УДК 316.485.26:316.776.23]:303.442.23
DOI: https://doi.org/10.21564/2075-7190.44.195923

***Чалапко Володимир Вікторович***, аспірант кафедри філософії
Національного технічного університету
«Харківський політехнічний інститут», Україна
e-mail: vvchalapko@gmail.com
ORCID ID: 0000-0001-9833-9851

# ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНСЬКОГО СУСПІЛЬСТВА В УМОВАХ «ГІБРИДНОЇ ВІЙНИ»

*Визначено характеристики «гібридної війни» та особливості її прояву в інформаційному просторі України. Розкрито базові загрози інформаційній безпеці вітчизняного суспільства в умовах гібридного протистояння. Досліджено сутність інформаційної зброї та напрями її застосування під час «гібридної війни». Проаналізовано характер небезпек і негативних впливів суб'єктів гібридних атак у соціальних мережах.*

***Ключові слова:*** *інформаційна безпека; гібридна війна; загрози інформаційній безпеці; інформаційна зброя; інформаційний простір; духовна безпека.*

***Постановка проблеми.*** Інформаційна безпека в сучасних умовах є важливою складовою національної безпеки держави як цілісної системи. Особливої актуальності проблематика інформаційної безпеки набуває під час «гібридних воєн». Останніми роками наша країна зіткнулася з різноманітними загрозами, зокрема спрямованими на інформаційно-комунікаційну сферу. Цілком очевидно, що захист національних інформаційних ресурсів, інформаційно-культурного простору України передбачає нівелювання низки загроз та викликів, що обумовлені розпочатою проти нашої держави «гібридною війною».

***Аналіз останніх досліджень і публікацій.*** Проблема інформаційної безпеки українського суспільства в умовах «гібридної війни» набула свого висвітлення в низці публікацій. Зокрема, автори ґрунтовного дослідження за редакцією В. Горбуліна показали багатоаспектність феномену «гібридної війни», розкрили його характерні риси та особливості. Системне розуміння сутності інформаційної безпеки та інформаційних загроз на сучасному етапі вітчизняного державотворення представлене в наукових працях О. Данильяна, О. Дзьобаня, Ю. Калиновського, Є. Мануйлова та ін. У свою чергу, Г. Шевченко розмірковує про взаємозв'язок інформаційної та духовної без-

пеки, визначаючи основні загрози в ціннісному, ментальному та культурному вимірах. Науковці Т. Кравченко та Я. Деркаченко зосередили увагу на особливостях застосування соціальних мереж у «гібридній війні» проти України, визначивши характер та засоби негативного впливу на інформаційну безпеку вітчизняного суспільства.

***Формулювання цілей.*** Метою нашої наукової розвідки є визначення основних загроз та викликів інформаційній безпеці українського суспільства в умовах «гібридної війни».

***Виклад основного матеріалу.*** Для реалізації окресленої мети виокремимо сутнісні характеристики «гібридної війни». Фахівці констатують, що «гібридну війну» в загальному вигляді розуміють як воєнні дії, що здійснюють шляхом поєднання мілітарних, квазімілітарних, дипломатичних, інформаційних, економічних та інших засобів із метою досягнення стратегічних політичних цілей. Специфіка такого поєднання полягає в тому, що кожний із військових і невійськових способів ведення гібридного конфлікту застосовується у воєнних цілях та використовується як зброя. Перетворення на зброю (weaponization) відбувається не тільки в медійній сфері. Так само в прямому сенсі в ролі зброї, яка завдає ураження різного рівня системам противника, застосовуються всі інші невійськові засоби ведення гібридної війни [1. с. 19].

