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

Оригиналан научни рад
UDK 004.738.5:316.775

ПРЕТЊЕ У САЈБЕР ПРОСТОРУ И ЊИХОВ УТИЦАЈ НА САВРЕМЕНУ БЕЗБЕДНОСТ

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 природе и еволуције претњи у сајбер простору и њихов утицај на савремено безбедносно окружење на националном и међународном нивоу. Полазећи од чињенице да је сајбер простор постао кључни домен друштвених, економских и војно-безбедносних активности, у раду се настоји да се идентификују главни облици сајбер претњи, као и механизми утицаја на стабилност држава и међународног система. Истраживање се заснива на квалитативној анализи садржаја научне литературе, као и анализи релевантних докумената и извештаја међународних и националних институција из области сајбер безбедности. Резултати истраживања показују да сајбер претње обухватају широк спектар активности које имају утицај на националну безбедност, суверенитет и међународну стабилност. Посебно се истичу изазови атрибуције, асиметрије моћи и „сивих зона“ сукобљавања, који отежавају ефикасно управљање ризицима. Закључно, рад указује на неопходност развоја интегрисаних приступа сајбер безбедности, који обједињују техничке, правне и институционалне мере у циљу јачања отпорности савремених безбедносних система.

Кључне речи: сајбер простор, претње, безбедност, критична инфраструктура.

УВОД

Сајбер простор је током последњих двадесетак година постао неизоставан оквир функционисања савремених друштава, јер у себи обједињује рад критичних информационих инфраструктура, комуникационих мрежа, економских активности и државних безбедносних система (Nye, 2011). Таква широка и дубока укљученост сајбер простора у друштвене процесе довела је до значајних промена у карактеру безбедносног окружења, у којем се класични облици претњи све чешће надопуњују и преплићу са новим, нетрадиционалним изазовима (Libicki, 2009; Rid, 2013). Услед тога, сајбер простор се више не може посматрати искључиво као технолошки домен, већ и као стратешки и политички простор у којем државни и недржавни актери артикулишу своје интересе, чиме се додатно усложњавају односи моћи у савременом међународном систему (Kello, 2017).

Предмет овог рада усмерен је на анализу сајбер претњи као посебног облика савремених безбедносних изазова, при чему се посебна пажња посвећује њиховим импликацијама по националну и међународну безбедност. Истраживање полази од становишта да се сајбер претње суштински разликују од традиционалних војних претњи, будући да их обележава изражена асиметричност односа актера, убрзана динамика развоја техника и облика напада, као и сложеност процеса приписивања одговорности за извршене активности. Управо ове карактеристике значајно отежавају правовремено откривање, ефикасну превенцију и успостављање механизама одвраћања у сајбер простору (Libicki, 2009; Rid, 2013). Додатно, растућа ослоњеност држава на информационо-комуникационе технологије условљава да последице сајбер инцидената имају све израженији системски карактер, са потенцијалом да угрозе функционисање критичне инфраструктуре и институција од посебног значаја, укључујући енергетски, финансијски, саобраћајни и одбрамбени сектор (Vuletić, 2018; ENISA, 2022; NATO, 2023).

Циљ овог рада усмерен је на идентификацију и анализу кључних облика сајбер претњи, као и на разматрање њихових безбедносних последица у савременом међународном окружењу. Посебна пажња посвећује се начину на који ове претње утичу на традиционалне и савремене концепте националне безбедности, државног суверенитета и међународне стабилности, као и изазовима које постављају постојећи механизми управљања ризицима у условима убрзаних технолошких промена и високе међузависности држава (Nye, 2011; UN GGE, 2021). У том смислу, у раду се покушава да се пронађе одговор на неколико кључних истраживачких питања, која се односе на идентификацију доминантних облика сајбер претњи у актуелном безбедносном контексту, анализу њиховог утицаја на националну и међународну безбедност, као и процену степена у којем постојећи нормативни и институционални оквири пружају адекватан одго-

вор на наведене изазове.

