ЗБОРНИК РАДОВА

VI међународни научни скуп

„Савремени изазови и пријетње безбједности”

Бања Лука, Република Српска, БиХ, 27. март 2026. године

Бања Лука, 2026. година

Издавач
Универзитет у Бањој Луци, Факултет безбједносних наука
Булевар војводе Живојина Мишића 10А, Бања Лука

Едиција
Зборници

Главни и одговорни уредник
Проф. др Предраг Ћеранић
Универзитет у Бањој Луци, Факултет безбједносних наука

Штампа:
"PRINT SHOP" d.o.o. Istočna Ilidža

Тираж:
120 примјерака

ISBN 978-99976-805-9-4

Прегледни научни рад
UDK 004.8:351.74/.76

ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА КАО ИЗАЗОВ САВРЕМЕНЕ БЕЗБЕДНОСТИ

Дејан Вулетић

Др Дејан Вулетић, виши научни сарадник, ради у Институту за стратегијска истраживања, Универзитета одбране у Београду, Министарства одбране Р. Србије.
dejan.vuletic@mod.gov.rs

Сажетак: Циљ рада је анализа на који начин вештачка интелигенција (ВИ) трансформише савремено безбедносно окружење, са фокусом на промене у природи претњи, импликације на савремену безбедност као и нормативне, правне и етичке изазове управљања ризицима. Рад се ослања на квалитативну анализу садржаја научне литературе, као и анализу релевантних докумената и извештаја међународних и националних институција. Резултати истраживања показују да ВИ делује као мултипликатор способности у доменима обавештајне анализе, надзора и извиђања, сајбер операција и подршке одлучивању, али истовремено ствара нове системске ризике: повећану брзину одлучивања и потенцијал „компресије времена“ у кризи, проблеме предвидљивости понашања комплексних модела, као и ризик нежељене ескалације услед грешака, пристрасности или интеракције аутономних система. Вештачка интелигенција представља један од кључних изазова савремене безбедности те су због тога неопходни интегрисани механизми управљања, од техничких стандарда и процена ризика до међународних норми и правних оквира.

Кључне речи: вештачка интелигенција, безбедност, управљање ризиком

УВОД

Интензивирање развоја ВИ током последњих година значајно је изменило савремено безбедносно окружење, с обзиром на то да се ове технологије све масовније користе у анализи великих количина података, благовременом уочавању ризика, сајбер операцијама и унапређењу система командовања и подршке одлучивању. У стручној и политичкој литератури све је заступљеније становиште да ВИ представља фактор који обликује однос снага и токове међународног надметања, не само посредством развоја наоружања већ и кроз утицај на широк дијапазон војних активности (Horowitz, 2018). Њена примена обухвата више нивоа војно-безбедносних структура, од логистике и обавештајне аналитике до система за препознавање и избор циљева, што чини да дискусија о безбедносним импликацијама превазилази оквир расправе о смртоносним аутономним платформама и усмерава се ка питањима стратегијске стабилности, управљања ескалацијом, одговорности и институционалне контроле (UNIDIR, 2023).

Предмет овог рада усмерен је на испитивање улоге ВИ као вишедимензионалног безбедносног чиниоца који истовремено производи нове врсте ризика, попут аутоматизованих сајбер дејстава и софистицираних информационих операција, трансформише начин употребе силе кроз раст алгоритамске подршке и степена аутономије система, и покреће комплексна нормативна и етичка питања у вези са концептом „смислене људске контроле“, применом међународног хуманитарног права и утврђивањем одговорности. Оваква проблематика посебно је истакнута у ставовима Међународног комитета Црвеног крста, који упозорава на опасност од маргинализације људског расуђивања у процесу употребе силе, као и на тешкоће у усклађивању аутономних система са правилима и принципима вођења оружаних сукоба (ICRC, 2021).

Циљ рада јесте да се издвоје и аналитички уобличе главне безбедносне последице примене ВИ кроз три међусобно повезане димензије: прво, оперативно-технолошку, која обухвата могућности и ограничења ВИ у извршавању безбедносних задатака; друго, стратегијско-политичку, која се односи на утицај ових технологија на расподелу моћи, динамику ескалације, одвраћање и трку у наоружању и иновацијама; и треће, нормативно-правну и етичку, у чијем су фокусу међународно хуманитарно право, питања одговорности, транспарентности и управљања ризицима. У оквиру таквог приступа анализирају се и институционални инструменти за ублажавање ризика, укључујући националне смернице и стандарде за развој „поуздане“ вештачке интелигенције (NIST, 2023).