Одним з основних засобів ведення «гібридної війни» є так звана інформаційна зброя, яка за своєю ефективністю та наслідками становить значну загрозу для будь-якої держави, втягнутої в гібридне протистояння, для України зокрема. На думку дослідників, інформаційна зброя – це інформація (дані), які є засобом ведення інформаційних воєн і призначення яких полягає в зміні системних якостей об'єкта інформаційного впливу за допомогою прихованих установок на здійснення задуманих користувачем інформаційної зброї дій. Напрями і приклади використання інформаційної зброї є такі:

– порушення, пошкодження або модифікація інформаційних ресурсів і знань людей про самих себе та про середовище яке їх оточує;

– здійснення впливу на суспільну думку та позицію політичної еліти;

– завдання шкоди протилежній стороні дипломатичними засобами;

– пропагандистські, психологічні та підривні акції у сфері культури й політики;

– дезінформація;

– чутки, створені навмисно;

– упровадження в ЗМІ своїх прибічників для проведення підривних акцій;

– проникнення в комп'ютерні мережі та системи управління базами даних, зараження комп'ютерних систем вірусами, навмисне введення різного роду помилок у програмне забезпечення об'єкта;

– інформаційна підтримка дисидентських та опозиційних рухів [2, с. 332].

Необхідно зазначити, що інформаційна зброя особливо ефективно діє проти тієї країни, яка знаходиться в кризовому стані, у суспільній свідомості якої панує ціннісна амбівалентність, соціально-політична невизначеність. Застосування інформаційної зброї стає особливо дієвим, коли у державі спостерігається протистояння між політичними силами, наявною є криза моральної та правової свідомості, слабкою патріотично налаштована еліта у всіх сферах суспільного життя [3, с. 149].

Застосовуючи інформаційну зброю, суб'єкти агресії здійснюють постійні атаки, спрямовані на інформаційно-комунікаційний простір нашої країни. За оцінками вітчизняних експертів із проблем інформаційної безпеки, що сформовані на основі аналізу іноземного впливу на інформаційний медіа- і кіберпростір України, існують ознаки реальних загроз для нашої держави. Про це свідчать такі основні тенденції:

– цілеспрямоване формування окремими іноземними державами негативного міжнародного іміджу України;

– активізація критики вищого державного керівництва України;

– здійснення низкою зарубіжних країн потужного інформаційного тиску на Україну з метою спонукання українського керівництва до прийняття вигідних для цих країн рішень у внутрішньо та зовнішньополітичній сферах;

– посилення інформаційних заходів із перешкоджання реалізації Україною її зовнішньополітичного курсу та спонукання її до участі в проектах, які в сучасних умовах не вигідні нашій державі;

– дискредитація нашої держави як конкурента у сфері міжнародного військово-технічного співробітництва;

– зростання для України загроз кібернетичних атак, що обумовлено появою нових, більш досконалих зразків кібернетичної зброї [4, с. 128].

З точки зору науковців, розуміння інформаційної безпеки має включати не тільки захист інформаційних ресурсів суспільства, держави та людини, а й збереження ціннісних аспектів історичної пам'яті, культурних традицій, специфічного національно-етнічного способу життя українського народу. У цьому контексті дослідники ведуть мову про захист інформаційного суверенітету нашої країни, розуміння якого вбирає в себе правові, політичні, ціннісно-культурні, безпекові й інформаційні процеси в державі. Цілком логічно, що програми з інформаційної безпеки спрямовані насамперед на захист інформаційного суверенітету держави [5, с. 17].

Аналізуючи характер загроз інформаційній безпеці українського суспільства в аксіологічному вимірі, фахівці наголошують на необхідності посилювати духовну безпеку нашої держави. Духовна безпека, на наше переконання, безпосередньо корелюється з інформаційною безпекою і передбачає захист національних цінностей, культури, ментальних особливостей українського народу.

У цьому сенсі Г. Шевченко зауважує, що серед загроз духовній безпеці є конфліктність та інтелектуалізація суспільства, яка не збігається з моральним удосконаленням особистості та супроводжується руйнацією національної культури, національної науки, освіти і виховання. На його думку, збереження духовної безпеки суспільства і кожної людини можливе завдяки слідуванню національно-культурним традиціям, їх примноженню Духом відповідальності, віри в справедливість, Людської гідності і чесності, високої моральності і краси. Фундаментом духовної безпеки може бути духовна культура і духовні цінності, які створюють архітектуру духовності особистості. Можна з упевненістю сказати, що найважливішими духовними цінностями суспільства є культура, наука, освіта та виховання, які підносять людину на вищий щабель її життєдіяльності, сприяють формуванню ціннісного світогляду, духовного світу, системи духовно-моральних ідеалів, які дозволяють особистості в будь-яких життєвих ситуаціях залишатися людиною духовною і впевнено тримати духовний стрижень [6, с. 367–368].