Са методолошког становишта, истраживање је засновано на квалитативној анализи садржаја релевантне научне литературе која се бави питањима безбедности у сајбер простору, као и на разматрању докумената и извештаја међународних и националних институција од значаја за ову област. Поред тога, примењен је компаративни приступ ради упоређивања различитих начина концептуализације сајбер претњи и модела њиховог управљања у оквиру различитих безбедносних и институционалних оквира (NIST, 2018; NATO, 2023). Комбиновањем наведених метода омогућено је целовитије сагледавање природе сајбер претњи и анализирање њихових последица по савремено безбедносно окружење.

Рад је структуриран у неколико међусобно повезаних целина. Након уводног дела, прво поглавље посвећено је анализи савремених облика претњи у сајбер простору, док се у наредном разматра њихов утицај на националну и међународну безбедност. Последње поглавље бави се нормативним, правним и институционалним одговорима на сајбер претње, након чега следи закључак са кључним налазима и препорукама за будућа истраживања.

САВРЕМЕНИ ОБЛИЦИ ПРЕТЊИ У САЈБЕР ПРОСТОРУ

Сајбер простор се може одредити као глобални домен који функционише у оквиру ширег информационог окружења и који обухвата међусобно повезане информационо-комуникационе технологије (ИКТ), заједно са садржајем који се у њима ствара, преноси и обрађује. Његову природу одликују висока сложеност и динамичност, ограничена предвидивост, као и изражена рањивост, при чему сајбер простор поседује и јасну физичку компоненту у виду материјалне инфраструктуре, као што су сервери и комуникациони уређаји. Иако омогућава ефикасну и брзу комуникацију, овај домен истовремено генерише бројне критичне слабости које могу бити предмет злоупотребе од стране различитих актера. Управо комбинација ниских трошкова приступа, лаке доступности ресурса, релативно скромних технолошких захтева и високог степена анонимности ствара услове у којима је могуће проузроковати значајну штету без поседовања упоредивих материјалних или војних капацитета (Vuletić & Đorđević, 2022).

Сајбер криминал спада међу најзаступљеније и најбрже растуће облике угрожавања у сајбер простору и обухвата различите врсте противправних активности усмерених ка злоупотреби информационих система и података. У овај корпус убрајају се, између осталог, неовлашћено прибављање података, финансијске злоупотребе, напади

са употребом изнуђивачког софтвера, као и различити облици злоупотребе дигиталног идентитета (Vuletić, 2012). У поређењу са класичним облицима криминала, сајбер криминал одликују изражена транснационална димензија, висок степен анонимности извршилаца и релативно ниски трошкови спровођења напада, што у значајној мери усложњава активности органа гоњења и функционисање механизама међународне правне сарадње (Anderson et al., 2019). Иако се у пракси често третира као питање унутрашње безбедности, последице сајбер криминала превазилазе тај оквир, будући да обимни напади на финансијски сектор, здравствене системе и институције јавне управе могу изазвати озбиљне поремећаје у друштвеном функционисању и подривање поверења грађана у државне институције, чиме он добија и изразиту димензију националне безбедности (ENISA, 2022).

Сајбер шпијунажа се у савременом безбедносном контексту издваја као један од значајних механизама пројекције државне моћи у сајбер простору. Путем различитих облика сајбер операција, државни актери настоје да прибаве информације од политичког, војног, економског и технолошког значаја, често кроз дуготрајне и технички сложене активности. У поређењу са традиционалним обавештајним деловањем, сајбер шпијунажа омогућава континуирано и обимно прикупљање података уз знатно снижени ниво ризика по актера који операције спроводи (Rid, 2013). Овај вид активности најчешће се одвија у простору такозване „сиве зоне“, између стања мира и оружаног сукоба, будући да се у постојећем међународноправном оквиру уобичајено не квалификује као оружани напад. Ипак, његови ефекти могу имати дугорочне и озбиљне последице, посебно у случајевима неовлашћеног приступа осетљивим војним технологијама или компромитовања рада кључних државних институција (Libicki, 2009; Kello, 2017).

