DOI:**10.33099/2311-7249/2019-36-3-53-58**

УДК 004:316.6

***Руслан Валентинович Грищук*** *(доктор технічних наук, професор)*
***Руслан Михайлович Жовноватюк*** *(кандидат технічних наук, с.н.с.)*
***Ганна Дмитрівна Носова***

***Житомирський військовий інститут імені С. П. Корольова, Житомир, Україна***

# ГІБРИДНІ ЗАГРОЗИ У КІБЕРПРОСТОРІ: ФАКТОРИ ВПЛИВУ НА ПРИРОДУ ВИНИКНЕННЯ

*Гібридна агресія Російської Федерації проти України поставила перед всією світовою спільнотою нові виклики воєнній безпеці не тільки окремих держав, а й колективній безпеці міждержавних інституцій. Загрози, породжені новими викликами, набули ознак гібридності, а прикмети найбільш небезпечних з них все частіше почали проявлятися у кіберпросторі, який на сьогодні, де-факто, став новим театром воєнних дій. На відміну від "класичних" кіберзагроз, гібридні загрози у кіберпросторі націлені одночасно на усі його рівні – не тільки на логічний та технічний (допоміжні рівні), а й, в першу чергу, на соціальний (основний рівень). Зважаючи на недостатню опрацьованість зазначеної проблеми, її актуальність, новизну та важливість для практики забезпечення кібербезпеки держави у воєнній сфері у статті всебічно досліджено даний новий феномен. Зокрема проаналізовані історичні, правові, політичні, економічні, технологічні, інформаційні та соціальні фактори впливу на природу виникнення гібридних загроз у кіберпросторі, а також приведено результати аналізу передумов їх виникнення. Обґрунтовано та доведено, що досліджувані загрози повинні розглядатися через призму еволюційних процесів трансформації сучасного високотехнологічного суспільства. У результаті проведеного дослідження показано, що негативні прояви ознак гібридних загроз у кіберпросторі мають прямий та опосередкований вплив на усі без винятку сфери функціонування держави – від воєнної до інформаційної. Хаос, невизначеність і нестабільність в суспільстві та державі є наслідками прояву гібридних загроз у кіберпросторі. Це в свою чергу вимагає від системи забезпечення воєнної безпеки держави вироблення адекватних, своєчасних та упереджувальних активних заходів протидії таким загрозам.*

***Ключові слова:*** *кібернетичний простір; гібридна загроза; неконвенційні бойові дії.*

## Вступ

**Постановка проблеми.** Гібридні загрози не є новим безпековим явищем. Наприклад, з часів "Холодної війни" спецслужби протиборчих держав використовували пропаганду та дезінформацію як інструмент асиметричної війни для досягнення власних військово-політичних цілей. Проте саме завдяки стрімкому розвитку технологій та цифровизації всіх сфер функціонування суспільства і держави, особливо воєнної сфери, гібридні загрози набули нового обрису та масштабу [1] й почали проявлятися у нових, до сьогодні нетипових для воєнної безпеки держави, середовищах. Таким середовищем на сьогодні є кіберпростір, який, де-факто, став новим театром воєнних дій [2].

**Аналіз останніх досліджень і публікацій** показав, що гібридні загрози досить ґрунтовно та всебічно вивчалися й досліджувалися провідними науковцями та міжнародними і національними безпековими організаціями, хоча і безвідносно до приналежності до кіберпростору.

Так, за концепцією НАТО від 2010 р., [3] гібридна загроза визначається як продемонстрована противником здатність до одночасного застосування традиційних і нетрадиційних засобів адаптивно до поставлених завдань. За результатами спільних досліджень та проведених навчань із залученням сил НАТО, США та провідних вищих військових навчальних закладів США у 2011 р. було підготовлено звіт, де визначено чинники гібридних загроз як всеохоплюючі за строком, такі, що складаються з великої кількості варіацій шкідливого впливу (акцій) відносно безпеки держави, зокрема тероризм, міграція, піратство, корупція, етнічні конфлікти тощо. У [3] гібридну загрозу визначено як різноманітні та динамічні (мінливі) застосування регулярних і нерегулярних військ та/або кримінальних елементів, об'єднаних разом з метою досягнення взаємокорисного ефекту. Автори в [4] додають до попереднього визначення наступне: застосування, які можуть бути запроваджені у будь-яких типах та різноманітних формах війни одночасно.

Позицію Європейського союзу у питаннях термінології в галузі гібридних загроз було оприлюднене у липні 2017 р. віце-президентом Європейської комісії з питань безпеки. За цим визначенням гібридна загроза – це дипломатичні, військові, економічні та технологічні методи, які держава-агресор спрямовує на те, щоб використати вразливість цілі та створити невизначеність з метою перешкоджання процесу прийняття рішення; охоплює традиційні і нетрадиційні методи атаки, які можуть бути використані як державою, так і недержавними гравцями [5].