Продовжуючи наведену логіку і спираючись на дослідження О. Дзьобаня, варто виокремити декілька основних груп загроз інформаційній безпеці України. Перша група пов'язана з бурхливим розвитком нового класу зброї – інформаційної, яка здатна ефективно впливати і на психіку, свідомість людей, і на інформаційно-технічну інфраструктуру суспільства й армії. Друга група інформаційно-технічних загроз для особистості, суспільства й держави − це новий клас соціальних злочинів, заснованих на використанні сучасної інформаційної технології (махінації з електронними грошима, комп'ютерне хуліганство тощо). Третя група інформаційно-технічних загроз – електронний контроль за життям, настроями, планами громадян, політичних організацій. Четверта група інформаційних загроз – використання нових інформаційних технологій у політичних цілях [7, с. 174].

Необхідно зазначити, що існуючі загрози інформаційній безпеці України значно посилюються у зв'язку з низкою проблем функціонування інформаційного простору нашої держави, які набули іншого виміру під впливом «гібридних атак». Зокрема, до головних негативних чинників, які зумовлюють сучасний стан українського інформаційного простору фахівці відносять такі:

– відсутність чіткої скоординованої державної інформаційної політики за умов наявності й активного виконання кількох, на жаль, недостатньо скоординованих державних програм за такими напрямами, як інформатизація, формування і захист національного інформаційного ресурсу і простору тощо;

– інвестування інформаційних структур (як державних, так і приватних) за «залишковим принципом» унаслідок економічних причин;

– експансія в Україну зарубіжних виробників інформаційної продукції, що об'єктивно переважають національні за якістю продукції, економічними можливостями, а також застосовують агресивну ринкову стратегію;

− недостатній професійний рівень працівників інформаційної сфери, недоліки вітчизняної системи їхньої підготовки (особливо це стосується електронних ЗМІ та нових інформаційних, зокрема глобальних систем);

− технічне відставання інформаційної інфраструктури і її повна залежність від постачання іноземної техніки, занепад вітчизняної телекомунікаційної промисловості [8, с. 130].

Безсумнівно, реалії «гібридної війни» вимагають від держави та структур громадянського суспільства більш системних, скоординованих та стратегічно спрямованих дій щодо зміцнення внутрішніх підвалин інформаційної безпеки України.

Як справедливо зазначає У. Ільницька, Україна стала об'єктом інформаційно-психологічних впливів, операцій, війн, а її інформаційна безпека опинилася під загрозою. Можна констатувати, що:

1) український інформаційний простір є незахищеним від зовнішніх негативних пропагандистсько-маніпулятивних впливів і стає об'єктом інформаційної експансії;

2) у світовому медіапросторі відсутній український національний інформаційний продукт, що поширював би об'єктивну, неупереджену та актуальну інформацію про події в Україні. Як наслідок, світова громадськість відчуває брак інформації або отримує її з інших джерел, які часом дезінформують, надають викривлену, спотворену, неповну інформацію. Водночас проти України активно застосовується потужний медіа-ресурс, здійснюється експансія іноземних суб'єктів на ринку інформаційних послуг, активізуються негативні інформаційні впливи, які спрямовані на викривлення реальності, заниження міжнародного іміджу держави;

3) діяльність вітчизняних ЗМІ щодо систематичного, об'єктивного висвітлення фактів, подій та явищ є недостатньою та позбавлена стратегічного планування; інформаційно-комунікативна політика України у сфері національної безпеки потребує невідкладного перегляду та удосконалення [9, с. 130].

Як демонструє практика «гібридної війни», розв'язаної проти України, одним з важливих каналів негативного впливу на суспільну свідомість стали соціальні мережі, за допомогою яких розповсюджувалася і розповсюджується фейкова інформація, здійснюється антиукраїнська агітація і пропаганда.

