измена КЗ из 2016. године, у склопу реформе привредних кривичних дела, посебно је издвојено кривично дело проневере у обављању привредне делатности (чл. 224 КЗ).

Још један од модалитета извршења рачунарске преваре видимо у пресуди ВСБГ СПК. По3 бр. 36/21. Наиме, окривљени је, са још једним лицем, даљинским путем приступио рачунару и рачунарском програму, те су сачинили 15 лажних електронских налога за пренос новца путем рачунара и рачунарске мреже са нетачним подацима да је између окривљених и оштећеног друштва извршен промет робе и услуга, а затим ове налоге проследили на реализацију". За ово кривично дело изречена је казна затвора у трајању од једне године (у варијанти извршења тзв. кућног затвора). Ипак, овај начин извршења кривичног дела је занимљив и са становишта односа са другим кривичним делима из Главе 27, посебно имајући у виду да је предметна радња предузета тако што су окривљени „приступили рачунару оштећеног привредног друштва путем 'Remote Desktop Protocole' начина приступа, као и програму за електронско плаћање 'FXClient' оштећеног, користећи корисничко име и шифру коју су прибавили коришћењем рачунарских вируса … а које су претходно неовлашћено унели у рачунар који је користила радница у оштећеном привредном друштву". Дакле, пре извршења рачунарске преваре, предузете су одређене припремне радње које представљају засебна кривична дела попут уношења рачунарског вируса (чл. 300 ст. 2 КЗ). Но, када је у питању то кривично дело, могло би бити речи и о привидном идеалном стицају по основу консумпције (а не правом стицају). Ипак, у контексту кривичног дела из чл. 300 КЗ има простора за другачије тумачење, али и другачије легислативно решење којим би се отклониле сличне дилеме и неке практичне недоследности које треба сагледати кроз призму чл. 304а КЗ (за конкретне законске предлоге, вид.: Милошевић 2022, 178-180).

Покушај рачунарске преваре постоји када су предузете радње овог кривичног дела, али „трансфер новца није реализован јер су радници банке обуставили пренос новца са рачуна оштећеног привредног друштва на рачуне окривљених" (Пресуда ВСБГ СПК. По3 бр. 36/21). Слично је утврђено и у Пресуди ВСБГ К.По3 бр. 18/17 када је окривљени „дао инструкције окривљенима (прим аут. у односу на које је поступак раздвојен) да отворе по 10 банкарских рачуна у 10 различитих банака на које ће бити извршена трансакција противправно прибављеног новца, те да ће их приликом подизања новца пратити и обезбеђивати друга лица … којима ће након преузимања предати целокупну документацију и подигнуте износе … тако што се неовлашћено укључио у рачунар оштећеног привредног друштва са непознате локације и извршио логовање у софтвер за електронско плаћање 'FXClient', уносећи нетачне податке да пренос података врши овлашћени представник оштећеног у корист лица која су претходно отворили рачуне у банкама …, те неосновано пребацили средства у укупном износу од 2.446.578,00 динара на ове рачуне и то две уплате у подељеним износима … који износи нису могли да буду подигнути услед реакције запослених у банци, када су окривљени који су покушали да подигну новац и лишени слободе". Ово су добри примери значаја оспособљености службеника у реаговању на незаконите радње у вези са безбедношћу рачунарских података, посебно у домену рада са новцем или средствима безготовинског плаћања.[6] У односу на потоње дело, осуђеном је изречена казна затвора у трајању од једне године и четири месеца.

[6] Посебан проблем представљају услуге које се извршавају према иностранству, а последица су рачунарске преваре, јер се и мимо материјалних и процесних сложености такви учиниоци тешко проналазе. Један од озбиљнијих примера представља тзв. BEC (business email compromise) одн. бизнис имејл превара, када налози за уплату одређених новчаних износа стижу са мејлова пословних партнера који су претходно хаковани, па оштећени на први поглед и не може да посумња у преварно поступање (НБС 2024).

Прављење и уношење рачунарских вируса – чл. 300 КЗ

Ово кривично дело практично у целости представља припремне радње које су подигнуте на ранг радњи извршења и састоје се у прављењу – основни облик и уношењу рачунарског вируса уз наношење штете (*sic!*) – тежи облик. Већ смо истакли потребу нормативног преиспитивања овог кривичног дела, а његов специфичан домашај се посебно може сагледати у домену уношења *ransomware* вируса који заробљавају рачунар док год оштећени не плати „откупнину" под претњом трајног закључавања или компромитације података. У овом случају реч је о посебним облицима рачунарске принуде, уцене или изнуде који нису изричито прописани, али могу имати озбиљне последице како на општи објекат заштите, тако и на свакодневни живот појединаца, група, те критичну инфраструктуру (Putnik *et al.* 2022, 336-338; Милошевић 2022, 179-180).

У вези са тим, на бази доступног узорка, размотрићемо једну одбијајућу пресуду потврђену у Пресуди АСБГ Кж1 По бр. 25/16 због наступања застарелости. Радње извршења се односе на „неовлашћен приступ и коришћење рачунара уношењем злонамерног рачунарског програма … стицањем контроле над зараженим рачунарима без воље и знања корисника рачунара ради њиховог искоришћавања за извршење кривичних дела, када је окривљени својим командама на рачунару покренуо његову инсталацију тј. активирање ради употребе, да би потом са интернета преузимао различите софтвере са различитих интернет сајтова за преузимање нелегалних рачунарских програма и садржаја као што су 'piratebay, mininova, demonoid', те након тога у те рачунарске програме према упутству које добије за употребу 'Butterf1y v 1.11' уносио злонамерне програмске кодове под називима 'AtillaEvil SD.7Z' и 'FacebookAddonUpdate.exe' и то у инсталационе фајлове преузетих програма чиме је омогућио прикривено наснимавање ради употребе злонамерних програмских кодова, након чега је тако припремљене 'заражене' рачунарске програме, постављао учитавањем путем свог рачунара на сајтове … ради даљег преузимања од стране њему непознатих лица а ради стављања истих под његову контролу, и на тај начин 'заразио' рачунаре других корисника који су наведене програме које је осумњичени поставио преузимали не знајући да се у њима налази злонамеран рачунарски програм, након чега се после покретања инсталације наведени злонамерни рачунарски програм по претходно програмираној наредби распакивао и инсталирао на рачунаре тих корисника у програмске датотеке и меморију њихових рачунара што је имало за последицу да су 'заражени' рачунари следећи програмску рутину контактирали рачунарски сервер под контролом окривљеног који се налази на наведној ИП адреси што је омогућило окривљеном да помоћу 'BFF Master Client' опције 'Butterf1y f100der v 1.1l' који представља центар за противправно управљање зараженим рачунарима користио исти и то најмање 521 рачунар, те је преко њих вршио приступ 'torrent' интернет сајту 'piratebay' фомрирајући на тај начин заражену рачунарску 'ботнет' мрежу заражених рачунара других корисника под његовом контролом чиме је проузроковао штету корисницима заражених рачунара у виду смањеног протока података у време када је окривљени постављао садржаје на 'torrent' сајтове коришћењем портал рачунара и ИП адреса заражених рачунара, као и смањену могућност ефективне употребе заражених рачунара због противправне употребе њихових ресурса".

У конкретном случају се поставило и питање постојања кривичног дела прања новца за које је суд ослободио окривљеног због недостатка доказа да „окривљени није поднео годишњу пореску пријаву, ни платио порез на доходак грађана у износу од 243.656,12 динара, тако да овај износ представља имовинску корист за окривљеног, па остаје нејасно због чега окривљени није пријавио приходе које је остварио по основу

уговора са компанијом 'Pinball Publicher Network' уколико су исти законито стечени". Наиме, Апелациони суд је потврдио да нема доказа да је окривљени извршио ово кривично дело на начин како му се оптужбом ставља на терет, тј. да је новац у износу од 85.504,34 УСД стекао и користио иако је исти прибавио извршењем кривичног дела рачунарске преваре, с обзиром да је првостепени суд окривљеног својом пресудом а због недостатка доказа ослободио од оптужбе за кривично дело рачунарске преваре, што самим тим значи да нема ни доказа да наведени износ потиче од извршења кривичног дела рачунарске преваре".[7] Иако на темељима овог разлога за ослобађајућу пресуду не можемо „захватити" суштину инкриминације, она нам даје повод да скренемо пажњу на постојање парадигме тзв. виртуелног криминала белог оковратника и трансформацију овог концепта. У односу на „класични" привредни криминалитет где је у средишту угледно лице на *високом положају*, сајбер „варијанту" карактерише поверење у лице које поседује *техничку стручност и вештине* (Reid 2018, 232-233, 245-246).

Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података – чл. 304а КЗ

Код овог кривичног дела реч је о типичним припремним радњама. Из идентичних разлога (застарелост) као у претходном примеру, у истом предмету, донета је одбијајућа пресуда у односу на окривљеног да је „од НН лица са псеудонимом … путем међународне рачунарске мреже 'Интернет' купио злонамерни рачунарски програм 'Butterf1y f100der v 1.11', који током инсталирања на рачунару врши копирање дела свог програмског кода у рачунарско програмско окружење циљаног рачунара и тиме омогућава успостављање делимичне контроле над 'зараженим' рачунаром, а за износ од 500,00 еура који је наведеном лицу платио уплатницом Western Union … да би након пријема уплате НН лица, лице … путем Интернет сервиса 'MSN' наведени злонамерни рачунарски програм проследио на налог електронске поште окривљеног … у виду интернет линка тј. програмске рачунарске везе која омогућава преузимање програмских садржаја, са кога је окривљени и преузео наведени рачунарски програм на свој кућни рачунар, да би након тога путем рачунарског праграма — апликације под називом 'Remote Desktop' исти преснимио – 'учитао' ради даље употребе на рачунарски сервер на интернет протокол адреси … а који сервер је закупио у сврху коришћења 'Butterf1y Rooder v 1.1' ради даљег коришћења".

Рачунарска саботажа – чл. 299 КЗ и Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података – чл. 302 КЗ

У стицају са кривичним делом рачунарске преваре, у предмету ВСБГ К.По3 бр. 18/17 поступак се водио и за предметна кривична дела у односу на која је донета одбијајућа пресуда због одустанка јавног тужиоца. С тим у вези, „окривљени је кршећи мере заштите приликом извршења рачунарске преваре извршио криптовање података на рачунару оштећеног предузећа и тако учинио податке и пословну документацију неупотребљивим". На правну квалификацију описаних деловања утицали су врста

[7] Интересантно је приметити да би разлог који се односи на непостојање предикатног кривичног дела рачунарске преваре у вези са прањем новца био упитан након измена КЗ из 2016. године. Наиме, од 1.3.2018., када су поменуте измене ступиле на снагу, захтева се „знање да имовина потиче од криминалне делатности", а не од „кривичног дела" у формалном смислу. Слично: Решење АСБГ Кж1 бр. 557/21 и Пресуда ВСБГ – ПОСК КПО4 бр. 20/20.

пасивног субјекта (код рачунарске саботаже) и начин извршења у виду кршења мера заштите (кривично дело из чл. 302 КЗ).

Закључак

Удео кривичних дела против безбедности рачунарских података у укупности криминалних понашања није велики. Томе сведоче приказани статистички подаци, нарочито о броју донетих пресуда, па и оптужења. Примећено је да се знатан број предмета који „дођу до суда" окончава споразумима о признању кривичних дела са изреченим краткотрајним казнама лишења слободе (између шест месеци и годину и четири месеца) или условним осудама. Анализа пресуђених случајева може допринети ваљанијем разумевању природе и манифестације ових кривичних дела и превазилажењу непознаница које баштине нове технологије. Посебно, јер је реч о делима која због „техничких особености" неретко могу бити погођена „тамном бројком" криминалитета и као таква створити ризично окружење које се може контролисати заједничким напорима стручњака из различитих области. Колико год савремене технологије биле аутоматизоване, видели смо и да људски фактор има значајну улогу – позитивну, када доприноси спречавању настанка тежих последица, али и негативну – када уместо да гарантује правилно функционисање делатности у вези са електронском обрадом, учествује у вршењу кривичних дела. Отуд се чини исправном тврдња Теда Нелсона да је „код компјутера добро што раде оно што им се каже, али и да је код компјутера лоше то што раде што им се каже".

Библиографија

Bachmaier Winter, Lorena. 2022. "Criminal Investigation, Technological Development, and Digital Tools: Where Are We Heading". In: *Investigating and Preventing Crime in the Digital Era, Legal Studies in International, European and Comparative Criminal Law 7*, edited by Lorena Bachmaier Winter and Stefano Ruggeri. Switzerland: Springer. https://doi.org/10.1007/978-3-031-13952-9_1

Banović, Jovana. 2023. "Criminal law aspects of Digital Assets – Contemporary Challenges". *International Scientific Conference – Investigating and Proving Contemporary Forms of Crime: Scientific Approaches, "Archibald Reiss Days" – University of Criminal Investigation and Police Studies Belgrade* 13: 89–99.

Делић, Наташа. 2021. *Кривично право Посебни део.* Београд: Универзитет у Београду – Правни факултет.

Директива 2011/93/ЕУ од 13. децембра 2011. о сузбијању сексуалног злостављања и сексуалне експлоатације деце и дечје порнографије и замени Оквирне одлуке Савета 2004/68/ПУП.

Директива 2013/40/ЕУ од 12. августа 2013. о нападима на информационе системе и о замени Оквирне одлуке Савета 2005/222/ПУП.

Директива 2019/713/ЕУ од 17. априла 2019. о борби против превара и фалсификата у вези са безготовинским средствима плаћања и замени Оквирне одлуке Савета 2001/413/ПУП.

Милошевић, Младен. 2022. *Кривично право – посебни део: изабране инкриминације за студије наука безбедности*. Универзитет у Београду – Факултет безбедности.

Поповић, Урош. 2023. *Евалуација ефективности постојећих протокола за спречавање прања новца у трговини дигиталном имовином*. Београд: мастер рад одбрањен на Правном факултету Универзитета у Београду.

Републички завод за статистику. 2023. *Билтен бр. 702*. Београд.

Putnik, Nenad R., Mladen M. Milošević i Vladimir N. Cvetković. 2022. „Rensomver kao pretnja bezbednosti ‑ društveni i krivičnopravni aspekti". *Sociološki pregled* LVI (1): 328–353. DOI: 10.5937/socpreg56-36845.

Radisavljević, Ivana. 2023. „Krivičnopravna zaštita digitalne imovine". U: *Kaznena reakcija u Srbiji: tematska monografija,* urednik Đorđe Ignjatović, 302–314. Beograd: Univerzitet u Beogradu – Pravni fakultet.

Reid, Alan S. 2018. "Financial Crime in the Twenty-First Century: The Rise of the Virtual Collar Criminal". In: *White Collar Crime and Risk Financial Crime, Corruption and the Financial Crisis*, edited by Nic Ryder, 231–251. United Kingdom: Palgrave Macmillan.

[ЗДИ] Закон о дигиталној имовини. 2020. Сл. гласник РС, бр. 153/2020.

[ЗВТК] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала. 2005. Сл. гласник РС, бр. 61/2005, 104/2009 10/2023 и 10/2023 - др. закон.

[ЗЈТ] Закон о јавном тужилаштву. 2023. Сл. гласник РС, бр. 10/23.

[КЗ] Кривични законик. 2006. Сл. гласник РС, бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019.

[Пресуда АСБГ Кж1 По бр. 25/16] Пресуда Апелационог суда у Београду. Кж1 По бр. 25/16 од 30. 6. 2017. године.

[Пресуда ВСБГ К.По3 бр. 131/11] Пресуда Вишег суда у Београду. К.По3 бр. 131/11 од 22. 10. 2015. године.

[Пресуда ВСБГ К.По3 бр. 18/17] Пресуда Вишег суда у Београду. К.По3 бр. 18/17 од 11. 4. 2019. године.

[Пресуда ВСБГ К.По3 бр. 28/15] Пресуда Вишег суда у Београду. К.По3 бр. 28/15 од 23. 4. 2015. године.

[Пресуда ВСБГ К.По3 бр. 43/16] Пресуда Вишег суда у Београду. К.По3 бр. 43/16 од 30. 8. 2017. године.

[Пресуда ВСБГ К.По3 бр. 61/15] Пресуда Вишег суда у Београду. К.По3 бр. 61/15 од 20. 11. 2015. године.

[Пресуда ВСБГ СПК. По3 бр. 36/21] Пресуда Вишег суда у Београду. СПК. По3 бр. 36/21 од 13. 7. 2021. године.

[Решење АСБГ Кж1 бр. 557/21 и Пресуда ВСБГ – ПОСК КПО4 бр. 20/20] Решење Апелационог суда у Београду. Кж1 бр. 557/21 од 13. 6. 2022. и Пресуда Вишег суда у Београду. ПОСК КПО4 бр. 20/20 од 10. 02. 2021. – Из Билтена Вишег суда у Београду, бр. 93/2022.

[Стратегија] Стратегија за борбу против високотехнолошког криминала за период 2019–2023. године. 2018. Службени гласник РС, бр. 71/2018.

НБС. 2024. "Email is not always sufficient when receiving instruction for payments". Народна банка Србије. Accessed 20 May 2024. https://www.nbs.rs/sr/scripts/showcontent/index.html?id=17627&konverzija=no

CRIMINAL OFFENCES AGAINST THE SECURITY OF COMPUTER DATA – CHALLENGES OF MODERN TECHNOLOGIES BASED ON SEVERAL COURT JUDGMENTS

Abstract: Besides its undeniable benefits, the overall technological advancement also brings certain, not insignificant, risks to individuals, organizations, infrastructure, and the functioning of society in general. When these risks take on a more serious dimension, they also become criminally relevant. Hence, cyber (or high-tech) crime is receiving increasing scientific and professional attention. Paradoxically or not, in the practice of domestic judicial authorities, criminal acts against the security of computer data do not appear that frequently (according to data from the Republic Statistical Office, since 2011, the number of filed criminal charges averages less than 15 annually, and the number of convictions is less than five). The normative framework of Serbian law, in addition to the Criminal Code, includes a special procedural-organizational Law on the Organisation and Competences of Government Authorities Combating Cyber Crime. Furthermore, digital assets as potential objects of criminal offences against the security of computer data present a new challenge for criminal justice authorities. However, despite the undeniable importance of "futuristic" issues, the focus of this paper is on analyzing the actual state based on several judgments of the High Court in Belgrade – Department for Combating Cyber Crime. The aim of this analysis is to consider the manifestations of the most common criminal acts from Chapter 27 of the Criminal Code (computer fraud, creating and introducing computer viruses, unauthorized access to protected computers, computer networks, and electronic data processing...), with a special emphasis on the actions and methods of their execution. We will also notice that the execution of these acts often "does not go alone", as evidenced by the variety of concurrent criminal acts such as document forgery, illegal trade, embezzlement, or money laundering. The assumption is that examining adjudicated cases can contribute to a better understanding of the nature and manifestation of these criminal acts and overcoming the unknowns that new technologies inherit. Especially since these acts, due to their "technical peculiarities", can often be affected by the "dark figure" of crime and as such create a risky environment that can be controlled through the joint efforts of experts from various fields.

Keywords: computer data, computer fraud, computer virus, unauthorized access, cyber security, high-tech crime.

ПРЕЛИМИНАРНИ ОСВРТ НА УПРАВЉАЊЕ РИЗИЦИМА И ЕКОЛОШКУ ОДРЖИВОСТ У КОНТЕКСТУ ОСТВАРИВАЊА ЕКОЛОШКЕ БЕЗБЕДНОСТИ

Милош Тошовић[1]

Апстракт: Савремени услови реализације различитих техничко-технолошких и пословних процеса, са тенденцијом сталног усавршавања и унапређења, прате посебно значајни управљачки и безбедносни аспекти. Управљачки аспекти осим стандардног и класичног дела управљања предметним процесима, посебно значајно обухватају део са дефинисањем, проценом и управљањем ризицима од непланираног одвијања ових процеса и њихових негативних последица. При томе се осим важног техничко-технолошког утицајног фактора, посебно мора имати у виду антропогени утицајни фактор, односно поступање човека као главног актера и субјекта реализације предметних процеса. Безбедносни аспекти се осим безбедносних ризика нарочито односе на веома значајан аспекат еколошке безбедности у радној и животној средини, уз очување и заштиту кључних производних ресурса (средстава рада, предмета рада и људских ресурса), очување материјалних добара у окружењу, али и медијума животне средине (земљишта, ваздуха и воде), као и биљних и животињских заједница у околној средини. У оквиру контекста предметног разматрања еколошке безбедности, према савременом приступу, посебно се значајно уклапа примена концепта одрживог развоја, базираног на уравнотежењу економске, друштвене и нарочито еколошке компоненте одрживости, као парцијалних видова одрживости. Међу њима се као посебно значајна може издвојити еколошка одрживост, важна и за пословне системе и за екосистеме на ближем и даљем простору подручја економских и друштвених активности. Основни циљ овог рада је да прелиминарно анализира, оквирно сагледа и прикаже функционалну повезаност управљања ризицима у техничко-технолошким и пословним процесима и питања обезбеђења еколошке одрживости. У наставку предметне анализе је нарочито важно разматрање контекстуалног утицаја на питања све значајније еколошке безбедности у производним објектима, насељеним подручјима, као и различитим екосистемима. При томе се полази од потребе осигуравања савременог нивоа еколошке безбедности, уз нарочиту анализу економске и друштвене компоненте одрживости, због чега је додатно испољен приоритетни значај укључивања управљања ризицима и еколошке одрживости у остваривање целовите еколошке безбедности.

Кључне речи: управљање ризицима, еколошка одрживост, техничко-технолошки процеси, пословни процеси, еколошка безбедност.

Увод

Менаџмент производних и пословних процеса, као савремени управљачки алат, обухвата одговарајуће основне функције, које између осталог подразумевају и управљање

[1] Факултет безбедности, Универзитет у Београду, milostosovic79@gmail.com

ризицима у техничко-технолошким системима различитих степена сложености. При томе поље деловања савремених модела управљања ризицима интензивно прати промене пословних модела и процеса, који представљају, нарочито у данашње време, конкурентску предност организације на актуелном турбулентном тржишту (Tošović 2023a). У савременим тржишним околностима појачане тржишне конкуренције, предузећа и компаније често, кроз различите облике сарадње, деле одговорност и ризик пословања (Bojanić 2021) и врше организациону и пословну поделу производних и непроизводних послова, уз специјализацију, побољшање и унапређење пословних активности (Tošović 2023a), ради спречавања евентуалних катастрофичних последица.

Успешно управљање ризицима пословања је веома значајна одговорност највишег менаџмента и нарочито битан фактор успешног пословања (Tošović 2023a). За исправну пословну одлуку о процени одређеног ризика и дефинисање одговарајуће активности у циљу његовог смањења, потребно је активно примењивати менаџмент ризика, као специфичан апликативни процес (Aven 2016). Менаџмент ризицима у предузећу, између осталог, подразумева системско смањивање могућности настанка безбедносно кардиналних грешака, у реализацији разноврсних техничко-технолошких и пословних процеса (Tošović 2022), заједно са превенцијом катастрофа и минимизирањем последица. За модерно предузеће наведене активности поред управљачких прате и посебни еколошки и безбедносни аспекти, који су значајни за функционалне и успешне производне, економске и финансијске ефекте пословања предузећа, као примарне циљеве менаџмента предузећа.

Предузећа, као пословни субјекти, у савременим условима функционисања глобалног политичког, еколошког и финансијског система под великим пословним и тржишним притисцима, суочени су са све већим ризицима и неизвесностима због утицаја човека на функционисање техничко-технолошких производних процеса и нарочито испољеног утицаја на радну и животну средину, као и екосистеме у окружењу (Collier 2008, 2010; Hallding, Nykvist and Persson 2013). Услед експанзивног тренда раста броја становника и достизања потребне стопе економског раста, у већем делу света појављују се знаци угрожавања одрживог развоја, услед великог повећања тражње за природним, животним и пословним ресурсима, преко њихове доступности у оквиру уобичајеног сценарија живота, рада и пословања (Hallding, Nykvist and Persson 2013). Посебан пратећи проблем је што у појединим производним областима, услед различитог утицаја производних процеса, критични екосистеми се приближавају или премашују свој капацитет (Del Monte-Luna et al. 2004), што изазива посебну забринутост због пословних система са потенцијално сложеним и тешко предвидивим последицама по друштво и животну средину (Bierbaum et al. 2014; Jager and Patel 2012; Steffen et al. 2004).

Интензивна конкуренција око потребних животних и производних ресурса у појединим земљама и континентима, повећава ризик од њихове несташице, пратећих поремећаја у ланцу снабдевања и нарочито скокова цена, што повратно доприноси расту економских, геостратешких и политичких тензија (Lee et al. 2012). Наведено додатно потврђују трогодишња геополитичка, стратешка, економска и тржишна збивања и кретања након почетка актуелног руско-украјинског војног сукоба (Tošović 2023b).

У односу на ранији конвенционални дискурс о безбедности, евидентна је неопходност проширења безбедносних аспеката на еколошке аспекте одрживости и еколошку безбедност (Tošović 2023d), као и потреба за савременим третирањем безбедности, уз значајно обухватање и елемената људске безбедности, односно безбедности хране и воде, животне средине и општег благостања појединца и друштва (Dalby 2009; Matthew

et al. 2010; Mobjork et al. 2010; Andersson et al. 2007). Експоненцијални раст еколошких безбедносних изазова у наредним деценијама, на регионалном и глобалном нивоу, захтева разматрање појачане еколошке безбедносне перспективе, способне да идентификује и решава овако широк спектар изазова (Stajić and Stanarević 2015). Управљање ризиком, нарочито у делу који се односи на катастрофе, не треба схватити као повремену активност безбедносног експерта, већ као културни и образовани начин размишљања у предузећу (Jakovljević, Cvetković і Gačić 2015), који захтева одговарајући маркетиншки приступ у промовисању значаја безбедности (Tošović 2023c).

У условима примене важећег концепта одрживог развоја савремени безбедносни приступ (Tošović 2022) налаже обавезу обухватања еколошке одрживости, еколошке безбедности и процене ризика, нарочито од техничко-технолошких катастрофа, и то ради: (а) превентивног деловања и (б) обезбеђења ефикасног поступања по принципима кризног менаџмента у случају евентуалног испољавања (Tošović 2023d). Прелиминарна анализа предметних безбедносних аспеката према извршеним аналитичким истраживањима у овом раду, нарочито укључује разматрање односа управљања ризицима и питања еколошке одрживости, имајући у виду целовити приступ безбедности и пратећи осврт са становишта еколошке безбедности.

Управљање ризицима пословних процеса

Различити модели управљања пословним ризицима у предузећима различитих облика материјалне производње, показали су одређене предности, али и недостатке. Они се првенствено односе на питања обухватања проблематике ризика од катастрофа и исказивања кроз одговарајуће финансијске показатеље укупних и нарочито еколошких ризика. У интегрисаном моделу управљања пословним процесима и ризицима потребно је обухватање свих ризика и показатеља успешности пословања предузећа, као и дефинисане стратегије и циљева предузећа, који ће помоћи у успешном пословању и стварању конкурентске предности, уз ефикасно смањење ризика од катастрофа. Посебно значајан аспект односи се на смањење ризика од техничко-технолошких катастрофа, као битног услова за одрживо пословање предузећа у савременим тржишним и производним условима (Tošović 2022, 2023d), нарочито битне примене концепта еколошке одрживости и остварења укупне и еколошке безбедности.

У организационом и менаџерском смислу предузеће као пословни, производни и економски систем, обухвата средства рада, предмете рада и људе, чијим деловањем се остварује одговарајући процес трансформације, производње и пословања (Tošović 2023a). При томе производни систем подразумева мрежу међусобно повезаних и зависних компоненти, које раде у спрези у остваривању циљева система (Deming 2018), а кроз чије функционисање се остварује одговарајућа производна или пословна активност, праћена мањим или већим ризицима. При томе је веома важно да без обављања неке функције, односно дефинисане сврхе рада и пословања нема ни система, што значи да он омогућује одређени облик рада и остваривања постављених пословних циљева (Ćosić, Radaković і Milić 1991). Класу производних и пословних система одликује динамичност (Bojanić 2021), са којом је повезана неопходност управљања радним процесима, што уз постојање ризика значи неопходност и управљања ризицима пословних процеса (Tošović 2023a).