Напади усмерени на критичну инфраструктуру спадају међу најозбиљније облике сајбер претњи, пре свега због њиховог потенцијала да произведу директне и индиректне последице по безбедност држава и свакодневно функционисање друштва. Под критичном инфраструктуром подразумевају се системи од суштинског значаја за нормално одвијање друштвених и економских активности, укључујући енергетски и финансијски сектор, саобраћај, здравство или системе водоснабдевања. Иако су процеси дигитализације и међусобног умрежавања допринели већој ефикасности ових система, они су истовремено довели до повећања њихове изложености различитим облицима сајбер напада (ENISA, 2022; NATO, 2023). Искуства из праксе, посебно у вези са нападима на индустријске контролне системе, указују на то да сајбер операције могу резултирати и опипљивим, физичким последицама, чиме се додатно замагљује граница између сајбер и конвенционалних облика сукобљавања. Управо ова способност трансформације дигиталних напада у реалне, материјалне ефекте чини угрожавање критичне инфраструктуре једним од централних

изазова савремене безбедности у сајбер простору (Kello, 2017).

Сајбер ратовање може се посматрати као посебан вид војно-безбедносног деловања који се реализује унутар сајбер простора и посредством њега, најчешће у спрези са другим инструментима државне моћи. Иако у научној литератури не постоји јединствено одређење овог појма, сагласност је присутна у оцени да сајбер операције све учесталије постају интегрални део ширих хибридних стратегија, усмерених ка остваривању политичких и стратешких циљева без преласка прага отвореног оружаног сукоба (Rid, 2013; NATO, 2023). У том оквиру, хибридне претње у сајбер простору обједињују различите облике деловања, укључујући сајбер нападе, активности у домену информационог утицаја, економске притиске и политичке механизме утицаја. Заједничка одлика ових активности јесте њихов постепен и прикривен карактер, који значајно отежава правовремену реакцију и јасно приписивање одговорности за спроведене операције (Kello, 2017).

Напредак у области вештачке интелигенције значајно мења природу и динамику сајбер претњи, доприносећи повећању њихове сложености, интензитета и оперативне ефикасности. Примена алгоритама машинског учења омогућава висок степен аутоматизације напада, напредније идентификовање и експлоатацију рањивости, као и адаптивно понашање које отежава откривање од стране постојећих система заштите. Истовремено, исти технолошки капацитети све више се интегришу у одбрамбене механизме, што условљава сталну технолошку ескалацију и динамику надметања између актера у сајбер простору (Brundage et al., 2018; Buchanan, 2020). Са безбедносног становишта, оваква примена вештачке интелигенције отвара низ нових питања која се односе на контролу ескалације, поузданост аутоматизованих процеса и управљање ризицима у условима убрзаних и временски компримованих процеса доношења одлука. Наведене околности указују на то да се сајбер претње више не могу посматрати искључиво кроз техничку призму, већ као структурни елемент савремених безбедносних студија и стратегијског промишљања (Kello, 2017; UN GGE, 2021).

УТИЦАЈ САЈБЕР ПРЕТЊИ НА САВРЕМЕНУ БЕЗБЕДНОСТ

Сајбер претње све израженије утичу на националну безбедност држава, јер непосредно погађају виталне функције државне власти, економске системе и друштвено функционисање. Растућа ослоњеност савремених држава на ИКТ додатно појачава њихову изложеност сајбер нападима који могу озбиљно нарушити рад јавне управе, одбрамбених структура, финансијског сектора и других сегмената критичне инфраструктуре. У таквом контексту, сајбер простор се све чешће препознаје као домен у

којем се директно преиспитују основни елементи државног суверенитета, као и способност државе да обезбеди континуитет кључних функција управљања и заштите грађана (Nye, 2011; ENISA, 2022; Vuletić & Stanojević, 2022).