Так, на думку Т. Кравченко, в мережевих спільнотах проявляються негативні риси, які впливають на ціннісний світ людини та суспільства, що, у свою чергу, відбивається на якісних показниках інформаційної безпеки держави. До таких негативних рис фахівці відносять такі:

− невпевненість у інформаційній безпеці особистих даних у мережі;

− право державних структур на перегляд інформації акаунтів соціальних мереж;

− інформаційні технології створюють можливість руйнування життєвого світу людей і їх життєвих пріоритетів і цінностей, залучення свідомості людей у небезпечну для психіки віртуальну реальність, тоді як інформація набуває статусу всезагальної цивілізаційної цінності, значного, життєво важливого ресурсу суспільства і держави [10, с. 57].

Соціальні мережі як інструмент ведення «гібридної війни» є особливо небезпечними, оскільки, по-перше, охоплюють велику кількість користувачів із різним соціальним статусом, по-друге, у мережевих спільнотах присутній достатньо високий рівень довіри до окремих суб'єктів, що дозволяє здійснювати латентний маніпулятивний вплив на об'єкт інформаційної атаки, і по-третє, інформація у мережі (в тому числі й негативного змісту) поширюється хвилеподібно й може бути по-різному інтерпретована користувачем.

З точки зору Я. Деркаченко, для досягнення цілей у соцмережах за основу беруться спеціальні маніпулятивні технології та бойові технології інформаційних війн. У соцмережах, як у найбільш довірчому каналі спілкування, особливу небезпеку становлять сугестивні технології. При цьому сугестивний вплив полягає саме в навмисній організації такого впливу з наперед заданою метою, що не обов'язково ґрунтується на достовірній інформації. Його ефективність є особливо дієвою в соцмережах з огляду на специфіку такого виду спілкування. Адже ця специфіка полягає в зовні абсолютно вільному, добровільному сприйнятті інформації, що переконує самим форматом довірливого спілкування і вже не потребує логічних аргументів чи мотивів. І сам об'єкт сугестивного впливу приймає ті чи інші рішення немов би добровільно, та не усвідомлює свого підкорення зовнішньому впливу. Такого виду технології можуть торкатися нервово-психічних процесів і соціальних уявлень, настанов, суспільних норм, цінностей, ду-

мок, а також індивідуальної самосвідомості користувачів інтернет-ресурсів [11, с. 55].

В українських реаліях боротьба з дезінформацією в соціальних мережах стала справою не тільки державних органів, а й волонтерських, громадських організацій, які змогли організувати спротив «гібридним атакам», посиливши таким чином інформаційну безпеку країни.

На переконання вітчизняних експертів, в умовах сьогодення ефективною виявилася модель взаємодії держави в галузі інформаційної безпеки з громадськими організаціями і волонтерськими проектами, наприклад «Інформнапалм», «СтопФейк», «Детектор медіа» та ін. Тому нормативно-правове регулювання процедур залучення громадських організацій до діяльності державних органів у інформаційній сфері визначає напрям підвищення ефективності функціонування системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах [12, с. 125].

В умовах перманентного «гібридного протистояння» Україна поступово напрацьовує дієві методи боротьби з інформаційними загрозами, але при цьому існує низка проблем організаційного, інституційного, технічно-комунікаційного, правового, економічного та іншого характеру.

Науковці доводять, що подальші зусилля інтеграції Української держави в європейську цивілізаційну спільноту потребує створення системи інформаційної (зокрема, кібернетичної) безпеки України, яка повинна мати наступальну спрямованість як із питань захисту, так і просування національних інтересів. Реалізація такої системи, на думку вітчизняних фахівців, передбачає такі напрями:

розробка й удосконалення нормативно-правової бази у сфері інформаційної безпеки, яка на сьогодні є фрагментарною та не повною мірою відповідає існуючим потребам;

створення (визначення) керівного та координаційного органу системи інформаційної безпеки України у структурі державних органів виконавчої влади;

визначення (уточнення) переліку суб'єктів підтримання інформаційної безпеки, їхніх функцій, завдань і повноважень, для чого необхідно внести відповідні зміни до чинного законодавства України;