Различита предузећа се баве разноврсним делатностима, а генерално се издвајају: (а) производна предузећа са производњом материјалних производа; и (б) услужна

предузећа са пружањем одређених услуга (Mankiw 2021). Поред разлика у реализацији постоје и значајне сличности у организацији производних и услужних предузећа, реализацији производа и услуга, као и карактера производних и пословних процеса, који су подложни одређеним врстама ризика (Tošović 2023d). Предметна подела нарочито је значајна са тематског становишта управљања ризицима, посебно ризика од катастрофа и еколошких ризика. Чињеница је да услужне делатности прати нижи степен техничко-технолошке опремљености, што значи и мањи ризик од техничко-технолошких катастрофа. Ипак и овај део пословне активности може бити ризичан, посебно у делу доставе производа купцима, што се нарочито односи на поступање са хемијским и одређеним опасним материјама. Производну активност, с обзиром на виши степен техничко-технолошке опремљености, прати знатно виши степен ризика од настанка и испољавања потенцијалних катастрофичних последица (Tošović 2023a).

У потпуној анализи основних пословних процеса предузећа, посебно са становишта управљања ризицима, полази се од дефинисања процеса (Hammer and Champy 1993, 2001), као скупа активности, који трансформишу један или више улаза у излаз, као повећану вредност за корисника (Liao 2020; Harrington 1991, 2006). С друге стране производни процес се може дефинисати као низ пословних активности кроз простор и време, са почетком и крајем, и јасно дефинисаним улазима и излазима (Davenport 1993, 1998, 2005; Bojanić, 2021). Стандард ISO 9000, као део система менаџмента квалитетом, дефинише процес као скуп међусобно повезаних или делујућих активности, које претварају улазне у излазне елементе, уз пратеће постојање одређених ризика.

Предузећа у суочавању са производним и безбедносним изазовима прихватају принципе управљања базиране на процесима, и при томе да безбедносно анализирају процесе, а не функционалне целине или одељења. Традиционални начин управљања оријентисан на функције може да доведе до појаве конкуренције између појединачних целина унутар предузећа. Због тога је неопходно успостављање организационом структуром, која је оријентисана на процесе, што доноси низ повољности (Hammer 1990, 2007). Постоји пет критичних покретача за успостављање високих производних перформанси процеса (Hammer 2007): (а) пројектовање; (б) мерење; (в) извршиоци; (г) инфраструктура; и (д) власници процеса; који су посебно значајни за управљање ризицима.

Данашњи процесни приступ је настао услед актуелних тржишних захтева у обезбеђењу потребног квалитета производа и услуга и настојања за ефикаснијим начином управљања производним процесима и безбедносним ризицима производње. Процесни приступ стиче све више присталица из више разлога: (а) повећање броја присталица стандардизованих система управљања квалитетом (QSM - Quality Management System); (б) популаризација Lean концепта управљања; (в) примене Six Sigma; и (г) управљања пројектима (Gebczynska and Bujak 2017). Оријентација на процесни приступ се додатно повећала, јер су предузећа усвојила програме усмерене на процесе, као што су ISO 9001 и Менаџмент тоталног квалитета (TQM - Total Quality Management) (Safari et al. 2013).

Генерално посматрано процеси у предузећима се деле на: (а) управљачке; (б) оперативне; и (в) процесе подршке (Bojanić 2021). Доминантни процеси који су предмет анализе и процене ризика обухватају оперативне послове, иако су менаџерски посматрано посебно значајни управљачки послови нарочито са становишта управљања ризицима. Генерално, пословни процеси, према трајности, обухватају две врсте (Lee and Dale 1998; Trkman 2010): (а) привремене; и (б) сталне процесе. Привремени процеси су процеси који започињу када је потребно и завршавају се у будућности, док се стални

процеси непрестано одвијају. Са становишта анализе, процене и управљања ризицима, укључујући и катастрофе посебно су интересантни стални процеси, иако аналитичку пажњу заслужују и поједини привремени процеси.

У сваком случају сви наведени савремени менаџерски и процесни алати представљају веома корисне менаџерске и управљачке поступке, који омогућују побољшање производних и пословних процеса, смањење грешака и пропуста, а тиме директно утичу на смањење и пратећих ризика предметне производње, укључујући и ризике од катастрофа.

Менаџмент ризика предузећа (ERM - Enterprise Risk Management) представља менаџере, односно руководство, које се бави неизвесностима у раду предузећа. Последњих деценија настају промене парадигме у начину на који компаније гледају на управљање ризиком (Zhao, Hwang and Low 2014). ERM се посматра као основна парадигма у тренду, који се креће ка холистичком управљању ризиком (Zhao, Hwang and Low 2016). Интересовање за ERM расте и велики број предузећа има ERM програме, који су већ имплементирани или су у фази имплементације (McCormack et al.2009). У процесу ERM-а појављују се: (а) кључни индикатори ризика (KRI - key risk indicators); и (б) кључни индикатори перформанси (KPI - key performance indicators), који се међусобно разликују са аспекта раног упозоравања. Ове две групе индикатора се могу користити при управљању ризицима у циљу праћења промена у условима настанка ризика и идентификовања нових ризика. Основна разлика између KRI и KPI је што први говоре о променама у ризик профилу и какви су утицаји и могућност за остваривање циљева, а други указују да ли ће се остварити циљеви. KRI пружају информације о настајању ризика и пружају могућност деловања на настанак ризика (Bojanić 2021) и окренути су будућности, док KPI више гледају у прошлост. При томе KRI су мера која показује ниво или тренд ризика (Scarlat, Chirita and Bradea 2012). KRI пружају информације унапред о ризицима који постоје и служе као систем за упозоравање на будуће догађаје, при чему се месечно или квартално ревидирају како би упозорили предузеће о променама, које могу да узрокују настанак ризичних догађаја (Coleman 2009).

Интеграција управљања пословним процесима и ризицима процеса је савремени концепт (Suriadi et al. 2014), који је мотивисао развој управљања пословним процесима свесних ризика (R-BPM - Risk-aware business process management), а који је настао интеграцијом BPM-а и ERM-а (Thabet et al. 2018). Ова интеграција повезује ефикасну идентификацију, откривање и управљање ризицима, везаним за пословне процесе (Jakoubi et al. 2010). Моделирање пословних процеса са свешћу о ризику веома је битан оперативни задатак у животном циклусу R-BPM, уз потребне информације везане за ризике. Укључивање ризика у процесне моделе је веома важно како би се перформансе пословног процеса могле одредити у глобалном смислу. При томе су неопходна даља истраживања и унапређење праксе моделирања пословних процеса са свешћу о ризику (Bojanić 2021), како би се остваривало успешно управљање ризицима посебно од катастрофа, а све у циљу подизања нивоа еколошке безбедности и стварања основа за успешно остваривање еколошке одрживости.

Еколошка одрживост и пратећи ризици

Еколошка одрживост има полазно исходиште у концепту одрживости (Tošović 2023b), при чему одрживост представља способност одржавања равнотеже одређених природних, друштвених и производних процеса или достигнутог жељеног стања у неком припадајућем систему. Посебно значајан безбедносни проблем за људску популацију,

а самим тим нарочито за производне системе, јесте одрживост и равнотежа и то на глобалном нивоу (Evans et al. 2009; Mladenović 2016), која је директно праћена одређеним врстама ризика и последичним утицајем на еколошку безбедност.

Поједини приступи појму одрживости, посебно појачавају еколошку димензију одрживости (Costanza 1991) и додатно је третирају као однос између постојећих економских система, које ствара људско постојање, активност и производња, и ширих динамичких еколошких система, који се самостално спорије мењају. Иако тај однос подразумева одређене предуслове, и то: (а) постојање човечанства у будућности; (б) раст људске популације; и (в) развој друштва и културе, ипак ефекти таквог деловања на окружење треба да остану у оквиру датих граница (Mladenović 2016), тако да не уништавају разноврсност, комплексност и функцију еколошког система, који подржава рад, живот и пословање људи. У наведеном релационом разматрању посебно се може анализирати утицај одређених безбедносних позиција производних процеса на еколошку безбедност и еколошку одрживост.

Одрживи развој, који узима у обзир тројство еколошких, економских и социјалних аспеката одрживости (Tošović 2023b), *обухвата заправо процес истовременог обезбеђивања континуитета економске, социјалне и еколошке базе живота човечанства, уз обухватање* три кључне сфере и то: (а) друштвене; (б) економске; и (в) сфере животне средине (Lele 1991). При томе сваку од димензија одрживости карактерише одговарајућа динамичка макро-варијабла, која је уједно и императив (Valentin and Spangeberg 2000), уз повезивање ових императива са одговарајућим димензијама одрживости, који заправо представља примену Кантовог „категоричког императива" на животни стил и проблеме животне средине (Kant and Kehrbach 1913).

Различитим дефиницијама одрживог развоја заједничка је изражена *временска димензија одвијања промене одговарајуће сфере одрживости, која се може повезати и са временском димензијом трајања одређених ризика, посебно еколошких*. Већа стопа експлоатације материјалних и производних ресурса условљава краће стање функционалности производног система пре евентуалног урушавања (Mladenović 2016). При томе у условима *ограничених ресурса, стопа конзумације и време могућег одржавања такве стопе су обрнуто пропорционални, нарочито у зони преласка границе критичног нивоа одрживости производног система* (Pereira 1993), спрам кога је посебно осетљив еколошки део, са захтевом умањења еколошких ризика и остваривања нивоа еколошке безбедности и нарочито еколошке одрживости (Tošović 2023d).

У пресеку три наведене сфере одрживости, које синхронизовано и балансирано функционишу, налази се подручје потребне одрживости, при чему посебан значај има еколошка одрживост (Tošović 2023d). Пресек сваке две сфере има своје посебно значење: (а) пресек економске и сфере животне средине је подручје способности за раст (viable); (б) пресек економске сфере и сфере друштва је подручје правичности (equitable); и (в) пресек сфере друштва и сфере животне средине је подручје подношљивости (bearable) (Mladenović 2016). Уочљива је тенденција да се овај концепт одрживог развоја прошири четвртом димензијом, према неким истраживањима *технологијом* (Hasna, 2006; Mani, Lyons and Sriram 2010) или виђења по којима би *култура* требало да представља четврту димензију одрживог развоја (Hawkes, 2001; Nurse, 2006; Trusins 2011). Полазећи од основа наука безбедности, садашњег и будућег значаја безбедности, нарочито са становишта 3 безбедносна аспекта (економске, еколошке и друштвене безбедности), које одговарају сферама одрживог развоја оправдано се намеће суштински значајно питање да ли се безбедност може појавити као четврта димензија одрживости, за шта,

према досадашњим истраживачким анализама аутора овог рада, постоје оправдани разлози и аналитички основи.

Саставни део предметне анализе еколошке безбедности полази од једног од кључних принципа одрживог развоја, а то је очување екосистема (Mensah and Ricart Casadevall 2019). Сасвим извесно да постоји потреба за очувањем екосистема и биодиверзитета, због даље егзистенције живих организама. При томе ограничена средства и ресурси на Земљи нису довољни за неограничене потребе људи. Прекомерна експлоатација ресурса има негативне ефекте на животну средину и, стога, да би развој био одржив, експлоатација природних ресурса мора бити у оквиру могућности планете Земље (Kanie and Biermann 2017). То са практичног становишта значи да се развојне активности морају спроводити у складу са капацитетом Земље. Због тога је важно, нпр. користити алтернативне изворе енергије као што су соларни, уместо велике зависности од нафтних деривата и фосилне енергије (Molinoario et al. 2019).

Концепт одрживости, чији саставни део је еколошка одрживост (Tošović 2023b) заправо се налази негде „на средини", између екоцентричног концепта квалитета средине (еколошка компонента) (environmental quality), и антропоцентричног концепта квалитета живљења (друштвено-економска компонента). При томе, са новим технолошким проналасцима и решењима који обезбеђују напредак и просперитет, отварају се нове развојне перспективе, али исто тако и могућности настанка техничко-технолошких катастрофа (Tošović 2022), *по којима је неопходно посебно анализирање релевантних ризика и истима управљање на ефикасан и ефективан начин*. С обзиром на достигнути степен деградације животне средине њена заштита, односно смањење и спречавање загађења медијума животне средине и заштита живог света су главне смернице у разматрању одрживости, које прате најважнији аспекат еколошку одрживост. Егзистенцијални, односно суштински значај животне средине, обухваћен кроз еколошку одрживост, која је услов за економску и друштвену одрживост, приоритетно је важна у разматрању одрживог развоја (Tošović 2023d).

Еколошка одрживост подразумева: (а) интегритет односно целовитост очувања екосистема; (б) обављање производних процеса уз превенцију загађења или минимални утицај на животну средину уз могућност санирања последица; (в) трошење природних ресурса које не угрожава могућност обнављања; (г) контролисани производни процес тзв. нултог отпада и (д) минималне количине отпада од производње, који се може безбедно збринути (Tošović 2022).

Еколошка димензија одрживости поред интегритета екосистема, нивоа засићености и биодиверзитета односи се и на утицај предузећа као привредног субјекта на животну средину (Tošović 2022) *уз потребну процену и управљање еколошким ризицима*. Предузеће током производне делатности треба да штити животну средину, што је више могуће. Менаџери који организују или реализују пословну активност треба да делују у смеру процене одређених ризика и смањивања утицаја на животну средину, тако што ће водити рачуна о коришћењу природних ресурса, радити на смањивању различитих врста отпада, али и тако што ће се побринути да отпад предузећа буде мање токсичан пре одлагања на сигуран и законит начин. Многа предузећа данас спроводе одговарајуће безбедносне процене производа по концепту „животног циклуса", како би утврдила праве еколошке трошкове, почев од обраде полазне сировине, преко производње и дистрибуције до евентуалног одлагања производа у отпад (Jacobs and Chase 2017). Док је конвенционални дискурс о безбедности фокусиран на тврду безбедност, све је евидентнија потреба за ширим разумевањем безбедности, која обухвата елементе

људске безбедности (Dalby 2009; Matthew et al. 2010; Mobjork et al. 2010; Andersson et al. 2007; Maksimović *2023).*

Функционална веза управљања ризицима, еколошке одрживости и еколошке безбедности

Перцепције безбедности и одрживости у савременим условима аналитичких разматрања пословних процеса се мењају (Collins 2013), од некадашње одвојености у два различита истраживачка поља, до садашњег препознавања њихове међусобне везе (Hallding, Nykvist and Persson 2013; Granit and Claassen 2013; Maksimović 2023). Као кључни аналитички фактор развоја предметне релације, којој се додаје и питање ризика, у задње време се издваја потпуније аналитичко разумевање динамике односа човека и екосистема, као што су еколошки утицаји на окружење, утицаји климатских промена и варијабилности, сиромаштва и потрошње ресурса на Земљин систем, нарочито током последњих деценија (Bierbaum et al. 2014; Steffen et al. 2004), са праћењем одговарајућих ризика. Реинтерпретација и преобликовање безбедности и одрживости истиче императив њиховог значајнијег и интензивнијег повезивања ради постизања снажних развојних исхода (Maksimović 2023), *али нарочито унапређења еколошке одрживости и еколошке безбедности као дела укупне одрживости и укупне безбедности* (Tošović 2023d), уз функционално проширење управљањем ризицима.

У аналитичким извештајима о глобалним ризицима запажају се неједнакости међу различитим земљама, које постају растући извор нестабилности (Ncube, Anyanwu and Hausken 2012; Maksimović 2023) са тенденцијом погоршања услед повећане оскудице производних и животних ресурса. Остваривање инклузивног економског раста, једнакости и друштвеног развоја се сматрају кључним за одрживи развој и опстанак екосистема (Tošović 2023d), као и пратећу еколошку безбедност и еколошку одрживост, које прате одређени ризици и безбедносна потреба управљања тим ризицима.

Полазна концептуализација безбедности се односила на интегритет државе и њене територије, дефинисане кроз конвенционалну или националну безбедност. Савремено схватање ризика и претњи националној безбедности у 21. веку (Maksimović 2023) се проширило на укључивање ограничења производних и животних ресурса, деградације животне средине, климатских промена и еколошке варијабилности, директно утичући на еколошку и националну безбедност. Узрочно-последична веза између еколошких питања животне средине, производних и животних ресурса и различитих нестабилности и сукоба, може довести до нарушавања еколошке безбедности и еколошке одрживости, која може водити и економској стагнацији, повећању корупције, нарушавању токова финансијских средстава и доводити до националних и етничких тензија (Liljedahl et al. 2012). Такви мултипликатори претњи представљају снажне ризике по остваривање економске, еколошке и друштвене одрживости држава, уз нарушавање људске, еколошке и националне безбедности.

У читавом еколошком, одрживом и безбедносном разматрању за обезбеђење функционалности и безбедности, држави и грађанима потребан је довољан приступ не само основним потребама, већ и економским ресурсима, у чему посебно место заузима глобализација. Глобална трговина је омогућила обезбеђење приступа производним и животним ресурсима, који су изван физичких граница државе, повећавајући конкуренцију око неравномерно распоређених ограничених животних и производних ресурса. Приступ људској безбедности је створио израженије везе између безбедности

и одрживости, као изазова традиционалном приступу заснованом на државноцентричном поимању безбедности и стављајући појединца и људско благостање у центар безбедносних анализа (Watson 2008). Дискурс о људској безбедности тежи да се посебно фокусира на услове за сиромашне и рањиве популације (Matthew et al. 2010). При томе шири концепт безбедности и његових импликација на безбедносну заједницу представља промену парадигме (Maksimović 2023), која проширује дијапазон ризика и претњи, нарочито укључујући шира и детаљнија питања процене ризика, еколошке безбедности и еколошке одрживости.

Шире аналитичко разумевање одрживог развоја, безбедности и еколошке безбедности може се поткрепити одговарајућим финансијским анализама, нарочито у регионима са неизвесним економским, друштвеним, политичким и еколошким приликама. У методолошки оквир анализе ризика, еколошке безбедности и еколошке одрживости, могу се укључити истраживачки сценарији, који помажу бољем разумевању њихове повезаности и интеракција (Maksimović 2023), како би се потпуније сагледала питања пратећих ризика, безбедности и људског развоја.

У актуелним аналитичким студијама везаним за управљање ризицима, еколошку безбедност и еколошку одрживост могу се разликовати три врсте применљивих техника, и то (Bradfield et al. 2005): (а) предвиђање или анализа тренда; (б) истраживачки сценарији; и (в) нормативни сценарији. Предвиђање се користи за краће временске периоде, када се динамика система релативно добро разуме. Истраживачки сценарији обично покривају дуже временске периоде (и до 100 година), са истраживањем веродостојних алтернативних путева развоја са проценом низа будућих услова. Нормативни сценарији полазе од жељене будућности, а затим се истражују могући путеви њеног остварења. Сва три наведена приступа сценаријима се користе како у студијама безбедности, укључујући и еколошку безбедност, тако и у студијама одрживог развоја, укључујући и питања еколошке одрживости.

Актуелне глобалне промене животне средине утичу на промену перцепције актера о безбедности и ризику, као и на одговарајуће мере за побољшање нивоа и степена нарочито еколошке безбедности. Додатно унакрсна геополитичка анализа може помоћи идентификовању синергије и конфликата у перцепцији одговарајућих ризика, еколошкој безбедности, еколошкој одрживости и резултирајућим одговорима пратећих политика. Интегрисани аналитички приступ истраживању одрживости и безбедности захтева сарадњу друштвених и природних истраживача (Maksimović 2023), заједно са планерима, стратезима, логистичарима и нарочито експертима безбедности (Tošović 2023d), уз посебно специјалистичко обухватање функционалне релације ризика, еколошке безбедности и еколошке одрживости.

Закључак

У савременим условима пословања предузећа се суочавају са директном одговорношћу за утицај прозводног процеса на животну средину. Остваривање пословног и производног учинка прате неопходне активности везане за идентификовање, дефинисање и управљање ризицима производних и пословних процеса, са посебним разматрањима еколошке безбедности, а у циљу остваривања производне, економске и еколошке одрживости предметне производње.

Промене у еколошкој и безбедносној сфери пословања одражавају се и на менаџмент производних и пословних процеса, који између осталог обухвата и управљање ризици-

ма у производним техничко-технолошким системима различитих степена сложености, што постаје битан фактор успешног пословања. Менаџмент ризицима омогућује системско смањивање настанка безбедносно кардиналних грешака у пословним процесима, заједно са превенцијом еколошких катастрофа и минимизирањем последица. Наведене менаџерске активности поред управљачких прате и посебни еколошки и безбедносни аспекти, значајни за функционалне и успешне ефекте пословања предузећа, као примарне циљеве менаџмента предузећа

Менаџмент ризика предузећа (ERM) се појављује као основна парадигма у тренду кретања ка холистичком управљању ризиком и посебно обухвата еколошке ризике, еколошку безбедност и аспекте еколошке одрживости. У практичном менаџерском поступању врши се утврђивање кључних индикатора ризика (KRI) и кључних индикатора перформанси (KPI), директно усмерених на праћење промена у настанку ризика и идентификовање нових ризика ради успешнијег управљања нарочито еколошким ризицима. Кроз интеграцију управљања пословним процесима и ризицима процеса развијено је управљање пословним процесима свесних ризика (R-BPM), усмерено на ефикасну идентификацију, откривање и управљање ризицима, у склопу успешног одвијања еколошки безбедног и еколошки одрживог пословног процеса предузећа.

Полазна концептуализација безбедности у актуелним условима, проширена је на пратећу еколошку компоненту безбедности, ограничења производних и животних ресурса и питања деградације животне средине. Узрочно-последична веза између еколошких питања животне средине, производних и животних ресурса и различитих друштвених и еколошких нестабилности, може довести до значајног нарушавања еколошке безбедности и еколошке одрживости производних и привредних система. У склопу савременог менаџмента ризицима неопходно је посебну пажњу посветити свеобухватним безбедносним анализама еколошких ризика, како би се подигао ниво еколошке безбедности у предстојећем времену и обезбедила економска, друштвена и нарочито еколошка одрживост производних, привредних и друштвених система у земљама и регионима.

Библиографија

Andersson, Scott A., Karl-Henrik Dreborg, Annica Waleij, and Mikael E. Wulff, 2007. *Environmental Security - an Overwiev* [Miljosakerhet - En oöversikt]. FOI-R--2287--SE. Swedish Defence Research Agency, Stockholm.

Aven, Terje. 2016. "Risk assessment and risk management: Review of recent advances on their foundation". *European Journal of Operational Research* 253 (1): 1-13.

Bierbaum, Rosina, Michael Stocking, Hindrik Bouwman, Amber Cowie, Santiago Diaz et al. 2014. *Delivering Global Environmental Benefits for Sustainable Development*. Report to the 5th GEF Assembly, Mexico. Global Environment Facility, 79 pp., Washington, DC.

Bojanić, Tamara. 2021. „Integrisani model menadžmenta rizika u poslovnim procesima u industrijskim sistemima". Fakultet tehničkih nauka, Univerzitet u Novom sadu, *doktorska disertacija*, 155 pp., Novi Sad.

Bradfield, Ron, George Wright, George Burt, George Cairns, and Kees Van Der Heijden. 2005. "The origins and evolution of scenario techniques in long range business planning". *Futures,* 37(8):795–812.

Coleman, Les. 2016. *Risk strategies: Dialling up optimum firm risk*. Routledge.

Collier, Paul. (2008). *The Bottom Billion: Why the Poorest Countries Are Failing and What Can Be Done about It*. Oxford: Oxford University Press.

Collier, Paul. (2010). *The Plundered Planet: Why We Must--and How We Can--Manage Nature for Global Prosperity*. Oxford: Oxford University Press.

Collins, Alan. 2013. *Contemporary Security Studies*. 3rd ed. Oxford University Press, Oxford, UK.

Costanza, Robert. 1991. *Ecological Economics: The science and Management of Uncertainty*. New York: Columbia University Press.

Ćosić, Ilija, Nikola Radaković, i Rado Milić. 1991. *Osnove radnih postupaka u industrijskim sistemima - Priručnik za vežbe*. FTN - Institut za industrijske sisteme, Novi Sad.

Dalby, Simon. 2009. *Security and Environmental Change*. Polity, 200 pp., Cambridge, UK.

Stajić, Ljubomir, and Svetlana Stanarević. 2015. "The role and importance of international organizations in maintaining ecological and human security". *Zbornik Radova Pravnog fakulteta u Novom Sadu* 49: 963 – 978.

Davenport, Thomas H. 1993. "Need radical innovation and continuous improvement? Integrate reengineering and TQM". Strategy & Leadership, *Planning review* 21 (3): 6-12.

Davenport, Thomas H. 1998. Putting the enterprise into the enterprise system. *Harvard Business Review* 76 (4): 121-131.

Davenport, Thomas H. 2005. "The Coming Commoditization of Processes". *Harvard Business Review* 83 (6): 100-108.

Del Monte-Luna, Pablo, Barry W. Brook, Manuel J. Zetina-Rejon, and Victor H. Cruz-Escalona. 2004. The carrying capacity of ecosystems. *Global Ecology and Biogeography* 13(6): 485–95.

Deming, Edwards E. 2018. *The New Economics for Industry, Government, Education.* Third edition, Cambridge, MA: MIT press, London, England.

Evans, Steve, Mike Gregory, Chris Ryan, Margareta N. Bergendahl, and Adrian Tan. 2009. *Towards a sustainable industrial system: With recommendations for education, research, industry and policy.* University of Cambridge, Institute for Manufacturing, 24 pp.

Gebczynska, Alicja, and Andrzej Bujak. 2017. "Assessment of the degree of process approach implementation in Polish businesses". *The TQM Journal* 29 (1): 118 – 132.

Granit, Jakob, and Marius Claassen. 2013. "A scalable approach towards realizing tangible benefits in transboundary river basins and regions". *In International Law and Freshwater*. Edward Elgar Publishing. 140–54.

Hallding, Karl, Bjorn Nykvis, and Asa Persson. 2013. "The new geopolitics of environmental constraints, changing ecosystems and resources competition". *In: Strategic Yearbook 2012-2013: The Emerging Global Security Environment*. Swedish National Defence College. 337 pp.

Hammer, Michael. 1990. "Reengineering work: don't automate, obliterate". *Harvard Business Review* 68 (4): 104-112.

Hammer, Michael. 2007. "The process audit". *Harvard Business Review* 85(4):111.

Hammer, Michael, and James Champy. 1993. *Reengineering the Corporation: A Manifesto for Business Revolution*. New York: Harper Business.

Hammer, Michael, and James Champy. (2001): *Reinženjering tvrdke: manifest za poslovnu revoluciju* (ažurirano i revidirano izdanje ed.). Zagreb: Mate doo.

Harrington, James. H. 1991. *Business Process Improvement: The Breakthrough Strategy for Total Quality, Productivity and Competitiveness*. New York: McGraw Hill.

Harrington, James. H. 2006. *Process Management Excellence: The Art of Excelling in Process Management*. Vol. 1, Paton Professional, Chico, California, USA.

Hasna, Abdallah M. 2006. "Dimensions of sustainability". *Journal of Engineering for Sustainable Community Development* 1(2), 47-57.

Hawkes, Jon. 2001. *The fourth pillar of sustainability: Culture's essential role in public planning*. Common Ground.

Jacobs, Robert F. and Richard Chase. 2017. *Operations and Supply Chain Management*. McGraw Hill; 15th Edition, New York City , 784 pp.

Jakoubi, Stefan, Simon Tjoa, Sigrun Goluch, and Gerhard Kitzler. 2010. "A formal approach towards risk-aware service level analysis and planning". In *2010 International conference on availability, reliability and security* pp. 180-187. IEEE.

Jager, Jerald, and Namrata Patel. 2012. *An Earth System Perspective*. In: Fifth Global Environment Outlook: Environment for the future we want. United Nations.

Jakovljević, Vladimir, Vladimir M. Cvetković, i Jasmina Gačić. 201). *Prirodne katastrofe i obrazovanje.* Fakultet bezbednosti, Beograd.

Kanie, Norichika, and Frank Biermann. 2017. *Governing through goals; sustainable development goals as governance innovation*. Cambridge: MIT Press.