За разлику од традиционалних безбедносних претњи, сајбер претње омогућавају актерима да спроводе активности које се одвијају испод прага отвореног оружаног сукоба, при чему анонимност и асиметричност представљају њихове кључне оперативне предности. Овакво деловање доводи државе у ситуацију у којој могу бити изложене значајним безбедносним притисцима, без постојања јасних правних и политичких основа за примену класичних механизама одбране и одвраћања (Libicki, 2009; Kello, 2017). На међународном плану, последице оваквих активности огледају се у порасту нестабилности и непредвидивости безбедносног окружења. Одсуство јасно утврђених међународних норми понашања у сајбер простору, у комбинацији са сложеним процесима атрибуције напада, повећава ризик од погрешних процена и нежељене ескалације у односима међу државама (UN GGE, 2021). Поред тога, сајбер операције се све чешће користе као средство политичког притиска, што додатно подрива међусобно поверење и стабилност међународног система.

Сајбер простор омогућава готово тренутно „ширење“ безбедносних претњи преко националних граница, чиме се традиционални концепти територијалне заштите доводе у питање. Ефекти сајбер напада често се испољавају далеко од места њиховог настанка, што додатно наглашава значај међународне сарадње и координисаног приступа у области сајбер безбедности (NATO, 2023). Један од кључних структурних проблема у овом домену односи се на питање атрибуције, односно на могућност поузданог утврђивања одговорности за спроведене сајбер активности. Комбинација техничких ограничења и политичких фактора у процесу идентификације извршилаца омогућава појединим актерима да негирају умешаност и делују у оквирима такозваних „сивих зона“ међународних односа (Rid, 2013). Овакве околности значајно умањују ефикасност механизама одвраћања и санкционисања, који представљају темељ традиционалних безбедносних архитектура. Додатно, ризици нежељене ескалације појачани су високом брзином сајбер операција и њиховом потенцијалном интеракцијом са конвенционалним војним капацитетима, будући да у кризним ситуацијама сајбер напади могу бити погрешно протумачени и представљати увод у оружани сукоб (Kello, 2017).

Државни и недржавни актери све учесталије прибегавају сајбер операцијама као средству за остваривање стратешких циљева, при чему се настоји да се избегне ризик од директне војне конфронтације. Такав облик деловања доприноси постепеном слабљењу постојећих безбедносних норми и додатно усложњава структуру савременог безбедносног окружења (Kello, 2017; NATO, 2023). У наведеном контексту, сајбер простор

се све више профилише као арена у којој се преиспитују домети међународног права, концепти одвраћања и механизми колективне безбедности. Одсуство јасно дефинисаних правила понашања и ефикасних механизама за управљање конфликтима у сајбер простору представља један од кључних изазова за очување стабилности међународног система у будућности (UN GGE, 2021).

НОРМАТИВНИ, ПРАВНИ И ИНСТИТУЦИОНАЛНИ ОДГОВОРИ НА САЈБЕР ПРЕТЊЕ

Интензивирање и све већа сложеност сајбер претњи подстакли су настојања међународне заједнице да се у сајбер простору успоставе заједничка правила, норме и принципи понашања. Посебно место у том процесу заузимају активности у оквиру Уједињених нација, које су усмерене на препознавање ризика повезаних са употребом информационо-комуникационих технологија, формулисање добровољних норми одговорног понашања држава, као и развој мера за изградњу поверења и унапређење међународне сарадње (UN GGE, 2021). Иако ове норме немају правно обавезујући карактер, оне играју значајну улогу у обликовању очекиваних образаца понашања држава, смањењу могућности неспоразума и успостављању минималног оквира за управљање кризама и деескалацију у сајбер простору.