проведення досліджень та визначення потреб у технічному, фінансовому кадровому забезпеченні функціонування системи з метою прийняття рішення стосовно розробки відповідної цільової державної програми або внесення змін до чинних цільових державних програм;

активізація заходів у Міністерстві оборони України та Генеральному штабі Збройних Сил України зі створення власної системи інформаційної безпеки, яка має стати складовою національної системи інформаційної без-

пеки, а також розробки відповідної нормативно-правової бази в межах реалізації Концепції забезпечення інформаційної безпеки Міністерства оборони та Збройних Сил України [13, с. 64].

***Висновки.*** Таким чином, сучасні загрози інформаційній безпеці українського суспільства в умовах "гібридної війни" мають різноспрямований характер і проявляються в комунікаційно-технічній, ціннісній, політико-правовій, соціально-економічній та інших сферах. Існування цих загроз обумовлено як зовнішніми негативними впливами, так і внутрішніми чинниками нестабільності. Виходячи з вищенаведеного попередження та нівелювання загроз інформаційній безпеці українського суспільства потребує від Української держави розробки й комплексного втілення низки програм, посилення співробітництва з міжнародними та регіональними безпековими структурами тощо.

## ЛІТЕРАТУРА


1. Світова гібридна війна: український фронт / за заг. ред. В. П. Горбуліна; Національний інститут стратегічних досліджень. Київ: НІСД, 2017. 496 с.
2. Шпига П. С., Рудник Р. М. Основні технології та закономірності інформаційної війни. *Проблеми міжнародних відносин.* 2014. Вип. 8. С. 326–339.
3. Калиновський Ю. Ю., Мануйлов Є. М. Роль і місце інформаційної безпеки у розбудові сучасної української держави. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». Серія: Філософія, філософія права, політологія, соціологія /* редкол.: А. П. Гетьман та ін. Харків: Право, 2016. №2 (29). С. 144–154.
4. Косогов О. М. Пріоритетні напрямки державної політики щодо забезпечення безпеки національного кіберпростору. *Збірник наукових праць Харківського університету Повітряних Сил.* 2014. Вип. 3. С. 127–130.
5. Калиновський Ю. Ю., Мануйлов Є. М. Аксіологічний вимір інформаційної безпеки української держави. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». Серія: Філософія, філософія права, політологія, соціологія /* редкол.: А. П. Гетьман та ін. Харків: Право, 2017. №3 (34). С. 13–31.
6. Шевченко Г. П. Духовна безпека: духовна культура і духовні цінності сучасної людини. *Духовність особистості: методологія, теорія і практика.* 2017. Вип. 3. С. 361–373.
7. Дзьобань О. П. До проблеми загроз інформаційній безпеці України: цивілізаційний контекст. *Побудова інформаційного суспільства: ресурси і технології:* матеріали XVIII Міжнародної науково-практичної конференції (Київ, 19–20 верес. 2019 р.). Київ: УкрІНТЕІ, 2019. С. 173–176.

8. Хімей В. Основні сучасні проблеми інформаційної безпеки України. *Теле- та радіожурналістика.* 2014. Вип. 13. С. 127–132.
9. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Humanitarian vision*. 2016. Vol. 2, No. 1. С. 27–32.
10. Кравченко Т. О. Аксіологічний аспект інформаційно-мережевої парадигми. *Філософія науки: традиції та інновації*. 2014. № 1. С. 53–63.
11. Деркаченко Я. А. Соціальні мережі, як середовище для технологій маніпулятивного впливу. *Сучасний захист інформації*. 2016. № 1. С. 51–59.
12. Молодецька-Гринчук К. В. Аналіз впливу загроз інформаційній безпеці держави у соціальних інтернет-сервісах на сфери суспільної діяльності. *Управління розвитком складних систем.* 2017. Вип. 30. С. 121–127.
13. Данильян О. Г., Дзьобань О. П. Інформаційна безпека України: загрози, зумовлені цивілізаційним вибором європейських цінностей. *Політологічний вісник*: зб. наук. пр. Київ, 2018. Вип. 81. С. 60–67.