Kant, Immanuel, and Karl Kehrbach. *Kritik der praktischen Vernunft*. Vol. 5. Reclam, 1913.

Lee, Bernice, Felix Preston, Jaakko Kooroshy, Rob Bailey, and Glada Lahn. eds. 2012. *Resources Futures*. Royal Institute of International Affairs, London: Chatham House, 212 pp.

Lee, Robert G., and Barrie Dale 1998. "Business process management: a review and evaluation". *Business Process Management Journale* 4(3):214-225.

Lele, Sharachchandra M. 1991. "Sustainable development: a critical review". *World development* 19(6), 607-621.

Liao, Junmin. 2020. "The rise of the service sector in China". *China Economic Review* 59: 101385.

Liljedahl, Birgitta, Annica Waleij, Bjorn Sandstrom, and Louise Simonsson, 2012. "Medical and environmental intelligence in peace and crisis-management operations". *In D. Jensen and S. Lonergan (eds.) Assessing and Restoring Natural Resources in Post-Conflict Peacebuilding*. Routledge, 99-112.

Maksimović, Goran. (2023). "Mogućnost integrisanja održivog razvoja i bezbjednosti". U: Gostimirović, L. & Maksimović, G. (Eds) *Zbornik radova Naučno-stručne konferencije*

„Održivi razvoj-usklađivanje interesa ili nužna potreba", Visoka poslovno tehnička škola, Doboj, Bezbjednosni istraživački centar, Banja Luka, Doboj, Banja Luka, 9-20 pp.

Mani, Mahesh, Kevin Lyons, and Ram Sriram. 2010. "Developing a sustainability manufacturing maturity model". *Proceedings from the IMS Summer School on Sustainable Manufacturing* pp. 311-321.

Mankiw, Gregory. 2021. *Principles of Macroeconomics*. Cengage Learning; 8th edition, 576 pp., Boston.

Matthew, Richard A., John Barnett, Betty McDonald, and Kelth L. O'Brien. eds. 2010. *Global Environmental Change and Human Security*. MIT Press, Cambridge, MA.

McCormack, Kevin, et al. 2009. "A global investigation of key turning points in business process maturity." *Business Process Management Journal* 15 (5):792-815.

Mensah, Justice, and Sandra Ricart Casadevall. 2019. "Sustainable development: Meaning, history, principles, pillars, and implications for human action: Literature review". *Cogent Social Sciences* 5:1.

Mladenović, Valentina. 2016. "Upravljanje procesom eko marketinga pomoću PLM alata". Univerzitet u Novom Sadu, Fakultet tehničkih nauka, *doktorska disertacija*, 131 pp., Novi Sad

Mobjork, Malin, Mikael Eriksson, and Henrik Carlsen. 2010. "On connecting climate change with security and armed conflict". *Investig. Knowl. Sci. Community FOI Stockh*. FOI-R-3021--SE. Swedish Defence Research Agency, Stockholm

Molinoario, Erica, Arie W. Kruglanski, Flavia Bonaiuto, Mirilia Bonnes, Lavinia Cicero, Ferdinando Fornara, ... and Wouter Degroot. 2019. "Motivations to act for the protection of nature biodiversity and the environment: A matter of "Significance". *Environment and Behaviour* 52(10) 1–31.

Ncube, Mthuli, John C. Anyanwu, and Kjell Hausken. 2014. "Inequality, economic growth and poverty in the Middle East and North Africa (MENA)." *African Development Review* 26 (3): 435-453.

Nurse, Keith. 2006. "Culture as the fourth pillar of sustainable development". *Small states: economic review and basic statistics* 11, 28-40.

Pereira, Winin. 1993. "Tending the Earth – Traditional Sustainable Agriculture in India". *Earthcare Books, Bombay* 98: 218-219.

Scarlat, Emil, Nora Chirita, and Ioana-Alexandra Bradea. 2012. "Indicators and metrics used in the enterprise risk management (ERM)." *Economic Computation and Economic Cybernetics Studies and Research Journal* 46(4): 5-18.

Safari, Hossein, Mohsen Moradi-Moghadam, Hosein Soleimani, and Reza Fathi. 2013. "Assessing process maturity by EFQM and maturity models and ranking by similarity-based approach", *Journal of Applied Sciences Research* 9(3):1875-1883.

Steffen, Will L., Angelina Sanderson, Peter Tyson, Jill Jager, Pamela Matson, et al. 2004. *Global Change and the Earth System: A Planet under Pressure*. Global change - the IGBP series. Berlin and New York: Springer, 336 pp.

Suriadi, Suriadi, Burkhard Weiss, Axel Winkelmann, Arthur H.M. ter Hofstede, Michael Adams, Raffaele Conforti, and Moe Wynn. 2014. "Current research in risk-aware business process management - overview, comparison, and gapanalysis". *Communications for the Association of Information Systems* 34(1), 933-984.

Thabet, Rafika, Elyes Lamine, Amine Boufaied, Ouajdi Korbaa, and Hervé Pingaud. 2018. "Towards a Risk- Aware Business Process Modelling Tool Using the ADOxx Platform". *Springer International Publishing AG*, part of Springer Nature 2018, pp. 235-248.

Tošović, Miloš. 2022. „Uticaj tehničko-tehnoloških katastrofa na ekološku komponentu održivog razvoja". Univerzitet u Beogradu - Fakultet bezbednosti, *master akademski rad*, 103 pp., Beograd.

Tošović, Miloš. 2023a. „Integrisani model upravljanja rizicima od katastrofa *u* poslovnim procesima". Univerzitet u Beogradu - Fakultet bezbednosti, *pristupni akademski rad*, 41 pp., Beograd.

Tošović, Miloš. 2023b. "Current Aspects of Environmental and Energy Security in the Strategic Framework of the Development and Functioning of the Green Economy". *International Scientific Conference: Green Economy in the Function of Solving Global Environmental Problems,* Book of abstracts, pp. 63, Belgrade.

Tošović, Miloš. 2023c. "Marketing in Security Education and Improvement of Environmental Security". *International Scientific Conference: Green Economy in the Function of Solving Global Environmental Problems*, Book od abstracts, pp. 90, Belgrade.

Tošović, Miloš. 2023d. "Security aspects of the relational connection of technical-technological disasters with the concept of sustainable development and environmental sustainability". In: N.Stekić, M.Milošević (eds.) *Zbornik radova II memorijalne naučno-stručne konferencije „Predrag Marić"*, pp. 380-393. Beograd: Fakultet bezbednosti, Univerzitet u Beogradu.

Trkman, Peter. 2010. "The critical success factors of business process management". *International Journal of Information Management* 30 (2): 125-134.

Trusins, Jekabs. 2011. "Sustainable development strategy of multilevel spatial system". *Scientific Journal of Riga Technical University. Ser. 14. Sustainable spatial development* 2, 8-13.

Valentin, Anke, and Joachim H. Spangenberg. 2000. "A guide to community sustainability indicators". *Environmental Impact Assessment Review* 20(3):381-392.

Watson, Cynthia. A. 2008. *U.S. National Security: A Reference Handbook*. 2nd ed. Contemporary World Issues. Bloomsbury Publishing, Santa Barbara, CA, US.

Zhao, Xianbo, Bon-Gang Hwang, and Sui Pheng Low. 2014. "Investigating enterprise risk management maturity in construction firms". *Journal of Construction Engineering and Management* 140(8): 05014006.

Zhao, Xianbo, Bon-Gang Hwang, and Sui Pheng Low. 2016. "An enterprise risk management knowledgebased decision support system for construction firms". *Engineering, Construction and Architectural Management* 23(3): 369 – 384.

A PRELIMINARY REVIEW OF RISK MANAGEMENT AND ENVIRONMENTAL SUSTAINABILITY IN THE CONTEXT OF ACHIEVING ENVIRONMENTAL SECURITY

Abstract: Modern conditions for the realization of various technical-technological and business processes, with the tendency of constant improvement and advancement, are accompanied by particularly significant management and security aspects. Management aspects, apart from the standard and classic part of managing the processes in question, significantly include the part with defining, assessing and managing risks from the unplanned development of these processes and their negative consequences. In addition to the important technical-technological influencing factor, the anthropogenic influencing factor must be taken into account, i.e. the actions of man as the main actor and subject of the realization of the processes in question. In addition to security risks, security aspects refer in particular to the very important aspect of environmental security in the working environment and the environment, along with the preservation and protection of key production resources (means of work, objects of work and human resources), the preservation of material goods in the environment, but also the environmental media (soil, air and water), as well as plant and animal communities in the surrounding environment. Within the context of the consideration of environmental security, according to the modern approach, the application of the concept of sustainable development, based on the balancing of the economic, social and especially environmental component of sustainability, as partial forms of sustainability, fits particularly well. Among them, environmental sustainability can be singled out as particularly important, important both for business systems and for ecosystems in the near and far areas of economic and social activities. The main goal of this paper is to preliminarily analyze, outline and display the functional connection of risk management in technical-technological and business processes and issues of ensuring environmental sustainability. In the continuation of the analysis in question, it is particularly important to consider the contextual impact on the more significant environmental security issues in production facilities, populated areas, as well as different ecosystems. It is based on the need to ensure a modern level of environmental security, with a special analysis of the economic and social component of sustainability, which is why the priority importance of including risk management and environmental sustainability in the achieving of entire environmental security is additionally expressed.

Keywords: risk management, environmental sustainability, technical-technological processes, business processes, environmental security.

4

НОВЕ ТЕХНОЛОГИЈЕ У ЈАВНИМ СЛУЖБАМА И УПРАВИ

СТРАТЕГИЈЕ ПАМЕТНОГ ГРАДА ЗА УПРАВЉАЊЕ ВАНРЕДНИМ СИТУАЦИЈАМА У БЕОГРАДУ[1]

Ана Параушић Маринковић[2], Милан Липовац[3]

Апстракт: Стратегије паметног града су утемељене у савременим информационим и комуникационим технологијама које се могу применити у области управљања градом, пружања јавних услуга, унапређењу безбедности, што у крајњем треба да допринесе бољем квалитету живота сваког становника града. Једна од области у којој стратегије паметног града могу имати нарочите користи јесте управљање ванредним ситуацијама у урбаним срединама. Уз помоћ дигиталних података, повезаности и аутоматизације, различити приступи који се повезују са концептом паметног града могу значајно унапредити рану детекцију, реаговање и адекватно управљање бројним појавама и процесима у граду. У овом раду, представићемо различите приступе, политике, активности и стратегије које су промовисане, усвојене или најављене у граду Београду, а које се могу означити као имплементација модела паметног града у области управљања ванредним ситуацијама. Осим тога, осврнућемо се на евидентне користи које дигитализација и аутоматизација има у случајевима превенције и реаговања на ванредне ситуације, али и постојећа ограничења у пракси промовисања Београда као паметног града са аспекта управљања ванредним ситуацијама.

Кључне речи: паметни град, управљање ванредним ситуацијама, урбана безбедност, Београд.

Увод

Савремени градови места су изузетне комплексности и разноликости, што чини проблеме урбане безбедности све сложенијим, начине њиховог испољавања непредвидљивијим, а потенцијалну штету за животе људи и урбани амбијент све већом. Безбедносни изазови урбаних средина су веома разноврсни те се могу односити на криминал и насиље, сиромаштво и неједнакост, као и природне и антропогене катастрофе. Развој градова, нарочито у протеклих неколико деценија, омогућио је да се, између осталог, на ове проблеме реагује или се превенирају посредством напредних технолошких решења. Стратегије паметног града су утемељене у савременим информационим и комуникационим технологијама које се могу применити у области управљања градом,

[1] Овај рад настао је као резултат ангажовања др Ане Параушић Маринковић у складу са Планом рада Института за криминолошка и социолошка истраживања за 2024. годину (на основу уговора бр. 451-03-66/2024-03/200039 са Министарством науке, технолошког развоја и иновација Републике Србије).

[2] Институт за криминолошка и социолошка истраживања, parausicana@gmail.com, https://orcid.org/0000-0002-7880-7379

[3] Факултет безбедности, Универзитет у Београду, milanlipovac@gmail.com, https://orcid.org/0000-0002-5051-3889

пружања јавних услуга, унапређењу безбедности, што у крајњем треба да допринесе бољем квалитету живота сваког становника града.

У постојећој литератури могуће је пронаћи већи број различитих одређења концепта паметног града. Имплементација концепта паметног града требало би да допринесе унапређењу квалитета живота кроз примену паметних технологија и урбаних иновација (Yigitcanlar and Kamruzzaman 2018) и решавање проблема урбанизације, климатских промена и недостатка ресурса (Ioppolo et al. 2016). Уобичајено се говори о градовима који су *одрживи, зелени, партиципативни*, а у средишту су напредна технолошка решења за унапређење свих аспеката функционисања града. У настојању да обухвате све аспекте овог концепта поједини аутори пишу о паметном граду као: „иновативном граду, у којем се информационе и комуникационе технологије користе као средство за унапређење квалитета живота, ефикасности услуга и компетитивности, при том водећи рачуна да су испуњене потребе садашње и будућих генерацију у односу са економске, друштвене и аспекте животне средине" (Arbolino et al. 2018). Као једно од свеобухватнијих јесте одређење овог феномена као „локалне заједнице која, захваљујући анализи података, ефикасно користи своју физичку инфраструктуру, у којој постоји ефективна сарадња локалне самоуправе и грађана кроз отворене и транспарентне процесе, е-партиципацију и е-управљање, и која се иновацијама на проактиван начин прилагођава променљивом окружењу" (Дамјановић 2021, 9). Чини се да, иако нужно не занемарују, оваква одређења недовољно истичу два важна аспекта концепта паметног града: 1) да је паметни град интегрисани систем напредних технолошких решења за управљање градом, а не скуп насумично повезаних пројеката и иницијатива; 2) да ова технолошка решења треба да унапреде пре свега безбедност становника града кроз решавање бројних урбаних проблема, што би у крајњем унапредило и квалитет живљења.

Једна од области у којој стратегије паметног града могу имати нарочите користи јесте управљање ванредним ситуацијама у урбаним срединама (Batty et al. 2012; Gosavi et al. 2019; Beg et al. 2020; Song et al. 2020; Das and Zhang 2021; Alshamaila et al. 2023). Уз помоћ дигиталних података, повезаности и аутоматизације, различити приступи који се повезују са концептом паметног града могу значајно унапредити рану детекцију, реаговање и адекватно управљање бројним догађајима у граду. У овом раду, представићемо различите приступе, политике, активности и стратегије које су промовисане, усвојене или најављене у граду Београду, а које се могу означити као имплементација модела паметног града у области управљања ванредним ситуацијама. Осим тога, осврнућемо се на евидентне користи које дигитализација и аутоматизација има у случајевима превенције и реаговања на ванредне ситуације, али и постојећа ограничења у пракси промовисања Београда као паметног града са аспекта управљања ванредним ситуацијама.

Управљање ванредним ситуацијама путем стратегија паметног града у Београду

Иако престоница са преко 1,5 милиона становника, Београд и централна власт немају јединствену стратегију или приступ развоју паметног града. Иницијативе везане за паметни град често се најављују од стране звничника, али осим појединачних акција или догађаја, не може се говорити о стратешкој имплементацији идејних решења концепта паметног града. Нешто озбиљнијим можемо сматрати фестивал *Smart City*, регионалну конференцију *Smart City SEE19* и појединачне конкурсе за *Најбоља решења за паметни*

ipag. И у овом раду о стратегијама везаним за концепт паметног града који могу бити од користи за управљање ванредним ситуацијама, закључује се посредно, односно осврtом на дигитализована решења имплементирана од стране градских власти.

Информационе и комуникационе технологије веома успешно се примењују у праћењу и предвиђању временских услова што може имати великог значаја за управљање ванредним ситуацијама. У оквиру активности Секретаријата за заштиту животне и Градски завода за јавно здравље Београда функционише ГИС систем за праћење квалитета ваздуха (План квалитета ваздуха у Агломерацји Београд 2021) и квалитета чинилаца животне средине.[4] ГИС се сасвим ефикасно може примењивати у условима превенције или реаговања на ванредне ситуације, кроз анализу свих прикупљених просторних сетова података, те конверзије тих података у формате подобне за веб или мобилне приказе, као и дизајнирање корисних интерактивних мапа. Израђена је интернет страница и апликација за мобилне телефоне на којој се грађани могу информисати о стању квалитета ваздуха. Информација се саопштава кроз индекс квалитета ваздуха израчунатог на основу података добијених са аутоматских мерних станица измерених у претходном сату, што је посебно значајно за податке о концентрацијама суспендованих честица. Индекс квалитета ваздуха се израчунава кроз пет категорија при чему су свакој категорији придружене и препоруке за понашање опште популације и посебно осетљивих група.[5] Од августа 2022. године постоји својеврстан аларм којим се Кабинет градоначелника, Кабинет председника Скупштине града, Градски штаб за ванредне ситуације и Градски завод за јавно здравље обавештавају о значајним загађењу ваздуха на појединим локацијама или на територији целог града.

[6]Београд је често један од најзагађенијих градова у Европи, а нивои неких опасних загађујућих материја по својим вредности могу се третирати готово као ванредне ситуације. Крајем 2019. и почетком 2020. године у Србији, па и у Београду, почео је са радом систем мерења квалитета ваздуха. Формирана је мрежа уређаја који треба да омогуће мониторинг и праћење података везаних за квалитет ваздуха у реалном времену.[7] Иницијатива се заснива на партиципативном приступу јер омогућава грађанима да наруче Климерко, уређај отвореног кода који мери спољни ниво загађености ваздуха и на сваких 15 минута бележи концентрацију штетних PM2.5 и PM10 и PM1 суспендованих честица, као и температуру, влажност ваздуха и ваздушни притисак, као податке које такође треба узети у обзир приликом оцене загађености ваздуха у неком делу града. Постоји и напредна верзија Klimerko Pro, који осим већ поменутих мери и сумпор диоксид (SO2) и азот диоксид (NO2). Креатори овог уређаја створили су и интерактивну мапу где сви заинтересовани у реалном времену могу пратити податке који региструју постављени уређаји.

Још један користан дигитални алат за праћење временских прилика на територији града Београда представља Дигитални атлас климе Србије. Иако је креиран како би презентовао климатске податке за територију Србије, преко ове платформе омогућен

[4] ГИС квалитета чинилаца животне средине налази се следећој адреси https://monitoring.beograd.gov.rs/

[5] Индекс квалитета ваздуха налази се на следећој адреси http://www.beoeko.com/#

[6] Извештај о реализованим активностима за смањење загађености ваздуха дефинисаних акционим планом за спровођење мера за смањење загађености ваздуха, у оквиру Плана квалитета ваздуха у агломерацији Београд за период јануар-децембар 2022. године доступно на https://www.beograd.rs/images/data/c66ead047de72126a798bdd43c692880_7076891497.pdf

[7] Више о целом пројекту видети на сајту https://klimerko.org/

је приступ подацима на нивоу појединачних општина укључујући и све општине града Београда. Сви климатски подаци који су доступни (температуре, падавине и велики број климатских индекса) могу се преузети у графичком облику (pgn и pdf) и дигитално читљивом облику (цсв и нетцдф). Овај сет података који укључује осмотрене промене климатских услова али и пројекције за будућност, чини основу за израду процена утицаја и рањивости на климатске промене, које су предуслов за израду планова за прилагођавање.[8]

Функционисање саобраћаја може бити од велике важности уколико дође до ванредне ситуације. Секретаријат за саобраћај града Београда подстакао је и имплементирао неколико технолошких решења која могу бити у функцији управљања ванредним ситуацијама. Сасвим очекивано, један од основних система који је значајно унапредио аспекте урбаног живљења, географски информациони систем (ГИС), искоришћен је како би се направила апликација са интерактивном мапом на којој су приказане измене режима саобраћаја на читавој територији Града. Преко ове апликације могуће је доћи до информација колико је тренутно локација на којима су активне измена режима саобраћаја у граду, које улице су затворене за саобраћај, у којим улицама је извођење радова под саобраћајем и на којим локацијама су планиране манифестације које имају утицај на измену функционисања саобраћаја.[9] У случајевима када наступи ванредна ситуација ове информације могу бити од великог значаја за планирање евакуације или снабдевања грађана, пружање помоћи, заштите објеката и сл.

Регулисање саобраћајне сигнализације, преусмеравање возила или затварање појединих улица дешава се у ситуацијама када треба усмерити активности у кризним ситуацијама. У Београду постоји систем паметних семафора који служе за анализу стварне потребе возила, густине саобраћаја и прилагођавање трајања зеленог светла на семафорима у реалном времену. Овакав систем за адаптибилно управљање светлосном сигнализацијом може да допринесе нормалном одвијању саобраћаја у оним ситуацијама када су неки правци у граду затворени јер њима морају без задржавања проћи возила хитних служби.

Један од идеја насталих у оквиру концепта паметног града јесу паметне соларне клупе, које су у центру града Београда постављене почетком 2021. године.[10] Осим бесплатног бежичног интернета, соларног напајања и модерног дизајна, ове клупе имају сензоре који приказују тренутне временске услове који се односе на температуру, влажност ваздуха али што је за тему рада још значајније стање загађености ваздуха и ниво буке. Дакле, тренутне временске прилике важне за праћење потенцијалних ванредних ситуација, могу да прате не само надлежни органи, већ и сами грађани, који се на овај начин директно информишу ситуацији у граду, што је и једна од основних идеја концепта паметног града. Поред овога, у фебруару 2022. године је у оквиру тржног центра Ушће постављен паметни систем за пречишћавање ваздуха на отвореном, јер је ваздух на саобраћајницама у близини ваздух изузетно загађен што угрожава велики број људи који свакодневно користи овај простор.

---

[8] Дигитални атлас климе Србије налази се на следећој адреси https://atlas-klime.eko.gov.rs/lat/map?dataType=obs&visualization=pro&area=regions

[9] Интерактивна мапа се налази на следећој адреси https://szsgis.beograd.gov.rs/portal/apps/webappviewer/index.html?id=ed921b0d5e6a4b168f5215aa766423bb

[10] Под покровитељством града Београда, компанија Strawberry energy креирала је паметни урбани мобилијар у оквиру пројекта Београд Паметни град (Belgrade Smart City). Више о компанији https://strawberrye.com/

Као део кампање подизања свести и активног укључивања грађана у заштиту амбијента и зеленила Београда, управа града је донела одлуку о развоју апликације Моје дрво за Београд које омогућава грађанима да купе саднице и посаде дрво на некој од локација у граду. Путем апликације може се израчунати и колико угљен-диоксида свако од нас троши и колико стабала треба да засадимо како би се ова потрошња компензовала. Осим тога путем ове апликације грађани могу да пријаве проблеме на постојећим јавним зеленим површинама и предложе нове локације за садњу дрвећа. На овај начин сваки грађанин може, употребом једног савременог информационо-комуникационог решења, учествовати у унапређењу животне средине главног града а тиме и до смањења ризика од појаве таквих временских прилика које могу довести до ванредне ситуације.

У граду Београду постоје предлози решења за паметно управљање ванредним ситуацијама која још нису заживела. Тако је предвиђен развој климатског мониторинг система и базе просторних података и информација о локалној промени климе, укључујући у то и информације о екстремним климатским појавама и непогодама, рањивости појединих подручја (Регионални просторни план административног подручја Београда 2004; Измене и допуне Регионалног просторног плана административног подручја Београда 2011). Осим тога градске власти су се определиле за успостављање и унапређење савремених метеоролошких и хидролошких система за рано упозоравање, метео-аларм, хидро-аларм и систем за климатски надзор, тзв. Climate Watch System (Градска управа града Београда, Секретаријат за заштиту животне средине 2015), који заправо представља онлајн платформу на којој је могуће наћи отворене податке о климатским условима, визуализације и друге ресурсе важне за праћење ефеката климатских промена. Осим тога, још се чека на активирање Интелигентног оперативног центра града Београда.

Потенцијални изазови и ризици примене стратегија паметног града у управљању ванредним ситуацијама

Иако је допринос имплементације стратегија паметног града у управљању ванредним ситуацијама неспоран, у обзир треба узети неке ризике који неминовно прате употребу информационих и комуникационих технологија. Неки од њих везани су за опште ризике увођења дигитализације у процесе управљања градом, док су други проблеми везани за специфичан контекст Београда. Када је прва група ризика у питању, посебно се истиче проблем безбедности похрањених података и приватности корисника технологија (Datta 2015; Townsend 2013). Ово је нарочито случај када су у питању друштвене мреже, имајући у виду да корисници остављају значајан број важних личних података који се могу користити у различите лукративне или криминалне сврхе. Приватне компаније, уколико имају аранжмане у области имплементације неког технолошког решења за унапређење безбедности у граду са локалним или државним властима, могу злоупотребити личне податке за друштвену категоризацију (social sorting), предиктивно профилисање, микро маркетинг и слично (Kitchin 2014). Осим угрожавања приватности грађана, градски системи који су махом руковођени подсредством технологије, могу бити изложени сајбер нападима (Little 2010; Townsend 2013; Kitchin & Dodge 2017).[11]

Постоји читав сет препрека када се говори о имплементацији паметних решења у унапређењу управљања и живота у Београду. У истраживању о паметним градовима

[11] У децембру 2023. године извршен је значајан хакерски напада на Електропривреду Србије, при чему је дошло до комплетног пада информационог система овог јавног предузећа.

у Србији реализованом средином 2020. године, испитаници, који су били стручњаци у јединицама локалне самоуправе и јавним комуналним предузећима, одговарали су на питања о потешкоћама са којима се градови сусрећу у процесу имплементације иницијатива и пројеката из области паметних градова (Дамјаовић, 2021). Као неке од главних проблема испитаници су истакли недовољно ресурса и финансија, затим недостатак експертизе и практичних знања у пословима планирања, реализације и праћења пројеката, као и отпор увођењу нових технолошких решења, недовољно добро препознати развојни изазови и стратешки приоритети, мањак кооперације између различитих нивоа управе и недовољно учешће организација цивилног друштва.

Једна од потенцијалних „кочница" развоју паметних решења у Београду јесте, што упркос вишегодишњим најавама, и даље није развијен систем 5G мреже. Имплементација ове мреже у Србији требало је да се оствари кроз сарадњу са кинеском компанијом Huawei, која је овакве пројекте реализовала у градовима у преко сто земаља на свету[12]. Србија и даље остаје једна од ретких европских земаља у којима није ни започело увођење ове мреже.

У Београду, али и другим градовима постоји велики проблем када је у питању партиципација грађана у унапређењу живота у градовима или пружању комуналних услуга. Једна од кључних компоненти концепта паметног града јесте активно учешће грађана у различитим иницијативама и програмима, тј. имплементација такозваног приступа „одоздо на горе" (*bottom-up*). У том смислу проблем је двострук јер градска власт са једне стране често превиђа реалне потребе грађана приликом покретања неких пројеката у области унапређења безбедности у градовима или уважава „глас народа" тек када дође до бурних реакција или протеста заинтересованих грађана. Са друге стране грађани на овим просторима ретко кад исказују потребу да сами иницирају активности које би за циљ имале унапређење виталних услуга у простору у којем живе. Један од великих проблема у истинској реализацији стратегија „паметног града" у Београду јесте одсуство дијалога између градских власти и грађана о кључни проблемима урбане безбедности и правцима за њихово заједничко решавање.

На београдским улицама постоји велики број надзорних камера. Оваква ситуација може имати далекосежне последице по квалитет живљења у граду, јер грађани прилагођавају своје понашање у ситуацијама када знају да су надзирани, те осим што ће се суздржати од друштвено девијантних понашања, генерално могу осећати мање слободе у коришћењу јавног простора који је покривен камерама. Са друге стране, већи број надзорних камера у граду може водити перцепцији грађана о неком простору као небезбедном сматрајући да су надзорне камере управо постављене на местима која су ризична за боравак.

Закључне напомене

Паметни град промовисан је у академским и стручним круговима као сет иновативних решења заснованих на информационим и комуникационим технологијама које

[12] Неки аутори овај застој у реализацији пројекта 5G мреже у Србији виде у Споразуму о економској нормализацији који је председник Србије Александар Вучић потписао 4. септембра 2020. године у Вашингтону. У споразуму, између осталог стоји: „Обе стране ће у својим мобилним мрежама забранити употребу 5G опреме коју испоручује непроверен продавац. Ако је таква опрема већ присутна, обе стране се обавезују да ће је благовремено уклонити и предузети друге посредничке напоре.", што је протумачено као захтев Сједињених Америчких држава да Србија одбаци опрему Huawei компаније (Prigoda, Bogavac і Čekerevac 2022).