Структура рада је организована тако да, након уводних разматрања, прво поглавље успоставља појмовни и теоријски оквир за разумевање улоге ВИ у области безбедности, укључујући кључне дефиниције, домене примене и услове под којима ове технологије истовремено делују као извор спосо-

бности и ризика. Друго поглавље усмерено је на анализу конкретних војно-безбедносних примена ВИ, од обавештајне аналитике и сајбер операција до система за подршку одлучивању и аутономних, односно полуаутономних платформи, при чему се аргументација ослања на релевантне међународне студије и истраживачке извештаје. У трећем поглављу разматрају се правни и етички изазови, модели управљања ризицима и препоруке за одговорну и безбедну употребу ВИ у сектору безбедности.

ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА У САВРЕМЕНОМ БЕЗБЕДНОСНОМ ОКРУЖЕЊУ: ПОЈМОВНИ И ТЕОРИЈСКИ ОКВИР

Иако се израз „вештачка интелигенција“ у јавном дискурсу често појављује као јединствен и недвосмислен појам, у научним и стратешким анализама он обухвата разнолик скуп технологија, алгоритама и система који се разликују по нивоу сложености и степену аутономног деловања. У најопштијем значењу, ВИ се дефинише као способност дигиталних система да извршавају задатке који су традиционално везани за људске когнитивне функције, укључујући препознавање образаца, учење на основу података, процену опција и решавање проблема (Russell & Norvig, 2021). У области безбедности, међутим, њен утицај не произлази само из техничких својстава ових технологија, већ и из начина на који су оне уграђене у институционалне, оперативне и доктринарне оквире деловања.

У научним расправама уобичајено је разликовање између тзв. уске и опште вештачке интелигенције. Док уска ВИ, која тренутно преовлађује у реалним применама, функционише у оквиру строго дефинисаних задатака и окружења, концепт опште ВИ који подразумева когнитивне способности упоредиве са људским за сада остаје предмет теоријских и истраживачких напора (Bostrom, 2014). Из перспективе безбедности, највећи ризици не произлазе из хипотетичких будућих система, већ из све интензивније употребе уске ВИ у осетљивим оперативним функцијама, где чак и ограничени степени аутономије могу произвести далекосежне и тешко предвидиве ефекте.

Један од најзаступљенијих аналитичких оквира у проучавању улоге ВИ у међународној безбедности заснива се на њеном схватању као фактора који увећава постојећу моћ држава. У том контексту, ВИ не редефинише саме циљеве државних актера, али битно мења начине и динамику њиховог остваривања, пре свега кроз убрзану обраду информација и аутоматизовано доношење закључака (Payne, 2021). Напредни алгоритми омогућавају брже препознавање образаца, ефикаснију алокацију ресурса и прецизније процене потенцијалних претњи, што утиче на укупну ефикасност безбедносних политика. Управо такво убр-

завање процеса одлучивања може произвести нове облике ризика. Укључивање ВИ у системе командовања и контроле ствара ситуацију у којој се временски простор за људску процену, проверу података и политичку деескалацију значајно смањује, што повећава вероватноћу погрешних или преурањених одлука. Алгоритамске грешке, пристрасни улазни подаци и непредвиђене интеракције између повезаних система у таквим околностима могу имати директан утицај на стабилност стратешких односа (UNIDIR, 2023). Из угла теорије одвраћања, увођење ВИ додатно усложњава постојеће моделе. За разлику од класичних концепата који се ослањају на релативно транспарентне и дугорочно стабилне војне капацитете, технолошки развој заснован на ВИ омогућава нагле и неравномерне промене у моћи актера. То може подстаћи интензивирање технолошке конкуренције и истовремено умањити јасноћу намера, посебно у областима као што су сајбер односно информациони простор, где је утврђивање одговорности и иначе отежано (Scharre, 2018).