Успостављање механизама за изградњу поверења и унапређење комуникације, укључујући системе „тачака контакта“, такозване „вруће линије“, протоколе за кризну комуникацију и размену информација о сајбер инцидентима, има посебан значај у условима отежане атрибуције и повећаног ризика од погрешних процена у сајбер простору (UN GGE, 2021). Овакви механизми доприносе постепеној институционализацији такозване сајбер дипломатије, у оквиру које се сајбер безбедносни ризици сагледавају као питање међународне стабилности и поверења, а не искључиво као проблем техничке заштите информационих система.

Поред развоја добровољних норми понашања, једно од кључних питања у сајбер домену односи се на применљивост постојећег међународног права. У том контексту, у теорији и пракси воде се расправе о томе у којој мери поједине сајбер активности могу бити квалификоване као повреда државног суверенитета, незаконито мешање у унутрашње послове, употреба силе или чак оружани напад, као и о дометима стандарда државне одговорности и обавезе дужне пажње (Schmitt, 2017). Управо услед различитих тумачења ових правних категорија, сајбер простор се и даље карактерише постојањем нормативних недоречености и високим степеном политичке и правне контроверзности.

У том контексту, „Талински приручник 2.0 о међународном праву примењивом на сајбер операције“ (*Tallinn Manual 2.0 on the International*

Law Applicable to Cyber Operations) представља један од најзначајнијих референтних оквира за правну анализу сајбер операција, будући да на систематичан начин обједињује ставове међународних експерата о примени постојећих правила међународног права у сајбер домену. Посебна вредност овог приручника огледа се у чињеници да се анализа не ограничава искључиво на ситуације оружаног сукоба, већ обухвата и мирнодопске правне режиме, укључујући питања суверенитета, људских права и државне одговорности (Schmitt, 2017). Ипак, неопходно је нагласити да поменути приручник нема формално обавезујући карактер, већ функционише као експертски оријентир који има значајан утицај на правну праксу, стручне расправе и академску дебату.

У области сузбијања сајбер криминала, централни међународни инструмент представља „Конвенција о сајбер криминалу“ (тзв. „Будимпештанска конвенција“), усвојена у оквиру Савета Европе. Овај документ успоставља заједничке стандарде у погледу инкриминације кривичних дела у сајбер простору, процесних овлашћења надлежних органа и механизама међународне сарадње у истрагама и кривичном гоњењу (Council of Europe, 2001). Њен значај огледа се у доприносу усклађивању националних законодавстава и олакшавању прекограничне сарадње, што је од посебне важности у окружењу у којем сајбер напади по правилу превазилазе оквире једне државне јурисдикције.

На регионалном нивоу, Европска унија (ЕУ) настоји да унапреди заједнички степен сајбер отпорности кроз регулаторни приступ који повезује управљање ризицима и обавезе извештавања о инцидентима. У том оквиру, такозвана „NIS2 директива“, успоставља свеобухватан сет мера усмерених ка постизању високог и уједначеног нивоа сајбер безбедности унутар ЕУ, обухватајући обавезе које се односе на „кључне“ и „важне“ субјекте, као и захтеве у погледу превентивног управљања ризиком и пријављивања значајних сајбер инцидената (European Union, 2022). Овакво регулаторно решење одражава ширу тенденцију да се сајбер безбедност концептуализује као питање системске отпорности и континуитета критичних услуга, а не искључиво као техничко питање заштите мрежа и информационих система.

Поред правних и нормативних оквира, институционални одговори на сајбер претње добијају све већи значај кроз развој националних стратегија, успостављање специјализованих капацитета као што су тимови за реаговање на рачунарске инциденте, сајбер команде и центри за отпорност, али и кроз јачање механизама координације између јавног и приватног сектора. У војно-политичком контексту НАТО алијансе (North Atlantic Treaty Organization) наглашава се да сајбер одбрана представља саставни део основних задатака одвраћања и колективне одбране, при чему је сајбер простор формално признат као домен операција. Овакво опредељење има директне импликације на процесе планирања, извођење заједничких вежби, размену информација и унапређење укупне колекти-

вне отпорности савезника (NATO, 2024).