треба да реше горуће проблеме све урбанизованијих градова и унапреде систем њиховог управљања. Област управљања ванредним ситуацијама може бити значајно унапређена кроз примену напредних технолошких решења, дигитализацију и аутоматизацију неких процеса, као и анализу податак у реалном времену, што је од пресудног значаја када наступи ванредна ситуација. У Београду је било могуће идентификовати већи број иницијатива и пројеката за које се посредно може закључити да су засноване на идеји паметног града, а које се могу користити у управљању ванредним ситуацијама. Највећи број ових решења односи се на праћење података о климатским условима, њихова визуелизација кроз ГИС и интерактивне мапе, као и извесне технолошке и „паметне" иновације у области управљања безбедности урбаног саобраћаја. Развој савремених градова темељи се на дигиталној трансформацији, за шта се декларативно определила и градска власт у Београду.

Упркос бројним предностима које предочене стратегије имају, постоји низ проблема у ефикаснијем имплементирању паметних решења за управљање ванредним ситуацијама. Међу њима се налазе недостатак ресурса, недовољна обученост запослених у Градској управи за имплементацију дигиталних решења у управљању и пружању услуга, недостатак политичке воље у имплементацији партиципативног приступа за паметна решења, непокривеност града 5г мрежом и сл. Међутим, један од кључних препрека овог процеса односи се на чињеницу да у Београду идеја паметног града не функционише као интегрисани систем смислено повезаних решења, већ пре као скуп парцијалних иницијатива и пројеката. Без обзира на то, постоји велики потенцијал као и потреба за увођењем савремених информационих и комуникационих технологија у процесе управљања ванредним ситуацијама, које би биле усмерене на превенцију и реаговање на ону врсту појава за коју је процењено да представља највећи ризик по урбану безбедност Београда, његове становнике, изграђено и природно окружење, као и укупан квалитет живљења.

Библиографија

Alshamaila, Yazn, et al. 2023. "Effective use of smart cities in crisis cases: A systematic review of the literature." International Journal of Disaster Risk Reduction 85: 103521. https://doi.org/10.1016/j.ijdrr.2023.103521

Arbolino, Roberta, et al. 2018. "Towards a sustainable industrial ecology: Implementation of a novel approach in the performance evaluation of Italian regions." *Journal of Cleaner Production* 178: 220-236. https://doi.org/10.1016/j.jclepro.2017.12.183

Batty, Michael, et al. 2012. "Smart cities of the future." *The European Physical Journal Special Topics* 214: 481-518.

Beg, Abdurrahman, et al. 2021. "UAV-enabled intelligent traffic policing and emergency response handling system for the smart city." *Personal and Ubiquitous Computing* 25(1): 33-50.

Damjanović, D. (ur.) 2021. *Pametni gradovi Srbije: inovativnost i rezilijentnost lokalnih zajednica u Srbiji 2021. godine.* Beograd: Palgo smart

Das, Diganta, and Jie J. Zhang. 2021. "Pandemic in a smart city: Singapore's COVID-19 management through technology & society." *Urban Geography* 42 (3): 408-416. https://doi.org/10.1080/02723638.2020.1807168

Datta, Ayona. 2015. "New urban utopias of postcolonial India: 'Entrepreneurial urbanization' in Dholera smart city, Gujarat." *Dialogues in human geography* 5(1): 3-22. https://doi.org/10.1177/2043820614565748

Gosavi, Abhijit, et al. 2019. "Discrete-event-based simulation model for performance evaluation of post-earthquake restoration in a smart city." *IEEE Transactions on Engineering Management* 67(3): 582-592.

Ioppolo, Giuseppe, et al. 2016. "Sustainable local development and environmental governance: A strategic planning experience." *Sustainability* 8(2): 180. https://doi.org/10.3390/su8020180

Kitchin Rob. 2014. *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*. London: Sage.

Little, Richard G. 2010. "Managing the risk of cascading failure in complex urban infrastructures." In: *Disrupted Cities*, edited by Stephen Graham, 39-52. London: Routledge.

Prigoda, Lyudmila, Milanka Bogavac, i Zoran Čekerevac. 2022. *Srbija i Pametni gradovi. FBIM Transactions*, 10(1): 71-85. https://doi.org/10.12709/fbim.10.10.01.08

Rob Kitchin and Martin Dodge 2017. "The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention". *Journal of Urban Technology*, 26(2): 47-65, https://doi.org/10.1080/10630732.2017.1408002

Song, Xuan, et al. 2020. "Big data and emergency management: concepts, methodologies, and applications." *IEEE Transactions on Big Data* 8(2): 397-419.

Townsend, Anthony M. 2013. *Smart cities: Big data, civic hackers, and the quest for a new utopia*. New York: WW Norton & Company.

Yigitcanlar, Tan, and Md Kamruzzaman. 2018. "Does smart city policy lead to sustainability of cities?." *Land use policy* 73 : 49-58. https://doi.org/10.1016/j.landusepol.2018.01.034

Градска управа града Београда, Секретаријат за заштиту животне средине. 2015. *Акциони план адаптације на климатске промене са процењом рањивости.* Београд: Градска управа града Београда, Секретаријат за заштиту животне средине

Извештај о реализованим активностима за смањење загађености ваздуха дефинисаних акционим планом за спровођење мера за смањење загађености ваздуха, у оквиру

Плана квалитета ваздуха у агломерацији Београд за период јануар-децембар 2022. приступљено 25.5.2024. https://www.beograd.rs/images/data/c66ead047de72126a798bdd43c692880_7076891497.pdf

План квалитета ваздуха у Агломерацији Београда. 2021. Службени лист град Београда број 46/2021

Регионални просторни план административног подручја Београда. 2004. Службени лист града Београда, број 10/04; Измене и допуне Регионалног просторног плана административног подручја Београда. 2011. Службени лист града Београда, број 38/11.

„SMART CITY" STRATEGIES FOR EMERGENCY MANAGEMENT IN BELGRADE

Abstract: Smart cities are embodied in the idea of using modern information and communication technologies in solving urban security problems and improving the provision of various public services, which should ultimately contribute to a better quality of life for citizens. One area where smart city strategies can be particularly beneficial is emergency management in urban environments. With the help of digital data, connectivity and automatization, different approaches that are connected to the concept of a smart city can significantly improve the early detection, response and adequate management of various events in the city. In this paper, different approaches, policies, activities and strategies that have been promoted, adopted or announced in the city of Belgrade, and which can be labelled as the implementation of the smart city model in the field of emergency management will be presented. In addition, the evident benefits that digitization and automatization have in prevention and response to emergency events, but also the existing limitations in the practice of promoting Belgrade as a smart city from the aspect of emergency management will be addressed.

Keywords: smart city, emergency management, urban security, Belgrade.

ИНТЕРНЕТ АПЛИКАЦИЈЕ ЗА ИНТЕГРИСАНО УПРАВЉАЊЕ ВАНРЕДНИМ СИТУАЦИЈАМА

Анита Кликовац[1]

Апстракт: Управљање системом заштите и спасавања у Републици Србији може се условно поделити на два нивоа, а то су: национални ниво и ниво локалних самоуправа. Централизовано управљање и командовање целокупним системом врши се преко Сектора за ванредне ситуације МУП-а РС кроз систем Одељења за ванредне ситуације која су у надлежности Сектора за ванредне ситуације. На врху ланца командовања налази се Републички штаб за ванредне ситуације, а на крају локални штабови за ванредне ситуације који кроз систем стручно-оперативних тимова обављају задатке на тактичком нивоу. Надлежности Републичког штаба за ванредне ситуације обухватају све нивое управљања па у том смислу Републички штаб непосредно командује како организационим јединица Сектора тако локалним самоуправама. Поменута подела на два нивоа захтева осмишљавање и спровођење система координације, који треба да осим успостављања интеракције републичког и локалног новоа управљања ванредним ситуацијама, омогућеи брзу и прегледну размену података. Овај текст пружа преглед дигиталних система за интегрисано управљање ванредним ситуацијама на подручју Републике Србије – који треба да омогуће имплеметацију законских решења али и координацију између државних институција, пре свега Сектора за ванредне ситуаицје МУП-а Рублике Србије и јединица локалне самопуправе. У тексту се ставља акценат на употребу субјеката од посебног значаја и средстава за заштиту и спасавање, предузимање одговарајућих корака и усклађивање деловања са другим штабовима за ванредне ситуације и мерама државниих органа. Такође, у тексту је указано и на слабости и опасности које претпоставља коришћење овог система, као и на друге електронске системе који настоје да допуне поменуту апликацију, и одговоре специфичнијим захтевима јединица локалне самоуправе – које су по новом закону препознате као носиоци примарних улога у управљању ризиком од катастрофа наодређеној територији.

Кључне речи: ванредне ситуације, интегрисано управљање, дигитална база података, интернет апликације.

Увод

Сва друштва у свету, без обзира на друштвено уређење или степен развијености економских, политичких, културних или других добара, подлежу одређеном облику угрожавања који носи већи или мањи степен опасности по њихов опстанак и развој. Територију Републике Србије непрекидно угрожавају бројне и разноврсне опасности које се, условно, могу сврстати у природне (елементарне) и техничко-технолошке несреће, а које угрожавају људе, материјална добра и животну средину. Друштве-

[1] Одељење за ванредне ситуације у Смедереву, Сектор за ванредне ситуације, Министарство унутрашњих послова, anita.klikovac@mup.gov.rs

на заједница им се супротставља, у границама својих техничких и организационих могућности. Учесталост катастрофалних последица елементарних непогода и технолошких инцидената у чудном је раскораку у односу на развој техничких средстава за заштиту и спасавање, и успостављених стандарда превенције. Иако су поменуте мере превенције и заштите очигледно пружиле значајне резултате – на шта јасно указује поређење последица елементарних непогода и других опасности у развијеном и неразвијеном делу света – промена климе и густина насељености представљају нове факторе ризика, који захтевају не само иновиране видове заштите и спасавања, него и знатно бољу организацију која треба да омогуће најбржи могући одговор на катастрофе.

Појам *ризика* у области о којој је реч, можда најадекватније одређују Ансел и Валатон, према којима се он може дефинисати као „производ вероватноће и последица догађаја".[2] То значи да се на основу процене вероватноће могу предвидети последице, али и да се може утицати на смањење вероватноће катастрофалних последица, одређеним поступцима и радњама, како у периоду пре него што дође до катастофе, тако и када се ради о брзини спасавања и ублажавању последица.

Са друге стране, појам угрожености је изведен из појма ризика, као специфичност, у смислу могућности нарушавања друштвеног или економског система, опасности по људе, имовину и функционисање базичних институција неке државне заједнице.[3]

Из претходних појмовних одређења произлази да су процене ризика са једне, и планови заштите и спасавања, са друге стране, оне делатности којима се могу спречити или умањити катастрофалне последице како елементарбних непогода, тако и техничко-технолошких инцидената.

У том смислу, може се говорити о (1) делатностима које треба да омогуће јасније очитавање могућности од катастрофа, и путем SWOT анализе подстакну јачање система за њихово спречавање односно смањење опасности по људе и имовину, и (2) о усавршавању организационо-комуникационих техника, у сврху успостављања интегрисаног управљања ванредним ситуацијама.

Пројекат DISARIMES (*Strengthening Integrated Disaster Risk Management Systemin Serbia*) представља стварање велике базе података, у коју би биле унете све релевантне информације о учесталостима катастрофа и њиховом току у прошлости, објективним условима њиховог понављања и могућим временским интервалима понављања и на основу тога стварање атласа и мапа рањивости – па самим тим и дефинисање непосредних опасности на одређеним деловима териоторије Србије. Овај пројекат се, међутим, не исцрпљује у стварању јединствене базе података досадашњих експертиза научних института и завода, него је отворен за нова истраживања, критичке анализе и сталне иновације, које треба да омогуће „широки спектар комуникације и ширење информација о резултатзима истраживања и иновативним решењима у свим фазама управљања ризиком од катастрофа" – а то значи да се он не исцрпљује у синтези научних података, него да се односи и на подручје непосредног одговора друштвене заједнице на опасности од потенцијлано катастрофалних догађаја.[4]

---

[2] Ansell J., Wharton F., Risk: analysis, assessment, management, John Wiley & Sons, 1992.

[3] Владимир М. Цветковбић, „Перцепција ризика од природних катастрофа изазаваних поплавама", Војно дело, 5/2017, стр. 160-175.

[4] Vladimir Cvetković, „Jačanje sistema inegrisanog upravqawa rizicima od katastrofa u Srbiji: DISARIMES – Strengthening Integrated Disaster Risk Management Systemin Serbia: DISARIMES, u (V. Cvetković, ur.) Taktika zaštite i spasavanja u vanrednim situacijama: iskustva sa terena i pouke, Naučno-stručno društvo za upravljanje rizicima od katastrofa i Međunarodni institut za istraživanje katastrofa, Beograd, 2021, str. 77-110.

Јединствена база података, дакле, треба да повећа степен превентивних мера, на основу адекватног предвиђања могућности и учесталости катасофалних догађаја, према различитим типовима потенцијалних опасности, за сваки део Србије, и самим тим утиче на трансформацију самог ситема из реактивног у проактивни – односно да афирмише приступ едукације становноштва на потенцијалне опасности, рано упозоравање, и примену унапред осмишљених мера у циљу заштите људи и имовине.[5]

Са друге стране, ова база података, и SWOT анализа захтевају не само осмишљавање локалних планова заштите и спасавања, него и утемљење непосредних организационих техника, које треба да допринесу што оптималнијем раду субјеката за спречавање катастрофа и управљање ванредним ситуацуијама, од републичког до нивоа локалних самоуправа.

Искуство поплава из 2014. године, на пример, указује на потребу да приликом стављања под контролу ванредних ситуација треба да буду задовољена два разлилчита аспекта: интерес локалне заједнице и општи интерес, односно да се заштита и спасавање у локланим срединама морају спроводити уз поштовање како локлалних потреба, тако и неких општих императива.[6]

Посебан проблем, према томе, представља такозвано интегрисано управљање ванредним ситуацијама, односно усмеравање свих субјеката од значаја, на разуђеној територији која је погођена катастрофом – на најбољи могући начин, у циљу спасавања људи, животиња и имовине.

Стратегија и законска регулатива

Према Закону о смањењу ризика од катастрофа и упрљвљању ванредним ситуацијама из 2018. године, јединице локалне самоуправе имају примарну улогу у управљању ризиком од катастрофа.[7] У складу са овом интенцијом законодавца, Уредба о саставу, начину и организацији штабова за ванредне ситуације из 2020. године одређује извесно проширење састава штабова у јединицама локалне самоуправе на представнике свих правних субјеката који могу да допринесу смањењу ризика од катастрофа, у три фазе раде – превентивној, оперативној и фази опоравка.

Тако, према члану 7, који се односи на општинске штабове за ванредне ситуације стоји да у њиховом саставу треба да буду, осим команданта, заменика команданта и начелника – представници органа општине „у чијем делокругу су послови из области: одбране; информисања; инспекције; комуналних делатности; стамбених послова; здравства; пољопривреде, водопривреде, шумарства; рада; социјалне политике; заштите животне средине; образовања; урбанизма; грађевинарства; саобраћаја; геологије, рударства и енергетике и други у складу са проценом општинске управе и организационе јединице Надлежне службе" – као и представници јавних предузећа, привредних друштава, МУП-а и Војске Србије, Црвеног крста, удужења грађана и других правних лица – што је стајало и у претходном Закону о ванредним ситуацијама.[8]

---

[5] Ibid, str. 84.

[6] На пример, заштита од поплава у некој јединици локлане самоуправе може да угрози заштиту и саопасавање уд ругој локалној самоуправи.

[7] Закон о смањењу ризикаод кастастрофа и управљању ванреднимситуацијама, Службени Гласник Републике Србије, 83/2018, члан 5. став 1.

[8] Уредба о саставу, начину и организацији рада штабова з аванредне ситуације, Службвени гласник Републике Србије, бр-. 27/2020, члан 7. став 6. алинеја 1.

У многим локалним самоуправама, сходно овој уредби, проширен је састав чланова Штаба, пре свега у функцији јаснијег сагледавања потенцијалних ризика и њиговог превенирања. Међутим, проширен састав штабова је наизвестан начин повећао проблем њиховог брзог сазивања, нарочито у оперативној фази, када је значајно што пре донети одговарајуће наредбе, у циљу спашавања људи и имовине од елемнтарних непогода и других опасности. Потреба за брзим реаговањем подстакла је да се успостави систем инегрисаног управљања ванредним ситуацијама, који би пружио могућност координације субјеката са републичког, окружног, градског и/или општинског нивоа.

Члан 22. *Закона о смањењу ризика од катастрофа и упрљвљању ванредним ситуацијама* уређује успостављање електронског, интерактивног регистра, односно географско-информационе базе података. У ставу 1. поменутог члана Закона утврђено је да ову базу података за територију Републике Србије води Министарство унутрашњих послова „у сарадњи са надлежним органима државне управе, другим надлежним органима и имаоцима јвних овлашћења".[9]

Под „имаоцима јавних овлашћења" подразумевају се такозвани „недржавни субјекти", којима се у складу са чланом 137. Устава Републике Србије могу поверити јавна овлашћења – а то су аутономне покрајне, јединице локалне самоуправе, јавне установе, јавне агенције, итд.[10]

На основу поменуте законске регулативе систем интегрисаног управљања ванредним ситуацијама путем информационог система, подразумева, најпре, (а) успостављање јединствене базе података – на основу процена ризика, планове заштите и спасавања, уз ажурне податке о свим субјектима који могу да буду искоришћени у функцији превенирања или смањења последица катастрофалних догађаја, систем раног упозорења који је праћен сценаријима развоја ситуације (највероватнијег и најгорег могућег следа догађаја), а потом, (б) електронски систем размене података између штабова за ванредне ситуације и субјеката на терену (субјеката од посебног значаја за заштиту и спасавање, повереника или јединица цивилне заштите опште намене или добровољних ватрогасних друштава, волонтера, и слично).

Софтверске апликације

На основу уводних запажања, јасно је показано да управљање системом заштите и спасавања у Републици Србији може се условно поделити на два нивоа, а то су: национални ниво и ниво локалних самоуправа. Централизовано управљање и командовање целокупним системом врши се преко Сектора за ванредне ситуације МУП-а РС кроз систем Одељења која су у надлежности Сектора за ванредне ситуације. На врху ланца командовања налази се Републички штаб за ванредне ситуације, а на крају локални штабови за ванредне ситуације који кроз систем стручно-оперативних тимова обављају задатке на тактичком нивоу. Надлежности Републичког штаба за ванредне ситуацијеобухватају све нивое управљања па у том смислу Републички штаб непосредно командује како организационим јединица Сектора тако локалним самоуправама.

[9] Закон о смањењу ризикаод кастастрофа и управљању ванреднимситуацијама, Службени Гласник Републике Србије, бр. 83/2018, члан 22. став 1.

[10] Милосављевић, Богољуб-Марић, Предраг-Бабовић, Живко – Марковић, Милан, Коментар Закона о смањењу ризика од катастрофа и управљању ванредним ситуацијама, Академска мисао, Београд, 2019, стр. 89.

У оквиру целокупног система заштите и спасавања не постоји јединствен софтвер за управљање, командовање и надзор, односно дигитализација у овој области је у односу на остале системе у Републици Србији на најнижем нивоу.

Из тог разлога, најпре, долази до отежаног прикупљања података на терену током ванредних ситуација, успореног и често закаснелог прослеђивања информација уз ланац командовања на локалном и републичком нивоу, дугог периода сакупљања информација на нивоу округа, односно споро пристизање информација о стању на терену у окружна Одељења Сектора за ВС. Такође, приликом испољавања више опасних ситуација истовремено, постојећи систем не пружа могућност систематичног и прецизног прикупљања информација и на основу њих процене стања у циљу предузимања адекватних мера.

Дакле, непостојање директног и перманентног увида у стање на терену током ВС, комаданата штабова (локални и Републички штаб), јединственог систем праћења евакуисаних лица од момента евакуације па све до њиховог смештаја у прихватне центре и након тога отпуштања, знатно отежава оперативну фазу рада и отвара могућности за грешке, које могу да угрозе људе и имовину. Такође, након ванредне ситуације, постојећи систем не пружа могућност упоредне анализе података као што су листа евакуисаних лица, локације појединачних догађаја током ВС и извештаја о штети се не врши, а у процесу опоравка и обнове извештаји о штети се израђују на папиру, без директног увида у рад лица која прикупљају те податке на терену. Постоји неколико софтверских решења, али ниједно од њих не обједињује поменута два нивоа управљања ванредним ситуацијама – односно ова су решења управљена ка једном или другом новоу – републичком или локалном. У овом тексту указаћемо на два таква софтвера, који би могли да буду интегрисана у јединствени и компатибилни инструмент за јединствено управљање ванредним ситуацијама, на оба нивоа.

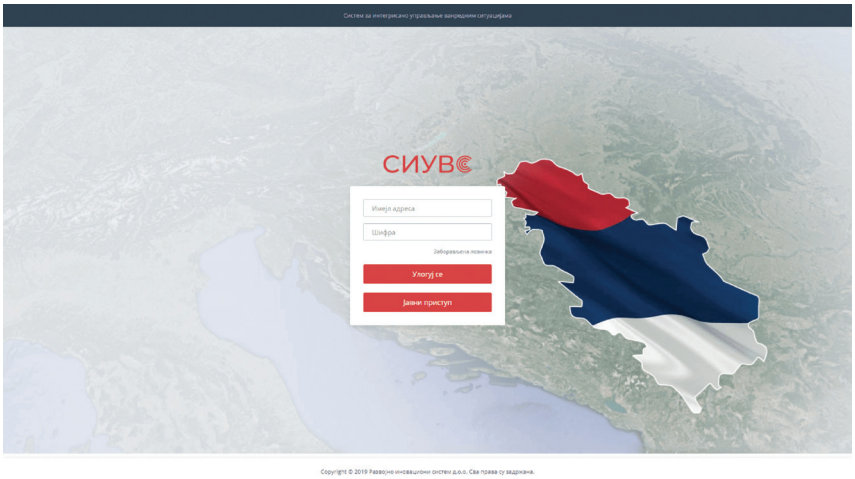
Сиувс апикација

Годину дана после доношења новог Закона, 2019. године, прва софтверска апликација, која омогућује размену информација и приступ бази података о ризицима са сваку општину на подручју Републике Србије.

ДРИС-апликација је у ствари – Систем за интегрисано управљање ванредним ситуацијама (СИУВС). Дигитализовање битних информација овде је комбиновано са различитим могућностима ажурирања. Министарство унутрашњих послова, односно Сектор за ванредне ситуације имају увид у податке из свих крајева Србије, уз могућност да непосредно, наредбама, утичу на субјекте заштите и спасавања. Са друге стране, апликација омогућује да јединице локалне самоуправе дигитализују садржај локалних Процена ризика од катастрофа и Планова заштите и спасавања – основна документа за поступање у циљу смањења ризика од катастрофа, у које ће истовремено имати увид и органи државне управе, првенствено Сектор за ванредне ситуације.

Подаци који су унети у СИУВС-апликацију чувају се на две централне локације, просторно значајно удаљене, тако да база података може да опстане и у случају великих катастрофичних догађаја, у којима би дошло до значајног оштећења инфраструктуре у већем делу Републике.

Ради лакпше доступности, предвиђено је да се СИУВС-апликацији приступа са централног интернет претраживача – тако да за њено коришћење није потребна никаква додатна инсталација рачунарских програма. Апликацији се приступа уношењем корисничког имена и лозинке.

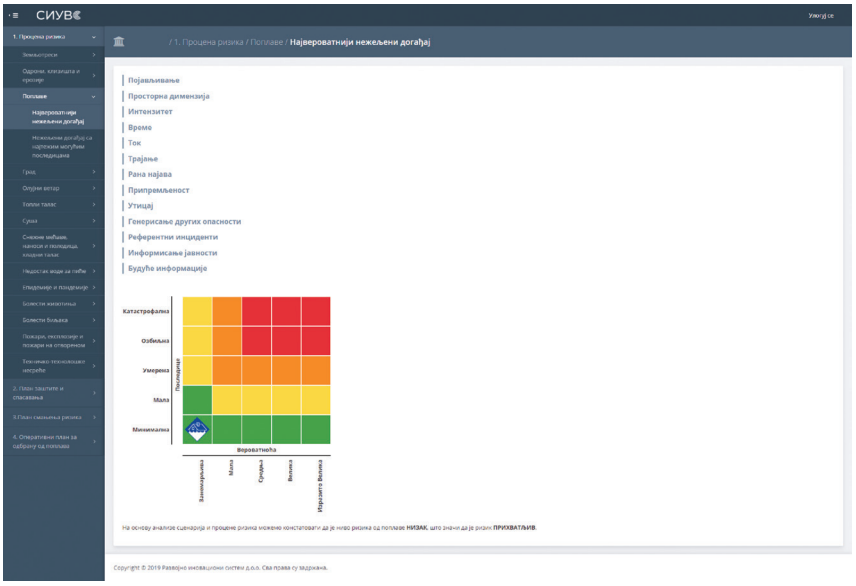


Слика 1: Приступ интернет-апликацији СИУВС

Корисници апликације могу се разврстати као администратори – који могу да уносе податке, бришу податке и мењају текстове већ унете на апликацију и корисници, који имају увид у целокупну базу података или њене поједине делове, али без могућности брисања података или уз ограничене могућности уношења података (уношење података одређеног нивоа). Уношење података и њихову контролу би требало да обављају или запослени у посебној стручној служби локалне самоуправе или овлашћени чланови штаба за ванредне ситуације. У другу категорију спадају командант, заменик команданта и начелних Штаба, који треба да имају увид у све информације, а у трећу категорију чланови Штаба – којима је, ради прегледности, омогућен увид у посебне делове апликације. Администратори и поменуте две категотије имају могућност интерактивне размене података, који се тичу деловања у току ванредне ситуације. Надаље, апикацији могу да приступе и субјекти од посебног значаја за заштиту и спасавање, повереници или заменици повереника цивилне заштите, чланови јединице цивилне заштите – а предвиђено је да путем посебног канала и инсталације на мобилном телефону, апликацији могу да приступе и грађани, како би се, као волонтери, укључили у акције заштите и спасавања.

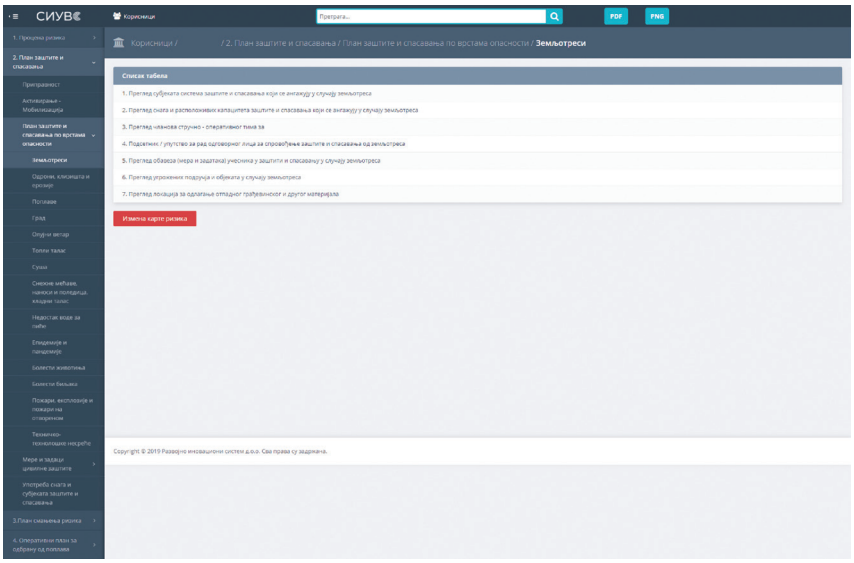
Основна сврха ове апликације је унос, односно дигитализација података – Процене ризика од катастрофа и Плана заштите и спасавања. Наиме, ови документи предвиђају сценарија, упозоравајуће сигнале и упућују на конкретне радње које треба предузети у складу са проценом вероватноће такозваног највероватнијег нежељеног догађаја и највероватнијег нежељеног догађаја са најтезим могућим последицама.