Таким чином, у результаті аналізу вказаних вище та інших відкритих джерел встановлено, що на сьогодні є усталена термінологія до тлумачення такої категорії як гібридна загроза. Визначено, що спільною рисою, яка притаманна багатьом визначенням гібридної загрози, є необмеженість її у часі, просторі та формах прояву. При цьому,

якщо часові ознаки та форми прояву гібридної загрози на сьогодні вже достатньо глибоко досліджені, то просторові прояви, зокрема в кіберпросторі, залишилися поза увагою більшості фахівців.

**Метою статті** є всебічне дослідження нового феномену – гібридної загрози в кіберпросторі для встановлення факторів впливу на природу її зародження, що у подальшому стане науковим підґрунтям для вироблення системою забезпечення воєнної безпеки держави адекватних, своєчасних та упереджувальних активних заходів протидії таким загрозам.

## Виклад основного матеріалу дослідження

Передумови виникнення гібридних загроз у кіберпросторі слід розглядати через призму еволюційних процесів трансформації суспільства. Якісний стрибок, спровокований виникненням Інтернету, стрімким розвитком цифрових технологій та відповідного комунікаційного устаткування, перетворив постіндустріальне суспільство на інформаційне, а нові високотехнологічні доробки, у свою чергу, започаткували сучасне високотехнологічне суспільство [6]. У новій, цифровій, ері світ "зменшився" до розмірів кіберпростору, проте став більш вразливим до загроз, зокрема гібридних, всередині цього простору. Тому провідним гравцям, які є регуляторами кіберпростору, все легше стає задовольнити власні геополітичні, фінансові, ресурсні, владні та інші амбіції приховано через кіберпростір.

У загальному фактори виникнення гібридних загроз у кіберпросторі можна виокремити, виходячи з самого поняття кіберпростору та ступеня залучення до нього держави та її громадян [7]. До них відносять і наявність необхідних потужностей для їх реалізації (технологічних, програмних, економічних, інтелектуальних тощо), і екстериторіальність (транскордонність) кіберпростору, доступність Інтернету, відсутність правового регулювання, чітких принципів співіснування та його мирного використання, і геополітичні процеси у світі, і розуміння та сприйняття кіберпростору як середовища для поширення зброї нового типу – кіберзброї [8], яка не заборонена жодними міжнародними конвенціями. Аналіз досвіду підготовки та ведення агресії Російської Федерації (РФ) проти України показав, що в умовах ведення неконвенційних бойових дій [9–14], факторами впливу на природу виникнення цього типу загроз стають історичні, правові, політичні, економічні, інформаційні, технологічні та соціальні процеси у суспільстві.

До *історичних факторів* впливу на природу виникнення гібридних загроз у кіберпросторі пропонується віднести:

маніпулювання історичними подіями (фактами) в інтересах держави-агресора з метою утвердження "права" на агресивні дії зокрема у кіберпросторі;

історична інтегрованість інформаційного простору між державою-агресором та державою, проти якої здійснюється агресія;

маніпулятивне протиставлення історичних зв'язків у світовому просторі, пошук "прямих аналогій" у світовій історії для дискредитації противника на світовому рівні;

пошук псевдодоказового історичного підґрунтя як "дозвільної грамоти" на агресивні дії. На прикладі агресії РФ проти України ця теза реалізована у постійному нагадуванні про нібито еквівалентні дії західних країн, зокрема одностороннє проголошення незалежності Косово в 90-х роках та вторгнення до Іраку у 2003 році;

перебільшення військових успіхів через екскурс в історію;

розбурхування масового руху за історичну справедливість (етнічних, національних, мовних, релігійних та інших меншин); [15].

вибіркове і тенденційне ставлення до історичних фактів, яке допомагає маніпуляторам видавати агресора за жертву чи миротворця.

Поява понять "гібридна загроза" та "гібридна війна" поставила перед фахівцями у галузі правових відносин низку питань щодо визначення місця цих понять у міжнародному праві [16] та внутрішньодержавної регуляторної і нормативно-правової діяльності [17]. Нажаль, більшість цих питань і досі залишається невирішеною [18]. Отже, вплив правових факторів на причини появи гібридних загроз у кіберпросторі важко переоцінити. До таких пропонуємо віднести:

застаріле право збройних конфліктів [19]; відсутність у сучасному міжнародному праві поняття "гібридна війна" як наслідок – безкарність;

зловживання законом як засобом ведення війни шляхом пошуку прогалин у нормативно-правовій базі та відсутності чіткого трактування понять;