## REFERENCES

1. Svitova gibry`dna vijna: ukrayins`ky`j front (2017) / za zag. red. V. P. Gorbulina. nacional`ny`j insty`tut strategichny`x doslidzhen`. Kyiv: NISD [in Ukrainian].
2. Shpy`ga, P. S., Rudny`k, R. M. (2014). Osnovni texnologiyi ta zakonomirnosti informacijnoyi vijny`. *Problemy` mizhnarodny`x vidnosy`n – Problems of international relations, issue 8, 326–339* [in Ukrainian].
3. Kaly`novs`ky`j, Yu. Yu., Manujlov, Ye. M. (2016). Rol` i misce informacijnoyi bezpeky` u rozbudovi suchasnoyi ukrayins`koyi derzhavy`. *Visny`k Nacional`nogo universy`tetu "Yury`dy`chna akademiya Ukrayiny` imeni Yaroslava Mudrogo". Seriya: Filosofiya, filosofiya prava, politologiya, sociologiya – Bulletin of the National University "Yaroslav Mudryi Law Academy of Ukraine". Series: Philosophy, Philosophy of Law, Political Science, Sociology, 2 (29), 144–154* [in Ukrainian].
4. Kosogov, O. M. (2014). Priory`tetni napryamky` derzhavnoyi polity`ky` shhodo zabezpechennya bezpeky` nacional`nogo kiberprostoru. *Zbirny`k naukovy`x pracz` Xarkivs`kogo universy`tetu Povitryany`x Sy`l – Scientific Works of Kharkiv National Air Force University*, *issue 3, 127–130* [in Ukrainian].
5. Kaly`novs`ky`j, Yu. Yu., Manujlov, Ye. M. (2017). Aksiologichny`j vy`mir informacijnoyi bezpeky` ukrayins`koyi derzhavy`. *Visny`k Nacional`nogo universy`tetu "Yury`dy`chna akademiya Ukrayiny` imeni Yaroslava Mudrogo". Seriya: Filosofiya, filosofiya prava, politologiya, sociologiya – Bulletin of the National University "Yaroslav Mudryi Law Academy of Ukraine". Series: Philosophy, Philosophy of Law, Political Science, Sociology, 3 (34), 13–31* [in Ukrainian].
6. Shevchenko, G. P. (2017). Duxovna bezpeka: duxovna kul`tura i duxovni cinnosti suchasnoyi lyudy`ny`. Duxovnist` osoby`stosti: metodologiya, teoriya i prakty`ka –

*Spirituality of a Personality: Methodology, Theory and Practice,* issue 3, 361–373 [in Ukrainian].
7. Dz`oban,` O. P. (2019). Do problemy` zagroz informacijnij bezpeci Ukrayiny`: cy`vilizacijny`j kontekst. *Pobudova informacijnogo suspil`stva: resursy` i texnologiyi*: proceedings of the Scientific and Practical Conference. Kyiv: UkrINTEI, *173–176* [in Ukrainian].
8. Khimey, V. (2014). Osnovni suchasni problemy informatsiynoyi bezpeky Ukrayiny. *Tele- ta radiozhurnalistyka − Tele- and radio journalism, issue 13, 127–132* [in Ukrainian].
9. Il`ny`cz`ka, U. (2016). Informacijna bezpeka Ukrayiny`: suchasni vy`kly`ky`, zagrozy` ta mexanizmy` proty`diyi negaty`vny`m informacijno-psy`xologichny`m vply`vam. *Humanitarian vision*, *Vol. 2, Num. 1, 27–32* [in Ukrainian].
10. Kravchenko, T. O. (2014). Aksiologichny`j aspekt informacijno-merezhevoyi parady`gmy`. *Filosofiya nauky`: trady`ciyi ta innovaciyi – Philosophy of Science: Traditions and Innovations, 1, 53–63* [in Ukrainian].
11. Derkachenko, Ya. A. (2016). Social`ni merezhi, yak seredovy`shhe dlya texnologij manipulyaty`vnogo vply`vu. *Suchasny`j zaxy`st informaciyi – Modern Information Security*, *1, 51–59* [in Ukrainian].
12. Molodecz`ka-Gry`nchuk, K. V. (2017). Analiz vply`vu zagroz informacijnij bezpeci derzhavy` u social`ny`x internet-servisax na sfery` suspil`noyi diyal`nosti. *Upravlinnya rozvy`tkom skladny`x sy`stem – Management of Development of Complex Systems*, *issue 30, 121–127* [in Ukrainian].
13. Dany`l`yan, O. G., Dz`oban,` O. P. (2018). Informacijna bezpeka Ukrayiny`: zagrozy`, zumovleni cy`vilizacijny`m vy`borom yevropejs`ky`x cinnostej. *Politologichny`j visny`k: zb. nauk. pr. – Politology Bulletin: Collection of Scientific Works, issue 81, 60–67* [in Ukrainian].