У том смислу, апликација пружа могућност непосредне комуникације са члановима штаба, односно хитно сазивање Штаба, и сигнализирање хитности, односно класификацију опасности у категорије „жуте", „наранџасте" и „црвене". Другим речима, омогућено је хитно сазивање штаба, једноставним избором одређене опције, које треба да обезбеди не самообавештеност чланова штаба о хитности доласка на место где штаб заседа, него и одређене детаље у вези са ванредном ситуацијом, који проистичу из сценарија, на основу процене ризика.



Слика 2: Информација о вероватном сценарију ванредне ситуације

Такође, будући да План заштите и спасавања садржи прецизан адресар субјеката заштите и спасавања, односно бројеве телефона и интернет адресе, уз помоћ апликације могуће је дневно ажурирање ових података али исто тако и преглед свих субјеката који су од значаја за заштиту и спасавање.

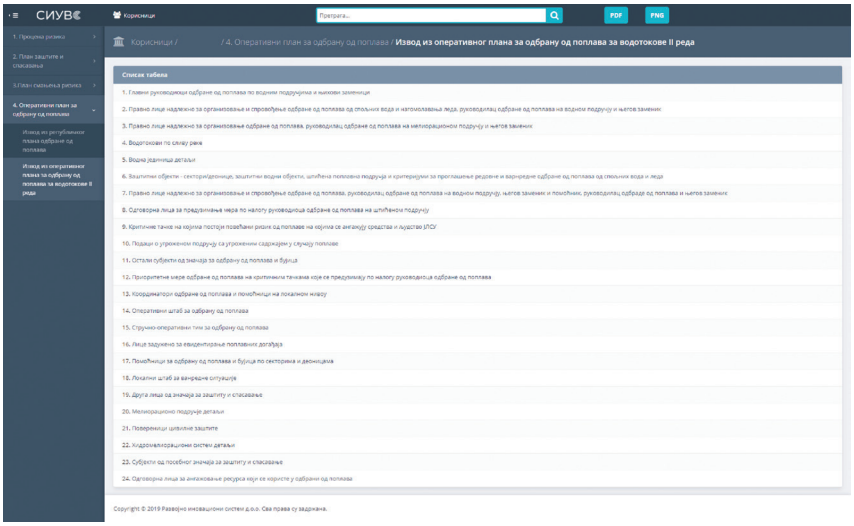


Слика 3: основни подаци за заштиту и спасавање према процени ризика

За сваки процењен ризик у апликацији су не само информације о системима заштите, него и подаци о субјектима од посебног значаја за заштиту и спасавање које

треба ангажовати, о члановима стручно-оперативних тимова, са свим неопходним бројевима телефона, чиме је омогућена лакша координација одозго на доле, односно од командантна штаба и његових чланова према јединицама које се непосредно ангажују на терену. Оно што представља основну предност оваквог система свакако је унапред планирани предлог конкретних мера на основу сценарија. Основна слабост, са друге стране, је у томе што саме локалне самоуправе, на основу искустава, доносе процене ризика, тако да је целокупан систем заснован искључиво на овој процени. На пример, мали број локланих самоуправа у Србији је у могуће ризике уврстио земљотрес, иако се већи део Србије налази у зони у којој су могући снажни земљотреси, а сеизмички хазард повећава и знатан број објеката који нису грађени према сеизмичким стандарнима. У случају катастрофалне ситуације, чији ризик није обухваћен планом, већи део ове апликације није употребљив, па би у том случају Штаб за ванредне ситуације практично могао да користи само адресар субјеката од посебног значаја за заштиту и спасавање.

Са друге стране, ова апликација подразумева и комуникацју одоздо према горе, односно могућност комуникације са рукводициома МУП-а РС.



Слика 4: Адресари субјеката за заштиту и спасавање

Протектис систем

За разлику од СИУВС-а, ПРОТЕКТИС је програм непосредног управљања ванредном ситуацијом општинских штабова за ванредне ситуације. Овај програм не предвиђа базу података о најучесталијим катастрофалним догађајима или елементарним непогодама, већ садржи само најосновније податке о јединицима или лицима која ће на терену бити ангажована за заштиту и спасавање, уз могућност уноса података са терена. Предност ове интернет апликације је у двосмерној комуникацији између разлилитих носиоца ангажованости у конкретној ванредној ситуацији на локланом ниовоу.

За разлику и СИУРС-а, који је дизајниран тако да задовољава потребе увида Републичког штаба за ванредне ситуације и догађаје у локалним самоуправама, ПРО-

ТЕКТИС настоји да развије систем управљања на нивоу самих локалних штабова за ванредне ситуације, односно да омогући лакшу комуникацију између команданта штаба, са члановима штаба, стручно-оперативним тимовима, субјектима од посебног значаја за заштиту и спасавање, и на крају са члановима јединица цивилне заштите опште намене на терену, односно члановима доборовољних ватрогасних друштава, као и волонтерима. Овај систем се може поделити на неколико нивоа командовања и управљања.

Предности „ПРОТЕКТИС" апликације:

Централизовано управљање целокупним системом заштите и спасавања;

Једноставно, прецизно и једнообразно прикупљање података;

Искључена је потреба за ангажовањем великог броја лица;

Није потребна дуготрајна обука за коришћење софтвера;

Формирање и достављање извештаја о стању на терену је једноставно, јасно формулисано и искључује могућност произвољног рада појединца;

Руководиоцима на свим нивоима омогућава тренутан увид у све битне параметре у реалном времену;

Прослеђивање информација јединицама на терену;

Архивирање о догађајима се врши аутоматски и врши се њихово трајно складиштење што искључује могућност губитка података о догађајима из прошлости и

Уштеде кроз смањен број потребних лица на терену, искључује потребу за скупим системима комуникације, јефтино одржавање система, лаку надоградњу и унапређивање система.

Међутим, овај систем не подразумева коришћење података о сценаријима могуће катастрофе, детаље из Планова заштите и спасавања, односно оне податке које треба да има у виду виша инстанца у командовању и зато је мање подесан као систем који би пружио јединствено управљање од СИУРС-а, који може бити надограђен у том правцу, мада је дизајн овог програма у целини неприлагођен брзом деловању на тарену (постојање много опција, чија прегледност није увек најоптималнија).

Протектис се састоји из три целине:

1. „Базе података", односно превентивног евиденти-рање георефернцираних критичних локација, као и евиденција рањивих категорија грађана пре ванредне ситуације;

2. „Протекти софтвер" је централни софтвер за управљање и командовање, током ванредне ситуације и

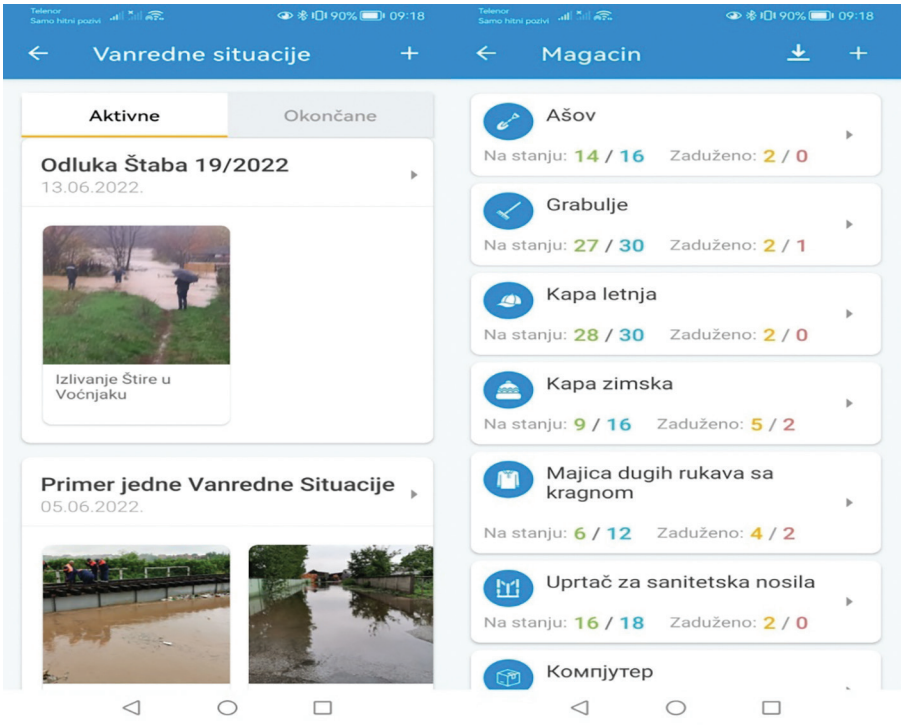
3. „Обнова" извештаји о штети-Електронски извештаји који служе да према унапред дефинисаним правилима и критеријумима, прикупе податке са терена, након настале штете.

Централни софтвер који служи да олакша комуникацију, надзор, прикупљање и обраду података током ванредне ситуације приказан је на слици бр.5.

Слика 5: Централни мени Протектиса за андроид платформу

Као што показује основни садржај ове апликације, он омогућује најпре приступ основним подацима о актуелној ванредној ситуацији, јединицама цивилне заштите (контакти чланова ових јединица, повереника и заменика повереника), стање у магацину (опреме која се користи у ванредним ситуацијама), мапе, које пружају преглед угроженог подручја и информације, које пристижу са терена.

Иако ова апликација пружа могућност јасне евиденције о делатностима чланова јединица као и тачно задуживање опреме и пражење стања у магацину – овде, као што се јасно може видети, изостају опсежније информације не само о природи ванредне ситуације, него и о могућем будућем сценарију. Овим ће информацијама, у току ванредне ситуације, свакако располагати Штаб, али не и јединице на терену. Тако се интерактивност, која треба да буде предност ове апликације у односу на СИУРС, поново затвара у подручје контроле Штаба, који, самим тим, не може да има ваљану интеракцију података, баш из разлога што јединице на терену и по јединци који њиме рукводе, немају комплетне информације, и нису у прилици да сагледају ширу слику. На пример, у случају поплава – припадницима цивилне заштите на терену је од значаја информација да ли се очекују нове падавине, и да ли је у изгледу евакуација становништва, са ког подручја и на које локације, јер ће у складу са тим лакше да осмисле одбрану и успоставе непосредну организацију и распоред људи и опреме на терену.



Слика 6: Опис ванредне ситуације и стање у магацину опреме

Несумњиво је да ПРОТЕКТИС апликација користицима допушта најпре размену података, укључујући и фотографије, надзор над радом и могућност комуникације са свим јединицама на терену; вођење евиденције о материјалним средствима, ефикасну

израду једнообразних извештаја, као и да систем садржи могућност надоградње сходно захтевима и потребама локланих самоуправа. Међутим, одсуство података о мрежи сарадника, субјеката од посебног значаја, а пре свега основних планских докумената – систем остаје при подели на кориснике ових информација и пуке извршиоце, што је заправо у суспротности са његовим примарним интенцијама.

Са друге стране, апликација предвиђа и евиденцију опреме за заштиту и спасавање у централном магацину, а могућ је и унос података о другој опреми, на локацијама које су у близини могућих или актуелних догађаја који захтевају брзо реаговање.

Потпуна листа опреме и материјалних средстава подразумева прегледну евиденција за сваку појединачну опрему уз јасно назначен приказ укупног, задуженог и расположивог стања, једноставан преглед задужене опреме по корисницима, једноставан процес завођења нове опреме и могућност креирања извештаја о опреми.

Са друге стране, ПРОТЕКТИС апликација омогућује и поједностављен процес обавештавања како члановима штаба, тако и јединицама, или волонтерима на терену. То је омогућено путем једноставног креирање наслова и текста обавештења, могућности таргетирања појединачних група којој су обавештења намењена, а историја обавештења налази се сачувана у апликацији.

Апликације и рано упозоравање

Опасност од поплава је у Србији детектована као једна од основних потенцијално катастрофалних догађаја. Из тог разлога, не само да се путем Процене ризика од катастрофа и Планова заштита и спасавања посебна пажња обраћа на усавршавање система за одбрану од ове елементарне непогоде, него је такође разрађен и систем за рано упозоравање. Овај систем је зансован на различитим облицима процене. Најпре, у функцији детектовања опасности од поплаве на одређеном подручју користи се статистички прорачун вероватноће, заснован на Пирсоновим функцијама трећег типа.[11] У основи, реч је о моделу за израчинавање вероватноће, који описује везу X (екстремне појаве) и вероватноће њене појаве P, у низу посматрања, односно забележених екстремних догађаја у претходном периоду (вероватноћа појаве задатог екстрема – P(X).[12] У том смислу, у функцију треба да буде уведена и појава случајне промењиве (x) што подразумева расподелу вероватноће превазилажења $F(x)=P\{X<=x\}$ и непревазилажења $P\{X>x\}=1 - F(x)$. Према томе, може се израчунати ниво обезбеђености за велике воде: $P\{X<=x\}= F(x)$ као обезбеђеност, односно $P\{X>x\}=1- F(x)$ као необезбеђеност, док се повратни период за велике воде израчунава путем формуле: $T(x) = 1/P\{X>x\} = 1/1 - F(x)$[13]

Статистички прорачиун је веома значајан када се ради о изградњи система за одбрану од поплава, јер се рачуна повратни период неке појаве и у складу са тим калкулише ниво безбедности и оправданост улагања. Слабост овог метода је, превасходно, у промени самих климатских карактеристика, односно у све чешћој појави метеоролошких екстрема, која згушњава лонгитудинални распон појава, али се на основу процену згушњавања таласа ипак може пружити релативно прецизан модел повратности екстремних појава.

---

[11] Владимир Јаковљевић, Цивилна заштита у републици Србији, Универзитет у Београду, Факултет безнедности, Београ, 2011, стр. 232.

[12] Biljana Popović, Matematička statistika i statističko modelovanje, PMF UN, Niš, 2003, str. 181 i dalje.

[13] У том смислу, ако је T, например, 200 метара кубних воде једнак 50, то значи да постоји вероватноћа да ће он бити барем једномпревазиђену том периоду.

Плувиометријска метода, са друге стране, подразумева процену максималних могућих падавина, према метеоролошким моделима, који су поодледњих година веома прецизни. Процена падавинског потенцијала циклона, и прориачун њиховог кретања, значајан је податак а у предвиђању могућих катастрофалних догађаја, али овај податак сам по себи не пружа јасну слику очекиване појаве; на пример, од засићености (сатурације) земљишта зависи да ли ће максимална прогнозирана количина падавина на неком простору изазвати катастрофалну последицу, или само упозоравајуће нивое водотокова.[14]

Промена рељефа, односно дотока и количине воде у сливу, што је у поседње време производ комасације, или изградње привредних хидролошким система (хидроцентрала, система за наводњавање, вештачких језера) претпоставља и процену на основу *емпиријске методе*.[15] У ову мероду спада и посматрање тренутног водостаја, сатурације земљишта претходним падавинама, нагомилавање леда. Ова метода, подразумева, дакле, праћење емпиријских параметара, у шта сапдају и подаци са аутоматских метеоролошких и хидролошких станица, постављених углавном на свим водотоковима за које је процењено да представљају потенцијалну опасност.

Прогноиза пораста водостаја за велике реке оставља места за накнадне дораде, односно за допуну предложених мера, јер је њихов пораст у највећем броју случајева постепен. Са друге стране, бујични водотокови предствљају специфичност, не само због брзог надоласка поплавног таласа, него и на бази микро-карактеристика, падавинскогрежима у непосредно претходећем периоду, и слично. Из тог разлога, посебно место међу интернет апликацијама заузимају дигитлани системи за упозоравање на бујичне поплаве. Ови системи намењени су такозваним брзим водотоковима, за које је искуство из 2014. показало да представљају основну опасност за живот људи, животиња и имовину, приликом великих падавина на одређеном простору.

Република Србија, са друге стране, поседује системе за рано упозоравање на водотоковима другог реда, али податке очитава Републички хидрометеоролошки завод (РХМЗ), и потом их презентује на свом сајту, дајући истовремено и прогнозу пораста, стагнације или пада новоа водотокова. Слабост оваквог система обавештавања је најпре у кашњењу података, јер оператери на сајту РХМЗ уносе податке са целокупне територије Србије, па они понекад касне и више часова. Исто тако, ови системи за упозоравање, иако најављују велике падавине и потенцијлно угрожавајуће метеоролошке појаве за неколико дана унапред, не дају аларм у случају непосредне угрожености. Другим речима, дежурни у оперативним центрима или штабовима би, на основу података о брзини подизања водостаја (такозвани Δ/h) сами доносили процену о предузимању одређених мера, укључујући и евакуацију.

Посебан проблем је то што уређаји на мерним местима некда нису у функционланом стању, а РХМЗ често није у стању да одмах приступи оправци. Зато се може догодити да у условима непосредне опасности од катастрофалног догађа, изостане очитавање значајних података. Из тог разлога, у свету, а однедавно и у суседним земљама, осмишљен је другачији концепт, који подразумева миниторинг уз помоћ софистицираних уређеја, који одмах шаљу податке оперативним центрима или задуженим лицима при штабовима за ванредне ситуације. У последње време популаран је систем који уз помоћ рачунара са картицама, и сензора на терену, мери количину воде изван минор корита

[14] О томе више види у Đuro Radinović, Analiza vremena, Zavod za izdavanje udžbenika SR Srbije, Beograd, 1969.

[15] Владимир Јаковљевић, стр. 233.

река, и региструје појаве воде на саобраћајницама и у приобалном подручју.[16] Такође, у циљу већег обухвата података, уређаји на терену могу поседовати и сензоре за мерење температуре, влажности ваздуха, брзине ветра, нивоа падавина, ваздушног притиска и слично. Ови подаци се уз помоћ гугл-мапе интегришу у веб-сервисе, односно интернет апликације за управљање ризиком, које онда администратор може да проследи јединицама цивилне заштите опште намене на терену, ради евакуације становништва или предузимања других хитних мера. Ови системи могу бити програмирани и на тај начин да пружају рана упозорења, односно да указује на најгори могући и оптимлани сценарио. Хардвери за поменуту сврху су веома мали, и зато се називају – картичним рачунарима. У литератити се посебно описују Ардуино уно и Розбери пи – који имају могућност слектронског спајања са склоповима сензора. Преносивост и мала потрошња електричне енергије чине ове системе изузетно погодним за теренски рад, и комуникацију питем вај-фаја или ГПРС мреже, интернет конекције или СМС порука.[17]

Слика 7: Пријемни читал картица АМС система (мреже)

Са друге стране, сами сензори се не резликују од оних који су већ у употреби. На тај начин локална самоуправа може доћи до података о количини падавина, изгледима за падавине у наредних неколико сати, брзини подизања водостаја, тренутној стању на терену, што је знатно погодније од ослањања на податке РХМЗ, који често касне више часова – а познато је да бујучни водотокови представљају посебну опасност управо због брзог надоласка поплавног таласа.

Аутоматски мерни системи, дакле, прецизно бележе параметре од значаја за процену метеоролошких догађаја – од водостаја до вибрација земљишта, које указују на стварање потенцијалних клизишта. На основу мреже мерних система, развијен је SMHI/HBV модел, који је развила Шведска метеоролошка служба. Овај модел подразумева континуирано праћење и анализу већег броја параметара, који могу да знатно утичу на епиријску анализу и доношење закључака о конкретним активностима.[18] Такође, подразумева континуирано порађење података на великом подручју уз помоћ разгранате мреже станица-модула, покривајући не само приобаља реке, него и планине, бележећи висинска струјања, врсту вегетације, сатурација земљишта падавинама, температуру, количину атмосферског талога који није у тећном агрегатном стању – и у случају прорачуна пружа јасан модел наступања катастрофалних догађаја и предлажен спровођење хитних мера.

[16] Енес Шакрак, Милан Добројевић, „Прототип система за раноупозороавање на бујичне поплаве у брдско-планинским пределима заснован на ионтренету ствари", Беозбедност, Vol. LXIII 1/2021, стр.98-114.

[17] Ibid, str. 104.

[18] Ivković M., Plavšić J., Vladiković D., „Primena modela HBV za hidrološkuprognozuna slivu reke Jadar", Vodoprivreda, 44 (2012) 258-260 p. 257-263.

Закључак

Упркос дигитализацији и настојању да се дизајнирају електронски системи који ће олакшати управљање ванредним ситуацијама у Србији и даље није успостављен јединствен систем управљања који би омогућио коришћење података и сарадњи више нивоа у ланцу комадовања, у функцији спречавања катастрофалних последица по људе и имовину. Предности СИУРС-а су у томе што омогуће јединствени увид свих нивоа комадовања ванредним ситуацијама, од републичког до локалног, и на основу тога могућност координираног деловања на већој територији. На другој страни, ПРОТЕКТИС омогућује адекватније управљање ванредним ситуацијама на подручијима локалних самоуправа. Његова је предност у складиштењу података која су од значаја у току саме ванредне ситуације. Недостатак овог програма је изостанак увида свих лица која учествују у спречавању катастрофа у планске документе, који, будући да нису у електронској форми, остају познати само сужбеницима локланих самоуправа задуженим за ову област рада. Основна опасност је у немогућности сагледавања свих потенцијалних опасности; интеракције је боља него што предвиђа СИУРС када је реч о комуникацији штаба и јединица на терену али изостаје непосредан увиод стручака на терену у све моделитете догађаја, односно они морају да буду ослоњени на штаб и његову процену, што у ствари битно ограничава интеракцију, која је комуникативно обезбеђена. У том смислу, стварање јединственог електронског система раног упозоравања, праћења и управљања ванредним ситуацијама чека адекватнији законски оквир.

Библиографија

Ansell, J -. Wharton, F:*Risk: analysis, assessment, management,* John Wiley & Sons, 1992.

Јаковљевић, Владимир. Цивилна заштита *у* републици Србији, Универзитет у Београду, Факултет безнедности, Београ, 2011.

Закон *о* смањењу ризика од кастастрофа *и* управљању ванредним ситуацијама, Службени Гласник Републике Србије, 83/2018.

Ivković,M. Plavšić, J. Vladiković,D. *„Primena modela HBV za hidrološku prognozuna slivu reke Jadar",* Vodoprivreda, 44 (2012) 258-260 p. 257-263.

Милосављевић, Богољуб - Марић, Предраг - Бабовић, Живко – Марковић, Милан, Коментар Закона о смањењу ризика од катастрофа и управљању ванредним ситуацијама, Академска мисао, Београд, 2019.

Popović, Biljana, *Matematička statistika i statističko modelovanje*, PMF UN, Niš, 2003.

Radinović,Đuro, *Analiza vremena*, Zavod za izdavanje udžbenika SR Srbije, Beograd, 1969.

Cvetković,Vladimir, *„Jačanje sistema inegrisanog upravqawa rizicima od katastrofa u Srbiji: DISARIMES – Strengthening Integrated Disaster Risk Management Systemin Serbia: DISARIMES*, u (V. Cvetković, ur.) Taktika zaštite i spasavanja u vanrednim situacijama: iskustva sa terena i pouke, Naučno-stručno društvo za upravljanje rizicima od katastrofa i Međunarodni institut za istraživanje katastrofa, Beograd, 2021.

Цветковић, Владимир М. „Перцепција ризика од природних катастрофа изазаваних поплавама", Војно дело, 5/2017, стр. 160-175.

Шакрак, Енес - Добројевић, Милан „Прототип система за раноупозороавање на бујичне поплаве *у* брдско-планинским пределима заснован на ионтренету ствари", Беозбедност, Vol. LXIII 1/2021, стр.98-114.

INTERNET APPLICATIONS FOR INTEGRATED MANAGEMENT EMERGENCY SITUATIONS

Abstract: The management of the protection and rescue system in the Republic of Serbia can be conditionally divided into two levels, namely: the national level and the level of local self-governments. Centralized management and command of the entire system is carried out through the Department for Emergency Situations of the Ministry of Internal Affairs of the RS through the system of Departments for Emergency Situations under the jurisdiction of the Department for Emergency Situations. At the top of the chain of command is the Republic Headquarters for Emergency Situations, and at the end the local headquarters for emergency situations that perform tasks at the tactical level through the system of expert-operational teams. The responsibilities of the Republican Headquarters for emergency situations include all levels of management, so in this sense, the Republican Headquarters directly commands both the organizational units of the Sector and local self-governments. The mentioned division into two levels requires the design and implementation of a coordination system, which should, in addition to establishing the interaction between the republican and local new management of emergency situations, enable a quick and transparent exchange of data.

This text provides an overview of digital systems for integrated management of emergency situations in the territory of the Republic of Serbia - which should enable the implementation of legal solutions, but also coordination between state institutions, primarily the Department for Emergency Situations of the Ministry of Internal Affairs of the Republic of Serbia and local self-government units. The text emphasizes the use of entities of special importance and means for protection and rescue, taking appropriate steps and harmonizing actions with other headquarters for emergency situations and measures of state authorities. Also, the text points out the weaknesses and dangers assumed by the use of this system, as well as other electronic systems that seek to complement the aforementioned application, and respond to more specific requirements of local self-government units - which are recognized by the new law as bearers of primary roles in management the risk of disasters in a certain territory.

Keywords*:* emergency situations, integrated management, digital database, Internet applications.

УТИЦАЈ ДИГИТАЛНЕ ТЕХНОЛОГИЈЕ НА СМАЊЕЊЕ ПОВРАТА И РЕСОЦИЈАЛИЗАЦИЈУ ОСУЂЕНИКА[1]

Александра Илић[2]

Апстракт: Савремени свет се не може замислити без дигиталне технологије која постоји у готово свим сегментима функционисања живота човека. С друге стране, извршење кривичних санкција, посебно казне затвора, нужно намеће ограничења осуђеним лицима у погледу могућности коришћења дигиталне технологије. Поставља се питање домашаја тих ограничења односно граница у којима је ипак могуће искористити предности дигиталне технологије на постизање важних циљева криминалне политике - смањење повратa и ресоцијализацију осуђеника. Ако посматрамо из угла извршења казне затвора, уколико пођемо од суштине концепта ресоцијализације, који подразумева припрему осуђеника за живот на слободи, неизоставно се мора наћи простор за употребу средстава дигиталне технологије. Ако бисмо у потпуности онемогућили осуђенике да током извршења казне затвора користе било који облик дигиталне технологије учинили бисмо корак назад у процесу њихове адаптације на услове живота на слободи што би се неповољно одразило и на контролу ризика од поновног вршења кривичних дела. С обзиром да је данас тенденција да се све дигитализује, почевши од неких основних ствари (попут издавања личних докумената) логично је да осуђенике који у затворској установи могу провести и по 10, 15 или више година треба припремати имајући у виду те околности на шта се такође мора обратити пажња и у фази пружања постпеналне помоћи али и током условног отпуста. У раду аутор разматра тренутну ситуацију у Републици Србији и указује на поједине примере добре праксе из упоредних система извршења кривичних санкција. Треба још истаћи и да јавност не гледа благонаклоно на „олакшавање" услова живота осуђеника на издржавању казне затвора па самим тим не постоји ни адекватна подршка већој примени дигиталне технологије током извршења казне. С тим у вези, аутор указује на значај едукације најшире јавности о значају дигиталног описмењавања осуђеника.

Кључне речи: дигитална технологија, ресоцијализација, извршење казне затвора, осуђеници, повратак, постпеналнa помоћ.

Уводне напомене

Ресоцијализација представља један од најважнијих савремених принципа извршења казне затвора уз индивидуализацију у извршењу казне затвора и хумано поступање са осуђеницима. Реч је о принципима који су се искристалисали након век и по трагања за најбољим могућим оквиром извршења казне затвора и основним смерницама које би на

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

[2] Факултет безбедности, Универзитет у Београду, aleksandra.ilic@fb.bg.ac.rs

универзалном плану представљале цивилизацијски помак у третирању осуђеника а све у циљу њихове припреме за живот на слободи и поновно укључивање у токове друштвеног живота како би наставили свој пут, што је више могуће, као корисни и прихваћени чланови друштвене заједнице. Поменути принципи модерног система извршења казне затвора су садржани превасходно у кључним документима у области извршења казне затвора: Стандардним минималним правилима о поступању са осуђеницима [СМП 1955] и Европским затворским правилима [ЕЗП 2006].