спроби нівелювання міжнародних договорів та домовленостей як недійсних та взагалі неіснуючих для сторони-агресора;

відсутність законодавчого уніфікованого визначення поняття "кібернетичні загрози" як на національному, так і на міждержавному рівні;

відсутність налагодженої і законодавчо закріпленої взаємодії між компетентними державними органами, які є суб'єктами кібербезпеки, і здійснення координації з такої діяльності;

відсутність правового механізму регулювання права доступу правоохоронних та інших державних органів щодо можливості перехоплення інформації (прослуховування телефонних переговорів, перлюстрацію електронних повідомлень) без дозволу суду;

слабкі глобальні зв'язки у сфері правового регулювання кібербезпеки, недостатній рівень міжнародного співробітництва;

низький рівень підтримки ініціатив НАТО щодо врегулювання на міжнародному рівні можливості визнання кібератаки "актом війни" [20].

Окрім того, для України актуальною проблемою залишається відсутність належного нормативно-правового забезпечення для процедур захисту діючих та створюваних в системі державного управління та зокрема у системі управління Збройними Силами України баз даних [21].

Зміна геополітичних конфігурацій, перерозподіл сфер впливу, політична та стратегічна невизначеність призводять до

постійного політичного, економічного, інформаційного тиску, що створює зону підвищеного ризику для новітніх гібридних загроз. Відтак *політичними факторами* пропонуємо вважати:

замовчування, небажання помічати диктаторські режими "заради загального миру"; надмірна лібералізація політики країн ЄС;

небажання розпізнати масштаб реальних загроз;

недалекоглядність політичних еліт провідних держав у сподіваннях на демократичну трансформацію еліти країни-агресора з ознаками диктаторського режиму;

окупація частини території сусідньої держави як засіб блокування інтеграції сусідніх держав у західний політичний та безпековий простір;

неефективність державного гарантування безпеки суспільства, низька довіра населення країни до політичних інституцій держави.

Поява на ринку великої кількості вітчизняних та зарубіжних комерційних структур, виробників інформації, засобів інформатизації та захисту інформації, включення інформаційної продукції в систему товарних відносин; розширення кооперації із зарубіжними країнами в розвитку інформаційної інфраструктури, стан вітчизняних галузей промисловості, яка виробляє засоби інформатизації та захисту інформації призводять до розширення спектру вразливостей для вдалої реалізації гібридних загроз.

До *економічних факторів* впливу на причини появи гібридних загроз у кіберпросторі відносимо:

низька конкурентоспроможність вітчизняної продукції, як програмної, так і апаратної (або її відсутність) – присутність, зокрема у державному сегменті, переважної більшості продукції іноземного виробництва ставить під загрозу безпеку цього сегмента [22];

збереження присутності бізнесу держави-агресора на територіях і у економічному просторі держави-жертви агресії;

економічна нестабільність всередині країни-жертви: значне економічне розшарування населення, присутність усіх відомих економічних проблем у суспільстві (безробіття, низький рівень життя тощо); низькі темпи економічного зростання;

контроль над важливими економічними активами з боку агресора, що робить можливим фізичне впровадження шкідливого програмного забезпечення на об'єктах критичної інфраструктури для подальших кібератак [23];

зовнішній економічний вплив на діяльність крупних підприємств;

залежність економіки від постачання ресурсів країною-агресором; взаємна залежність від торгових партнерів;

низький загальний рівень урядових витрат у кіберсекторі [24].

Комерційний фундамент сучасних комунікаційних технологій, залежність їх розвитку та ступеню доступності від загального стану економіки – характерні риси кібернетичного простору в цілому та його технологічних складових зокрема. Враховуючи цей взаємозв'язок та на основі аналізу попередньої групи факторів до *технологічних факторів* впливу на причини появи гібридних загроз у кіберпросторі можна віднести наступні:

зростання обсягів інформації, що зберігається на електронних інформаційних ресурсах;

уніфікація обладнання та комплектуючих; прив'язаність до ресурсної виробничої бази інших країн [25];

вразливість мікропроцесорних платформ, зумовлена зосередженістю їх виробництва в розвинених країнах; відсутність власної мікропроцесорної бази; монополізація технологічно розвиненими країнами виробництва мікропроцесорів як елемент економічного, технологічного та силового (воєнного) тиску на інші країни;

вразливість додатків, що вирішують критичні з точки зору безпеки, задачі, таких як віддалений та термінальний доступ, системи керування (наприклад, підприємством), доступні з інтернету або внутрішньої мережі елементи систем управління (наприклад, виробничим процесом) [26] технічні можливості переховування справжніх виконавців злочинів у кіберпросторі;

використання неліцензійного програмного забезпечення іноземного виробництва (виробництва підприємств країни-агресора);

технологічні труднощі у вирізненні кібервпливу від технологічного збою [27];

низький рівень захищеності систем державних баз даних та дата-центрів для обробки і резервування відомостей електронних інформаційних ресурсів;

відсутність комплексного підходу до захисту (програмна частина + апаратна частина + інформаційна частина);

невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам [28];

технологічна неготовність до попередження та відбиття гібридних загроз;

відсутність прогнозних моделей гібридних загроз;

недостатня кількість і якісний склад засобів забезпечення кібербезпеки зокрема на об'єктах критичної інфраструктури.