Утицај ВИ не ограничава се само на државне институције, већ све израженије обликује и оперативне способности недржавних актера. Алати засновани на ВИ омогућавају аутоматизовано извођење сајбер операција, ефикасније креирање и ширење дезинформација, као и напредну анализу података, чиме се значајно снижавају техничке и финансијске баријере за учешће у сложеним безбедносним активностима (Brundage et al., 2018). Последично, безбедносно окружење постаје фрагментиранije и мање предвидљиво, што умањује делотворност класичних механизама превенције и одвраћања. У том контексту, све више аутора указује да ВИ подстиче процес „распршивања моћи“, при чему стратешка предност више не зависи искључиво од количине расположивих ресурса, већ од способности актера да ефикасно интегришу напредне технологије у своје безбедносне праксе (Allen & Chan, 2017). Оваква динамика има значајне последице по регионалну и међународну стабилност, нарочито у условима појачаног ривалства међу водећим силама.За разлику од класичних оружаних система, ВИ представља општу, хоризонталну технологију која продире у готово све сегменте војног деловања, од логистичке подршке и обуке људства, до обавештајне обраде података и процеса командовања. Управо због те ширине примене и функционалне флексибилности, ВИ заузима централно место у анализи савремених безбедносних изазова (Horowitz, 2018).

ПРИМЕНА ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ У БЕЗБЕДНОСТИ И ОДБРАНИ

Међу првим и најинтензивније развијаним областима у којима је ВИ нашла примену у сфери безбедности налази се домен обавештајно-надзорних и извиђачких активности. Савремене безбедносне инфраструктуре производе изузетно велике количине информација које потичу из хетеро-

гених извора, укључујући сателитске системе, електронска пресретања, јавно доступне садржаје, друштвене мреже и различите врсте сензора. Обим и сложеност таквих података превазилазе могућности класичних аналитичких приступа. У том контексту, ВИ обезбеђује технолошку основу за њихову аутоматску обраду, међусобно повезивање и приказивање у облику који је употребљив за доношење одлука, што значајно убрзава и продубљује обавештајне процене (Johnson, 2019).

Методе машинског и дубоког учења показале су висок степен успешности у аутоматском уочавању образаца у визуелним подацима, што их чини посебно корисним за обраду снимака добијених са сателита и беспилотних летелица. Према релевантним анализама, алгоритми засновани на ВИ већ имају значајну улогу у препознавању објеката, надзору кретања и детекцији одступања у реалном времену (UNIDIR, 2023). Ове способности омогућавају знатно брже и свеобухватније обавештајне процене него што је то било могуће традиционалним средствима. Ипак, такво повећање ефикасности истовремено отвара и нове изазове, пре свега у вези са поузданошћу улазних података и интерпретацијом резултата у комплексним политичким и друштвеним контекстима. Поред техничких питања, појављује се и институционални проблем растуће зависности од алгоритамских система. Ако се људски аналитичари превише ослоне на аутоматизоване процене, њихове сопствене аналитичке способности могу временом ослабити, што у кризним ситуацијама повећава вероватноћу некритичког прихватања излаза које генерише вештачка интелигенција (Jensen, 2020).

Једна од централних тачака у разматрању безбедносних последица примене вештачке интелигенције односи се на питање аутономије технолошких система. Аутономне платформе су у стању да, након што буду активиране, самостално извршавају задатке на основу података које прикупљају и алгоритама који управљају њиховим понашањем, без континуиране људске контроле (Boulanin & Verbruggen, 2017). Међутим, аутономија није бинарна категорија већ спектар, што значајно отежава њено прецизно правно и нормативно дефинисање. У области безбедности то отвара посебно осетљива питања, нарочито када се алгоритамима препуштају одлуке које могу довести до употребе силе или изазвати ескалацију сукоба. Иако су алгоритамски системи способни да изузетно ефикасно оптимизују задате параметре, они немају способност да разумеју шири контекст, да врше моралну процену или да интуитивно процене ризик, што су кључне карактеристике људског одлучивања (Cummings, 2017). Додатни проблем представља феномен познат као аутоматизациона пристрасност, односно тенденција да се препоруке система заснованих на ВИ прихватају без довољно критичког преиспитивања, чак и онда када постоје назнаке да су оне нетачне (Parasuraman & Riley, 1997). У кри-

зним и временски осетљивим ситуацијама, оваква динамика може значајно умањити простор за људску интервенцију и исправљање погрешних одлука.