Укључивање у живот заједнице односно повратак у друштво углавном није једноставан и лак процес. Тај процес, између осталог, подразумева деловање на чиниоце криминалног понашања који су довели до чињења кривичног дела у конкретном случају, како би осуђеник био спреман за живот напољу без поновног вршења кривичних дела (Zivanai and Mahlangu, 2022). Иако се процес ресоцијализације веома дуго спроводио у традиционалним оквирима, у време када дигитална технологија није била присутна у животима људи, било би погрешно занемарити значај њеног увођења у животе осуђеника и не омогућити им да се, до одређене могуће мере, упознају са њеним карактеристикама и могућностима. Посебно је важно да осуђеници науче како да користе ту технологију у свакодневном животу када изађу из затвора. Аутори McDougall et al. су развили самостални рехабилитациони модел под називом „Теорија промене за затворене људе“ који подстиче употребу киоска у затвору како би се повећале дигиталне вештине затвореника, контакт са службеницима завода, приступ образовним програмима, осећај одговорност и контакт са блиским лицима (2017).

Процес ресоцијализације практично почиње врло брзо након ступања осуђеника на издржавање казне затвора када се, у склопу опсервације осуђеника и спровођења индивидуализације у извршењу казне затвора, сваком осуђенику израђује посебан, индивидуализовани програм поступања у циљу деловања на узрочнике криминалног понашања. Програм поступања се примењује током целог трајања казне затвора а један битан аспект програма је и припрема осуђеника за живот на слободи односно тзв. постпеналну фазу. Другим речима, боравак у затвору треба да се разуме од самог почетка као пут ка слободи који треба да буде осмишљен тако да стварно припреми осуђеника за живот ван затворских зидина односно да се не сведе на пуко поштовање правила без дубљег смисла. Уосталом, и сам термин пенитенцијарни третман као скуп свесних и несвесних поступака усмерених ка остваривању циља казне односно затварања (Игњатовић 2019, 182) претпоставља активно учешће затвореника у његовом спровођењу а део тих активности су и разна учења, стицања нових знања, ширење видика како би се и догодила промена на боље. С обзиром да се нико научен није родио, тако се мора научити и како да се користе предности дигиталне технологије а са макар елементарним познавањем тога осуђеници имају више самопоуздања и воље да по изласку на слободу и нешто позитивноураде са својим животом. Иако ништа не представља гаранцију за успех, почетне позиције таквих осуђеника су сигурно боље од оних који нису имали прилику да стекну знања и вештине од кључне важности за савременог човека.

У наставку ће бити речи конкретније о различитим проблемима који се налазе на путу ширег увођења дигиталне технологије у затворима као и сферама у којима се, током издржавања казне затвора, технологија може искористити за побољшање ефеката примене програма поступања са осуђеницима у циљу њихове ресоцијализације. Посебно значајну примену дигитална технологија има у контексту едукације осуђеника.

Опште напомене о употреби дигиталне технологије током извршења казне затвора

Затворски системи су по природи ствари конзервативни и затворени, у којима је у великој мери акценат на поштовању јасно постављених и прецизних правила понашања као и одржавању реда и безбедности, па се не може очекивати да се достигнућа савремене технологије тек тако користе у свакодневном раду са осуђеницима. Различити могући ризици који се могу реализовати као резултат коришћења дигиталне технологије довели су до тога да се њено коришћење у већини затворских система сведе на минимум при чему је важно направити разлику између затвора с обзиром на степен обезбеђења који се у њима примењује.

Степен обезбеђења затвора је у корелацији са категоријом осуђеника која је смештена у конкретном затвору односно тежином учињеног кривичног дела, висином изречене казне затвора као и преваспитним могућностима осуђеника односно претходно процењеним ризиком у погледу способности адаптације осуђеника на услове живота у затвору. Сви поменути фактори се узимају у обзир и у оквиру тзв. унутрашње односно интерне класификације затвореника приликом њиховог разврставања у одређене третманске групе. Све то утиче и на начин организовања односно систем обезбеђења у затворима па је уобичајена подела затвора на оне отвореног, полуотвореног и затвореног типа с тим што што се последњих деценија у многим државама, па и код нас, развија концепт тзв. *supermax* затвора односно затвора затвореног типа са посебним обезбеђењем, у терминологији која се користи у нашем Закону о извршењу кривичних санкција (ЗИКС, Члан 14)[3].

Друго питање које се може поставити је да ли су наметнута ограничења у погледу могућности коришћења дигиталне технологије у затвору претерана, да ли је то само линија мањег отпора, одржавања *status quo* система. Свака промена у функционисању затворског система је својеврсни експеримент са непознатим резултатом па се често чини да је боље не ризиковати иако би се тако могао направити помак на боље, превасходно у интересу осуђеника. У једној студији спроведеној у три британска затвора резултати истраживања су показали да постоји значајно противљење затворских службеника увођењу технологије засноване на интернету. Многи службеници су изразили бојазан да би било који уређај са омогућеним интернетом могао бити хакован или изманипулисан ради добијања пуног приступа Интернету, што би, заузврат, довело до озбиљних повреда безбедности. Та забринутост је била посебно изражена упркос чињеници да *Wi-Fi* није био доступан ни у једном од затворских објеката (Reisdorf and Jewkes 2016). С друге стране, резултати друге студије су показали да се отпор затворских службеника смањује са применом дигиталне технологије у свакодневном животу затвореника, да многе предрасуде и страхови нестају односно постају мањи. Ипак, и у таквим околностима већи отпор пружају службеници на тзв. нелидерским позицијама (*non-leadership positions*) у односу на оне који су у хијерархији службе за обезбеђење на „шефовским" позицијама. То је све логично јер обични службеници су чешће у непо-

[3] У заводима отвореног типа не постоје физичко-техничке препреке за бекство док у заводима полуотвореног типа запослени у служби за обезбеђење представљају основну препреку за бекство. У заводима затвореног типа, поред запослених у служби за обезбеђење, постоје и друге физичко-техничке препреке за спречавање бекства, а у заводима затвореног типа са посебним обезбеђењем постоје физичко-техничке препреке, којима се постиже највиши степен обезбеђења.

средном односу са осуђеницима, један на један, и више размишљају о ризицима него о бенефитима дигитализације (Mufarreh et al. 2022).

Повећање приступа интернету, електронској пошти и рачунарима у затворима може дати затвореницима вештине и способности које су им потребне у циљу лакшег запошљавања по изласку из затвора (Kerr and Willis 2018). То посебно важи за она лица која су осуђена на дуготрајније казне затвора када бивају одсечена од света напољу на један дужи временски период. У међувремену се технологија развија и ако та лица нису у прилици да се упознају са новинама које су генерално битне за успешно функционисање у различитим сферама живота појединаца онда се шансе за њихову успешну ресоцијализацију значајно смањују. Дигитална технологија се мора сматрати веома важним аспектом пенитенцијарног третмана иако смо још увек далеко од решења која би и у пракси омогућила њено ефикасно коришћење.

Државе се разликују у погледу помака које су направиле у сфери дигитализације различитих области друштвеног живота. Неке од њих, попут Финске али и већине западних држава, дигитализовале су у великој мери систем здравствене и социјалне заштите. У пракси је то значило пораст дигиталних резервација, дигиталних формулара, виртуелних термина, различитих облика онлајн терапије и независно доступних база података и програма самопомоћи. То је све довело до дискусије о ширем омогућавању приступа тој дигитализацији и лицима која се налазе у затворима. Дигитализација услуга здравствене и социјалне заштите ствара многе могућности за рехабилитацију затвореника и њихову припрему за излазак из затвора. Развијен је низ дигиталних платформи и технолошких решења која нуде вишеструке могућности за решавање приватних проблема осуђеника било путем видео конференцијске везе, е-поште или неког другог дигиталног формата у самом затвору (Rantanen, Järveläinen and Leppälahti 2022).

Парадокс који се у контексту употребе или могућности употребе дигиталне технологије у затворима јавља је да је оним лицима којима би упознавање са макар основним аспектима њене употребе то највише значило су управо она лица којима је то углавном, у потпуности или у већој мери, ускраћено због типа завода у којем су смештени односно због строжих безбедносних протокола и многобројних ризика који постоје у таквим установама. Међутим, та лица су неретко у затвору већ дуги низ година а нека од њих су у потпуности прескочила радикалне моменте у развоју те технологије. Једног дана се очекује њихов излазак из затвора, осим у случају казне доживотног затвора без права на условни отпуст, па није тешко замислити какав би то био шок за особу која треба да настави свој живот у условима који су јој потпуно непознати.

С друге стране, у позадини отпора према употреби дигиталне технологије у затворима, па чак и за потребе образовања односно шире гледано остваривања циљева преваспитавања и прилагођавања условима живота на слободи, налази се, између осталог, страх да нешто не крене наопако. Тако нпр. и даље постоји значајно противљење глобално гледано да се омогући шири приступ интернету осуђеницима како не би на тај начин предузели неке недозвољене активности. Ипак, у време пандемије Ковид-19 дошло је до изнуђеног помака у сфери коришћења дигиталне технологије у затворима широм света. Затворске управе суочене са чињеницом да није хумано лишити осуђенике било каквог контакта са блиским лицима, морале су, у недостатку контакта уживо, да омогуће, у многим државама и по први пут, употребу различитих апликација за комуникацију попут Скајп (Skype) і Вибер односно Вајбер (Viber). Та пракса је и даље остала у одређеним оквирима, посебно за лица која због неких других разлога не могу да остварују контакт уживо са блиским лицима (налазе се у иностранству, болест или неки други разлог).

Могућности коришћења дигиталне технологије у извршењу казне затвора у Србији

Наше кривично извршно право не препознаје могућност употребе дигиталне технологије као средства које би се могло искористити у сврху ресоцијализације, као део програма поступања, или у склопу остваривања неког права осуђеника. С друге стране, не постоји ни забрана коришћења дигиталне технологије па је конкретна употреба дигитализације сива зона односно подручје у вези са којим постоји правна празнина која се може тумачити на различите начине (Илић, Бановић 2022, 191). Уколико пођемо од основног оквира извршења казне затвора и ту тражимо одговоре како и где можемо да искористимо дигиталну технологију за побољшање положаја осуђеника, неминовно морамо у то разматрање да укључимо и још неке аспекте извршења. Ти аспекти су постпенална помоћ и условни отпуст. Оба аспекта се надовезују на извршење казне затвора тако да без обзира на међусобне различитости института заједничко им је да имају као крајњи циљ постизање успеха у ресоцијализацији осуђеника.

Ако се разматра у контексту реализације програма поступања са осуђеником, дигитална технологија своје место треба превасходно да има у оквиру остваривања права осуђеника на образовање а посредно и у вези са проблематиком права на рад осуђеника. Поменута пандемија Ковид-19 је и код нас проблематизовала питање остваривања права на посете осуђеника у таквим околностима што је отворило могућност коришћења дигиталних средстава комуникације.

Свакако треба поћи од права осуђеника на образовање које је као и сва остала права осуђеника прописано у ЗИКС. Тако осуђени има право на основно и средње образовање, које се сходно прописима који уређују образовање[4] организује у заводу али се могу организовати и други видови образовања осуђених (ЗИКС 2014, Члан 122). У контексту других видова образовања важно је осврнути се на то како ту проблематику уређује Закон о образовању одраслих (ЗОО 2013) који би се морао примењивати на проблематику образовања осуђених пунолетних лица при чему посебно треба нагласити полазиште наглашено у члану 2. став 1. ЗОО по коме је образовање одраслих део јединственог система образовања Републике Србије, који обезбеђује одраслима током целог живота стицање компетенција и квалификација потребних за лични и професионални развој, рад и запошљавање, као и друштвено одговорно понашање (Илић 2022, 244).

Остали видови образовања који се помињу у ЗИКС регулисани су у ЗОО, који разликује формално и неформално образовање, као и информално учење. Формално образовање одраслих обухвата основно и средње образовање које се остварује на основу наставних планова и програма основног и средњег образовања, и програма других облика стручног образовања прилагођених потребама и могућностима одраслих и захтевима тржишта рада, у складу са законом. Неформално образовање одраслих је организован процес учења одраслих на основу посебних програма ради стицања знања, вредности, ставова, способности и вештина усмерених на лични развој одраслих, рад и запошљавање и социјалне активности. Информално учење одраслих је процес самосталног стицања знања, вредности, ставова, способности и вештина у свакодневном животном, радном и социјалном окружењу (ЗОО Члан 2. Став 2-6). С тим у вези, завод

[4] Овде треба поменути законе у области основног и средњег образовања: Закон о основама система образовања и васпитања, Закон о основном образовању и васпитању, Закон о средњем образовању али и Закон о образовању одраслих коме ће бити посвећено највише пажње у раду.

може да организује различите програме образовања из оквира формалног и неформалног образовања одраслих међу којима се, између осталог, истиче и програм обуке за рад на рачунару (као облик неформалног образовања) (Илић 2022, 245). ЗОО такође наглашава посебно, у оквиру разматрања проблематике планова и програма образовања одраслих, да је један од битних циљева допуне знања, вештина, способности и ставова одраслих и владање информацијско-комуникационом технологијом (Члан 43. Став 1. Тачка 4).

Имајући у виду да се поменути законски оквир примењује подједнако на образовање свих одраслих, па и оних који се налазе на издржавању казне затвора, требало би доследно и континуирано спроводити информатичку едукацију свих осуђеника који то желе (принцип добровољности) па су и заводи у обавези да воде рачуна о том сегменту остваривања права осуђеника на образовање. С тим у вези, поред нормативног оквира подједнако важно је осврнути се и на стварно стање по питању употребе дигиталне технологије у појединим заводима за извршење кривичних санкција. Основни документ који служи као полазиште за ту анализу је Стратегија развоја система извршења кривичних санкција за период 2021-2027. године (Стратегија 2021) у којој се налазе одређени званични подаци из којих се могу извести одређени закључци у вези са коришћењем дигиталне технологије у појединим затворима у Србији. Додуше у питању су донекле застарели подаци јер представљају петогодишњи пресек стања, у периоду од 2015. до 2020. године, и односе се на спроведене обуке у заводима за извршење кривичних санкција у циљу стручног оспособљавања лица лишених слободе. У наведеном периоду обуке за разна занимања прошло је 3100 осуђених лица. Међу многобројним занимањима за која се оспособљавају помиње се и основна информатичка обука а конкретно је истакнута сертификована обука жена у Казнено-поправном заводу за жене у Пожаревцу, где је у поменутом петогодишњем периоду 130 осуђеница завршило различите видове обука, између осталог и основе информатике[5]. Стручно оспособљавање спроводиле су средње техничке школе и школе за образовање одраслих, након чега су издавани сертификати о оспособљености за рад (Стратегија 2021, 25).

Треба се осврнути на поменуту основну информатичку обуку што је недвосмислено остваривање осуђеничког права на образовање а само посредно се тиче и остваривања права на рад ако се из тога реализује и неки облик радног ангажмана у заводима за извршење кривичних санкција. Ипак, оно што остаје нејасно из текста Стратегије је за које се конкретно занимање оспособљавају осуђеници кроз ту обуку. У Стратегији се поред основне информатичке обуке помињу и друга занимања за која се осуђеници оспособљавају попут: кувар, гајење и обрада лековитог биља, производња раног поврћа у заштићеном простору, рестаурација намештаја, дуборез... и друга. Ипак све наведено, осим основне информатичке обуке, и јесу занимања па је самим тим дилема како повезати информатичку обуку и конкретно занимање. Такође је нејасно да ли се осуђеницима касније, након завршетка основне обуке, омогућава приступ рачунару ради одржавања стечених знања и вештина, што је посебно важно ако се ради о дугим казнама затвора па је битно да осуђеници буду у прилици да испрате све битне новине с тим у вези. Суштина свега треба да буде информатички оспособљен осуђеник који ће бити у стању да реализује низ активности по изласку из затвора а које захтевају употребу рачунара и

[5] Иако није истакнуто у Стратегији, информатичка обука се спроводи и у другим заводима у Србији, као нпр. у Казнено-поправном заводу Београд - Падинска Скела где се једном недељно спроводи информатичка обука за групу заинтересованих осуђеника (отприлике 15 осуђеника).

интернета. Ипак мора се признати да поједини затвори показују иницијативу у погледу унапређења програма стручног оспособљавања и усавршавања а који се могу повезати са употребом дигиталне технологије. Тако је у Казнено-поправном заводу за жене заживела обука за сценску фотографију како би се осуђенице које то желе оспособиле за рад у дигиталном простору попут нпр. могућности уређивања неких дигиталних платформи односно свега онога што је данас популарно и корисно у тој сфери.

Обука и рад током боравка у затвору морају да се наставе у континуитету, и као део постпеналне фазе која је подједнако битна за спречавање поврата и нормализацију живота одређеног лица као и сам боравак у затвору уз примену третмана. Ипак, без обзира на постојање минимума информатичке обуке, неретко осуђеник излази из затвора без довољно или икаквог информатичког знања (најчешће због незаинтересованости) а неопходно је да нпр. електронским путем поднесе различите захтеве односно оствари нека своја права, а нема никога ко би му у томе помогао. Адекватан постпенални прихват би морао да подразумева спровођење програма информатичке обуке за сва заинтересована лица по изласку из затвора. Међутим, на путу те реализације могу да се нађу многобројне препреке а посебно је важно обезбедити довољно ресурса (људских, просторних, техничких...) како би сваки заинтересовани осуђеник имао приступ тој врсти помоћи.

Код нас је постпенална помоћ регулисана како у ЗИКС-у тако и у Закону о извршењу ванзаводских санкција и мера (ЗИВСИМ 2014). У члану 48. ЗИКС прописује да се лицу отпуштеном са издржавања казне пружа неопходна помоћ и подршка како би се умањио ризик вршења нових кривичних дела и како би му се олакшао успешан повратак у заједницу. Сматра се да је постпенална помоћ одувек била једна од најслабијих карика извршења казне затвора код нас и да се мора унапредити тај сегмент како би се поступак ресоцијализације осуђеника заокружио и проблем рецидива значајно смањио (Игњатовић 2018, 217). Реализација постпеналне помоћи има две димензије: прва се дешава у заводу у склопу програма третмана (о чему је било речи) а друга се активира уочи изласка осуђеника из затвора и траје одређено време по изласку из заводске установе. ЗИВСИМ у члану 57. став 1. прописује да је програм помоћи (постпенални програм) скуп мера и поступака које лице после извршене казне затвора добровољно прихвата, а који се примењује у циљу укључивања у живот на слободи. Програм помоћи се састоји од: пружања помоћи приликом проналажења смештаја и исхране, пружање помоћи у остваривању права на здравствену и социјалну заштиту, давања савета у циљу усклађивања породичних односа, пружања подршке и помоћи приликом проналажења запослења, односно довршавања школовања или стручног оспособљавања, успостављања сарадње са надлежним центром за социјални рад у циљу давања новчане подршке за подмиривање најнужнијих потреба, пружање подршке и помоћи у уздржавању од употребе опојних дрога и алкохола и пружање других облика помоћи и подршке. Управо у аспекту помоћи у вези са стручним оспособљавањем треба тражити основ за организацију информатичке обуке лица у постпеналном прихвату.

У још једном сегменту извршења који је повезан са казном затвора може се и мора пронаћи простор за значајнију употребу дигиталне технологије. У питању је условни отпуст који има практично идентичан смисао као и постпенална фаза јер се ради о отпуштању (додуше условном) осуђеника са издржавања казне затвора уз евентуално наметање одређених обавеза како би се одржао позитиван учинак постигнут током издржавања казне затвора и спречило чињење дела до истека изречене казне. Кривични законик (КЗ 2006, Члан 46) наглашава да, поред објективног критеријума за одређивање

условног отпуста односно протека најмање две трећине казне, мора да буде испуњен и субјективни који се тиче процене заводске установе о поправљању осуђеника при чему се та процена, између осталог, заснива на дотадашњем залагању осуђеника у погледу обуке и стручног оспособљавања као и радног ангажмана. Извршење условног отпуста се, попут постпеналне помоћи, налази у надлежности Повереничке службе. ЗИВСИМ у члану 44 прописује да се у склопу надзора над условно отпуштеним лицем уколико је то потребно, односно одређено у одлуци суда о условном отпусту, надзире извршење одређених обавеза. То могу бити следеће обавезе: јављање органу надлежном за извршење заштитног надзора[6]; оспособљавање учиниоца за одређено занимање; прихватање запослења које одговара способностима учиниоца; уздржавање од посећивања одређених места, локала или приредби, ако то може бити прилика или подстицај за поновно вршење кривичних дела; благовремено обавештавање о промени места боравка, адресе или радног места; уздржавање од употребе дрога или алкохолних пића; посећивање одређених професионалних и других саветовалишта или установа, и поступање по њиховим упутствима и испуњење других обавеза које су предвиђене кривичноправним одредбама. Основ за информатичку обуку се може наћи у реализацији обавезе која се односи на оспособљавање учиниоца за одређено занимање. С тим у вези, ЗИВСИМ прецизира у члану 49. да је осуђени дужан да испуњава обавезе редовног или ванредног школовања или друге утврђене облике стручног оспособљавања или стицања вештина. Без проблема се и обука за рад на рачунару односно континуирана обука ако је започета у затвору, као и сличне обуке, могу подвести под члан 49 ЗИВСИМ.

Закључак

Иако због ограниченог простора за писање у овом раду нису обухваћени нити проблематизовани сви аспекти извршења казне затвора који би се могли побољшати употребом дигиталне технологије, недвосмислено је указано на важност бављења том проблематиком која се неизоставно мора разматрати у контексту остваривања ресоцијализације као сврхе извршења казне затвора. Из тога произилази и закључак да успешно припремање за живот на слободи мора да подразумева колико год је могуће симулацију стварних животних околности које се одвијају ван затворске зграде.

Како је дигитализација све више део наших живота и развија се убрзаним темпом који се мора пратити да би се ухватио корак са достигнућима модерне технологије, тако и затворски системи не би требало да заостају у великој мери за тим процесима. Иако су депривације саставни део осуђеничког живота, оне се морају свести на минимум а пожељно је и избећи их тамо где је то могуће односно где се не доводи у питање сврха извршења. Депривација дигитализације у животима осуђеника је нешто што је неумитна последица затварања али у овом раду акценат је стављен на омогућавању оптималног нивоа дигитализације у сврху остваривања циљева у вези са ресоцијализацијом осуђеника како би спремнији дочекали тренутак изласка из затвора и започињање новог

[6] Овде законодавац једноставно преписује формулацију из члана 73. КЗ-а који се односи на садржину заштитног надзора уз условну осуду. Иако КЗ у члану 46. став 3. прописује да суд може у одлуци о условном отпусту одредити да је осуђени дужан да испуни неку од обавеза из члана 73. истог закона, као и неку другу обавезу предвиђену кривичноправним одредбама, то не значи да се одредбе могу тек тако преписивати без уклапања у контекст и суштину института који се прописује. Није јасно зашто се није могло написати да је једна од обавеза и јављање органу надлежном за извршење условног отпуста.

живота. У том новом животу постоји пуно изазова за људе који су били у затвору, од најосновнијих као што су подизање личних докумената, отварање здравственог картона и одлазак код лекара, преко подношења пријава за посао и одласка на разговор у вези са тим, до проналаска стана за живот и наставка борбе у сузбијању чинилаца који су довели до чињења кривичних дела. Иако није сваки сегмент те борбе односно изазова повезан са дигитализацијом, доста тога ипак јесте па познавање механизама њеног функционисања у великој мери може побољшати изгледе сваког појединца на слободи а то онда повезано смањује стопу повратa.

Несумњиво је да без дигиталне технологије не можемо замислити затворе данас као и у будућности али је неопходно да се осуђеници више сусрећу са различитим аспектима њене примене него што је то случај сад. Отпор затворске администрације али и комплетног система извршења кривичних санкција у многим државама је логична последица потребе да се ствари држе под контролом и спречи наступање нежељених ситуација. Зато је важно указивати на позитивне примере њене примене попут резултата многобројних истраживања у различитим државама који су показали да свеобухватни програми поновног уласка који се фокусирају на дигиталну инклузију могу бити ефикасни у ресоцијализацији осуђеника. Дигитализација затвора је изазовна, али је корисна како за затворску администрацију тако и за осуђенике односно њихове породице и друга блиска лица што олакшава нови почетак ван затвора. Проналажење посла по пуштању на слободу и генерално проналажење свеобухватног повратка у друштво које се креће брзим технолошким темпом може довести до изазова не само за оне затворенике који су издржавали дугу казну затвора, већ и за оне који су краћи временски период провели у затвору (Zivanai and Mahlangu, 2022).

Коначно, како би се било какав значајнији помак направио у вези са овим питањем неопходно је радити на едукацији шире јавности која не гледа благонаклоно на омогућавање осуђеницима приступа дигиталној технологији, не размишљајући да је та дигитална инклузија осуђеника важна како за тог појединца тако и за друштво у целини.

Библиографија

Zivanai Eugenia and Gilbert Mahlangu. 2022. „Digital prison rehabilitation and successful re-entry into a digital society: A systematic literature review on the new reality on prison rehabilitation". *Cogent Social Sciences*, 8:1, 2116809, DOI: 10.1080/23311886.2022.2116809

[ЗИВСИМ] Закон о извршењу ванзаводских санкција и мера. 2014. Службени гласник Републике Србије, бр. 55/2014 и 87/2018.

[ЗИКС] Закон о извршењу кривичних санкција. 2014. Службени гласник Републике Србије, бр. 55/2014 и 35/2019.

[ЗОО] Закон о образовању одраслих. 2013. Службени гласник Републике Србије, бр. 55/2013, 88/2017 – др. закон, 27/2018 – др. закон и 6/2020 – др. закон.

Игњатовић, Ђорђе. 2018. *Криминолоīија*. Београд: Правни факултет Универзитета у Београду

Илић, Александра. 2022. *Коменīар Закона о извршењу кривичних санкција.* Београд: ЈП Службени гласник

Илић, Александра и Божидар Бановић. 2022. „Дигитализација у систему извршења кривичних санкција Републике Србије", У: *Диīиīализација у казненом īраву и īравосуђу*, Јелена Костић, Марина Матић Бошковић (ур), 185-200. Београд: Институт за упоредно право и Институт за криминолошка и социолошка истраживања.

Kerr, Aysha and Matthew Willis. 2018. „Prisoner use of information and communications technology". *Trends & issues in crime and criminal justice.* Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti107289

[КЗ] Кривични законик 2022. Службени гласник Републике Србије, бр. 85/2005, 88/2005 – испр., 107/2005 – испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 и 94/2016 и 35/2019.

McDougall, Cynthia, Dominic A. S. Pearson, David J. Torgerson and Maria Garcia-Reyes. 2017. „The effect of digital technology on prisoner behavior and reoffending: a natural stepped-wedge design". *Journal of Experimental Criminology* 13(1), https://doi.org/10.1007/s11292-017-9303-5

Mufarreh, Andrea, Jason Waitkus and Teresa A. Booker. 2022. „Prison official perceptions of technology in prison". *Punishment & Society*, 24(3), 410-432. https://doi.org/10.1177/1462474521990777

Препорука Комитета министара Савета Европе – Европска затворска правила [Rec (2006)2]

Rantanen Teemu, Eeva Järveläinen and Teppo Leppälahti. 2022. „Self-efficacy and Use of Digital Health Care and Social Welfare Services Among Incarcerated People: Cross-sectional Survey Study". *J Med Internet Res*. 24(5):e36799. doi: 10.2196/36799. PMID: 35639446; PMCID: PMC9198817.

Reisdorf, Bianca and Yvonne Jewkes. 2016. „(B)Locked Sites: Cases of Internet Use in 3 British Prisons". *Information, Communication, and Society*, 19(6), 771-786.Quello Center Working Paper.