Провідні держави здійснюють глобальний моніторинг світових політичних, економічних, воєнних, екологічних та інших процесів, розповсюджують інформацію з метою здобуття односторонніх переваг, прагнуть досягнути монополії на інформаційні ресурси. Прикладом цього є події, що розпочались у 2014 році в Україні. Російські засоби масової інформації реалізовували заздалегідь підготовлені програми інформаційно-психологічного тиску на населення України на територіях Автономної Республіки Крим та у південно-східних регіонах. Своєрідна інтервенція Росії в інформаційний простір України стала найбільш небезпечною гібридною загрозою сьогодення, а *інформаційні фактори* – впливовим чинником появи гібридних загроз у кіберпросторі. До них відносимо:

контроль держави-агресора над медіаресурсом;

применшення у інформаційному просторі значення та можливостей кіберпростору у розповсюдженні гібридних загроз;

розповсюдження хибної інформації щодо стану захищеності об'єктів критичної інфраструктури;

використання медіаресурсу для формування суспільної свідомості позитивного сприйняття гібридних загроз (формування "стокгольмського синдрому");

створення псевдоісторичної продукції із подальшим її розповсюдженням у кіберпросторі;

низький рівень поінформованості споживача (користувача, суб'єкта кіберпростору) про можливі загрози та заходи захисту від них;

використання інформаційно-пропагандистських інструментів задля розпалювання внутрішніх конфліктів;

використання кіберпростору для інтегрування пропагандистських медіа у медіапростір інших регіонів (приклад: інформаційна агенція Sputnik (РФ) поширює інформацію більш ніж 30-ма мовами у десятках країн ЄС, досягнувши рівня місцевого ньюз-мейкера) [29];

формування у кіберпросторі на міжнародному рівні негативного іміджу держави-жертви агресії, наприклад, через створення хибної уяви про криміногенну обстановку в цій країні;

застосування кібернетичних впливі (атак) на окремі політичні фігури держави з метою керування суспільною думкою щодо держави-жертви шляхом розповсюдження "прямої мови" впливових представників, експертів і т. ін., наприклад, злам персональних сторінок з подальшою підміною контенту тощо;

дискредитаційна кампанія через зарубіжні ЗМІ у бізнес-сфері;

комбіновані дії з метою нарощування протестного потенціалу всередині країни-жертви агресії;

недосконала інформаційна політика уряду;

використання технічних можливостей кіберпростору для маніпулювання інформацією з боку противника, зміна її за форматом представлення [30];

активне впровадження цифрових технологій як інструмент створення залежності суспільства від інформації;

низький рівень інформування про успішні атаки противника у кіберпросторі з метою набуття "нетравматичного" досвіду боротьби з ними.

Останні два пункти витікають з цілої низки суспільно-політичних та соціальних явищ у світі, тож окремий розгляд групи *соціальних факторів* впливу на природу виникнення гібридних загроз є цілком доцільним. До цієї групи відносимо:

рівень стійкості суспільства до маніпулювання, навіювання;

рівень обізнаності щодо можливих загроз у кіберпросторі та методів і підходів протидії чи захисту від них;

вплив підконтрольної агресору релігійної складової на адекватне сприйняття будь-яких суспільно-політичних чи інших явищ у країнах-сторонах конфлікту;

рівень культури та знань серед держслужбовців щодо забезпечення безпеки своєї робочої та приватної переписки у кіберпросторі та комунікацій через електронні засоби;

хибне уявлення про склад суспільства як з одного, так і з іншого боку протистояння;

активний розвиток кібертероризму;

незнання населенням основ кібербезпеки і особиста неграмотність в питаннях кіберзагроз серед приватних підприємців та керівників великих підприємств (установ);

можливості кіберпростору щодо реалізації майже усіх видів соціальних небезпек [31];

вплив недержавних організацій (суспільних, громадських) на формування як відношення до самого явища (гібридних загроз у кіберпросторі), так і на сприйняття користувачем цих загроз;

релігійні передумови політичної та військової експансії як засіб для її виправдання [32].