Управљање ризицима у сајбер простору све се више заснива на примени стандардизованих оквира који омогућавају систематску процену претњи, њихову приоритизацију и континуирано унапређење мера заштите. У том контексту, оквир за сајбер безбедност који је развио амерички Национални институт за стандарде и технологију(National Institute of Standards and Technology) представља један од најшире прихваћених модела управљања ризиком, будући да интегрише проверене најбоље праксе и пружа организацијама структуриран приступ усклађивању активности спречавања, откривања, реаговања и опоравка од сајбер инцидената (NIST, 2018). Истовремено, повезивање нормативних, правних и организационих мера указује на то да ефикасан одговор на сајбер претње захтева интегрисан приступ, у којем се технички стандарди и процене ризика надовезују на правне инструменте, институционалне капацитете и механизме међународне сарадње (European Union, 2022; UN GGE, 2021).

ЗАКЉУЧАК

Сајбер простор је у савременом безбедносном окружењу еволуирао из претежно технолошког окружења у стратешки домен у којем се преламају интереси држава, недржавних актера и приватног сектора. Продубљивање дигитализације и међузависности критичних система условило је да сајбер претње поприме системски карактер, при чему њихове последице све чешће превазилазе оквир ИКТ и непосредно погађају функционисање институција, економске токове и друштвену стабилност. У том смислу, сајбер безбедност се више не може посматрати као изоловано техничко питање, већ као интегрални део националне и међународне безбедности, са директним импликацијама по суверенитет, одвраћање и управљање кризама.

Анализа савремених облика сајбер претњи показује да се спектар угрожавања креће од финансијски мотивисаних криминалних активности и сајбер шпијунаже, до напада на критичну инфраструктуру и елемената сајбер ратовања. Посебну тежину имају активности усмерене на индустријске контролне системе и виталне услуге, будући да оне могу произвести и физичке последице, чиме се додатно замагљује граница између сајбер и конвенционалних облика угрожавања. Истовремено, убрзани развој вештачке интелигенције додатно трансформише природу сајбер претњи, повећавајући њихову брзину, прилагодљивост и обим, што намеће потребу за сталним прилагођавањем механизама одбране.

На међународном нивоу, сајбер претње доприносе расту нестабилности и непредвидивости безбедносног окружења. Деловање

испод прага оружаног сукоба, отежана атрибуција и различита тумачења примене међународног права повећавају ризик од погрешних процена и нежељене ескалације, посебно у кризним ситуацијама. Због тога се сајбер простор све чешће користи као средство политичког притиска и пројекције моћи, што додатно оптерећује механизме међународне стабилности и поверења.

Нормативни, правни и институционални одговори на ове изазове развијају се кроз више међусобно повезаних нивоа. Развој норми одговорног понашања држава, експертска тумачења примене међународног права и јачање кривичноправних и регулаторних механизама указују на постепену институционализацију сајбер безбедности као трајног питања међународне безбедносне агенде. Истовремено, растући значај управљања ризицима и сајбер отпорности потврђује да ефикасан одговор није могућ без интеграције техничких стандарда, правних инструмената и институционалних капацитета.

На основу спроведене анализе може се закључити да успешно супротстављање сајбер претњама захтева интегрисан, континуиран и прилагодљив приступ, који обједињује националне политике, међународну сарадњу и партнерство јавног и приватног сектора. У условима убрзаних технолошких промена и деловања у „сивим зонама“, посебан значај имају мере изградње поверења, транспарентности и кризне комуникације, као предуслови за смањење ризика ескалације и очување стабилности савременог међународног система (UN GGE, 2021; NATO, 2023).