***Чалапко Владимир Викторович***, аспирант кафедры философии
Национального технического университета
«Харьковский политехнический институт», Украина

## УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УКРАИНСКОГО ОБЩЕСТВА В УСЛОВИЯХ «ГИБРИДНОЙ ВОЙНЫ»

*Определены характеристики «гибридной войны» и особенности ее проявления в информационном пространстве Украины. Раскрыты базовые угрозы информационной безопасности украинского общества в условиях гибридного противостояния. Исследована сущность информационного оружия и направления его применения во время «гибридной войны». Проанализирован характер угроз и негативных воздействий субъектов гибридных атак в социальных сетях.*

***Ключевые слова:*** *информационная безопасность; гибридная война; угрозы информационной безопасности; информационное оружие; информационное пространство; духовная безопасность.*

***Chalapko Volodymyr Viktorovych***, graduate student of the Department of Philosophy of the National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

## THREATS TO INFORMATION SECURITY OF UKRAINIAN SOCIETY UNDER THE CONDITIONS OF "HYBRID WAR"

***Problem setting.*** *In the present conditions, information security is an important component of national security of the state as a whole system. During the "hybrid wars", information security issues become especially relevant. In recent years, our country has faced a variety of threats, including those which aimed at the information and communication sphere.*

***Recent research and publications analysis.*** *The problem of information security of the Ukrainian society in condition of the "hybrid war" has been covered in a number of publications. In particular, authors of a thorough study, edited by V. Gorbulin, showed the multifaceted nature of phenomenon of the "hybrid war" and revealed its characteristic features and peculiarities. The systematic understanding of the essence of information security and information threats at the present stage of national state formation is presented in the scientific works of O. Danilian, O. Dzoban, Y. Kalynovsky, E. Manuilov and others. In its turn, G. Shevchenko reflects on the interconnection of information and spiritual security, identifying major threats of value, mental and cultural nature.*

***Paper objective.*** *The purpose of our scientific research is identifying the major threats and challenges to the information security of Ukrainian society in the "hybrid war".*

***Paper main body.*** *One of the main means of conducting a "hybrid war" is the so-called information weapon, which in its effectiveness and consequences poses a significant threat to any state involved in hybrid confrontation, particularly for Ukraine. It should be noted that information weapons are especially effective against a country in crisis, where the public consciousness is dominated by value ambivalence, socio-political uncertainty. The use of information weapons becomes especially effective when there is a confrontation between political forces in the state, there is a crisis of moral and legal consciousness, and a weak patriotic elite in all spheres of public life. Understanding the information security should include not only the protection of information resources of society, the state and individual, but also the retention of valuable aspects of historical memory, cultural traditions, specific national and the ethnic way of life of Ukrainian people. In this context, researchers talk about protection of the informational sovereignty of our country, the understanding of which absorbs the legal, political, value-cultural, security and information processes in the country.*

***Conclusions of the research.*** *Thus, present threats to the information security of Ukrainian society in condition of the "hybrid war" have multidirectional nature and appeared in communication, technical, value, political, legal, socio-economic and other spheres. The existence of these threats is caused by both external negative influences and internal instability factors.*

***Keywords:*** *informational security; hybrid war; threats to information security; information weapons; information space; spiritual security.*