Једна од најосетљивијих области примене ВИ односи се на системе намењене подршци командовању и доношењу одлука. Сврха ових платформи је да лидерима и штабовима обезбеде интегрисане процене стања, прогнозе развоја ситуације и препоруке за деловање. Иако такви алати могу значајно побољшати оперативну свест, истовремено се отвара питање у којој мери се одговорност за одлуке постепено преноси са људи на алгоритме. У условима високе брзине и притиска савремених операција постоји ризик да доносиоци одлука све више прихватају улогу надзорника аутоматизованих система, уместо да остану активни тумачи и процењивачи безбедносних информација (Black et al., 2024). Такав развој је нарочито проблематичан у сфери нуклеарног одвраћања и управљања кризама, где и наизглед мале грешке могу имати несразмерно тешке последице. Истраживања сугеришу да примена ВИ може допринети стабилизацији у почетним фазама кризе, али истовремено повећати опасност од ескалације у њеним каснијим етапама, када аутоматизовани системи почињу да реагују на унапред дефинисане индикаторе без довољне политичке и стратешке процене (Acton, 2019). Због тога се као централно намеће питање граница у којима ВИ треба укључивати у процесе који директно утичу на одлуке о употреби силе.

Највеће полемике у вези са применом ВИ у области безбедности изазивају аутономни и полуаутономни борбени системи. Иако у потпуности самостални „смртоносни“ системи још увек нису често у употреби. Трендови развоја указују на постепено повећање степена аутономије у функцијама навигације, селекције циљева и употребе силе (Scharre, 2018). Такав тренд додатно наглашава јаз између брзине технолошких иновација и постојећих правних и нормативних механизама њихове контроле. Један од кључних проблема јесте одсуство општеприхваћене дефиниције „смртоносног аутономног оружаног система“, што значајно отежава међународне покушаје његове регулације (Boulanin, 2020). Разлике у војним доктринама и интересима држава додатно умањују изгледе за брзо постизање глобалног консензуса. Са безбедносног становишта, посебан ризик произлази из сценарија у којима више аутономних система истовремено делује и имају међусобну интеракцију. У таквом окружењу је тешко предвидети понашање како сопствених, тако и противничких платформи, што повећава неизвесност и потенцијал за ненамерну ескалацију (Payne, 2021). Управо у сајбер простору, као домену у којем је примена ВИ нарочито интензивна и двосмерна, ови изазови долазе до пуног изражаја.

Вештачка интелигенција има двоструку улогу у сајбер домену, јер се примењује и у заштити информационих система и у извођењу напада. Са одбрамбене стране, технике машинског учења омогућавају ефикасније

откривање упада, идентификацију злонамерних програма и предвиђање слабих тачака у дигиталним инфраструктурама (Buchanan, 2020). Истовремено, исте технолошке могућности могу се употребити и за унапређивање офанзивних активности, као што су фишинг, напади ускраћивања услуга и развој све сложенијих облика малициозног софтвера (Vuletić, 2012; Vuletić & Nojković, 2018). Овај паралелни развој одбрамбених и офанзивних капацитета доводи до процеса који се у литератури описује као „динамична спирала надметања“, у оквиру које актери континуирано унапређују своје сајбер способности како би одржали или стекли предност (Rid, 2020). За разлику од класичних војних окружења, у сајбер простору је утврђивање порекла напада често веома сложено, што слаби ефикасност традиционалних механизама одвраћања (Vuletić, 2018). У таквом амбијенту, убрзано увођење ВИ може повећати интензитет и брзину конфликата, сузити простор за дипломатско управљање кризама и појачати ризик од ненамерне ескалације.

За разлику од већине ранијих технолошких достигнућа у војној и безбедносној сфери, ВИ је у значајној мери доступна и актерима ван државних институција. Широка комерцијална понуда алата за машинско учење и напредну анализу података омогућава терористичким и криминалним групама да ове технологије користе за припрему операција, ширење пропаганде и извођење финансијских злоупотреба (Brundage et al., 2018). Таква широка доступност ВИ смањује техничке и организационе баријере за учешће у сложеним безбедносним активностима и истовремено подрива ефикасност традиционалних механизама контроле. У оваквим условима, ВИ постаје фактор који додатно замагљује границу између рата и мира, као и разлику између државних и недржавних извора претњи.

ЕТИЧКЕ И НОРМАТИВНО-ПРАВНЕ ДИЛЕМЕ ПРИМЕНЕ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ

Један од кључних проблема које увођење ВИ поставља пред међународну безбедност односи се на очување стратегијске стабилности. Класични модели стабилности ослањају се на релативно јасно сагледавање војних капацитета и намера супарника, као и на постојање механизама који ограничавају ескалацију кроз одвраћање и контролу ризика. Међутим, увођење ВИ у војне и безбедносне системе подрива ове претпоставке на више начина. Пре свега, ВИ драматично убрзава прикупљање и обраду информација, што скраћује време доступно за политичку и војну процену у кризним околностима. Такав временски притисак може повећати склоност ка превентивним или преемптивним потезима, нарочито када је ниво неизвесности висок.