Стандардна минимална правила о поступању са затвореницима – Нелсон Мендела правила [A/RES/70/175]

THE INFLUENCE OF DIGITAL TECHNOLOGY ON THE REDUCTION OF RE-OFFENDING AND REHABILITATION OF CONVICTS

Abstract: The modern world cannot be imagined without digital technology that exists in almost all segments of the functioning of human life. On the other hand, the execution of criminal sanctions, especially imprisonment, necessarily imposes restrictions on convicted persons regarding the possibility of using digital technology. The question arises of the scope of those limitations, i.e. the limits within which it is still possible to use the advantages of digital technology to achieve important goals of criminal policy - reduction of recidivism and rehabilitation of convicts. If we look from the point of view of the execution of the prison sentence, if we start from the essence of the concept of rehabilitation, which implies the preparation of convicts for life in freedom, there must inevitably be a space for the use of digital technology. If we were to completely prevent convicts from using any form of digital technology during the execution of their prison sentence, we would take a step back in the process of their adaptation to the conditions of life in freedom, which would adversely affect the control of the risk of re-offending. Given that the tendency today is to digitize everything, starting with some basic things (such as issuing personal documents), it is logical that convicts who may spend 10, 15 or more years in a prison should be prepared, taking into account the circumstances, and must also pay attention in the phase of providing post-penal assistance as well as during parole. In the paper, the author examines the current situation in the Republic of Serbia and points to some examples of good practice from comparative systems of execution of criminal sanctions. It should also be pointed out that the public does not look favorably on „easing" the living conditions of convicts serving their prison sentences, and therefore there is no adequate support for the greater use of digital technology during the execution of the sentence. In this regard, the author points to the importance of educating the general public about the importance of digital literacy for convicts.

Keywords: digital technology, rehabilitation, prison sentence execution, convicts, re-offending, post-penal assistance.

УПОТРЕБА ИНФОРМАЦИОНО – КОМУНИКАЦИОНИХ ТЕХНОЛОГИЈА У РАДУ ВАТРОГАСНО – СПАСИЛАЧКИХ ЈЕДИНИЦА

Милош Миленковић[1], Данијела Спасић[2], Никола Митровић[3]

Апстракт: Савремени изазови у одговору на елементарне непогоде и техничко – технолошке несреће намећу професионалним службама заштите и спасавања потребу коришћења савремених информационо – комуникационих технологија у циљу ефикасног и ефективног одговора. Ватрогасно – спасилачке јединице, као носиоци оперативног дела система заштите и спасавања, кроз све фазе управљања ванредним ситуацијама у свом раду могу користити информационо – комуникационе технологије. У делу припреме, обуке и стручног усавршавања ватрогасци – спасиоци употребом информационо – комуникационих технологија имају могућност симулације реалних ванредних догађаја. Коришћење различитих симулатора и софтверских решења током обуке припадника ватрогасно – спасилачких јединица у великој мери доприноси унапређењу преношења знања и ранијих искустава у делу припреме за будући оперативни рад. Значај употребе информационо – комуникационих технологија посебно се огледа у оперативном раду ватрогасно – спасилачких јединица. Софтверски пакети попут геоинформационих система, различитих програма за подршку одлучивању, као и базе података које се односе на преглед становништва, путне и друге инфраструктуре, од велике користи могу бити у акцијама заштите и спасавања. На пример, одлука о евакуацији угроженог становништва у одређеним ванредним ситуацијама може бити комплексна и временски ограничена. У циљу доношења оптималне одлуке у случају евакуације становништва, као и у сличним околностима када руководиоци ватрогасно – спасилачких јединица одлучују о заштити и спасавању људи, материјалних и културних добара, употреба информационо – комуникационих технологија доприноси оптимизацији коначне одлуке. Пракса у раду ватрогасно – спасилачких јединица је да се после реаговања на различите ванредне догађаје подаци о интервенцијама складиште у базама података. Анализа оперативног рада ватрогасно – спасилачких јединица доприноси побољшању будућих активности. У овом делу се такође огледа значај коришћења информационо – комуникационих технологија да се кроз различите анализе база података дају препоруке и смернице за унапређење и развој рада ватрогасно – спасилчаких јединица.

Кључне речи: информационо – комуникационе технологије, ватрогасно – спасилачке јединице, географски информациони системи, симулација.

[1] Сектор за ванредне ситуације, Министарство унутрашњих послова Републике Србије, milos.milenkovic@mup.gov.rs

[2] Криминалистичко – полицијски универзитет, Београд, danijela.spasic@kpu.edu.rs

[3] Криминалистичко – полицијски универзитет, Београд, nikola.mitrovic@kpu.edu.rs

Увод

Управљање ванредним ситуацијама у савременим условима карактерише се низом изазова за институције, организације и појединце који учествују како у превенцији и припремљености, тако и у реаговању, као и у фази обнове и опоравка. Имајући у виду да се заштита људских живота, материјалних и културних добара истиче као примарни циљ, може се истаћи да је део који се односи на реаговање и пружање одговора на ванредне доагађаје и ситуације једна од најкомплекснијих фаза у управљању ванредним ситуацијама.

Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама у Републици Србији израз управљање ванредним ситуацијама дефинише на начин да „управљање ванредним ситуацијама обухвата координацију и руковођење субјектима и снагама система заштите и спасавања у циљу организованог одговора на катастрофе и брзог опоравка" (Закон о смањењу ризика од катастрофа и управљања ванредним ситуација 2018, члан 2). Како се може закључити из законског одређења нагласак је на координацији и руковођењу субјектима и снагама система заштите и спасавања. Ако се уђе у детаљнију анализу, узевши у обзир нагласак на организованом одговору на катастрофе и брзом опоравку, поставиће се питање ко су ти субјекти и снаге од којих се очекује испуњење претходно дефинисани циљ. Кровни закон у Републици Србији који ближе уређује област управљања ванрендим ситуацијама одређује које су то системске снаге. Сигурно да се у делу пружања одговора на ванредне догађаје фокус усмерава ка ватрогасно – спасилачким јединицама. Ватрогасно-спасилачке јединице јесу снаге система смањења ризика од катастрофа и управљања ванредним ситуацијама и реагују у акцијама усмереним на елиминисање појава несреће, спасавање угроженог становништва и материјалних добара и отклањање последица катастрофа (Закон о смањењу ризика од катастрофа и управљања ванредним ситуација 2018, члан 49). У циљу пружања ефикасног и ефективног одговора на различите облике ванредних догађаја, ватрогасно – спасилачким јединицама у свакодневном раду у великој мери може помоћи употреба информационо - комуникационих технологија. Наиме, промене које наступају у животној средини, насељеним местима, индустријским зонама, у смислу изражене урбанизације, оптерећености инфраструктуре и сл., намећу припадницима ватрогасно – спасилачких јединица потребу да прате савремене трендове како би били што спремнији. Иновативна технологија је одувек била важан део рада ватрогасно – спасилачких јединица.Технологија у ватрогасној служби покрива много више од рачунара и софтвера. Од личне заштитне опреме преко ватрогасних пумпи до радио и комуникационих система, ватрогасна технологија унапређује све заједно како би се побољшала безбедност и ефикасност ватрогасаца. Међутим, ватрогаство је област која високо цени традицију. А понекад, припадници ватрогасно – спасилачких јединица могу оклевати да усвоје нову технологију. На неки начин, овај отпор је разумљив. Технологија која се користи у раду ватрогасно – спасилачких јединица може бити скупа и сложена, а примена нове опреме и технологије може захтевати прилагођавање обука и оперативних процедура (Bashoor 2020). Без обзира што се спомиње и отпор према примени савремених информационо – комуникационих технологија у раду ватрогасно – спасилачких јединица, у обзир се мора узети да се у ватрогасну службу све више запошљавају представници генерација који свакодневни живот заснивају на коришћењу мобилних телефона, друштвених мрежа и сл. На тај начин у великој мери је олакшана имплементација одређених софтверских решења, геоинформационих система и разних апликација које се користе у раду ватрогасно – спасилачких јединица.

Са развојем информационих технологија и ватрогаства, постојала је могућност, али и све већа потреба за увођењем компјутеризације у процесима рада ватрогасне службе. Термин „информатизација“ се може дефинисати као увођење програмских алата који олакшавају проток, складиштење и приступ информација, чиме се омогућава добар преглед података неопходних за доношење одлука. Основни услови за успех употребе ових алата је, осим самих апликација и одговарајућа инфраструктура, стандардизација пословних процеса у ватрогаству, добро образовање корисника и квалитетна корисничка подршка (Јагодин 2017).

Кроз приказ употребе информацино – комуникационих технологија у различитим сегментима рада ватрогасно – спасилачких јединица, аутори настоје да укажу на низ предности у циљу олакшања припреме, оперативног ангажовања и анализе ванредних догађаја у ватрогасној служби. Аутори су се определили да прикажу употребу информационо – комуникационих технологија у раду ватрогасно – спасилачких јединица кроз део који се односи на обуку, затим кроз примену у оперативном раду и руковођењу на интервенцијама, односно на крају у делу анализе ванредних догађаја.

Употреба информационо – комуникационих технологија у обуци ватрогасно – спасилачких јединица

Институције које се баве оспособљавањем и стручним усавршавањем припадника ватрогасно – спасилачких јединица препознали су значај употребе информационо – комуникационих технологија у циљу што реалнијег приказа и симулације начина поступања и одговора на различите ванредне догађаје. За потребе различитих облика обуке ватрогасно – спасилачких јединица користе се информационо – комуникационе технологије како би се реализовала симулација пожара, поплава, земљотреса или ванредних догађаја узрокованих опасним материјама.

У пракси, обуку и тренинг ватрогасно – спасилачких јединица спроводе националне институције које се организационо посматрано део министарстава, дирекција или других владиних тела у чијој је надлежности област управљања ванредним ситуацијама. Најчешће су то тренинг центри основани на националном нивоу, док у неким државама постоје примери и регионално основаних тренинг центара (Миленковић и други 2019). Савремени тренинг центри за обуку припадника ватрогасно – спасилачких јединица у великој мери користе симулације ванредних догађаја. На тај начин се настоји да се полазницима обука приближе реални услови са којима ће се суочавати касније током ангажовања на пружању одговора на ванредне догађаје.

Данас се у употреби могу пронаћи различита софтверска решења која омогућавају употребу симулације ванредних догађаја за потребе обуке припадника ватрогасно – спасилачких јединица. Један од примера је софтвер XVR. Неке од најзначајнијих карактеристика овог софтвера су:

- Тражење и препознавање визуелних знакова – софтверско решење омогућава учесницима да вежбају препознавање визуелних знакова и опасности,
- Неограничено вежбање без обзира на локацију - сценарији ванредних догађаја нуде могућност обуке кад год и где год то желе крајњи корисници,
- Процена опасности и комуникација – полазници обуке виде сценарио да би имали увид у целокупну ситуацију. Током тимске обуке полазници могу користити различита средства комуникације,

- Евалуација и повратне информације - након обуке инструктор прегледа радње, активности и одлуке са полазником обуке,
- Командовање и контрола током обуке – полазници су током целе обуке контролисани преко софтвера од стране инструктора. Инструктор има потпуну контролу и увид у пружена решења и одговоре, односно предлоге употребе различитих материјално – техничких и људских ресурса (E-Semble 2012).

Употреба инфомационо – комуникационих технологија у обуци припадника ватрогасно – спасилчаких јединица има низ предности. Очигледна је могућност укључивања већег броја корисника истовремено. Такође, један од инструктора може пратити рад неколико полазника и заустављати обуку уколико препозна током симулације и решавања задатака да долази до грешака. На то се надовезује и следећа предност употребе различитих апликација у контексту да је врло једноставна и евалуација обуке, као и оцена полазника. Софтвер константно прати рад припадника ватрогасно – спасилачких јединица током обуке и аутоматски генерише оцене на основу успешно или неуспешно реализованих задатка на симулираном ванредном догађају. Једна од предности је што је омогућена и мобилност у обуци. Информациона опрема и техника која се користи за потребе оваквог вида обуке може се транспортовати и у пракси не захтева изражене логистичке захтеве.

Поред низа предности, јављају се и одређени недостаци приликом употребе информационо – комуникационих технологија у обуци припадника ватрогасно – спасилачких јединица. Један од недостатака се може повезати са финансијским аспектом. Наиме, већина софтверских решења која је тренутно доступна на тржишту није нимало јефтина. С тим у вези се јавља и каснија отежавајућа околност која такође може изискивати увећана финансијска средства у делу одржавања информационо – комуникационе опреме и лиценце за коришћење најажурније верзије софтвера. Не сме се заборавити и још један потенцијални недостатак, а то је кадровски потенцијал који ће практично радити на употреби одређеног софтверског решења у обуци припадника ватрогасно – спасилачких јединица. Ту се превасходно мисли на лица која су креатори сценарија, као и стручна лица из области информационо – комуникационих технологија.

Допринос употребе информационо – комуникационих технологија унапређењу оперативног рада и руковођења у ватрогасно – спасилчаким јединицама

Ватрогасно – спасилачке јединица свакодневно пружају одговор на различите облике ванредних догађаја. Том приликом се захтева брзина у циљу заштите и спасавања људи, материјалних и културних добара. То подразумева и брзину приликом доношења одлука које се односе на ангажовање снага и ресурса, тактичко поступање приликом интервенције, упућивање додатних снага и слично. У циљу олакшања процеса одлучивања током оперативног ангажовања ватрогасно – спасилачких јединица од велике користи је и употреба информационо – комуникационих технологија.

Употребом информационо – комуникационих технологија током оперативног рада припадницима ватрогасно – спасилачких јединица омогућено је следеће:

- да сагледају размере ванредног догађаја – коришћење беспилотних летелица,
- олакшано је одлучивање о распореду ресурса на интервенцијама,

- управљање информационим токовима на различитим хијерархијским нивоима – употребом радио веза, информациона средства,
- ефикаснија логистичка подршка током оперативног рада ватрогасно – спасилачких јединица.

Приликом тактичког одлучивања током оперативног рада ватрогасно – спасилачких јединица на различитим облицима интервенција инсистира се да се у сваком тренутку располаже релевантним информацијама о размерама ванредних догађаја. Имајући у виду да се се често не може простим физичким обиласком терена закључити докле је стигао поплавни талас или који је степен захваћености територије услед пожара на отвореном простору неопходна је употреба информационо – комуникационих технологија. Савремена технолошка решења, попут беспилотних летелица, показују се врло корисним у циљу унапређења оперативног одговора ватрогасно – спасилачких јединица. Наиме, ако се за пример узме пожар на отвореном простору, тачније шумски пожар, у пракси је врло отежано спознати колики је степен захваћености терена. За некога које руководилац акције заштите и спасавања и који уобичајено долази из редова ватрогасно – спасилачких јединица од изузетног значаја је да на једном месту сагледа докле се проширио пожар на отвореном простору, да ли има угрожених насељених места у близини, какав је распоред приступних путева, да ли у близини има водозахвата и слично. Управо снимак који се генерише употребом беспилотних летелица може бити употребљив у оперативном штабу где се доносе одлуке о распореду ватрогасно – спасилачких јединица, као и о правцима евакуације угроженог становништва.

У оперативном раду ватрогасно – спасилачких јединица препознање се и корист од употребе геоографског информационог система (ГИС). Организација ватрогасно – спасилачких јединица уобичајено подразумева и постојање организационе јединице која је задужена за пријем дојаве о ванредном догађају, анализу и обраду информација и комуникацију са другим хитним службама. Ове организационе целине имају улогу оперативних центара, а често се називају и командно – оперативним центрима. Један од примарних задатака је да пруже подршку руководству ватрогасно – спасилачких јединица у свим фазама руковођења приликом пружања одговора на ванредне догађаје. С тим у вези употреба географског информационог система у оперативним центрима ватрогасно – спасилачких јединица добија на значају како би се олакшало доношење одлука. Називи центара у којима се прикупљају, обрађују и шаљу информације о ванредним догађајима могу бити другачији. Међутим, пракса показује да то што се називају оперативним центрима показује њихову главну функцију. Једна од значајних функција оперативних центара ватрогасно – спасилачких јединица је прикупљање информација са локација где је дошло до ванредног догађаја, затим управљање и одржавање статуса о ангажовању ватрогасно – спасилачких јединица са различитих локација, као и управљање информационим токовима на различитим хијерархијским нивоима (ESRI 2008). Наведене функције коју обављају оперативни центри ватрогасно – спасилачких јединица немогуће је реализовати без конкретне употребе информационо – комуникационих технологија. Употребом ГИС-а може се врло лако и брзо генерисати мапа која ће приказати низ неопходних информација за доносиоца одлуке током оперативног ангажовања ватрогасно – спасилачких јединица. Како је већ неколико пута наглашено у раду, ефикасност и ефективност у раду ватрогасно – спасилачких јединица посебно долази до изражаја током фазе одговора на ванредне догађаје. Поред тога, брзина реаговања, која обухвата целокупни циклус од времена изласка из ватрогасне станице, стизања на место где је дошло до ванредног догађаја, до времена потребног за спасавање

угрожених лица или окончање интервенције, служи на неки начин као коначна оцена о поступању ватрогасно – спасилачких јединица. Управо ГИС помаже руководству ватрогасно – спасилачких јединица да доноси брзе и квалитетне одлуке. Постоји неколико функција које ГИС може да пружи у фази одговора на ванредне догађаје, а од интереса су за ватрогасно – спасилачке јединице, као што су:

- пружање упозорења и обавештења јавности на основу локације или подручја на које последице ванредног догађаја могу утицати,
- одржавати континуитет функционисања логистичке подршке ватрогасно – спасилачким јединицама – снабдевање водом и гориво, снабдевање другим средствима за гашење пожара,
- подршка ангажованим припадницима ватрогасно – спасилачких јединица и командном саставу, обезбеђује потребне ресурсе и размењује интерне и екстерне информације,
- припрема мапа, тренутних извештаја и извештаја о статусу интервенције за извршно руководство (ESRI 2008).

Постоје примери и других софтверских решења које користе ватрогасно – спасилачке јединице у циљу подршке одлучивању током пружања одговора на ванредне догађаја, али ГИС је један од најзаступљенијих. Такође, како је разнолик опис интервенција ватрогасно – спасилачких јединица, од пожара и експлозија, земљотреса, поплава, хемијских акцидената, саобраћајних незгода, одређене информационо – комуникационе апликације прилагођавају се различитој врсти ангажовања. Тако на пример, током пружања одговора на ванредне догађаје узроковане опасним материјама ватрогасно – спасилачке јединице користе апликације које располажу низом корисних информацијама о карактерситикама опасних материја. Једно од таквих софтверских решења је и ALOHA (Areal Locations of Hazardous Atmospheres). ALOHA је софтверско решење за моделирање опасности у случају акцидената са опасним материјама који се широко користи за планирање и реаговање на хемијске акциденте. ALOHA омогућава да се у сам програм унесу детаљи о стварном или потенцијалном ослобађању опасних материја, а затим ће генерисати процене зона претње за различите врсте опасности. ALOHA може да моделира облаке токсичног гаса, облаке запаљивих гасова, такозвани BLEVE ефекат (експлозија течности која се шири), као и друге облике последица ванредних доагађаја узрокованих опасним материјама. Процене зоне претње су приказане на мрежи у самом софтверу, а могу се уцртати и на мапама у другим апликацијама. На пример, црвена зона претње представља најгори ниво опасности, а наранџаста и жута зона опасности представљају области смањења опасности (EPA 2022).

У оперативном раду ватрогасно – спасилачких јединица користе се и различите информационо – комуникационе технологије које олакшавају сам процес комуникације између ватрогасаца – спасилаца на интервенцији, као и током размене информација са командним саставом који се налази у близини локације ванредног догађаја или је позициониран у оперативном штабу.

Анализа ванредних догађаја употребом информационо – комуникационих технологија

У циљу унапређења даљег рада и функционисања ватрогасно – спасилачких јединица значајно је анализирати претходно поступање током оперативног ангажовања. Како би се анализа спроводила на адекватан начин потребно је генерисати информације

о оперативном раду ватрогасно – спасилачких јединица. Тачније, неопходне су базе података које у себи садрже прецизне податке о свакој интервенцији, односно времена која су кључна када се анализира рад ватрогасно – спасилачких јединица, затим подаци о ангажованим ресурсима, подаци о последицама ванредног догађаја и броју спасених/евакуисаних лица, мапе које су коришћене током интервенције и слично. Коришћењем информационо – комуникационих технологија могуће је креирати базе података које ће дозвољавати једноставан унос података о ангажовању ватрогасно – спасилачких јединица. Такође, оно што је од значаја за анализу поступања је да апликације омогућавају задавање различитих упита и статистичке обраде. На пример, захтева се анализа ангажовања ватрогасно – спасилачких јединица на пожарима на грађевинским објектима. Ако би се посматрали појединачни извештаји о интервенцијама требало би доста времена да се дође до решења задатог упита. Међутим, ако се употребе савремене базе података у електронском облику одговор на предметни упит биће генерисан након свега неколико секунди и дозволиће и креирање различитих визуелних додатака, попут графикона, табела или мапа. Сектор за ванредне ситуације Министарства унутрашњих послова Републике Србије, у чијој надлежности су и професионалне ватрогасно – спасилачке јединице, користи централну базу података која се назива „Евиденција о догађајима – ДОГ". У овој бази података складиште се подаци о ангажовању ватрогасно – спасилачких јединица, ангажованим припадницима, возилима, спасеним лицима и сл. База података ДОГ се користи примарно за евиденцију података и генерисање различитих врста извештаја и статистика (Министартсво унутрашњих послова 2018).

Закључак

Употреба информационо – комуникационих технологија показује се као врло корисна у свим фазама рада и поступања ватрогасно – спасилачких јединица. Ако се посматра значај у делу обуке и припреме, јасно је да се коришћењем савремених софтверских решења могу симулирати различити ванредни догађаји и на тај начин приближити реални услови будућим и садашњим ватрогасцима – спасиоцима, у зависности од нивоа обуке или другог облика стручног усавршавања. Даље, када је реч о фази одговора на ванредне догађаја, комплексност интервенисања ватрогасно – спасилачких јединица огледа се низом фактора попут изражене урбанизације и индустријализације. Подршка одлучивању током оперативног ангажовања ватрогасно – спасилачких јединица најефикасније се остварује коришћењем информационо – комуникационих технологија. На крају, анализа рада ватрогасно – спасилачких јединица умногоме се показала сврсисходнијом ако се користе савремене базе података.

Велики је број предности од употребе информационо – комуникационих технологија у раду ватрогасно – спасилачких јединица. Међутим, не сме се заборавити и на недостатке, попут ограничења у делу кадровског потенцијала и опреме који су подразумевани када је реч о употреби информационо – комуникационих технологија у ватрогасно – спасилачким јединицама. Ипак, узевши у обзир неопходност константног развоја и унапређења рада ватрогасно – спасилачких јединица намеће се и потреба употребе информационо – комуникационих технологија.

Библиографија

Bashoor, M. 2020. ''Technology in the Fire Service". Policy Management // Fire. Преузето 10 маја 2024. https://www.powerdms.com/policy-learning-center/technology-in-the-fire-service

E-Semble. 2012. ''XVR brochure". Преузето 12 маја 2024. https://www.futureshield.com/img/brochures/XVR-Brochure-UK.pdf

Environmental Systems Research Institute. 2008. ''Geographic Information Systems Providing the Platform for Comprehensive Emergency Management". Environmental Systems Research Institute White Paper. Преузето 20 маја 2024. http:// www.esri.com

Environmental Protection Agency. 2022. ''ALOHA Software". Преузето 21 маја 2024. https://www.epa.gov/cameo/aloha-software

Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама.2018. Службени гласник, број 87/2018

Јагодин, Никола. 2017. ''Информатизација Хрватске ватрогасне заједнице". *Ватрогаство и управљање пожарима. бр. 1/2017., вол. VII, Загреб*

Миленковић, Милош. Кекић, Далибор. Главаш, Дарко. Марковић, Душан. 2019. Употреба савремених софтверских решења у припреми и обуци за реаговање у ванредним ситуацијама". Рад представљен на Шестој међународној научној конференцији Синтеза, Универзитет Сингидунум, април 2019.

Министарство унутрашњих послова Републике Србије. (2018). *Делатност Сектора за ванредне ситуације.* Преузето 10. марта, 2023., са http://prezentacije.mup.gov.rs/svs/HTML/delatnost.html

USE OF INFORMATION - COMMUNICATION TECHNOLOGIES IN THE WORK OF FIRE - RESCUE UNITS

Abstract: Modern challenges in the response to natural disasters and technical-technological accidents require to professional fire and rescue services to use modern information and communication technologies in order to provide an effective and efficient response. Firefighting and rescue units, as base of the operational part of the protection and rescue system, can use information and communication technologies in their work through all phases of emergency management. In the part of preparation, training and professional development, firefighters use information and communication technologies in order to have the opportunity to simulate real emergency events. The use of various simulators and software solutions during the training of members of the fire and rescue units greatly contributes to the improvement of the transfer of knowledge and previous experiences in the preparation for the work of the future. The importance of the use of information and communication technologies is particularly reflected in the operational work of fire and rescue units. Software packages such as geoinformation systems, various decision support programs, as well as databases related to population surveys, road and other infrastructure, can be of great use in protection and rescue operations. For example, the decision to evacuate the vulnerable population in certain emergency situations can be complex and time-limited. In order to make an optimal decision in the case of evacuation of the population, as well as in similar circumstances when the leaders of the fire and rescue units decide on the protection and rescue of people and goods, use of information and communication technologies contributes to the optimization of the final decision. The practice in the work of fire and rescue units is that after responding to various emergency events, data on interventions are stored in databases. The analysis of operational work of fire and rescue units contributes to the improvement of future activities. This part also reflects the significant use of information and communication technologies to provide recommendations and measures for the improvement and development of the work of fire and rescue units through various analysis databases.

Key words: information - communication technologies, fire and rescue units, geographic information systems, simulation.

ТРАНСПАРЕНТНОСТ ЈАВНЕ УПРАВЕ У ФУНКЦИЈИ СУЗБИЈАЊА КОРУПЦИЈЕ СА ОСВРТОМ НА ЗАШТИТУ ОД ПОЖАРА

Наташа Марковић[1]

Апстракт: Скоро да нема друштва где не постоји корупција. Појављује се у различитим облицима и на свим нивоима власти. Узроци могу да буду различити, али и начин борбе. Последице корупције су очигледне и утичу на економски развој, улагање страних инвеститора, конкуренцију на тржишту, али и делује деморалишуће на службенике јавне управе. Премда борба против корупције може бити кривичноправно процесуирање учинилаца кривичних дела, државе могу предузимати и друге мере ради сузбијања и борбе против корупције. Управно поступање службеника јавне управе, правни оквир, спровођење закона, примена стандарда, као и увођење електронских услуга и електронског управног поступања у јавној управи значајно може допринети смањењу корупције. Посебан акценат у раду се ставља на услуге из области заштите од пожара и других ризика и утицаја на безбедност грађана, као и могућност електронског информисања о потребним прилозима, трајању поступка, изјављивању жалбе, других правних лекова и другим важним питањима од значаја за прибављање исправа, односно остваривања права и извршавања обавеза. Дигитализација (електронско подношење захтева и издавање исправа у електронском облику) и оптимизација (поједностављење) поступака у области издавања уверења, дозвола, решења и других аката је од великог значаја за превенцију корупције. У раду се поред појма и облика корупције, као и извора корупције у вези са поступањем службеника јавне управе, разматра и процес реформе јавне управе у делу превенције и борбе против корупције. Такође се разматра међународни правни оквир и принципи рада јавне управе у функцији смањења бирократије и корупције. Даје се приказ правног оквира Републике Србије, увођења јавних услуга као најважније, али и других мера за спречавање корупције.

Кључне речи: јавна управа, корупција, правни оквир, јавне услуге, регистар административних поступака.

Увод

Корупција се може дефинисати као злоупотреба поверених овлашћења ради стицања приватне користи (© Savet Evrope, 2015). То је друштвена појава за коју не постоји универзално прихваћена дефиниција упркос мноштву научних истраживања и знатном броју међународних инструмената чија је основна сврха да се поставе законодавни темељи и оквир борбе против корупције. Овај појам који се користи за широки дијапазон ситуација. Чак се користи и за неке ситуације где је понашање службеника и негативан исход у предмету у односу на странку (одбачена пријава за посао, изгубљена парница или одбијен захтев) резултат личног неуспеха, нестручност службеника или несавршеног поступка, а у којима не постоје намере службеника за подмићивање.