ЛИТЕРАТУРА

- Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2019). Measuring the cost of cybercrime. In R. Anderson (Ed.), Security engineering (3rd ed.). Wiley.
- 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. (2012). Napadi na računarske sisteme. Vojnotehnički glasnik, 60(1), 235–249.
- Vuletić, D. (2018). Psihološka dimenzija hibridnog ratovanja. Vojno delo, 70(6), 274–281.
- Vuletić, D., & Đorđević, B. D. (2022). Rivalry between the United States of America and Russia in cyberspace. Međunarodni problemi, 74(1), 51–73.

- Vuletić, D., & Stanojević, P. (2022). Concepts of information warfare (operations) of the United States of America, China and Russia. The Review of International Affairs, 73(1185), 51–71.
- Council of Europe. (2001). Convention on Cybercrime (ETS No. 185). Council of Europe.
- European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333.
- ENISA. (2022). ENISA threat landscape 2022. European Union Agency for Cybersecurity.
- Kello, L. (2017). The virtual weapon and international order. Yale University Press.
- Libicki, M. C. (2009). Cyberdeterrence and cyberwar. RAND Corporation.
- NATO. (2023). NATO 2022 Strategic Concept. North Atlantic Treaty Organization.
- NATO. (2024). Cyber defence policy and implementation. North Atlantic Treaty Organization.
- NIST. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). National Institute of Standards and Technology.
- Nye, J. S. (2011). The future of power. PublicAffairs.
- Rid, T. (2013). Cyber war will not take place. Oxford University Press.
- Schmitt, M. N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.
- United Nations Group of Governmental Experts – UN GGE. (2021). Final report of the Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security. United Nations.

УГРОЗЫ В КИБЕРПРОСТРАНСТВЕ И ИХ ВЛИЯНИЕ НА СОВРЕМЕННУЮ БЕЗОПАСНОСТЬ

Резюме: Цель работы — анализировать природу и эволюцию угроз в киберпространстве и их влияние на современную среду безопасности на национальном и международном уровнях. Исходя из того, что киберпространство стало ключевой областью общественной, экономической и военно-безопасной деятельности, работа направлена на идентификацию основных форм киберугроз, а также механизмов их влияния на стабильность государств и международной системы. Исследование основано на качественном анализе содержания научной литературы, а также на анализе соответствующих документов и отчетов международных и национальных институтов в области кибербезопасности. Результаты исследования показывают, что киберугрозы охватывают широкий спектр действий, оказывающих влияние на национальную безопасность, суверенитет и международную стабильность. Особое внимание уделяется вызовам атрибуции, асимметрии власти и «серых зон» конфликтов, которые затрудняют эффективное управление рисками. В заключение, работа подчеркивает необходимость развития интегрированных подходов к кибербезопасности, объединяющих технические, правовые и институциональные меры с целью повышения устойчивости современных систем безопасности.

Ключевые слова: киберпространство, угрозы, безопасность, критическая инфраструктура.

CYBERSPACE THREATS AND THEIR IMPACT ON MODERN SECURITY

Abstract: The aim of this paper is to analyze the nature and evolution of threats in cyberspace and their impact on the modern security environment at both national and international levels. Considering that cyberspace has become a key domain for social, economic, and military-security activities, the paper seeks to identify the main forms of cyber threats and the mechanisms through which they affect the stability of states and the international system. The research is based on a qualitative content analysis of scientific literature, as well as an analysis of relevant documents and reports from international and national cybersecurity institutions. The findings indicate that cyber threats encompass a wide range of activities impacting national security, sovereignty, and international stability. Particular emphasis is placed on the challenges of attribution, power asymmetry, and “gray-zone” conflicts, which hinder effective risk management. In conclusion, the paper highlights the need to develop integrated cybersecurity approaches that combine technical, legal, and institutional measures to enhance the resilience of modern security systems.

Keywords: cyberspace, threats, security, critical infrastructure.