Иако ВИ сама по себи не мора нужно да буде извор дестабилизације, она може интензивирати већ постојеће тензије и погрешна тумачења понашања противника (Acton, 2019). Додатни изазов представља ограничена транспарентност начина на који сложени алгоритми, а нарочито модели дубоког учења, генеришу своје закључке и препоруке, што отежава њихову проверу и контролу у осетљивим безбедносним контекстима (UNIDIR, 2023).

Етичке расправе о употреби ВИ у сектору безбедности у великој мери се усмеравају ка принципу такозване „смислене људске контроле“, који полази од претпоставке да одлуке о примени силе морају остати у домену људске одговорности. Овај концепт је током последњих година постао једна од централних тема у раду међународних експертских тела и форума (ICRC, 2021). Полазна етичка напетост произилази из чињенице да алгоритамски системи немају сопствену моралну способност, већ делују искључиво у складу са унапред задатим правилима и моделима, без разумевања ширих хуманитарних и друштвених последица. Када се одлучивање о животу и смрти у већој мери препусти аутоматизованим системима, мења се сама морална логика вођења рата. Иако се људска улога може формално задржати, у пракси она често постаје симболична, јер оператери све више функционишу као потврђивачи одлука које генерише систем (Sparrow, 2007). Такав однос подстиче аутоматизациону пристрасност и истовремено слаби принцип индивидуалне и институционалне одговорности (Cummings, 2017).

Укључивање ВИ у вођење оружаних сукоба отвара бројна питања у погледу применљивости међународног хуманитарног права. Његови кључни принципи, као што су разликовање између војних и цивилних циљева и захтев пропорционалности у употреби силе, подразумевају сложене контекстуалне процене које је тешко у потпуности преточити у алгоритамске моделе (ICRC, 2021). Посебан правни изазов представља утврђивање одговорности за последице деловања аутономних система. У ситуацијама у којима дође до погрешне идентификације мете или несразмерне примене силе, остаје нејасно да ли правну одговорност треба да сносе програмери, произвођачи, војни команданти или државе које такве системе користе. Постојећи правни режими нису прилагођени технологијама са високим степеном самосталности, што доводи до појаве такозваног „јаза одговорности“ (Heyns, 2016). Овај проблем је додатно наглашен у транснационалним околностима, где се ВИ може развијати у једној држави, производити у другој, а примењивати у трећој, што додатно компликује примену и националних и међународних правних механизама.

Као одговор на наведене изазове, међународни актери настоје да успоставе механизме за управљање ризицима које употреба ВИ доноси у области безбедности. Један од кључних форума за ту расправу представља процес у оквиру Конвенције о одређеним конвенционалним оружјима (*Convention on Certain Conventional Weapons – CCW*), у чијем се оквиру кроз

рад експертских група анализирају питања аутономних оружаних система. Паралелно са напорима за формално правно уређење, све већи значај добијају и такозване „меке норме“, укључујући принципе, смернице и стандарде који промовишу одговорну примену вештачке интелигенције. У том контексту, посебно се истиче оквир за управљање ризицима који је развио амерички Национални институт за стандарде и технологију(National Institute of Standards and Technology – NIST), а који наглашава потребу за транспарентношћу, одговорношћу и континуираним људским надзором над системима заснованим на вештачкој интелигенцији (NIST, 2023). Иако овакви инструменти немају правно обавезујућу снагу, они представљају важан корак ка усклађивању пракси и јачању међусобног поверења међу актерима.