## Висновки й перспективи подальших досліджень

Аналіз вивчення досвіду підготовки та ведення РФ агресії проти України, світових тенденцій цифровізації суспільства, міжнародних практик у галузі забезпечення кібербезпеки підтверджує особливе значення кіберпростору у збройних конфліктах гібридного типу, у якому і самі загрози стають гібридними. Враховуючи те, що діюча на сьогодні система забезпечення інформаційної безпеки воєнної сфери не призначена для виявлення та протидії гібридним загрозам у кіберпросторі, а система забезпечення кібербезпеки воєнної сфери перебуває лише на стадії становлення та набуття необхідних бойових спроможностей питання всебічного вивчення таких загроз стоїть вкрай гостро.

Організація процесу моніторингу, попередження та адекватної протидії гібридним загрозам в кіберпросторі майже не можлива без усвідомлення та розуміння, що собою являють такі загрози, у чому полягає їх сутність та зміст, що є джерелом, з якою метою вони реалізуються, які завдання на них покладаються тощо.

У зв'язку з цим, всебічне вивчення усіх складових гібридних загроз у кіберпросторі та їх класифікація є перспективним напрямком подальших наукових досліджень, результати яких сприятимуть створенню системи оперативного виявлення та реагування на них, у воєнній сфері зокрема, та розвитку військової науки в цілому.

## *Література*

**1.** Hybrid Warfare: The Next Generation Tool. Asian Warrior. Sp.13, 2016**. 2.** Заява за результатами саміту у Варшаві. URL: .nato.int/cps/uk/natohq/official_texts_133169.htm (дата звернення: 26.08.2019). **3.** Концепція НАТО 2010. cf BI-SC input for new NATO Capstone Concept for the Military contribution to countering hybrid enclosure 1 to 1500/CPPCAM/FCR/10-270038 and 5000 FXX/0100/IT-0651/SER:NU0040, 25 August 2010. **4.** US Army's Training Circular 7-100. **5.** Cyber War in Perspective: Russian Aggression Against Ukraine. Edited by Kenneth Geers. NATO Cooperative Cyber Defense Centre of Excellence. Tallinn. Estonia. 2015. 175 p. **6.** Основи кібернетичної безпеки: монографія/за заг. ред. Ю. Г. Даника. Житомир. 2016. 636 с. **7.** Прес-конференція Віце-президента Єврокомісії Ірки Катаінена, присвячена питанню гібридних загроз. URL: https://www.5.ua/svit/yevrokomisiia-vyznachylasia-shcho-iavliaie-soboiu-hibrydna-zahroza-150683.html (дата звернення: 19.09.2018). **8 С. Вдовенко, Ю. Даник, С. Фараон.** Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення / Комп'ютерні науки та кібербезпека, (1), с. 18-30. **9. Andrei Josan, Cristina Voicu.** Hybrid wars in the age of asymmetric conflicts. The Scientific Informative Review, №1(28) 2015, p. 49. **10.** The U.S. Army Operating Concept: Win in a Complex World. 2020-2040. TRADOC Pamphlet