[1] Специјалиста криминалиста, natamarko@yahoo.com

Узроци корупције могу бити различити, као што су сиромаштво (ниске плате службеника), похлепа, али и сама култура и обичај који је уврежен да службеник који је надлежан и поступа у управном поступку треба да буде „награђен“. Као један од главних узрока корупције у свакодневном људском понашању истичу се њене две димензије: первазивност и арбитрарност. Первазивност подразумева учесталост сусретања са коруптивним активностима у свакодневном додиру са људима, а арбитрарност независност државних чиновника у одлучивању, уз велику слободу и малу одговорност. Окидач да државни службеник прибегне коруптивном понашању може бити висок степен дискреционих овлашћења као и низак степен одговорности. Ипак, да ли ће до корупције и доћи, зависи од многобројних фактора, а најчешће од комбинације личног склопа и интегритета појединца. Организациона култура носи веома важну улогу у вршењу коруптивних дела. Она може утицати на отклон од неетичког понашања, али може и подстакнути овакво понашање у смислу „неморалног тона“организације. Она тиме доприноси да се коруптивно понашање посматра као средство за рад, које не само да није забрањено него је и пожељно (Сакач 2021,149).

Последице корупције су очигледне, она осујећује економски развој и умањује приход који држава остварује, одвраћа стране инвестиције и чини да тржишта буду у мањој мери ефикасна – зато што на њима предност не ужива најбољи производ, већ производ најкорумпиранијег произвођача. Такође она деморалише државне службенике који нису корумпирани, зато што је јавност веома склона да генерализује и све државне службенике гледа истим очима. Што је виши ниво корупције, то је мањи порески приход, будући да се умањују сопствене пореске обавезе.

Корупција се јавља у више појавних облика као што је подмићивање, проневера, фаворитизам, непотизам, трговина утицајем (© Savet Evrope 2015). У области јавне управе углавном се јавља “ситна“, административна или бирократска корупција и одвија се када државни службеници послују са грађанима или привредним субјектима. Придев „ситна” користи се као супротност „крупној“ корупцији како би се означиле размере корупције, тј. сразмера између корупције у јавној упрви и у поступању у судској власти или неким другим областима. Међутим, „ситна” корупција може бити веома значајна за људе који су њоме погођени. Износ незваничне цене услуге коју корисник услуге мора да плати може представљати знатан део расположивог прихода породичног буџета тог лица. И „крупна“ и „ситна“ корупција могу имати тешке последице.

Министарство унутрашњих послова један је од кључних актера у борби против корупције. Полиција истражује случајеве, док их тужилаштво даље процесуира. Такође се обучавају кадрови и граде и повећавају капацитети специјализованих полицијских јединица, као и тужилаштва за борбу против корупције. Поступање Министарства унутрашњих послова и тужилаштава не може искоренити ову „опаку болест друштва“. Истраживање случајева и процесуирање у ситуацији високе распрострањености корупције поскупљује државу те би пре свега требало радити на превенцији кроз примену стандарда у јавној управи.

Међународни правни оквир од значаја за борбу против корупције

Међународне организације и институције Европске уније одувек су биле снажно ангажоване у међународној борби против корупције промовишући законитост, стабилност демократских институција, заштиту људских права и друштвени и економски напредак. Не треба занемарити иницијативе других међународних и регионалних

организација – Организације Уједињених нација, Савета Европе и других. Међународни принципи за јавну управу имају за циљ да подрже државе у успостављању јасног и конзистентног правног оквира и у спровођењу владавине права, развијању добро организованих и адекватно финансираних судских, административних, безбедносних и других институција, као и развој цивилног друштва које доприноси јачању владавине права и одговорности јавних званичника и институција (Вукашиновић Радојичић, Чогурић 2021, 6).

Акти Уједињених нација промовишу: принцип законитости, владавину права, правну сигурност, легитимна очекивања, професионализам, транспарентност, ефикасност, ефективност, једнакост, одговорност, етичко понашање, као и успостављање и примену интегрисаних и повезаних елемената система управљања људским ресурсима. Један од најважнијих међународних аката у погледу јачања мера и развоја међународне сарадње за ефикасно спречавање и сузбијање корупције је Конвенција Уједињених нација против корупције, коју је ратификовала и Србија и Црна Гора (Закон о ратификацији Конвенције уједињених нација против корупције 2005). Због значаја борбе против корупције и сукоба интереса у јавној управи држава потписница, Конвенција се примењује на све „носиоце јавних овлашћења" (јавне службенике) – лица која обављају законодавне, извршне, административне или судске функције.

Правни оквир Републике Србије од значаја за спречавање и борбу против корупције

Доношење прописа који регулишу корупцију је један аспект спречавања и борбе против ове друштвене појаве. У многим земљама је реформа законодавства покренула питање борбе против корупције кроз кривичноправно кажњавање коруптивних дела али и кроз усвајање закона о транспарентности и одговорности, као што су: закони којима се државни службеници обавезују да пријаве имовину, о слободи изражавања и медијској слободи или о финансирању политичких странака и предизборних кампања.

Закони из области јавне управе значајно могу да допринесу превенцији корупције. Темељ за поједностављење управних поступака постављен је Законом о општем управном поступку и њиме је по први пут уведен појам „јединствено управно место" на коме странке могу да добију више информација и услуга на једном месту, било да се ради о електронском (Портал е-Управа) или физичком месту (члан 42.). Наглашена је обавезност размене података из службених евиденција између органа управе као један од битних услова за остваривање начела економичности и делотворности рада јавне управе и њеног претварања у стваран сервис грађана (члан 103.). Нагласак је дат на размену података, а не на размену докумената органа управе. Омогућено је да се од грађана и привредних субјеката не захтевају докази и исправе које иначе орган поседује у својим евиденцијама или у евиденцијама других органа и превазилази се могућност коруптивног понашања службеника - тражења непотребних прилога у смислу „фали ти још један папир".

Правила општег управног поступка гарантују законитост, правичност, ефикасност, једнак третман, сразмерност, правилно вршење дискреционог права, отвореност, транспарентност, непристрасност, објективност и правну заштиту.

Законом о електронској управи, који је усвојен 2018. године утврђен је правни оквир за њено функционисање и усклађивање са европским прописима у том домену. Један од кључних резултата овог Закона је успостављање интероперабилности база података између

државних органа и размена података електронским путем. Закон је прописао обавезу да се у раду органа јавне управе употребљава информационо-комуникациона технологија, како у управном поступању, тако и у комуникацији са грађанима, привредним субјектима и организацијама. Примена овог Закона значајно смањује могућност коруптивних радњи, пре свега „ситне" корупције, с обзиром да је Закон широм отворио врата подношењу захтева без доласка на шалтере и без контакта са могућим корумпираним службеницима.

Законом о Регистру административних поступака се такође значајно доприноси сузбијању корупције. Њиме се прописују административни поступци као управни и други који спроводе државни и други органи и организације и који се покрећу по захтеву привредних субјеката и грађана ради остваривања одређеног права или испуњавања прописане обавезе. Они се односе на издавање лиценце, дозволе, одобрења, сагласности, решења, уверења, потврда, сертификата, извештаја, мишљења, обавештења, сведочанстава, услова, декларација, записника, личних и других исправа, извода из службених евиденција или уношење достављених података и докумената у одређене јавне евиденције.

Закон је добар алат да се грађани и привредни субјекти информишу о поступцима и административним захтевима али и као основ за анализу података који се налазе у Регистру на основу које се утврђује могућности укидања поступка или евентуалног спајања поступка са другим, што такође доприноси смањењу корупције.

Реформа јавне управе у функцији превенције корупције – стратешка и програмска документа

Реформски процеси у области превенције корупције у Републици Србији се групишу у два тока: развој е-управе и регулаторна реформа и поједностављење управних поступака који се пре свега спроводи кроз Програм „е-Папир", као наставак и надградња Плана приоритетних активности за смањење административних терета у Републици Србији „Стоп бирократији". Намера је да се Стратегијом реформе јавне управе у Републици Србији за период од 2021. до 2030. године системски успостави оквир развоја, управљања и контроле политике пружања услуга, уз активно укључивање крајњих корисника у развој нових и оптимизацију постојећих услуга како би оне у највећој могућој мери биле усклађене са њиховим потребама. Како би се ово постигло успостављен је Регистар административних поступака као сигуран темељ добре координације и јединственог система за креирање и оптимизацију услуга, као и управљање квалитетом пружања услуга. Регистром управља Републички секретаријат за јавне политике, уз техничку подршку Канцеларије за информационе технологије и електронску управу. Њиме се обезбеђује квалитетан начин надзора и подршке у креирању нових услуга, као и ажурирање свих измена постојећих, а што се све благовремено објављује на Порталу е-Управа.

Потребно је поменути и Програм за поједностављење административних поступака и регулативе „е-Папир" за период 2023-2025.године. Овим документом јавне политике детаљније се разрађују циљеви и мере утврђене усвојеним документима јавних политика у вези са оптимизацијом, односно поједностављењем и дигитализацијом административних поступака. Програмом се први пут свеобухватно и системски приступа реформи јавне управе у делу који се односи на повећање ефикасности у спровођењу административних поступака, односно подизања квалитета пружања јавних услуга привредним субјектима и грађанима. Процес поједностављења административних поступака подразумева и анализу усклађености спровођења поступка са одредбама Закона

о општем управном поступку, оправданости достављања документације у зависности од потребе прибављања података за спровођење административног поступка, могућности размене података између надлежних органа и организација преко сервисне магистрале у складу са Законом о електронској управи, усклађивање документације коју је потребно доставити и рокова за спровођење поступака, оправданости постојања такси и накнада и њихове висине у конкретним поступцима, могућност дигитализације, односно спровођења поступка у свим случајевима где је то изводљиво у електронском облику.

Фокус реформи у области пружања услуга до 2030. године јесте стварање прилагодљиве јавне управе која у кратком року, уз разумне трошкове пружа интегрисане кориснички оријентисане услуге. За то се континуирано укључује шира друштвена заједница у процес развоја услуга и употребљавају иновативни алати, а следећи вредности Европске Уније и примењујући њене стандарде у овој области. Ефикасно пружање квалитетних услуга ће зависити и од капацитета јавне управе да ефикасно искористи велике сетове података, вештачку интелигенцију и блокчејн технологију како би брзо идентификовала просторе за оптимизацију постојећих и развој нових услуга, као и за унапређење интерних позадинских процеса у пружању услуга.

Анализа управног поступања у вези са појавом корупције

Успостављањем Регистра административних поступака омогућена је јавна доступност информација о поступцима, исправама и подацима потребним за њихово спровођење, на једном месту. Овим се омогућавају значајније уштеде за привреднике и грађане у вези са подношењем захтева, односно испуњавањем пословних обавеза, доприноси се спречавању вршења коруптивних дела од службеника јавне управе, ефикаснија сарадња између приватног сектора и јавне управе и постизање униформности у спровођењу административних поступака, чиме се трошкови јавног сектора у значајној мери смањују, али и простор за корупцију. Регистар је успостављен по угледу на земље које су успешно формирале сличне регистре (Финска, Естонија, Аустрија, Португалија и Словенија) и представља јединствену структурирану базу података и информација, обухвата податке потребне за успостављање Јединствене електронске контактне тачке, а коју ће, као обавезу Србија преузети транспоновањем Директиве 2006/123/ЕЗ о услугама на унутрашњем тржишту.

Пословно окружење за привреднике оптерећено је бројним препрекама које често нису видљиве и јасне при отпочињању пословања. С обзиром да се Република Србија већ дуже време налази у транзиционом периоду, који карактеришу честе измене прописа, а тиме и промене правила пословања, привредници имају тешкоће да се на време прилагоде свим тим променама. Административно оптерећење је високо и карактеришу га бројни поступци за остваривање права или испуњавање обавеза, као и високи трошкови њиховог спровођења. То представља трошак за привредне субјекте и у међународним оквирима се препознаје као значајна препрека даљем привредном развоју, а њихово смањење као кључни основ за унапређење услова пословања[2]. При-

[2] Иначе, од стране Републичког секретаријата за јавне политике израђено је више од 1057 препорука за оптимизацију (поједностављење и/или укидање и дигитализацију) поступака од којих су три добила законодавни оквир, а чија је примена почела 1. јануара 2019. године (укидање обавезе попуњавања МУН и М4 обрасца и укидање маркице за брашно), те је укупна годишња уштеда за привреду процењена на 3.466.835.553,00 РСД чиме је потврђен значај поједностављења поступака и смањења трошкова.

ликом утврђивања реформског правца у овој области, у обзир су посебно узета искуства СР Немачке, Молдавије и Португалије.

Током анализе административних поступака и спровођења јавно-приватног дијалога са привредним субјектима и државним службеницима утврђено је следеће:

Неуређеност поступка и неуједначеност у поступању - законска регулатива предвиђа постојање поступка и утврђује услове којим се доказује одређено чињенично стање, али се не прецизира ко утврђује испуњеност услова нити је прецизирана документација којом се испуњеност услова доказује због чега може доћи до неуједначеног приступа у истоветном поступку, као и већег ризика од корупције;

Непостојање обрасца за подношење захтева доводи до недоумица по питању које податке је потребно унети у образац захтева и непрецизног упутства о доказивању испуњености одређених услова, као и непоштовања обавезе прибављања података по службеној дужности. Ова обавеза се ретко примењује у пракси, доводи до непотребног административног оптерећења за подносиоца захтева, што може бити узрок корупције од стране службеника, који захтева достављање прилога који он сам може прибавити;

Немогућност електронског подношења захтева/поднеска - ово је нарочито приметно у поступцима у којима се поступак своди на достављање одређеног извештаја или једноставног обрасца са минимумом пратеће документације и инсистирање на оригиналима докумената - чак и када за тим нема потребе, што може бити погодно тле за развој корупције у јавној управи;

Непостојање рокова за поступање или непоштовање рокова за поступање – уколико се спровођење поступка састоји од неколико радњи које представљају услов за реализацију поступка, непостојање или непоштовање рокова за поступање повећава несигурност поступања и утиче на висину потенцијалног административног трошка, као и на могућност тражења мита како би се убрзало са доношењем одлуке;

Нетранспарентност административних поступака - неретко су административни поступци нејасни, услед чега долази до непотребног административног оптерећења за подносиоца захтева, који на разне начине прикупља информације о поступку. Чак и након подношења захтева, поставља се питање да ли је поднети захтев уредан или ће се од подносиоца тражити „још један папир", што оставља могућност службенику јавне управе да уз одговарајући поклон или награду поступа тако што ће да „наплати" своје ангажовање за доношење одлуке.

Електронска управа од значаја за сузбијање корупције

Дигитализација управе је битна претпоставка за законито, ефикасно, и економично остваривање улоге управе. Електронска управа уводи значајне промене у структури друштва, вредностима, организационој култури, као и у пословању свих субјеката на тржишту. Њена примена снажно утиче на развој информационог друштва у областима јавне управе, здравства, образовања, правосуђа, социјалне политике, јавних набавки, партиципације у одлучивању, сигурности података и електронских трансакција, доступности и приступачности, безбедности података о личности (Вукашиновић-Радојичић, Марковић 2019, 296).

Савремени начин живота подразумева употребу интернета и намеће потребу стварања модерне управе, са циљем да се, употребом нових технологија, побољша ефикасност, ефективност, транспарентност и одговорност јавне управе. Електронска управа је један од начина да се оствари овај циљ, тако што се, поред поједностављења управних процедура остварују права за грађане и привреду на лакши, једноставнији

начин, осигурава приступ информацијама и услугама од јавног значаја на погодан начин, уз што већу уштеду времена и средстава (Анамарија Муса 2006).

Доступност информација и поједностављење пружања услуга грађанима, кроз унапређивање управних поступака и поједностављивање њихове примене коришћењем информационо-комуникационих технологија уз постепено уклањање класичног начина пружања услуга за које постоји могућност комплетне реализације путем *on line* сервиса, доводи до рационализације и реорганизације управе, смањења трошкова у раду и ефикаснијег остваривања права грађана и привредних субјеката. Е-Управа поспешује сарадњу и координацију органа и организација јавне управе на централном и локалном нивоу и свих државних и недржавних субјеката и грађана чиме се обезбеђује системско поступање на свим нивоима управе. С обзиром на то да се пословни процеси дигитализују и смањује улога људског фактора у реализацији јавних услуга, електронска управа је значајна у борби против корупције и сиве економије (Вукашиновић-Радојичић, Марковић 2019, 286).

Електронске услуге и друге мере у функцији превенције корупције

Дигитализација поступака је могућност за подносиоца захтева да електронским путем покрене поступак пред органом јавне управе, поднесе прилоге, плати таксе, прати статус предмета, комуницира у поступку са органом и по потреби допуни захтев и, на крају, прими акт за који је поднео захтев. За обрађивача дигитализација је могућност да путем портала прими захтев и евентуалне прилоге, аутоматски добије потребне податке из регистара за одлучивању у процесу и изда захтевани акт у електронском облику. Користи дигитализације се огледају у томе што не постоји физички контакт подносиоца и обрађивача, као и што се било какво одлагање доношења одлуке и пробијање рокова аутоматски детектује, чиме се смањује могућност за корупцију у поступку.

Процес дигитализације једног административног поступка обухвата успостављање дигиталних регистара или евиденција, њихово повезивање на сервисну магистралу, израду дијаграма претходно поједностављеног поступка и на крају израду самог техничког решења на платформи за дигитализацију.

Електронске услуге за грађане и привредне субјекте којих на порталу еУправе има све више такође доприносе смањењу могућности корупције. На овом порталу се може поднети захтев у електронском облику, без доласка на шалтер, као и преузимање исправа на кућној адреси или у електронско поштанско сандуче. Чињеница да грађани не остварују контакте са службеницима јавне управе значајно онемогућава давање мита и вршење других коруптивних радњи. Кључни изазов у овој области представља квалитет пружених услуга крајњим корисницима, неуједначена приступачност услугама, као и недовољно доступне и јасне информације о услугама, што повећава ризик од корупције, јер електронске услуге које нису једноставне за коришћење и даље терају грађане и привредне субјекте да се обраћају службеницима на шалтерима.

Регистар администратитвних поступака у функцији превенције корупције у области заштите од пожара

Регистар административних поступака као јавно доступна електронска база података садржи податке, између осталог и о административним поступцима и административним захтевима из области заштите од пожара.

За привредне субјекте и грађане јавно је доступно 49 административних поступака из ове области, а неки од њих су: Мишљење са условима заштите од пожара и експлозија за потребе израде планског документа, Услови за безбедно постављање објеката са запаљивим и горивим течностима, запаљивим гасовима и експлозивним материјама у погледу мера заштите од пожара и експлозије, који се издају ван обједињене процедуре, Услови у погледу мера заштите од пожара за објекте за које је прописана обавеза давања сагласности на техничку документацију, који се издају ван обједињене процедуре, Одобрење локације за изградњу и безбедно постављање објеката са запаљивим и горивим течностима, запаљивим гасовима и експлозивним материјама, Сагласност на техничку документацију у погледу мера заштите од пожара која се издаје у обједињеној процедури, Утврђивање подобности за употребу објеката у погледу спроведености мера заштите од пожара, Сагласност на План заштите од пожара, Уверење о насталом пожару, Овлашћење за израду Главног пројекта заштите од пожара и други.

За сваки од поступака јавно је доступно коме је намењен поступак, како остварити право или испунити обавезу у вези са поступком, који су финансијски издаци, који су рокови за поступање органа, да ли се може поднети приговор, изјавити жалба или се водити управни поступак.

Детаљном претрагом привредни субјекти и грађани се могу информисати и о општим подацима, правном основу, сврси административног поступка, да ли постоји комуникација приликом управног поступања са другим органима и прибављање података по службеној дужности, која је потребна документација, који су финансијски издаци подносиоца захтева, остали елементи административног поступка, као и жалбени поступак или други правни лек.

Информације које постоје у Регистру административних поступака су добар алат који је у фунцији транспарентности управног поступања а тиме и смањења ризика од корупције. На великом броју ових поступака се ради на оптимизацији и дигитализацији која између осталог подразумева и електронско подношење захтева, плаћање накнада и пријем потврде, решења или другог акта електронски, што значајно доприносе борби против корупције у овој области.

Закључак

Корупција је злоупотреба поверених овлашћења ради стицања приватне користи. Узроци ове појаве могу бити различити, као што су сиромаштво (ниске плате службеника), похлепа, али и сама култура и обичај да службеник који је надлежан и поступа у управном поступку треба да буде „награђен“. Она осујећује економски развој и умањује приход који држава остварује, одвраћа стране инвестиције и чини да тржишта буду у мањој мери ефикасна. Такође деморалише државне службенике који нису корумпирани, зато што је јавност веома склона да генерализује и све државне службенике гледа истим очима. Што је виши ниво корупције, то је мањи порески приход. Корупција се јавља у више појавних облика као што је подмићивање, проневера, фаворитизам, непотизам, трговина утицајем. У области јавне управе углавном се јавља “ситна“, административна или бирократска корупција и одвија се када државни службеници послују са грађанима или привредним субјектима.

Међународне организације и институције Европске уније одувек су биле снажно ангажоване у међународној борби против корупције, промовишући законитост, стабилност демократских институција, заштиту људских права и друштвени и економски на-

предак. Акти Уједињених нација промовишу: принцип законитости (владавина права), правну сигурност, легитимна очекивања, професионализам, транспарентност, ефикасност, ефективност, једнакост, одговорност, етичко понашање, као и успостављање и примену интегрисаних и повезаних елемената система управљања људским ресурсима. Један од кључних циљева одрживог развоја односи се на изградњу ефикасних, одговорних, транспарентних институција на свим нивоима.

Закони из области јавне управе такође значајно доприносе превенцији корупције. Закон о општем управном поступку је „отворио врата" подношењу захтева без доласка на шалтере, а Закон о електронској управи поставио темеље електронског управног поступања које умногоме умањује могућност корупције. Применом Закона о Регистру административних поступака се значајно превенира корупција, јер се кроз регистар административних поступака, као јавно доступне електронске базе података о административним поступцима и административним захтевима омогућава транспарентоност јавне управе.

Дигитализација поступака представља могућност за подносиоца захтева да електронским путем покрене поступак пред органом јавне управе, поднесе прилоге, плати таксе, прати статус предмета, комуницира у поступку са органом и по потреби допуни захтев и, на крају, прими акт за који је поднео захтев. Користи дигитализације се огледају у томе што не постоји физички контакт подносиоца и обрађивача, као и што се било какво одлагање доношења одлуке и пробијање рокова аутоматски детектује, чиме се смањује могућност за корупцију у поступку.

Мере за смањење корупције, осим правног оквира, доследног спровођења закона и других прописа, увођења електронских услуга и електронског управног поступања, обухватају и утврђивање правичних, транспарентних поступака, јачање одговорности и ефикасности, увођење етичких кодекса или кодекса понашања да би се вредности непристрасности и поштења поставиле као основне вредности у јавној управи.

За привредне субјекте и грађане из области заштите од пожара јавно је доступно 49 административних поступака.

За сваки од поступака јавно је доступно коме је намењен поступак, како остварити право или испунити обавезу у вези са поступком, који су финансијски издаци, који су рокови за поступање органа, да ли се може поднети приговор, изјавити жалба или се водити управни поступак, што значајно може допринети превенцији корупције.

Поред адекватног правног оквира још је важније и спровођење закона, што је прави изазов како се закони не би примењивали селективно, односно да се не би доносили да би се задовољила форма без да се спречи постојање корупције.

Поред електронских услуга, од значаја за смањење корупције је и смањење дискреционих овлашћења државних службеника. Дискрециона овлашћења омогућавају службеницима доношење одлука којим могу да одступају од уобичајеног, чиме се корисници управе доводе у ситуацију да не могу предвидети исход поступка.

Библиографија

Вукашиновић Радојичић Зорица, Чогурић Весна, Convergence and Symbiosis of Public Administration Principles - International and European Perspective, *Часопис Безбедност 1/2021*

Вукашиновић Радојичић Зорица, Марковић Наташа, Изазови примене савремених информационих технологија и реформа јавне управе у Републици Србији, *Правни живот број 10/2019, Том II*

Муса.Анамарија, Е управа и проблем дигиталне подјеле: активности усмјерене на побољшање приступа интернету у еуропској унији и Републици Хрватској, *Правни факултет у Заīребу, Заīреб, 2006. https://www. pravo.unizg.hr*

Сакач Александар, Фактори корупције са освртом на стање у Републици Србији, *Часопис Безбедност 3/2021*

Savet Evrope, Борба против корупције: основни појмови, Приручник, *https://rm.coe.int/borba-osnovni-pojmovi-protiv-korupcije/16806eed0d* Прво издање ©, *мај 2015*.

Европска Унија, Директива 2006/123/ЕЗ о услугама на унутрашњем тржишту, *https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32006L0123*, 2023

Стратегија реформе јавне управеве у Републици Србији за период од 2021. до 2030. године ("Службени гласник РС", бр. 42/2021, 9/2022)

Програм за поједностављење административних поступака и регулативе "Е папир" за период од 2023. до 2025. године https://www.srbija.gov.rs/prikaz/703110., 2023.

Закон о општем управном поступку ("Службени гласник РС", бр. 18/2016, 95/2018 – Аутентично тумачење, 2/2023 – УС)

Закон о Регистру административних поступака ("Службени гласник РС", број 44/ 2021.)

Закон о електронској управи ("Службени гласник РС", број 27/2018)

Закон о ратификацији Конвенције уједињених нација против корупције („Сл. лист СЦГ - Међународни уговори, бр. 12/2005)

TRANSPARENCY OF PUBLIC ADMINISTRATION IN THE FUNCTION OF COMBATING CORRUPTION WITH REFERENCE TO FIRE PROTECTION

Abstract: There is almost no society where there is no corruption. It appears in different forms and at all levels of government. The causes can be different, but also the way of fighting. The consequences of corruption are obvious and affect economic development, investment by foreign investors, competition on the market, but also have a demoralizing effect on public administration officials. Although the fight against corruption can be criminal prosecution of the perpetrators of criminal acts, states can take other measures to suppress and fight against corruption. The behavior of public administration officials, the legal framework, law enforcement, application of standards, as well as the introduction of electronic services and electronic government in public administration can significantly contribute to the reduction of corruption. A special emphasis in the work is placed on services in the field of fire protection and other risks and impacts on the safety of citizens, as well as the possibility of electronic information about the necessary attachments, the duration of the procedure, filing a complaint, other legal remedies and other important issues of importance for obtaining documents, that is, exercising rights and fulfilling obligations. Digitization (electronic submission of requests and issuance of documents in electronic form) and optimization (simplification) of procedures in the area of issuing certificates, permits, decisions and other acts is of great importance for the prevention of corruption. An addition, the concept and form of corruption, as well as sources of corruption in conection with the actions of public administration officials, the paper also discusses the process of public administration reform in the part of prevention and fight against corruption. It also considers the international legal framework and principles of public administration in order to reduce bureaucracy and corruption. The legal framework of the Republic of Serbia and the introduction of public services as the most important and other measures have a huge impact on preventing corruption.

Keywords: public administration, corruption, legal framework, public services, register of administrative procedures.

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

351.862.21(082)
005.334:351.759.6(082)
004(082)

МЕМОРИЈАЛНА конференција „Предраг Марић“ (3 ; 2024 ; Београд)
Зборник радова / Меморијална конференција „Предраг Марић“, 24. 04. 2024. године ; [уредници] Младен Милошевић, Ненад Стекић. - Београд : Факултет безбедности Универзитета, 2024 (Београд : Академска мисао). - 223 стр. : илустр. ; 24 cm

"Конференција и израда овог Зборника су реализовани у оквиру пројекта који финансира Фонд за науку Републике Србије у оквиру Програма „ИДЕЈЕ” – Management of New Security Risks - Research and Simulation Development, NEWSIMR&D, #7749151."--> Колофон. - Тираж 100. - Стр. 9-10: Предговор / Младен Милошевић, Ненад Стекић. - Напомене и библиографске референце уз текст. - Библиографија уз сваки рад. - Summaries.

ISBN 978-86-80144-66-5

а) Ванредне ситуације -- Безбедност -- Зборници б) Управљање ризиком -- Безбедносни сектор -- Зборници в) Кризни менаџмент -- Зборници г) Вештачка интелигенција -- Примена -- Зборници

COBISS.SR-ID 158909449