Први формални глобални став Уједињених нација (УН) о употреби ВИ у војне сврхе изражен је кроз резолуцију Генералне скупштине УН под називом „Вештачка интелигенција у војној области и њене импликације за међународни мир и безбедност“ (Artificial Intelligence in the Military Domain and Its Implications for International Peace and Security). Овај документ, фокусиран на безбедносне последице примене ВИ у војном домену, усвојен је на 79. заседању Првог комитета Генералне скупштине УН 24. децембра 2024. године и касније потврђен у пленарној седници Генералне скупштине. Он означава први пут да је Генерална скупштина формално адресирала питање ВИ у војном контексту у оквиру универзалног међународног форума. У време усвајања, већина чланица УН је подржала резолуцију, што одражава широку међународну подршку за наставак мултилатералног дијалога о овом питању. Резолуција наглашава да се међународно право, укључујући Повељу УН, међународно хуманитарно право и норме о људским правима, примењује на све фазе живота система заснованих на ВИ у војном домену, од развоја до употребе и повлачења из употребе. Она позива државе да наставе процене и размену искустава о могућностима и ризицима везаним за примену ВИ у војним операцијама, укључујући подстицање мултилатералне сарадње и дијалога у релевантним међународним форматима.

ЗАКЉУЧАК

Све интензивнија примена ВИ представљају један од најзначајнијих процеса преобликовања савременог безбедносног окружења. За разлику од претходних технолошких достигнућа, ВИ не функционише као појединачно средство или изоловани систем, већ као технологија која прожима готово све сегменте безбедности и одбране, од обавештајне обраде података и командних структура до употребе аутономних платформи. Управо та ширина примене чини ВИ истовре-

мено изузетно значајном и аналитички изузетно сложеном појавом.

У том контексту, вештачка интелигенција делује и као појачивач постојећих способности и као извор нових системских ризика. С једне стране, она омогућава бржу и прецизнију анализу информација, бољу ситуациону свест и ефикасније процесе доношења одлука, што може унапредити делотворност безбедносних структура. С друге стране, скраћивање временских оквира за одлучивање, ограничена транспарентност алгоритама и растући степен аутономије технолошких система повећавају вероватноћу грешака, погрешних процена и ненамерне ескалације. Посебно осетљива остаје интеграција ВИ у системе раног упозорења и командовања, где такве динамике могу нарушити постојеће моделе одвраћања и управљања кризама, нарочито у условима високог нивоа неповерења међу актерима. Истовремено, доступност ВИ ван оквира државних институција доприноси процесу распршивања моћи и додатно замагљује границе између рата и мира, као и између државних и недржавних облика претњи. То чини безбедносно окружење флуиднијим, мање предвидљивим и теже контролисивим традиционалним инструментима.

Анализа етичких, правних и нормативних аспеката показује да постојећи међународни механизми нису у потпуности прилагођени технологијама са високим степеном аутономије. Посебно су проблематична питања одговорности и обезбеђивања стварне људске контроле над системима чије одлуке могу имати директне последице по људске животе. Иако су покренути бројни међународни процеси и иницијативе, изостанак обавезујућих норми указује на дубоке разлике у стратешким и доктринарним интересима држава.

Све то указује да вештачка интелигенција представља структурни изазов савремене безбедности који не може бити адекватно адресиран искључиво кроз техничка решења или појединачне националне политике. Делотворно управљање њеним импликацијама захтева интегрисани приступ који укључује развој техничких стандарда, јачање институционалног надзора, унапређење међународне сарадње и изградњу нормативних оквира за одговорну употребу вештачке интелигенције. У супротном, постоји реална опасност да брзина технолошког напретка превазиђе способност друштава и држава да њиме управљају, са потенцијално озбиљним последицама по међународни мир и безбедност.

ЛИТЕРАТУРА

- Acton, J. M. (2019). Escalation through entanglement: How the vulnerability of command-and-control systems raises the risks of an inadvertent nuclear war. Carnegie Endowment for International Peace.
- Allen, G., & Chan, T. (2017). Artificial intelligence and national security. Belfer Center for Science and International Affairs, Harvard Kennedy School.
- Black, J., Lucas, R., Kennedy, J., Hughes, M., & Fine, H. (2024). Command and control in the future: Concept Paper 1 — Grappling with complexity (RR-A2476-1). RAND Corporation. https://doi.org/10.7249/RRA2476-1
- Bostrom, N. (2014). Superintelligence: Paths, dangers, strategies. Oxford University Press.
- Boulanin, V. (2020). Limits on autonomous weapons. Stockholm International Peace Research Institute.
- Boulanin, V., & Verbruggen, M. (2017). Mapping the development of autonomy in weapon systems. Stockholm International Peace Research Institute.
- Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Ó hÉigeartaigh, S., Beard, S., Belfield, H., Farquhar, S., & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Future of Humanity Institute, University of Oxford.
- Buchanan, B. (2020). The hacker and the state: Cyber attacks and the new normal of geopolitics. Harvard University Press.
- Vuletić, D., & Nojković, N. D. (2018). Realization of a TCP SYN flood attack using Kali Linux. Military Technical Courier, 66(3), 640–649. https://doi.org/10.5937/vojtehg66-17788
- Vuletić, D. (2012). Napadi na računarske sisteme. Vojnotehnički glasnik, 60(1), 235–249.
- Vuletić, D. (2018). Psihološka dimenzija hibridnog ratovanja. Vojno delo, 70(6), 274-281. https://doi.org/10.5937/vojdelo1806274V
- Cummings, M. L. (2017). Artificial intelligence and the future of warfare. Chatham House Research Paper.
- Heyns, C. (2016). Autonomous weapons systems: Living a dignified life and dying a dignified death. South African Journal on Human Rights, 32(2), 263–291.
- Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. Texas National Security Review, 1(3), 37–57.
- International Committee of the Red Cross. (2021). ICRC position on autonomous weapon systems. ICRC.
- Jensen, B. (2020). Information warfare and the future of strategic competition. Georgetown University Press.