525-3-1. URL: www.tradoc.army.mil/tpubs/pams/tp532-3-1.pdf (дата звернення: 16.03.2018). **11. Larson Eric, Peters John**. Prepearing the U.S. Army for Homeland Secutity. Concepts, Issues, and Options. URL: books.google.com.ua (дата звернення: 16.03.2018). **12 Бєлоусова Н. Б., Афанасьєва П. А.** Основні вимоги щодо забезпечення безпеки інформаційного простору / Актуальні проблеми міжнародних відносин. 2017. Вип. 133. С. 95-98. **13.** Кіберпростір як новий вимір геополітичного суперництва: монографія/Дубов Д. В. Київ, 2015. 328 с. **14.** Гібридна війна: in verbo et in praxi: монографія/під заг. ред. Р. О. Додонова. Вінниця, 2017. 412 с. **15. Рибак В.** Гібридні виклики міжнародного гуманітарного права / Тиждень.UA/ URL: tyzden.ua/World/145884 (дата звернення: 11.10.2018). **16. Чуприна В.** Кіберпростір як поле битви. URL: yur-gazeta.com/dumka-eksperta/kiberprostir-yak-pole-bitvi.html (дата звернення: 27.09.2018). **17**. Власюк В. В., Карман Я. В. Деякі основи поняття "гібридна війна" в міжнародному праві / Право і громадянське суспільство. 2015. № 1. С. 226. **18. Діордіца І.** Поняття і зміст кіберзагроз на сучасному етапі / Підприємництво, господарство і право. 2017. №4. С. 99. **19. Пузиренко О. Г.** Математична модель загроз інформаційній безпеки в інформаційно-телекомунікаційних системах спеціального призначення/Наука і техніка Повітряних Сил Збройних Сил України. 2015. № 3 (16). С. 57. **20. Бурячок В. Л., Толюпа С. В.** Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: навч. посіб. Київ. 2016. 14 с. **21.** Світова гібридна війна: український фронт: монографія/під заг. ред. В. П. Горбуліна. Київ. 2017. 496 с. **22. Кулицький С.** Економічна складова гібридної війни Росії проти України. http://nbuviap.gov.ua/images/ukrain/2016/ukr20.pdf (дата звернення: 14.03.2018). **23. Прузовский А.О.** форуме по кибербезопасности в Европейском союзе и НАТО 2017. URL: http://m.20minut.ua/Noviny-Vinnitsi/Vid-Chitachiv/artue-pruzovskiy-o-forume-po-kiberbezopasnosti-v-evropeyskom-soyuze-i-nato-10638382.html (дата звернення: 18.09.2018). **24.** Угрозы безопасности в глобальном киберпространстве_ИНЭУМ. URL: www.ineum.ru/ugrozy-bezopasnosti-v-globalnom-kiberprostranstve (дата звернення: 08.06.2018). **25. Стиран В.** Дика природа кіберпростору. Стратегія виживання. URL:http://blog.styran.com/2017-02-20-cyber-jungle-idc-talk/ (дата звернення: 20.02.2018). **26.** Про Стратегію кібербезпеки України: Рішення Ради національної безпеки і оборони України від 27 січня 2016 року. Київ. 2017. 11 с. **27.** Гібридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства/Аналітичний документ. Київ. 2018. 106 с. **28.** Угрозы информационной безопасности в кризисах и конфликтах XXI века: монография/под общ. ред. А. В. Загорского, Н. П. Ромашкиной. Москва. 2015. 151 с. **29. Почепцов Г.** Інфовійни в кіберпросторі. URL: https://ms.detector.media/ethics/manipulation/infoviyni_v_kiberprostori/ (дата звернення: 28.05.2018). **30. Бартош А. А.** Смыслы гибридной войны. URL: nic-pnb.ru/vneshnepoliticheskie-aspecty-bezopasnosty/smysly-gibridnoj-vojni (дата звернення: 15.07.2018). **31.** Соціальні фактори, що впливають на життя і здоров'я людини. URL: //studopedia.su/5_47912_sotsiani-faktori-shcho-vplivaut-na-zhittya-ta-zdorovya-ludini.html (дата звернення: 16.03.2018). **32. Почепцов Г.** Гибридная война: когда население оказывается целью. https://ms.detector.media/trends/1411978127/gibridnaya_voyna_kogda_naselenie_okazyvaetsya_tselyu/ (дата звернення: 17.09.2018).

## ГИБРИДНЫЕ УГРОЗЫ В КИБЕРПРОСТРАНСТВЕ: ФАКТОРЫ ВЛИЯНИЯ НА ПРИРОДУ ВОЗНИКНОВЕНИЯ

***Руслан Валентинович Грищук*** *(доктор технических наук, профессор)*
***Руслан Михайлович Жовноватюк*** *(кандидат технических наук, с.н.с.)*
***Анна Дмитриевна Носова***

***Житомирский военный институт имени С. П. Королева, Житомир, Украина***

*Гибридная агрессия Российской Федерации против Украины поставила перед всем мировым сообществом новые вызовы как внутренней безопасности отдельных стран, так и коллективной безопасности межгосударственных организаций, реализация которых сместилась в кибернетическое пространство. Его активное влияние на все сферы жизни современного человека послужило причиной одновременно как развития его возможностей, так и возрастания уязвимости. Становление киберпространства как новейшего театра военных действий требует своевременного реагирования, которое невозможно без всестороннего изучения такого явления как гибридные угрозы в киберпространстве.*

*В статье рассмотрено исторические, правовые, политически, экономические, технологические, информационные и социальные факторы влияния на природу возникновебния гибридных угроз в кибернетическом пространстве. Проведено анализ предпосылок появления гибридных угроз в кибернетическом пространстве. Отмечено, что они взаимосвязаны и их следует рассматривать через призму эволюционных процессов трансформации общества. Указано на то, что изменение геополитических конфигураций, перераспределение сфер влияния, политическая и стратегическая неопределенность приводят к постоянному политическому, экономическому и информационному давлению. Это в свою очередь влечет за собой создание зон повышенного риска, в которых возможно появление и реализация новейших гибридных угроз в кибернетическом пространстве, следовательно, требует адекватных действий по защите от них.*

*Определено актуальные проблемы защиты действующих и создаваемых баз данных в системе государственного управления Украины, в частности в системе управления Вооруженными Силами Украины.*

*Кроме того, освещены основные геополитические процессы, на которые осуществляют влияние ведущие станы мира з целью получения монополии на те или иные информационные ресурсы. Основными среди таких процессов, относительно которых необходимо проводить постоянный глобальный мониторинг, являются политические, экономические, военные и экологические.*

***Ключевые слова:*** *кибернетическое пространство, гибридная угроза, неконвенционные боевые действия.*

## HYBRID THREATS IN CYBER SPACE: FACTORS OF INFLUENCE ON NATURE OF EMERGENCE

***Ruslan Hryshchuk*** *(Doctor of Technical Sciences, Professor)*
***Ruslan Zhovnovatiuk*** **(***Candidate of Technical Sciences, Senior Research Scientist)***
***Hanna Nosova***

***Zhytomyr Military Institute n. a. S.P. Korolev, Zhytomyr, Ukraine***

*The hybrid aggression of the Russian Federation against Ukraine posed a new challenge to the entire world community, both for the internal security of individual countries and for the collective security of intergovernmental organizations, the implementation of which shifted into cyberspace. His active influence on all spheres of life of modern man was the cause of both the development of its capabilities and the increase in vulnerability. The emergence of cyberspace as the newest theater of war requires a timely response, which is impossible without a comprehensive study of the phenomenon of hybrid threats in cyberspace.*

*The article considers the historical, legal, political, economic, technological, informational and social factors influencing the nature of the emergence of hybrid threats in cyberspace. The analysis of the prerequisites for the emergence of hybrid threats in cyberspace. It is noted that they are interrelated and should be viewed through the prism of the evolutionary processes of transformation of society. It is noted that changes in geopolitical configurations, the redistribution of spheres of influence, political and strategic uncertainty lead to constant political, economic and informational pressure. This, in turn, entails the creation of high-risk areas in which the emergence and introduction of the newest hybrid threats in cyberspace is possible, therefore adequate actions are required to protect them.*

*The actual problems of protection of existing and created databases in the state administration system of Ukraine, in particular in the control system of the Armed Forces of Ukraine, are identified.*

*In addition, the main geopolitical processes that are influenced by the leading countries of the world for the purpose of obtaining a monopoly on certain information resources are covered. The main processes for which ongoing global monitoring is necessary are political, economic, military and environmental.*