- Johnson, J. (2019). Artificial intelligence and future warfare. Defense & Security Analysis, 35(2), 147–169.
- National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1). U.S. Department of Commerce.
- Parasuraman, R., & Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. Human Factors, 39(2), 230–253.
- Payne, K. (2021). Artificial intelligence: A revolution in strategic affairs? Survival, 63(2), 7–32.
- Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Farrar, Straus and Giroux.
- Russell, S., & Norvig, P. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson.
- Scharre, P. (2018). Army of none: Autonomous weapons and the future of war. W. W. Norton.
- Sparrow, R. (2007). Killer robots. Journal of Applied Philosophy, 24(1), 62–77.
- United Nations Institute for Disarmament Research. (2023). Artificial intelligence beyond weapons: Application and impact of AI in the military domain. UNIDIR.
- United Nations General Assembly – UNGA. (2024). Artificial intelligence in the military domain and its implications for international peace and security: Resolution A/RES/79/239 (A/RES/79/239). United Nations.
- United Nations Office for Disarmament Affairs. (2023). Report of the Group of Governmental Experts on Lethal Autonomous Weapons Systems. United Nations.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ВЫЗОВ СОВРЕМЕННОЙ БЕЗОПАСНОСТИ

Аннотация: Цель работы — анализ того, как искусственный интеллект (ИИ) трансформирует современную среду безопасности, с акцентом на изменения в природе угроз, последствия для современной безопасности, а также нормативные, правовые и этические вызовы управления рисками. Работа основана на качественном анализе содержания научной литературы, а также на анализе соответствующих документов и отчетов международных и национальных институтов. Результаты исследования показывают, что ИИ действует как мультипликатор возможностей в сферах аналитики разведданных, наблюдения и разведки, кибероперациий и поддержки принятия решений, одновременно создавая новые системные риски: увеличение скорости принятия решений и потенциал «сжатия времени» в кризисных ситуациях, проблемы предсказуемости поведения сложных моделей, а также риск нежелательной эскалации из-за ошибок, предвзятости или взаимодействия автономных систем. Искусственный интеллект представляет собой один из ключевых вызовов современной безопасности, поэтому необходимы интегрированные механизмы управления, от технических стандартов и оценки рисков до международных норм и правовых рамок.

Ключевые слова: искусственный интеллект, безопасность, управление рисками.

ARTIFICIAL INTELLIGENCE AS A CHALLENGE OF MODERN SECURITY

Abstract: The aim of this paper is to analyze how artificial intelligence (AI) is transforming the modern security environment, with a focus on changes in the nature of threats, implications for contemporary security, and the normative, legal, and ethical challenges of risk management. The study is based on a qualitative content analysis of scientific literature, as well as an analysis of relevant documents and reports from international and national institutions. Research findings indicate that AI acts as a capability multiplier in the domains of intelligence analysis, surveillance and reconnaissance, cyber operations, and decision support, while simultaneously generating new systemic risks: increased decision-making speed and the potential for "time compression" during crises, predictability issues of complex model behaviors, and the risk of unintended escalation due to errors, biases, or interactions of autonomous systems. Artificial intelligence represents one of the key challenges of modern security, and therefore integrated management mechanisms are necessary, ranging from technical standards and risk assessments to international norms and legal frameworks.

Keywords: artificial intelligence, security, risk management.