***Keywords:*** *cyberspace, hybrid threat, non-conventional fighting.*

## *References*

**1.** Hybrid Warfare: The Next Generation Tool. Asian Warrior. Sp.13, 2016. **2.** Zajava za rezuljtatamy samitu u Varshavi. URL: nato.int/cps/uk/natohq/official_texts_133169.htm (data zvernennja: 26.08.2019). **3.** Koncepcija NATO 2010. cf BI-SC input for new NATO Capstone Concept for the Military contribution to countering hybrid enclosure 1 to 1500/CPPCAM/FCR/10-270038 and 5000 FXX/0100/IT-0651/SER:NU0040, 25 August 2010. 4. US Army's Training Circular 7-100. **5.** Cyber War in Perspective: Russian Aggression Against Ukraine. Edited by Kenneth Geers. NATO Cooperative Cyber Defense Centre of Excellence. Tallinn. Estonia. 2015. 175 p. **6.** Osnovy kibernetychnoji bezpeky: monoghrafija/za zagh. red. Ju. Gh. Danyka. Zhytomyr. 2016. 636 s. **7.** Pres-konferencija Vice-prezydenta Jevrokomisiji Irky Katainena, prysvjachena pytannju ghibrydnykh zaghroz. URL: https://www.5.ua/svit/yevrokomisiia-vyznachylasia-shcho-iavliaie-soboiu-hibrydna-zahroza-150683.html (data zvernennja: 19.09.2018). **8 S. Vdovenko, Ju. Danyk, S.Faraon.** Definicijni problemy terminologhiji u sferi kiberbezpeky i kiberoborony ta shljakhy jikh vyrishennja / Komp'juterni nauky ta kiberbezpeka, (1), c. 18-30. **9. Andrei Josan, Cristina Voicu**. Hybrid wars in the age of asymmetric conflicts. The Scientific Informative Review, #1(28) 2015, p. 49. **10.** The U.S. Army Operating Concept: Win in a Complex World. 2020-2040. TRADOC Pamphlet 525-3-1. URL: www.tradoc.army.mil/tpubs/pams/tp532-3-1.pdf (data zvernennja: 16.03.2018). **11. Larson Eric, Peters John.** Prepearing the U.S. Army for Homeland Secutity. Concepts, Issues, and Options. URL: books.google.com.ua (data zvernennja: 16.03.2018). **12. Bjelousova N. B., Afanasjjeva P. A.** Osnovni vymoghy shhodo zabezpechennja bezpeky informacijnogho prostoru / Aktualjni problemy mizhnarodnykh vidnosyn. 2017. Vyp. 133. S. 95-98. **13.** Kiberprostir jak novyj vymir gheopolitychnogho supernyctva: monoghrafija/Dubov D. V. Kyjiv, 2015. 328 s. **14.** Ghibrydna vijna: in verbo et in praxi: monoghrafija/pid zagh. red. R. O. Dodonova. Vinnycja, 2017. 412 s. **15. Rybak V.** Ghibrydni vyklyky mizhnarodnogho ghumanitarnogho prava / Tyzhdenj.UA/ URL: tyzden.ua/World/145884 (data zvernennja: 11.10.2018). **16. Chupryna V.** Kiberprostir jak pole bytvy. URL: yur-gazeta.com/dumka-eksperta/kiberprostir-yak-pole-bitvi.html (data zvernennja: 27.09.2018). **17. Vlasjuk V. V., Karman Ja. V.** Dejaki osnovy ponjattja "ghibrydna vijna" v mizhnarodnomu pravi / Pravo i ghromadjansjke suspiljstvo. 2015. № 1. S. 226. **18. Diordica I.** Ponjattja i zmist kiberzaghroz na suchasnomu etapi / Pidpryjemnyctvo, ghospodarstvo i pravo. 2017. №4. S. 99. **19. Puzyrenko O. Gh.** Matematychna modelj zaghroz informacijnij bezpeky v informacijno-telekomunikacijnykh systemakh specialjnogho pryznachennja/Nauka i tekhnika Povitrjanykh Syl Zbrojnykh Syl Ukrajiny. 2015. # 3 (16). S. 57. **20. Burjachok V. L., Toljupa S. V.** Informacijnyj ta kiberprostory: problemy bezpeky, metody ta zasoby borotjby: navch. posib. Kyjiv. 2016. 14 s. **21.** Svitova ghibrydna vijna: ukrajinsjkyj front: monoghrafija/pid zagh. red. V. P. Ghorbulina. Kyjiv. 2017. 496 s. **22. Kulycjkyj S.** Ekonomichna skladova ghibrydnoji vijny Rosiji proty Ukrajiny. http://nbuviap.gov.ua/images/ukrain/2016/ukr20.pdf (data zvernennja: 14.03.2018). **23. Pruzovskyj A.O.** forume po kyberbezopasnosty v Evropejskom sojuze y NATO 2017. URL: http://m.20minut.ua/Noviny-Vinnitsi/Vid-Chitachiv/artue-pruzovskiy-o-forume-po-kiberbezopasnosti-v-evropeyskom-soyuze-i-nato-10638382.html **24.** Ughrozy bezopasnosty v ghlobaljnom kyberprostranstve_YNƏUM. URL: www.ineum.ru/ugrozy-bezopasnosti-v-globalnom-kiberprostranstve **25. Styran V.** Dyka pryroda kiberprostoru. Strateghija vyzhyvannja. URL:http://blog.styran.com/2017-02-20-cyber-jungle-idc-talk/ (data zvernennja: 20.02.2018). **26.** Pro Strateghiju kiberbezpeky Ukrajiny: Rishennja Rady nacionaljnoji bezpeky i oborony Ukrajiny vid 27 sichnja 2016 roku. Kyjiv. 2017. 11 s. **27.** Ghibrydni zaghrozy Ukrajini i suspiljna bezpeka. Dosvid JeS i Skhidnogho partnerstva/Analitychnyj dokument. Kyjiv. 2018. 106 s. **28.** Ughrozy ynformacyonnoj bezopasnosty v kryzysakh y konflyktakh XXI veka: monoghrafyja/pod obshh. red. A. V. Zaghorskogho, N. P. Romashkynoj. Moskva. 2015. 151 s. **29. Pochepcov Gh.** Infovijny v kiberprostori. URL: https://ms.detector.media/ethics/manipulation/infoviyni_v_kiberprostori/ **30. Bartosh A. A.** Smysly ghybrydnoj vojny. URL: nic-pnb.ru/vneshnepoliticheskie-aspecty-bezopasnosty/smysly-gibridnoj-vojni. **31.** Socialjni faktory, shho vplyvajutj na zhyttja i zdorov'ja ljudyny. URL: //studopedia.su/5_47912_sotsiani-faktori-shcho-vplivaut-na-zhittya-ta-zdorovya-ludini.html (data zvernennja: 16.03.2018). 32. Pochepcov Gh. Ghybrydnaja vojna: koghda naselenye okazyvaetsja celjju. https://ms.detector.media/trends/1411978127/gibridnaya_voyna_kogda_naselenie_okazyvaetsya_tselyu/